ISSN 0178-8930
HZ204011

G 20 141

RDV

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

2/2020

Recht der Datenverarbeitung

Herausgegeben von Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

PAAL, **Kritische Würdigung des Konzepts der Datenschutzaufsichtsbehörden zur Bußgeldzumessung**

PILTZ/LÜHE, **DSFA-Blacklists nach Art. 35 Abs. 4 DS-GVO als Allgemeinverfügungen? Verwaltungsrechtliche Einordnung und mögliche Rechtsschutzmöglichkeiten**

SCHWARTMANN/WEIß, **Ein Entwurf für einen Code of Conduct zum Einsatz DS-GVO-konformer Pseudonymisierung**

SCHWARTMANN/GRZESZICK, **Die datenschutzrechtliche Stellung von Abgeordneten und Fraktionen**

Kurzbeiträge

GOLA, **Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden(46): Einzelaspekte des Beschäftigtendatenschutzes im TB des Sächsischen Datenschutzbeauftragten**

CLAUS/REIF, **Praxisfälle zum Datenschutzrecht IV: Musterfalllösungen zur Personalarbeit in Zeiten der Digitalisierung**

Rechtsprechung

Aus dem Inhalt

BAG, **Beendigung der DSB-Benennung und Sonderkündigungsschutz bei Wegfall der Bestellvoraussetzungen**

BVerwG, **Kein Anspruch auf Zugang zu Informationen über Aufsichtsmaßnahmen bei Tiertransporten (Ls)**

BVerwG, **Beginn der allgemeinen archivrechtlichen Schutzfrist bei Personenakten des Bundesamtes für Verfassungsschutz (Ls)**

OLG DRESDEN, **Änderung der Nutzungsbedingungen eines sozialen Netzwerks**

OLG DRESDEN, **Kein DS-GVO-Schadensersatzanspruch bei bloßen Bagatellverstößen**

36. Jahrgang
April 2020
Seiten 55–108

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Unverzichtbar für alle, die mit Personaldaten arbeiten:

Prof. Golas Datenschutzhandbuch.

auch für Nicht-Juristen geeignet!

PRAXISNAH

- **klar strukturierte Fallbeispiele mit konkreten Lösungsansätzen**

INFORMATIV

- **ausgewertete Stellungnahmen der Aufsichtsbehörden**

UMFASSEND

- **Rechtsprechungsübersicht mit Leitsätzen**

Handbuch Beschäftigtendatenschutz
8. völlig neu bearbeitete Auflage 2019
726 Seiten / Hardcover / € 139,99 inkl. E-Book
ISBN 978-3-89577-801-8

Bestellen Sie direkt unter:
datakontext.com/handbuch

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

36. Jahrgang 2020
Heft 2
Seiten 55–108

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Editorial 55

Veranstaltungen 56

Aufsätze

Prof. Dr. Boris PAAL, M. Jur. (Oxford)
Kritische Würdigung des Konzepts der Datenschutzaufsichtsbehörden zur Bußgeldzumessung 57

Dr. Carlo PILTZ/Carolin LÜHE
DSFA-Blacklists nach Art. 35 Abs. 4 DS-GVO als Allgemeinverfügungen? Verwaltungsrechtliche Einordnung und mögliche Rechtsschutzmöglichkeiten 65

Prof. Dr. Rolf SCHWARTMANN/RA Steffen WEIß, LL.M.
Ein Entwurf für einen Code of Conduct zum Einsatz DS-GVO-konformer Pseudonymisierung 71

Prof. Dr. Rolf SCHWARTMANN/
Prof. Dr. Bernd GRZESZICK, LL.M.
Die datenschutzrechtliche Stellung von Abgeordneten und Fraktionen 75

Kurzbeiträge

Prof. Peter GOLA
Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (46): Einzelaspekte des Beschäftigtendatenschutzes im TB des Sächsischen Datenschutzbeauftragten 81

Miriam CLAUS, LL.M./RAin Yvette REIF, LL.M.
Praxisfälle zum Datenschutzrecht IV: Musterfalllösungen zur Personalarbeit in Zeiten der Digitalisierung 83

Rechtsprechung

Beendigung der DSB-Benennung und Sonderkündigungsschutz bei Wegfall der Bestellvoraussetzungen
(BAG, Urteil vom 05.12.2019) 87

Kein Anspruch auf Zugang zu Informationen über Aufsichtsmaßnahmen bei Tiertransporten (Ls)
(BVerwG, Urteil vom 30.01.2020) 91

Beginn der allgemeinen archivrechtlichen Schutzfrist bei Personenakten des Bundesamtes für Verfassungsschutz (Ls)
(BVerwG, Urteil vom 11.12.2019) 91

Streitwert bei Auskunftsklagen nach Art. 15 DS-GVO
(OLG Köln, Beschluss vom 06.02.2020) 91

Änderung der Nutzungsbedingungen eines sozialen Netzwerks
(OLG Dresden, Beschluss vom 19.11.2019) 92

Kein DS-GVO-Schadensersatzanspruch bei bloßen Bagatellverstößen
(OLG Dresden, Beschluss vom 11.06.2019) 94

Zum datenschutzrechtlichen Widerspruchrechts gegenüber der Erhebung von Sozialdaten
(LSG Hessen, Beschluss vom 29.01.2020) 95

Löschung von personenbezogenen Daten aus dem polizeilichen Vorgangs- und Bearbeitungssystem (VBS) NIVADIS (Ls)
(OVG Lüneburg, Urteil vom 14.01.2020) 97

Zur Reichweite von Auskünften nach dem Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG) (Ls)
(VerwGH Baden-Württemberg, Beschluss vom 13.12.2019) 97

Sorgfaltspflichten vor Klageeinreichung; zur Kenntnisnahmepflicht von Erklärungen über „WhatsApp“
(LG Bonn, Urteil vom 31.01.2020) 97

Streitwert bei Tracking-E-Mails (n. Anm. von RA Jonas Breyer)
(LG Wiesbaden, Beschluss vom 22.08.2019) 98

Kein Schadensersatz-Anspruch nach der DS-GVO wegen fehlerhaften Basisscores
(LG Karlsruhe, Urteil vom 02.08.2019) 99

Zum Anspruch eines Polizeibeamten auf Akteneinsicht nach § 3 Abs. 1 Satz 1 des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin – IFG Berlin
(VG Berlin, Urteil vom 31.01.2010) 99

Berichte, Informationen, Sonstiges

Ein Leben für den Datenschutz 102

Qualifizierte Mitarbeiter sind der beste Schutz vor Sabotage, Datendiebstahl oder Spionage 104

EDSA: Europäische Leitlinie zur Videoüberwachung beschlossen 104

Literaturhinweise

Buchbesprechungen

Utz Kramer (Hrsg.)
Sozialdatenschutzrecht (ZILKENS) 105

Michael Nitsch (Hrsg.)
Compliance und soziale Verantwortung im Unternehmen. Tagungsband 4. Wiesbadener Compliance-Tag der EBS Law School – Center for corporate Compliace, Schriften der EBS-Law School (REDAKTION) 105

Katharina Höhne
Auswirkungen der unionsrechtlichen Öffnungsklausel nach Art. 88 DS-GVO auf den Beschäftigtendatenschutz nach deutschem Recht (SCHRIFTLEITUNG) 106

Neuerscheinungen

Aufsätze 107

Nachgefasst 108

Herausgegeben von

Prof. Peter GOLA, Königswinter

Andreas JASPERS, Rechtsanwalt, Bonn

Prof. Dr. Rolf SCHWARTMANN, Leiter der Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln

Prof. Dr. Gregor THÜSING, LL.M. (Harvard), Universität Bonn

in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Herausgeberbeirat

Prof. Dr. Ralf Bernd ABEL, Rechtsanwalt, Hamburg

Dietrich BOEWER, Vorsitzender Richter am Landesarbeitsgericht Düsseldorf i.R.

Prof. Dr. Alfred BÜLLESBACH, Universität Bremen

Prof. Dr. Horst EHMANN, Universität Trier

Dr. Joachim W. JACOB, Bundesbeauftragter für den Datenschutz a.D.

Prof. Dr. Friedhelm JOBS, Richter am Bundesarbeitsgericht a.D.

Prof. Dr. Tobias O. KEBER, Hochschule der Medien, Stuttgart

Prof. Dr. Karl LINNENKOHL, Universität Kassel

Dr. Alexander OSTROWICZ, Präsident des Landesarbeitsgerichts Schleswig-Holstein a.D.

Prof. Dr. Michael RONELLENFITSCH, Hessischer Datenschutzbeauftragter

Prof. Dr. Friedhelm ROST, Vorsitzender Richter am Bundesarbeitsgericht a.D.

Peter SCHAAR, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D.

Prof. Dr. Mathias SCHWARZ, Rechtsanwalt, München

Prof. Dr. Dres. h.c. Spiros SIMITIS, Universität Frankfurt

Prof. Dr. Jürgen TAEGER, Universität Oldenburg

PD Dr. Irini VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 2/2020; DATAKONTEXT, Frechen; C.H. Beck, München

Manuskripte:
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Urheber- und Verlagsrechte:
Sie sind einschließlich der Veröffentlichung als PDF im Online-Archiv vorbehalten. Sie erstrecken sich auch auf die veröffentlichten Gerichtsentscheidungen und deren Leitsätze; diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erstellt oder bearbeitet sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen: Diese bedürfen zur Auswertung einer Genehmigung des Verlages.
Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestraße 49, 80336 München, entrichtet wird, von der die Zahlungsweise zu erfragen ist.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis
Jahresabonnement € 139,–
Einzelheft € 25,–
MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Vertrieb:
Dieter Schulz
Tel.: 02234/98949-99
dieter.schulz@datakontext.com

Abo-Service:
Telefon: 089-2183-7110
Telefax: 089-2183-32
aboservice@hjr-verlag.de

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Willmuthstraße 30, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf
Telefon: (0221) 25 08-60 71
wolfgang.scharf@agentur-8020.de
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
36. Jahrgang 2020 Heft 2
Seiten 55 – 108

RDV
Recht der Datenverarbeitung

36. Jahrgang · April 2020 · Seiten 55 – 108

Editorial

Corona und Datenschutz

Corona sorgt in Unternehmen für viele, auch existenzielle Probleme. Das ist schlimm genug. Dennoch stellt die Seuche nicht von der Einhaltung des Rechts frei. Es kommen gerade durch Corona neue Fragen auf, insbesondere zum Datenschutz. Weil es sich bei persönlichen Informationen im Zusammenhang mit Infektionen um Gesundheitsdaten handelt, muss man besonders sensibel sein.

Darf ein Arbeitgeber etwa Daten über erkrankte Mitarbeiter zu Aufenthalten von Beschäftigten in Risikogebieten oder über Kontakte zu Infizierten an Behörden übermitteln, wenn die Gesundheitsbehörden dazu auffordern? Diese Fragen sind insbesondere im betrieblichen Pandemierecht des Infektionsschutzgesetzes (IfSG) geregelt. Dort geht es etwa um Quarantäneanordnungen und berufliche Tätigkeitsverbote durch das Gesundheitsamt. Die Rechtsgrundlagen der Datenherausgabe unterscheiden sich je nach der konkreten behördlichen Anfrage, die man sich am besten von der anfragenden Behörde nennen lässt. Anfragen zu erkrankten Beschäftigten im Betrieb muss man in der Regel beantworten und die Daten an die zuständige Behörde übermitteln.

Das Datenschutzrecht lässt solche Maßnahmen zu. Sowohl private Arbeitgeber als auch öffentliche Dienstherrn sind zur gesundheitlichen Fürsorge für ihre Beschäftigten insgesamt verpflichtet. Darauf, dass sie angemessen auf die pandemische Ausbreitung einer Seuche reagieren können, weisen die unabhängigen Datenschutzbehörden in Deutschland aktuell hin. In der Datenschutz-Grundverordnung und im Bundesdatenschutzgesetz finden sich entsprechende gesetzliche Erlaubnisgründe, zur Weitergabe der Infektionsdaten. Auf die Einwilligung der Betroffenen kommt es hier in der Regel nicht an. Die Aufsicht stellt aber auch klar, dass alle Maßnahmen immer auch verhältnismäßig sein müssen. Es geht um die Wahrung der Vertraulichkeit und die ausschließlich zweckgebundene Verwendung der Gesundheitsinformationen. Wenn die Daten nicht mehr zur Seuchenbekämpfung gebraucht werden, sind sie unverzüglich zu löschen.

Die Rechtsfragen zwischen Pandemie- und Datenschutzrecht sind vielschichtig. Ihre Beantwortung ist vor allem für den juristische Laien schwierig. Wer erste Hilfe zum Thema Datenschutz und Corona sucht, wird bei der Gesellschaft für Datenschutz und Datensicherheit fündig. Dort findet sich eine Liste mit Links.

Linksammlung GDD:
https://www.gdd.de/aktuelles/startseite/linksammlung-zu-datenschutz-und-corona

Zitierte Position der Aufsichtsbehörden:
https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5217154

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Termin	Thema	Ort	Kontakt
04.05.2020	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Köln	GDD e.V. und DATAKONTEXT
04.-08.05.2020	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
11.05.2020	Datenschutz International	Köln	GDD e.V. und DATAKONTEXT
18.05.2020	Basiswissen IT-Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
26.05.2020	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
26.05.2020	Verzeichnis von Verarbeitungstätigkeiten	Köln	GDD e.V. und DATAKONTEXT
08.06.2020	Videoüberwachung nach BDSG und DS-GVO	Düsseldorf	GDD e.V. und DATAKONTEXT
15.06.2020	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT
22.06.2020	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
23.06.2020	Datenschutz-Folgeabschätzung	Stuttgart	GDD e.V. und DATAKONTEXT
03.-05.08.2020	GDD-Sommer-Workshop	Timmendorfer Strand	GDD e.V. und DATAKONTEXT
01.09.2020	GDD-Forum Joint Controller – Gemeinsame Verantwortlichkeit: Die neue Auftragsverarbeitung?	Frankfurt/M.	GDD e.V. und DATAKONTEXT
02.09.2020	Big Data-Analysen nach DS-GVO und BDSG	Berlin	GDD e.V. und DATAKONTEXT
02.09.2020	Compliance-Tests und Schwachstellenscannen	Berlin	GDD e.V. und DATAKONTEXT
10.09.2020	Datenschutz-Management light	Köln	GDD e.V. und DATAKONTEXT
07.-11.09.2020	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
17.09.2020	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
22.09.2020	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
22.09.2020	Teleworking unter Beachtung von Datenschutz und Sicherheit	Stuttgart	GDD e.V. und DATAKONTEXT
23.09.2020	Grundlagen der Auftragsverarbeitung	Köln	GDD e.V. und DATAKONTEXT
24.09.2020	Hacker-Tools für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
28.09.2020	Datenschutz aktuell	Düsseldorf	GDD e.V. und DATAKONTEXT
29.09.2020	Die ePrivacy-Verordnung im Zusammenspiel mit der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
30.09.2020	Löschen nach DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.10.2020	Planung und Umsetzung der Überwachungsaufgabe des DSB	Köln	GDD e.V. und DATAKONTEXT
06.10.2020	Verteidigung gegen Bußgelder bei Datenschutzverstößen	Frankfurt/M.	GDD e.V. und DATAKONTEXT

Datakontext GmbH, www.datakontext.com, Tel. 0 22 34 / 9 89 49 40

Aufsätze

Prof. Dr. Boris Paal, M. Jur. (Oxford)

Kritische Würdigung des Konzepts der Datenschutzaufsichtsbehörden zur Bußgeldzumessung

Die große öffentliche Aufmerksamkeit für die Datenschutz-Grundverordnung (DS-GVO), deren Anwendbarkeit sich am 25. Mai 2020 zum zweiten Mal jährt, gründet auch und gerade auf dem im Vergleich zur vormaligen Rechtslage deutlich erhöhten Bußgeldrahmen. Während die neuen datenschutzrechtlichen Sanktionsmöglichkeiten durch Aufsichtsbehörden in anderen EU-Mitgliedstaaten bereits zu Bebußungen in zweistelliger Millionenhöhe geführt haben,[1] war es in Deutschland bis vor wenigen Monaten vergleichsweise ruhig geblieben. Dies dürfte – neben anderen Umständen, wie etwa begrenzte (finanzielle, personelle und sächliche) Ressourcen, Priorisierung anderer Aufgaben in Umsetzung der veränderten rechtlichen Rahmenbedingungen – nicht zuletzt auch auf die von der DS-GVO nur abstrakt adressierte Frage zurückzuführen sein, nach welchen Maßgaben die Aufsichtsbehörden innerhalb des gesetzlichen Rahmens („wirksam, verhältnismäßig und abschreckend", vgl. Art. 83 Abs. 1 DS-GVO) die Höhe der Geldbuße konkret zu bestimmen haben.

Zum Zwecke der Herstellung von – erhöhter – Transparenz in dieser Frage hat die deutsche Datenschutzkonferenz (im Folgenden: DSK), sprich der Zusammenschluss der Datenschutzbehörden des Bundes und der Länder, im Oktober 2019 ein Konzept veröffentlicht, das die Bußgeldzumessung bis auf Weiteres (nämlich bis zur Vorlage von abschließenden Leitlinien zur Methodik der Bußgeldzumessung durch den Europäischen Datenschutzausschuss – EDSA) einheitlich regeln soll.[2] Es steht zu erwarten, dass die hierin enthaltenen Leitlinien künftig zu einer Festsetzung deutlich höherer Bußgelder gegenüber Unternehmen führen werden.[3]

In diesem Beitrag soll das Konzept der DSK zur Bußgeldzumessung dargestellt und kritisch gewürdigt werden. Dazu wird der Blick insbesondere zu richten sein auf die Weichenstellung der Inbezugnahme des Unternehmensumsatzes als Berechnungskriterium, auf den zugrunde zu legenden Unternehmensbegriff und auf generelle unions- sowie verfassungsrechtliche Erwägungen. Zudem wird die neue nationale Bußgeldpraxis anhand zweier aktueller Fälle, namentlich der Bußgelder gegen die Deutsche Wohnen SE und gegen die 1&1 Telecom GmbH, auf den Prüfstand gestellt.

I. Das DSK-Konzept zur Bußgeldzumessung

Das Sanktionspotenzial des Datenschutzrechts und damit auch dessen Praxisbedeutung hat unter dem neuen Rechtsregime der DS-GVO deutlich zugenommen: In Art. 83 Abs. 4 und 5 DS-GVO ist nunmehr ein Bußgeldrahmen von bis zu € 10 Mio. respektive € 20 Mio. bzw. von 2% respektive 4% des weltweiten Jahresumsatzes eines Unternehmens niedergelegt. Die Berechnung des Umsatzes orientiert sich dabei am Vorbild des Kartellrechts, worauf noch zurückzukommen sein wird; berücksichtigt werden nach der Gesetzeskonzeption die Umsätze der gesamten Unternehmensgruppe. Möglich wird vor diesem Hintergrund die Verhängung von Bußgeldern bis hin zu Milliardenhöhen für Datenschutzverstöße.

Dem Unionsgesetzgeber war bewusst, dass die einheitliche Anwendung der in der DS-GVO vorgesehenen Sanktionen im Sinne der Rechtssicherheit und des gleichförmigen Normvollzugs entscheidend sein würde. Aus diesem Grund ermächtigt Art. 70 Abs. 1 S. 1 Buchst. k) DS-GVO den EDSA zur Ausarbeitung von Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Sanktionsmaßnahmen und die Festsetzung von Geldbußen. In der Folge hat sich der

1 So verhängte die französische Aufsichtsbehörde CNIL bereits im Januar 2019 ein Bußgeld in Höhe von € 50 Mio. gegen Google LLC, vgl. die PM der Behörde vom 21.01.2019, abrufbar unter https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (zuletzt abgerufen am 15.02.2020). Zudem kündigte das englische ICO im Juli 2019 an, ein Bußgeld in Höhe von umgerechnet rund € 216 Mio. gegen die Fluggesellschaft British Airways zu verhängen, vgl. die PM vom 08.07.2019, abrufbar unter https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/ (zuletzt abgerufen am 15.02.2020). Das ICO hat im Januar 2020 allerdings bekannt gegeben, das Sanktionsverfahren zunächst bis März 2020 zu verlängern. Eine Liste der bisher durch EU-Datenschutzaufsichtsbehörden verhängten Sanktionen findet sich unter https://www.enforcementtracker.com/ (zuletzt abgerufen am 15.02.2020).

2 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, abrufbar unter https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf (zuletzt abgerufen am 15.02.2020).

3 Handel, K&R 2019, 757, 760.

EDSA den in einem Arbeitspapier (Working Paper) als Leitlinie niedergelegten Ausführungen der Art.-29-Datenschutzgruppe angeschlossen,[4] in denen Kriterien unter anderem der Bußgeldzumessung ausgearbeitet und konkretisiert werden. Das betreffende Arbeitspapier stellt jedoch auch klar, dass es sich hierbei gerade nicht um einen abschließenden Leitlinienkatalog handeln soll.[5] Vor diesem Hintergrund liegen Bedarf und Raum für eine weitergehende Vereinheitlichung auf der Hand. Zum Zwecke einer solchen Vereinheitlichung will das neue Konzept der DSK die Bußgeldzumessung in Verfahren gegenüber Unternehmen in Deutschland regeln.

1. Vorgaben der DS-GVO

Das Konzept der DSK fußt auf den in der DS-GVO niedergelegten Kriterien zur Bußgeldzumessung. Zentrale Norm ist insoweit Art. 83 DS-GVO, nach dessen Abs. 1 das durch die zuständige Aufsichtsbehörde verhängte Bußgeld „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein soll. Was unter Wirksamkeit, Verhältnismäßigkeit und Abschreckung genau zu verstehen ist, wird allerdings vom Normtext nicht weiter präzisiert. Diesbezüglich verweist auch die Art.-29-Datenschutzgruppe lediglich auf eine durch die Praxis und die Gerichte vorzunehmende Begriffsbestimmung. Im Schrifttum wird in diesem Sinne unter einer „wirksamen" und „abschreckenden" Sanktion vornehmlich die Eignung der Maßnahme verstanden, general- und spezialpräventive Wirkung zu entfalten.[7]

Darüber hinaus führt Art. 83 Abs. 2 DS-GVO eine Reihe von Indikatoren auf, die durch die Aufsichtsbehörde bei der konkreten Bemessung der Bußgeldhöhe zu berücksichtigen sind, darunter etwa die Art, Schwere und Dauer des Verstoßes, die Zahl der betroffenen Personen (Art. 83 Abs. 2 S. 2 Buchst. a) DS-GVO) sowie der Verschuldensgrad[8] des Verantwortlichen (Art. 83 Abs. 2 S. 2 Buchst. b) DS-GVO). Zudem sind im Sinne einer Auffangklausel „jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall" zu berücksichtigen (Art. 83 Abs. 2 S. 2 Buchst. k) DS-GVO). In Art. 83 Abs. 4 bis Abs. 6 DS-GVO wird schließlich festgelegt, dass Bußgelder insgesamt bis zu € 10 Mio. bzw. € 20 Mio. oder, soweit dieser Betrag höher ist, 2 % bzw. 4 % des (Vor-)Jahresumsatzes des Unternehmens betragen dürfen.

2. Mehrstufiges Berechnungsmodell

Unter Zugrundelegung dieser gesetzlich festgelegten Kriterien soll das Konzept der DSK eine einheitliche, für die Normadressaten vorhersehbare Berechnungsweise der Bußgelder in Deutschland etablieren.[9] Das Konzept versteht sich dabei als Übergangsregelung bis zur Verabschiedung von EU-weit geltenden Kriterien durch den EDSA.[10] Der Anwendungsbereich des DSK-Konzepts ist zum einen inhaltlich beschränkt auf Verarbeitungstätigkeiten von Unternehmen im Inland. Nicht umfasst sind hiernach grenzüberschreitende Verarbeitungsvorgänge sowie die Bußgeldzumessung gegenüber natürlichen Personen oder Vereinen.[11] Zum anderen ist der Geltungsbereich des Konzepts beschränkt auf interne Bindungswirkungen gegenüber inländischen Aufsichtsbehörden. Das Konzept bindet also nur die Ermessensausübung der deutschen Behörden, nicht hingegen Aufsichtsbehörden in anderen Mitgliedstaaten oder die Gerichte.[12]

Konzeptionell sieht das Berechnungsmodell der DSK zur Bußgeldzumessung ein mehrstufiges Vorgehen vor:[13]

- In einem ersten Schritt wird das betroffene Unternehmen auf Grundlage seines Vorjahresumsatzes einer von vier Größenklassen zugeordnet. Innerhalb dieser Größenklassen wird sodann differenziert zwischen insgesamt 20 Untergruppen, wodurch eine genau(er)e Erfassung des Vorjahresumsatzes ermöglicht werden soll. Auf diese Weise wird das Unternehmen einer Kategorie zwischen Kleinstunternehmen mit geringem Umsatz (Jahresumsatz bis € 700.000) und sehr umsatzstarken Großunternehmen (Jahresumsatz über € 500 Mio.) zugeordnet. Unter Zugrundelegung des sog. funktionalen Unternehmensbegriffs im Sinne des unionalen Kartellrechts (so insbesondere Art. 101 und 102 AEUV) soll hierbei der Vorjahresumsatz der gesamten Unternehmensgruppe maßgeblich sein.
- In einem zweiten Schritt wird jeder der definierten Untergruppen ein mittlerer Jahresumsatz zugeordnet. Dabei sind die in dem Konzept niedergelegten, abstrakten Festlegungen maßgeblich, nicht dagegen der tatsächliche Jahresumsatz des Unternehmens. So wird etwa bei einem Kleinunternehmen, dessen Jahresumsatz zwischen € 2 Mio. und € 5 Mio. liegt, ein mittlerer Umsatz in Höhe von € 3,5 Mio. zugrunde zu legen sein – dies gilt unabhängig davon, ob der tatsächliche Jahresumsatz über oder unter diesem Wert liegt. Lediglich in der Gruppe der Großunternehmen mit einem Umsatz

4 Art.-29-Datenschutzgruppe, WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, S. 4.

5 Art.-29-Datenschutzgruppe, WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, S. 4.

6 Art.-29-Datenschutzgruppe, WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, S. 6.

7 Kühling/Buchner-Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 50; Paal/Pauly/Frenzel, DS-GVO, 2. Aufl. 2018, Art. 83 Rn. 6, 7; BeckOK/Holländer, Datenschutzrecht (30. Edition, Stand 01.11.2019), Art. 83 DS-GVO Rn. 22.

8 BeckOK/Holländer, Datenschutzrecht (30. Edition, Stand 01.11.2019) Art. 83 DS-GVO Rn. 26 weist insoweit zutreffend darauf hin, dass das Verschulden bereits Voraussetzung der Verhängung einer Geldbuße ist. Der Grad des Verschuldens kann jedoch darüber hinaus eine höhere Bußgeldzumessung indizieren.

9 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 1 f.

10 Timner/Radlanski/Eisenfeld, CR 2019, 782, 782.

11 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 1.

12 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 1.

13 Vgl. zum Berechnungsmodell auch DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 3 ff. Weiterhin auch Handel, K&R 2019, 757, 758 f.; Timner/Radlanski/Eisenfeld, CR 2019, 782, 782 f.

von über € 500 Mio. wird auf die abstrakte Festlegung verzichtet und der tatsächliche Jahresumsatz ermittelt.
- Der auf diese Weise ermittelte Wert wird anschließend durch den Faktor 360 geteilt, um einen durchschnittlichen Tagessatz („wirtschaftlicher Grundwert") zu errechnen. Der kleinstmögliche Tagessatz eines Kleinstunternehmens liegt nach dieser Rechenart bei € 972, ein Großunternehmen mit einem Umsatz zwischen € 400 Mio. und € 500 Mio. wird hingegen mit einem Tagessatz in Höhe von € 1,25 Mio. bemessen. Bei Großunternehmen mit einem Umsatz von über € 500 Mio. richtet sich der Tagessatz nach dem in Schritt zwei konkret ermittelten Umsatz.
- In einem vierten Schritt wird anhand des Schweregrads der Tat ein Faktor zwischen eins und zwölf bestimmt, mit dem der in Schritt drei ermittelte Tagessatz sodann multipliziert wird. Der Multiplikationsfaktor richtet sich dabei zum einen nach dem oben erläuterten Kriterienkatalog des Art. 83 Abs. 2 DS-GVO. Zum anderen wird berücksichtigt, ob es sich um einen formellen DS-GVO-Verstoß im Sinne von Art. 83 Abs. 4 DS-GVO oder um einen materiellen Verstoß im Sinne von Art. 83 Abs. 5, 6 DS-GVO handelt. Während leichte, formelle Verstöße zu einem niedrigen Multiplikationsfaktor führen, können schwere, materielle Verstöße einen Faktor von bis zu zwölf begründen. Zu beachten ist allerdings, dass auch bei Anwendung hoher Multiplikationsfaktoren die in Art. 83 Abs. 4 bis 6 DS-GVO genannten Höchstgrenzen der Bußgeldzumessung (von bis zu € 10 Mio. respektive € 20 Mio. bzw. von 2% respektive 4% des weltweiten Jahresumsatzes eines Unternehmens) nicht überschritten werden dürfen.
- Schließlich wird den Aufsichtsbehörden die Möglichkeit eingeräumt, den so berechneten Bußgeldbetrag anhand sonstiger, das Unternehmen betreffender Umstände anzupassen. Dies soll die Berücksichtigung täterbezogener Kriterien im Einzelfall ermöglichen, soweit diesen Kriterien nicht bereits zuvor in Schritt vier Rechnung getragen wurde.

3. Kritische Würdigung

In Ansehung der erheblichen wirtschaftlichen Bedeutung der Bußgeldzumessung für betroffene Unternehmen ist das Ziel der DSK, einen einheitlichen Rahmen für die Sanktionierung zu schaffen, uneingeschränkt begrüßenswert. Gleichwohl existieren rechtliche Bedenken gegenüber dem DSK-Berechnungsmodell, die im Folgenden aufgegriffen und analysiert werden sollen.

a) Umsatz als maßgebliches Berechnungskriterium

Dem Bußgeldkonzept der DSK liegt entscheidend die Annahme zugrunde, der Umsatz eines Unternehmens stelle „eine geeignete, sachgerechte und faire Anknüpfung" für die Bußgeldzumessung dar.[14] Bereits diese Grundannahme bedarf – jedenfalls in ihrer Absolutheit – der rechtlichen Vergewisserung.[15] So sieht Art. 83 Abs. 2 DS-GVO einen Kriterienkatalog zur Bußgeldzumessung vor,[16] in dem das für das DSK-Konzept zentrale Kriterium des Unternehmensumsatzes allerdings gerade nicht genannt wird. Zwar eröffnet der Auffangtatbestand des Art. 83 Abs. 2 S. 2 Buchst. k) DS-GVO grundsätzlich die Möglichkeit, jegliche sonstigen Milderungs- oder Erschwerungsgründe zu berücksichtigen.[17] Insoweit steht der Gesetzeswortlaut einer grundsätzlichen Berücksichtigung des Unternehmensumsatzes also nicht im Wege. Es ist aber kritisch zu hinterfragen, ob und inwieweit der nach dem Wortlaut vor allem bei der Festlegung von Obergrenzen (vgl. Art. 83 Abs. 4 bis 6 DS-GVO) zu berücksichtigende Umstand „Umsatz" zum entscheidenden Faktor der Bußgeldzumessung gemacht werden sollte.[18] Nach dem Konzept der DSK ist der Unternehmensumsatz gerade maßgebender Ausgangspunkt der Berechnung, der die konkrete Bußgeldhöhe in erheblicher Weise determiniert.

Als Folge dieser zentralen Rolle des Unternehmensumsatzes treten konsequenterweise die tatsächlich gesetzlich normierten Kriterien, konkret also jene aus Art. 83 Abs. 2 S. 2 Buchst. a) bis j) DS-GVO, bedenklich in den Hintergrund: Diese Kriterien werden lediglich auf den Stufen vier und fünf des DSK-Konzepts in die Berechnung einbezogen und können insoweit nur begrenzte Wirkung entfalten. Besonders stark wirkt sich in diesem Kontext aus, dass bei der Wahl eines Multiplikationsfaktors (unter Berücksichtigung des Kriterienkatalogs des Art. 83 Abs. 2 S. 2 DS-GVO) als geringster Faktor „1" gewählt werden kann. Der gesetzlich festgelegte Kriterienkatalog kann demnach im Ergebnis nur strafschärfend, nicht jedoch auch strafmildernd wirken.[19] Während also die Anknüpfung an den Unternehmensumsatz sich wirtschaftlich durchaus als sinnvoll darstellen mag, dürfte die Degradierung gesetzlich vorgesehener Berechnungskriterien zu bloßen „Korrekturfaktoren" den Intentionen des Unionsgesetzgebers kaum hinreichend Rechnung tragen. Damit ist jedenfalls eine unionsrechtskonforme Auslegung der aufsichtsbehördlichen Leitlinie zur Bußgeldzumessung anzuempfehlen.[20]

b) Konzernumsatz als Anknüpfungspunkt

Anlass zu Kritik[21] gibt ferner der Ansatz der DSK, wonach bei der Bestimmung des Vorjahresumsatzes des betroffenen

14 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 2.

15 So auch Timner/Radlanski/Eisenfeld, CR 2019, 782, 783.

16 Vgl. oben II. 2.

17 Sydow/Popp, Europäische DS-GVO, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 11.

18 So auch Timner/Radlanski/Eisenfeld, CR 2019, 782, 783.

19 Handel, K&R 2019, 757, 760.

20 So sollte, um die Intentionen des Gesetzgebers stärker zu berücksichtigen, zumindest auf fünfter Stufe der Begriff der „Anpassung" der Bußgeldhöhe im Geiste des Unionsrechts dahingehend verstanden werden, dass auch starke Abweichungen von dem zuvor errechneten Betrag möglich sind. In diesem Sinne auch Handel, K&R 2019, 757, 760, der darüber hinaus sogar die Option eines kompletten Absehens von der Festsetzung einer Geldbuße für geboten hält.

21 Vgl. Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 39 ff.; Sydow/Popp, Europäische DS-GVO, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 6 ff.; Timner/Radlanski/Eisenfeld, CR 2019, 782, 783.

Unternehmens im Sinne eines „funktionalen Unternehmensbegriffs" der Umsatz des gesamten Konzerns heranzuziehen sei.[22] Die insoweit aufgeworfene Frage, ob das „Unternehmen" im Sinne von Art. 83 DS-GVO als rechtliche Einheit oder – unter Einbeziehung der gesamten Konzernstruktur – als wirtschaftliche Einheit zu verstehen ist, hat erhebliche praktische Auswirkungen: Gerade bei Tochterunternehmen umsatzstarker Konzernmütter stellt die Entscheidung in dieser Frage maßgeblich die Weiche für die Größenordnung der festzusetzenden Geldbuße.

aa) Ausgangspunkt: Wortlaut der DS-GVO

Ausgangspunkt der Überlegungen in dieser Frage ist die Legaldefinition des Begriffs „Unternehmen" in Art. 4 Nr. 18 DS-GVO, wonach ein Unternehmen jede natürliche oder juristische Person ist, die eine wirtschaftliche Tätigkeit ausübt. Diese Definition spricht zunächst, insbesondere in Abgrenzung zu der Definition der „Unternehmensgruppe" nach Maßgabe von Art. 4 Nr. 19 DS-GVO, für eine Berücksichtigung (nur) der rechtlichen Unternehmenseinheit.[23] In Erwägungsgrund 150 Satz 3 zur DS-GVO heißt es hingegen ausdrücklich, im Kontext von Geldbußen sei der Unternehmensbegriffs „im Sinne der Art. 101 und Art. 102 AEUV" zugrunde zu legen. Dieser kartellrechtliche Unternehmensbegriff stellt ab auf eine Berücksichtigung der gesamten wirtschaftlichen Einheit, der das betroffene Unternehmen zugehörig ist, insbesondere also auch unter Einbeziehung der verschiedenen (Unter-)Einheiten eines Konzerns, sofern die Möglichkeit einer bestimmenden Einflussnahme durch die Konzernmutter besteht.[24] Somit besteht ein offener sprachlicher Widerspruch zwischen dem Normtext des Art. 4 Nr. 18 DS-GVO und dem Wortlaut des Erwägungsgrunds 150 Satz 3 DS-GVO.

Aus methodischer Perspektive kommt den Erwägungsgründen lediglich erläuternde Wirkung ohne normativen Gehalt zu,[25] sodass grundsätzlich von einem Vorrang der in Art. 4 Nr. 18 DS-GVO enthaltenen Definition auszugehen wäre. Zwar dienen die Erwägungsgründe als feste Bestandteile der Rechtsquelle DS-GVO als Kriterien der Auslegung, auf welche die Gerichte regelmäßig in Urteilsbegründungen zurückgreifen; gleichwohl entfalten die Erwägungsgründe aber gerade keine normgleiche Bindungswirkung.[26] Bei der Auslegung der DS-GVO können überdies jedenfalls korrigierend auch die anderen Sprachfassungen der DS-GVO herangezogen werden.[27] In diesem Sinne ist festzustellen, dass in der englischsprachigen Fassung von Art. 83 DS-GVO von „undertaking" die Rede ist – einem Begriff, der zum einen vom EuGH zur Umschreibung des kartellrechtlichen Unternehmensbegriffs verwendet wird[28] und der sich zum anderen von dem in Art. 4 Nr. 18 DS-GVO gewählten Begriff „enterprise" unterscheidet. Dieses Auseinanderfallen der Begriffsbedeutungen in der englischen wie auch in einigen anderen Sprachfassungen[29] lässt sich mit guten Gründen dahingehend interpretieren, dass das „Unternehmen" in Art. 83 DS-GVO als eigenständiger, von Art. 4 Nr. 18 DS-GVO unabhängiger Begriff zu verstehen ist, der unter Rekurs auf den Willen des Unionsgesetzgebers im Sinne eines funktionalen Unternehmensbegriffs auszulegen ist.[30]

bb) Parallelen zum Kartellrecht

Über den Wortlaut der DS-GVO hinaus ist der Blick zu richten auf die grundsätzliche, mit teleologischen Erwägungen aufgeladene Frage, ob die Bezugnahme auf den kartellrechtlichen, funktionalen Unternehmensbegriff im Kontext der datenschutzrechtlichen Bußgeldzumessung rechtsdogmatisch angemessen ist. Hiergegen wird vorgebracht, der kartellrechtliche Unternehmensbegriff sei als „Kehrseite" des sogenannten Konzernprivilegs zu verstehen, wonach das Verbot wettbewerbsbeschränkender Vereinbarungen nicht innerhalb eines Konzernverbundes gilt.[31] Dem europäischen Datenschutzrecht sei demgegenüber ein solches Konzernprivileg fremd; so müssen insbesondere auch Datenverarbeitungsvorgänge zwischen Untereinheiten eines Konzerns den Anforderungen der DS-GVO entsprechen.[32] Eine schematische Übertragung der nachteiligen Konzernhaftung ohne gleichzeitige Übertragung des Konzernprivilegs stellt sich vor diesem Hintergrund als fragwürdig dar.[33]

Zudem wird zutreffend darauf verwiesen, dass die Konzernhaftung im Kartellrecht gerade deshalb Relevanz entfaltet, weil bei der Bußgeldbestimmung der Wert der „verkauften Waren oder Dienstleistungen, die mit dem Wettbewerbsverstoß in [...] Zusammenhang stehen", als Ausgangspunkt dient.[34] Die Sanktionierung ist hier also (auch) auf die Abschöpfung solcher Vermögensvorteile gerichtet, die gerade durch den Verstoß erwirtschaftet wurden. Da sich solche Vermögensvorteile, so etwa insbeson-

22 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 3.

23 Zum Unternehmensbegriff in der DS-GVO Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 39 ff. m.w.N.; Gola, K&R 2017, 145, 146; Spindler, DB 2016, 937, 946; Uebele, EuZW 2018, 440.

24 Grünwald/Hackl, ZD 2017, 556, 558; Uebele, EuZW 2018, 440, 441.

25 Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 43 m.w.N.; Sydow/Popp, Europäische DS-GVO, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 7.

26 Siehe bereits Paal/Pauly/Paal/Pauly, DS-GVO, 2. Aufl. 2018, Einleitung Rn. 10.

27 Weiterführend zur sprachvergleichenden Auslegung Weiler, ZEuP 2010, 861.

28 Vgl. die Grundsatzentscheidung EuGH, Urt. v. 23.04.1991, C-41/90, ECLI:EU:C:1991:161 – Klaus Höfner und Fritz Elser/Macrotron GmbH.

29 Aufzählung in Uebele, EuZW 2018, 440, 443 m.w.N. Hinzuweisen ist allerdings darauf, dass die dort aufgezählte kroatische Sprachfassung – anders als von Uebele ausgeführt – wohl nicht zwischen dem Unternehmensbegriff in Art. 4 Nr. 18 DS-GVO und Art. 83 DS-GVO unterscheidet. Vielmehr dürfte unter „poduzetnik" (wörtlich „Unternehmer") das Gleiche zu verstehen sein wie unter „poduze e" (wörtlich „Unternehmen"). Dies zeigt sich schon daran, dass auch die Unternehmensgruppe in Art. 4 Nr. 19 DS-GVO als „grupa poduzetnika" („Unternehmergruppe") definiert wird.

30 So Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 39 ff.; Sydow/Popp, Europäische DS-GVO, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 7, der insoweit von der „Brüsseler Nonchalance im Umgang mit dem Bestimmtheitsgebot" spricht; aA Timner/Radlanski/Eisenfeld, CR 2019, 782, 783 f.

31 EuGH, Urt. v. 24.10.1996, C-73/95, ECLI:EU:C:1996:405 – Viho Europe BV/Kommission; Wiedemann/Schroeder, Kartellrecht, 3. Aufl. 2016, § 9 Rn. 2 ff.

32 Timner/Radlanski/Eisenfeld, CR 2019, 782, 784.

33 Faust/Spittka/Wybitul, ZD 2016, 123; Grünwald/Hackl, ZD 2017, 556, 559; Sydow/Popp, Europäische DS-GVO, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 7; aA Uebele, EuZW 2018, 440, 444.

34 EU-Kommission, Leitlinien für das Verfahren zur Festsetzung von Geldbußen gemäß Art. 23 Abs. 2 Buchstabe a) der Verordnung (EG) Nr. 1/2003, 2 f.

dere bei Produktionsketten, häufig bei mehreren unterschiedlichen Einheiten eines Konzerns manifestieren (können), sei eine funktionale Betrachtungsweise insoweit folgerichtig. Im Datenschutzrecht hingegen sei ein Anknüpfen an die erlangten Vermögensvorteile durch den Datenschutzverstoß weder vom Gesetzgeber intendiert noch überhaupt realisierbar; denn Datenschutzverstöße ließen sich vielfach nicht ohne weiteres in Gewinnzahlen übersetzen.[35] Auf Sanktionsebene erscheint nach alledem eine pauschale Übertragung des kartellrechtlichen Unternehmensbegriffs auf das Datenschutzrecht (vor allem auch) aus teleologischer Warte als zweifelhaft.

cc) Bewertung

Trotz der bestehenden Zweifel an einer Übertragbarkeit kartellrechtlicher Prinzipien auf das Datenschutzrecht lässt sich in Ansehung des Normtextes der DS-GVO gleichwohl vertreten, dass eine Anwendung des funktionalen Unternehmensbegriffs im Rahmen der Bußgeldzumessung rechtlich zulässig ist. Diese Einschätzung kann nicht zuletzt auch gestützt werden durch Berufung auf Steuerungspotenziale von Muttergesellschaften, das Effizienzziel (effet utile)[36] und das Bestreben zur Verhinderung von taktisch gezielt eingesetzten Insolvenzen.[37] Für die Praxis muss in Ansehung des DSK-Berechnungsmodells, das sich auf den „funktionalen Unternehmensbegriff" und Erwägungsgrund 150 der DS-GVO beruft,[38] einstweilen davon ausgegangen werden, dass der Konzernumsatz als maßgebliches Berechnungskriterium herangezogen wird.[39]

Eine kritische Hinterfragung dieses Ansatzes in den künftig geltenden Leitlinien des EDSA ist nach dem Vorherigen allerdings wünschenswert. Denn eine so weitreichende Auslegung, wie die Zugrundelegung des Konzernumsatzes als Anknüpfungspunkt bedarf einer belastbareren Stütze als die bloße Existenz eines (unverbindlichen) Erwägungsgrundes, um den Wortlaut von Art. 83 DS-GVO zu überspielen.[40] Letztlich wird es auf den EuGH ankommen bei der Frage, ob die Heranziehung des kartellrechtlichen Unternehmensbegriffs sich im Datenschutzrecht wird durchsetzen können. Zutreffend ist insoweit darauf verwiesen worden, dass der Gerichtshof bei der historischen Auslegung und in Ansehung des Bestimmtheitsgebots zurückhaltend judiziert.[41] Rechtspraktisch ist zu bedenken, dass bei der Bußgeldzumessung unter Anknüpfung an den Konzernumsatz ein solches Bußgeld die finanzielle Leistungsfähigkeit der den Datenschutzverstoß begehenden Gesellschaft leicht übersteigen kann.

c) Verfassungs- und unionsrechtliche Erwägungen

Schließlich wird gegen das Konzept der DSK vorgebracht, es verstoße gegen grundlegende unions- und verfassungsrechtliche Prinzipien. So wird teilweise in der Anknüpfung an den Unternehmensumsatz als maßgebliches Berechnungskriterium ein Verstoß gegen die rechtsstaatlichen Gebote der Bestimmtheit und der Gleichbehandlung erkannt: Kleinere Unternehmen würden gegenüber umsatzstärkeren diskriminiert, da bei umsatzstärkeren häufig die Höchstgrenze aus Art. 83 Abs. 4 bis 6 DS-GVO überschritten und die Geldbuße daher bei dem Höchstbetrag gekappt würde, wohingegen umsatzschwächere Unternehmen den vollen Umfang des errechneten Bußgelds tragen müssten.[42] Es darf allerdings bezweifelt werden, dass die Festsetzung einer höheren/niedrigeren Geldbuße – sei sie auch durch die Vorschrift des Art. 83 Abs. 4 bis 6 DS-GVO begrenzt – als rechtfertigungsbedürftige Privilegierung gegenüber der Festsetzung einer niedrigeren/höheren Geldbuße verstanden werden kann.

Wirkungsmächtiger erscheint vor diesem Hintergrund die Auseinandersetzung mit der Anknüpfung an den Verhältnismäßigkeitsgrundsatz aus Art. 20 Abs. 3 GG, der sich für den Fall der Bußgeldzumessung neben seiner primärrechtlichen Verankerung[43] überdies direkt aus dem Wortlaut des Art. 83 Abs. 1 DS-GVO ergibt. Hiernach muss die Härte der Sanktion zu der Schwere der Tat in einem angemessenen Verhältnis stehen.[44] Durch die Fokussierung auf den Unternehmensumsatz besteht die Gefahr, dass insoweit kaum mehr Raum für eine einzelfallbezogene, schuldorientierte Bußgeldzumessung verbleibt.[45] Denn es drohen die Bemessungskriterien aus Art. 83 Abs. 2 S. 2 DS-GVO, die gerade der Anknüpfung an den Einzelfall dienen sollen, zu bloßen Korrektiven auf vierter und fünfter Stufe der DSK-Berechnung zu verkümmern. Diese vorstehend bereits adressierte Problematik schlägt sich somit auch auf Ebene der Verhältnismäßigkeit nieder, indem und insoweit die „Schwere der Tat" als Abwägungsfaktor nicht hinreichend berücksichtigt wird. In diesem Sinne ist es geboten, der täter- und tatbezogenen „Anpassung" der Geldbuße im fünften Schritt eine weitergehende Bedeutung beizumessen. So sollte es den Aufsichtsbehörden im Rahmen des fünften Schrittes des DSK-Konzepts eröffnet werden, auch starke Abweichungen von dem zuvor errechneten Betrag vorzunehmen.[46] Auf diese Weise ließe sich im Ergebnis eine Wahrung des Verhältnismäßigkeitsgrundsatzes bei der Festsetzung von Bußgeldern sicherstellen, was na-

35 Timner/Radlanski/Eisenfeld, CR 2019, 782, 784.

36 Bergt, DuD 2017, 555, 559; zur kartellrechtlichen Bußgeldhaftung nach der 9. GWB-Novelle vor diesem Hintergrund siehe etwa Mäger/von Schreitter, NZKart 2017, 264.

37 Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 43 m.w.N.

38 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 3.

39 So auch Specht/Mantz/Born, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 8 Rn. 57.

40 Faust/Spittka/Wybitul, ZD 2016, 123, 124.

41 Kühling/Buchner/Bergt, DS-GVO BDSG, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 43 m.w.N.

42 Timner/Radlanski/Eisenfeld, CR 2019, 782, 786.

43 Art. 49 Abs. 3, 52 Abs. 1 S. 2 GRCh.

44 EuGH, Urt. v. 27.03.2014 – C-565/12, ECLI:EU:C:2014:190 – LCL Le Credit Lyonnais SA/Kalhan, EuZW 2014, 514 Rn. 45; Taeger/Gabel-Moos/Schefzig, DS-GVO BDSG, 3. Aufl. 2019, Art. 83 DS-GVO Rn. 25.

45 Handel, K&R 2019, 757, 760; Timner/Radlanski/Eisenfeld, CR 2019, 782, 787.

46 So auch Handel, K&R 2019, 757, 760.

turgemäß allerdings wieder einer schematischen Einheitlichkeit der Bußgeldzumessung entgegenstehen würde.

d) Zwischenergebnis

Eine Selbstbindung des Ermessens der Aufsichtsbehörden bei der Festsetzung von Geldbußen ist im Sinne einer Einheitlichkeit der Rechtspraxis über Ländergrenzen hinweg sowie im Sinne der Rechtssicherheit für den Normadressaten begrüßenswert. Die Anknüpfung an den funktionalen Unternehmensbegriff und damit an den Konzernumsatz bei der Ermittlung des Vorjahresumsatzes ist zwar dogmatisch kritikwürdig, aber unter Heranziehung verschiedener Sprachfassungen der DS-GVO nach dem Wortlaut sowie dem Telos einer effektiven Sanktionierung letztlich tragfähig. Die weitgehende Anknüpfung an den Unternehmensumsatz als (ganz überwiegend) maßgebliches Berechnungskriterium hingegen ist zwar rechtspolitisch nachvollziehbar, stößt aber infolge ihrer mangelnden Tatbezogenheit auf gravierende Bedenken. Diesen Bedenken sollte in der Praxis mit einer stärkeren Berücksichtigung der tat- und täterbezogener Kriterien des Art. 83 Abs. 2 S. 2 DS-GVO bei der Bußgeldzumessung begegnet werden.

II. Die Praxis der Bußgeldzumessung in Deutschland

Vor Geltung der DS-GVO waren in Deutschland nach dem BDSG a.F. lediglich Bußgelder in Höhe von bis zu € 300.000 vorgesehen.[47] Die substanzielle Erhöhung des Bußgeldrahmens durch die DS-GVO ließ insoweit eine veränderte, deutlich strengere Bußgeldpraxis der Aufsichtsbehörden erwarten. Dass eine solche Veränderung – anders als in anderen Mitgliedstaaten[48] – in Deutschland zunächst ausblieb, dürfte rückblickend nicht zuletzt auch auf die laufenden Abstimmungsprozesse der inländischen Aufsichtsbehörden zurückzuführen gewesen sein, die im Oktober 2019 in der Ausarbeitung des Konzepts der DSK mündeten. Seit Veröffentlichung des Konzepts sind dann auch bereits mehrere, im Vergleich zur früheren Praxis deutlich höhere Bußgelder verhängt worden. Vor diesem Hintergrund erfolgt im Folgenden eine Auseinandersetzung mit den besonders öffentlichkeitswirksamen, da millionenschweren Bußgeldern gegen die Deutsche Wohnen SE und gegen die 1&1 Telecom GmbH.

1. Deutsche Wohnen SE

Am 30.10.2019 erließ die Berliner Datenschutzaufsichtsbehörde gegen die Wohnungsgesellschaft Deutsche Wohnen SE einen Bußgeldbescheid in Höhe von rund € 14,5 Mio.[49] Dieser Bescheid erregte als bislang höchstes datenschutzrechtliches Bußgeld in Deutschland hohes mediales Interesse.[50] Die Deutsche Wohnen SE hat erklärt, sich gegen den Bußgeldbescheid wehren zu wollen.[51]

a) Aufsichtsbehördliche Beurteilung

Die zuständige Aufsichtsbehörde hatte datenschutzrechtlich beanstandet, dass das Unternehmen für personenbezogene Daten von Mieterinnen und Mietern ein Archivsystem verwendet habe, das keine Möglichkeit zur Löschung nicht mehr benötigter Daten vorsehe.[52] Auf diese Weise seien Daten zu persönlichen und finanziellen Verhältnissen der Betroffenen auch Jahre, nachdem der Zweck der Speicherung entfallen war, abrufbar gewesen.[53] Die Behörde ordnete dies als Verstoß gegen die Pflicht aus Art. 25 Abs. 1 DS-GVO ein, geeignete technische und organisatorische Maßnahmen zur Einhaltung der DS-GVO-Vorschriften zu treffen.[54] Zugleich wurde ein Verstoß gegen die Grundsätze der Datenverarbeitung aus Art. 5 DS-GVO gerügt, wodurch offenbar Verstöße gegen die Grundsätze der Datenminimierung (Art. 5 Abs. 1 Buchst. c) DS-GVO) und der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e) DS-GVO) in Bezug genommen wurden. Letztere scheinen jedoch aus Sicht der Behörde gegenüber der Pflicht aus Art. 25 DS-GVO in den Hintergrund zu treten, nahm die Berliner Beauftragte für Datenschutz und Informationsfreiheit doch bei der Bußgeldzumessung implizit einen auf formelle Verstöße im Sinne der in Art. 83 Abs. 4 DS-GVO ausgerichteten Bußgeldrahmen an, wohingegen eine Nichtbeachtung der in Art. 83 Abs. 5 DS-GVO genannten Vorschriften einen materiellen Verstoß darstellen würde. Näheren Aufschluss über die diesbezüglichen Überlegungen der Behörde bringt – hoffentlich – das weitere Verfahren.

b) Anwendung des DSK-Bußgeldberechnungskonzepts

Im Rahmen der öffentlich verfügbaren Erläuterungen der Berliner Datenschutzaufsichtsbehörde zur Bestimmung der Bußgeldhöhe wird (erstaunlicherweise) kein ausdrücklicher Bezug auf das Konzept der DSK genommen. Denkbar ist, dass hierfür schlicht der geringe zeitliche Abstand von 16 Tagen zwischen Veröffentlichung des Konzepts und dem Erlass des Bußgeldbescheids ursächlich war. Es dürfte jedenfalls davon auszugehen sein, dass Erwägungen des DSK-Berechnungsmodells eine wesentliche Grundlage der Bußgeldberechnung waren. Daher soll nunmehr als Anwendungsbeispiel des oben Erläuterten die Bußgeldberechnung mittels der von der DSK vorgegebenen Methode nachvollzogen werden: Zu betrachten ist im Ausgangspunkt der Vorjahresumsatz der

47 Vgl. § 43 Abs. 2 BDSG a.F.

48 Beispiele und Nachweise zu bisherigen aufsichtsbehördlichen Verfahren in den Mitgliedstaaten finden sich bereits vorstehend in Fn. 1.

49 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (zuletzt abgerufen am 15.02.2020).

50 Siehe exemplarisch nur FAZ vom 05.11.2019, Deutsche Wohnen bestraft, abrufbar unter https://www.faz.net/aktuell/wirtschaft/datenschutz-deutsche-wohnen-bestraft-16470354.html (zuletzt abgerufen am 15.02.2020).

51 Süddeutsche Zeitung vom 18.11.2019, Widerspruch eingelegt, abrufbar unter https://www.sueddeutsche.de/wirtschaft/deutsche-wohnen-widerspruch-eingelegt-1.4687525 (zuletzt abgerufen am 15.02.2020).

52 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, S. 1.

53 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, S. 1.

54 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, S. 1.

Deutsche Wohnen SE, wobei der gesamte Konzernumsatz zu berücksichtigen ist. Am Beispiel der Deutsche Wohnen SE zeigt sich dabei besonders anschaulich die Reichweite der Weichenstellung für den funktionalen Unternehmensbegriff; denn die Deutsche Wohnen SE agiert als Holding, deren Geschäftsbereiche in zahlreichen Tochtergesellschaften organisiert sind.[55]

Mit einem Konzernumsatz von € 1,4 Mrd. im Jahr 2018[56] ist die Gesellschaft in die Gruppe der Großunternehmen mit einem Umsatz von mehr als € 500 Mio. einzuordnen. Die abstrakte Berechnung eines mittleren Jahresumsatzes entfällt daher zugunsten der Betrachtung des tatsächlichen Umsatzes. Aus diesem tatsächlichen Umsatz kann sodann durch Division mit 360 ein Tagessatz in Höhe von ca. € 3,9 Mio. ermittelt werden. In einem vierten Schritt ist nach dem geeigneten Multiplikationsfaktor zu suchen: Auf Grundlage der Ausführungen der Behörde ist (vornehmlich) von einem formellen Verstoß auszugehen. Das beanstandete Archivsystem betraf teils sehr persönliche (Finanz-)Daten, wurde von dem Unternehmen bewusst eingerichtet und über mehrere Jahre betrieben, sodass grundsätzlich ein mittelschwerer (Faktor zwei bis vier) bis schwerer Verstoß (Faktor vier bis sechs) anzunehmen ist. Wählt man für die Zwecke dieses Beitrags hier exemplarisch als Mittelweg den Faktor vier, ergibt sich ein Bußgeld von € 15,6 Mio. als Mittelweg. Da dieser Betrag unter der nach Art. 83 Abs. 4 DS-GVO ermittelten Höchstgrenze von € 28 Mio. liegt, ist hierbei keine Begrenzung vorzunehmen. Schließlich können in einem letzten Schritt sonstige tat- und täterbezogene Kriterien berücksichtigt werden. So wurde von der Aufsichtsbehörde vorgebracht, das Unternehmen habe gut kooperiert, bereits erste Schritte zur Bereinigung des Verstoßes eingeleitet und es habe keine missbräuchlichen Zugriffe auf die Daten gegeben.[57] Auf diese Weise ließe sich der Betrag korrigieren auf € 14,5 Mio., was dem konkret verhängten Betrag entspricht.

c) Bewertung

Während sich die tatsächlichen Erwägungen der Aufsichtsbehörde wohl frühestens im weiteren Verfahren zeigen werden, ist gleichwohl bereits hier festzuhalten, dass die Anwendung der Berechnungsmethode der DSK jedenfalls bei der sich derzeit abzeichnenden restriktiven Handhabung der Anpassungsmöglichkeiten auf fünfter Stufe fast zwangsläufig zu einem Bußgeld in der Größenordnung des tatsächlich verhängten führen muss.

2. 1&1 Telecom GmbH

Im Dezember 2019 erließ der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit das zweite Bußgeld in Millionenhöhe gegen die 1&1 Telecom GmbH. Das Unternehmen 1&1 Telecom GmbH soll € 9,55 Mio. zahlen, da es keine technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO implementiert habe, die der Authentifizierung von Kunden am Telefon dienten.[58]

a) Aufsichtsbehördliche Beurteilung

Im konkret gerügten Fall habe der ehemalige Lebenspartner einer Betroffenen (allein) durch die Angabe ihres Namens und Geburtsdatums weitreichende Informationen zu ihren personenbezogenen Daten erhalten können.[59] Die 1&1 Telecom GmbH hat ebenfalls angekündigt, gegen das verhängte Bußgeld vorgehen zu wollen.[60] Das Unternehmen stützt sich dabei explizit auf die Unverhältnismäßigkeit der zugrundliegenden Berechnungsmethode der DSK.[61] Das verhängte Bußgeld soll nunmehr anhand der DSK-Berechnungsmethode nachvollzogen werden.

b) Anwendung des DSK-Bußgeldberechnungskonzepts

Die 1&1 Telecom GmbH ist eine hundertprozentige Tochtergesellschaft der 1&1 Telecommunication SE, die ihrerseits eine hundertprozentige Tochter der 1&1 Drillisch AG ist. Letztere wird mehrheitlich von der Konzernmutter United Internet AG gehalten.[62] Zu betrachten ist also der Konzernumsatz der United Internet AG, der im Jahr 2018 bei € 5,1 Mrd. lag.[63] Somit liegt auch 1&1 Telecom in der Gruppe der umsatzstärksten Großunternehmen, deren tatsächlicher Umsatz für die Berechnung maßgeblich ist. Teilt man diesen Betrag durch 360, so ergibt sich hieraus ein Tagessatz von € 14,2 Mio.

c) Bewertung

An der Höhe des Tagessatzes von € 14,2 Mio. wird die vorstehend ausgeführte Gefahr der Bußgeldberechnung mittels des Unternehmensumsatzes deutlich. So wird nicht zuletzt im Vergleich zum Fall der Deutsche Wohnen SE, deren schwerwiegender Verstoß letztlich mit einem ähnlichen Betrag beziffert wurde, die mangelnde Tatangemessenheit der Bußgeldberechnung deutlich. Zwar hat sich die Aufsichtsbehörde offenbar bemüht, dieses Ergebnis auf letzter Stufe durch eine Korrektur abzufangen, wird doch strafmildernd angeführt, die 1&1 Telecom GmbH habe sich „äußerst ko-

55 Deutsche Wohnen, Geschäftsbericht 2018, abrufbar unter https://www.deutsche-wohnen.com/fileadmin/pdf/ueber-uns/pressedownload/Deutsche_Wohnen_SE_Geschaeftsbericht_2018.pdf (zuletzt abgerufen am 15.02.2020), S. 25.

56 Deutsche Wohnen, Geschäftsbericht 2018.

57 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, S. 2.

58 Bundesbeauftragter für Datenschutz und Informationsfreiheit, PM vom 09.12.2019, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html;jsessionid=C8B427F6622D7A24195A6B29B73DEEAA.2_cid354 (zuletzt abgerufen am 15.02.2020).

59 Bundesbeauftragter für Datenschutz und Informationsfreiheit, PM vom 09.12.2019.

60 1&1, PM vom 09.12.2019, abrufbar unter https://newsroom.1und1.de/2019/12/09/11-klagt-gegen-bussgeldbescheid-der-datenschutzbehoerde/#page-content (zuletzt abgerufen am 15.02.2020).

61 1&1, PM vom 09.12.2019.

62 Zur Konzernstruktur s. United Internet, Geschäftsbericht 2018, abrufbar unter https://www.united-internet.de/uploads/tx_unitedinternetpublication/United_Internet_Konzern_2018.pdf (zuletzt abgerufen am 15.02.2020).

63 United Internet, Geschäftsbericht 2018, S. 7, 53, 78.

operativ" gezeigt und ein neues, datenschutzkonformes Authentifizierungsverfahren eingeführt. Gleichwohl zeigt sich auch hier die Unzulänglichkeit einer Korrektur erst auf letzter Stufe, da diese die Größenordnung der Geldbuße nicht mehr maßgeblich zu determinieren vermag. Aus generalpräventiven Gesichtspunkten bleibt für Unternehmen womöglich sogar die Frage offen, ob sich eine Kooperation mit der Aufsichtsbehörde überhaupt „lohnt", wenn eine solche Kooperation lediglich in sehr begrenztem Umfang strafmildernd berücksichtigt werden kann.

III. Zusammenfassung und Ausblick

Der Blick auf die beiden datenschutzaufsichtsrechtlichen Bußgeldbescheide gegen die Deutsche Wohnen SE und die 1&1 Telecom GmbH bestätigt die Einschätzung, wonach das neue Berechnungsmodell der DSK deutlich höhere Bußgelder erwarten lasse.[64] Somit werden Datenschutz(recht) und Datensicherheit – nicht nur – für Unternehmen auch und gerade in Ansehung der Sanktionen immer wichtiger.[65] Obgleich die Aufsichtsbehörden bislang ihre Rechenweise in den beiden Sachverhalten (noch) nicht öffentlich gemacht haben, kann unter Rekurs auf die im DSK-Konzept dargelegten Berechnungsschritte dennoch eine belastbare Annäherung an das Zustandekommen der jeweiligen Bußgeldhöhe erfolgen.

Bei diesem Vorgehen treten zudem die Schwächen der Berechnungsmethode deutlich zutage. Dies gilt insbesondere betreffend das Bußgeld gegen die 1&1 Telecom GmbH, welche trotz zügiger Kooperation mit den Behörden infolge ihres hohen Konzernumsatzes ein sehr hohes Bußgeld erhalten hat. Eine stärkere Orientierung an angemessenen, risikobasierten Kriterien wäre bei der Fortentwicklung der Bußgeld-Leitlinien, konkret im Sinne einer Harmonisierung der Vorgaben durch den EDSA, wünschenswert. Auf Sanktionsebene ist überdies ganz grundsätzlich die pauschale Übertragung des kartellrechtlichen Unternehmensbegriffs auf das Datenschutzrecht sowohl nach dem Wortlaut als auch nach der Systematik sowie der Zielsetzung der DS-GVO kritisch zu hinterfragen.

Die Berechnung von Bußgeldern im Rahmen der DS-GVO ist im Lichte des Spannungsfelds zwischen effektiver Sanktionierung auch gerade umsatzstarker Unternehmen einerseits und tatangemessener, verhältnismäßiger Bußgeldhöhe andererseits zu betrachten. Dabei lassen die gesetzlichen Vorgaben des maßgeblichen Art. 83 DS-GVO einigen Raum, den die DSK mittels ihres neuen Konzepts zur Bußgeldberechnung auszufüllen sucht. Grundsätzlich orientiert sich das DSK-Berechnungsmodell – rechtspolitisch zwar verständlich, in Ansehung des Verhältnismäßigkeitsgrundsatzes aber in der Rechtspraxis zweifelhaft – bei der Ausfüllung des eröffneten Anwendungsspielraums hauptsächlich an dem Umsatz des betroffenen Unternehmens. Insgesamt stellt sich die Frage, ob nicht im Sinne eines Systemwechsels stärker auf einen risikobasierten Ansatz abgestellt werden sollte, der vor allem auch die konkrete Gefährdung anstelle der Unternehmensumsätze in Bezug nimmt.

Die aktuellen Bußgeldverfahren zeigen, dass durch das neue Konzept in Zukunft jedenfalls mit deutlich höheren Geldbußen gerechnet werden muss. Abzuwarten bleibt, wie die Gerichte über die Verhältnis- und Rechtmäßigkeit der aufgrund des DSK-Konzepts verhängten Bußgelder urteilen werden. Denn im Grundsatz gilt, dass ein näherungsweise gleich schwerer Verstoß wegen des ungleichen Umsatzes des datenschutzrechtlich verantwortlichen Unternehmens ungleich bebußt wird. Eine Bindungswirkung des als Leitlinie einzustufenden Bußgeldzumessungskonzepts für die Gerichte besteht im Übrigen jedenfalls anerkanntermaßen nicht. Das letzte Wort wird in Ansehung des von der DS-GVO vorgegebenen Rechtsrahmens vom EuGH zu sprechen sein.

Prof. Dr. Boris Paal
Direktor des Instituts für Medien- und Informationsrecht, Abt. I (Privatrecht), Albert-Ludwigs-Universität Freiburg. Forschung und Lehre, Beratung und Expertentätigkeiten im gesamten Zivil- und Wirtschaftsrecht mit Schwerpunkten auf Daten(schutz)-, Wettbewerbs-, Medien- und Informationsrecht.

64 Handel, K&R 2019, 757, 760.

65 Zu Schadensersatzansprüchen wegen Datenschutzverstößen unlängst Paal, MMR 2020, 14.

Dr. Carlo Piltz/Carolin Lühe

DSFA-Blacklists nach Art. 35 Abs. 4 DS-GVO als Allgemeinverfügungen? Verwaltungsrechtliche Einordnung und mögliche Rechtsschutzmöglichkeiten

Nach Art. 35 Abs. 1 DS-GVO müssen öffentliche und nicht-öffentliche Stellen für Datenverarbeitungsvorgänge, die voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind, eine Datenschutzfolgeabschätzung (DSFA) durchführen. Art. 35 Abs. 4 DS-GVO verpflichtet die Aufsichtsbehörden zur Erstellung von Listen, die (wenn auch nicht abschließend) Verarbeitungsvorgänge aufzählen, bei deren Vorliegen eine DSFA zwingend durchzuführen ist. Der vorliegende Beitrag untersucht, wie diese Listen im Kontext des deutschen Verwaltungsrechts rechtlich eingeordnet werden können und was für die Praxis daraus folgt.

I. Die Blacklist nach Art. 35 Abs. 4 DS-GVO

Nach Art. 35 Abs. 4 DS-GVO muss die Aufsichtsbehörde eine Positivliste von Verarbeitungsvorgängen im Sinne des Abs. 1 erstellen, für die eine Datenschutzfolgeabschätzung (DSFA) erforderlich ist. Teilweise wird auch die Bezeichnung „Muss-Liste“ oder der Begriff „Blacklist“ verwendet. Diese Positivliste muss solche Verarbeitungsvorgänge enthalten, die nach Auffassung der Aufsichtsbehörde voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind.

Ziel einer solchen Positivliste ist die Klarstellung darüber, wann eine DSFA durchgeführt werden muss. Eine DSFA muss nach Art. 35 Abs. 1 DS-GVO grundsätzlich vom Verantwortlichen durchgeführt werden, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Es obliegt dem Verantwortlichen, sich die notwendigen Informationen zu beschaffen und beispielsweise konkret bei Auftragsverarbeitern oder Herstellern anzufordern.[1] Bei unvollständiger oder nicht korrekter DSFA droht gemäß Art. 83 Abs. 4 lit. a) DS-GVO im schlimmsten Fall eine Geldbuße.

Momentan existiert eine gemeinsame Liste aller deutschen Aufsichtsbehörden für Datenverarbeitungsvorgänge von nicht-öffentlichen Stellen.[2] Für Verarbeitungsvorgänge öffentlicher Stellen verweisen die Aufsichtsbehörden der Länder entweder auf die Liste für nicht-öffentliche Stellen oder haben zum Teil eigene Listen erstellt. Aus der Liste geht die Beschreibung verschiedenster Verarbeitungstätigkeiten hervor sowie typische Einsatzfelder und Beispiele für diese Art der Verarbeitung. Nach Ansicht der deutschen Aufsichtsbehörden ist eine DSFA durchzuführen, wenn eine Verarbeitung des Verantwortlichen die Voraussetzungen einer der dort gelisteten Verarbeitungstätigkeiten erfüllt.

II. Blacklists als normenumschaltende Verwaltungsmaßnahmen

Bei den Blacklists dürfte es sich um sogenannte „normumschaltende Verwaltungsmaßnahmen“ handeln.[3] Diese sind abzugrenzen von normkonkretisierenden Verwaltungsvorschriften, die unbestimmte Rechtsbegriffe in Normen konkretisieren und dieses Ergebnis einer nur begrenzten gerichtlichen Kontrolle zugänglich machen.[4]

Der Anwendungsbereich normkonkretisierender Verwaltungsvorschriften umfasst mittlerweile das gesamte Umwelt- und Technikrecht.[5] Sie entfalten nach ständiger Rechtsprechung des Bundesverwaltungsgerichts nur Bindungswirkung, wenn sie dem wesentlichen Erkenntnis- und Erfahrungsstand Rechnung tragen, der aufgrund eines umfangreichen Beteiligungsverfahrens ermittelt worden ist.[6] Da das Ziel der Blacklist nicht die Sicherstellung der einheitlichen Auslegung von Begriffen im Umwelt- und Technikrecht ist, sondern es vielmehr um eine wertende Entscheidung der Aufsichtsbehörde geht, welche Datenverarbeitungsvorgänge sie als risikoreich einstuft, dürfte es sich nicht um normkonkretisierende Verwaltungsvorschriften handeln.

Normumschaltende Verwaltungsmaßnahmen liegen hingegen vor, wenn Normen so konstruiert sind, dass die dort angeordneten Rechtsfolgen nur dann eintreten sollen, wenn die Behörde das Vorliegen bestimmter tatsächlicher Umstände (verbindlich) festgestellt hat und diese Feststellung öffentlich bekanntgibt. Die Rechtsnatur dieser Maßnahmen ist umstritten.[7] Bei bisherigen Konstruktionen dieser Art (Beispiel: Feststellung des Vorliegens einer austauscharmen Wetterlage nach § 40, § 49 Abs. 2 BImSchG aF, die den Smog-Alarm auslösten) wurde dieses Vorgehen der Verwaltung von der herrschenden Meinung als Erlass einer perso-

1 Hansen, in: Wolff/Brink, BeckOK Datenschutzrecht, 29. Ed 2018, Art. 35, Rn. 10.

2 Abzurufen unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

3 Begriff nach Winkler, DVBl 2003, 1490, 1491.

4 Riese, in: Schoch/Schneider/Bier/Riese, VwGO, 37. El 2019, § 114, Rn. 169.

5 Sachs, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 40, Rn. 217. Bekannteste Beispiele sind wohl die TA Luft und TA Lärm.

6 BVerwG, Beschl. v. 15.02.1988, 4 NB 2/87, NVwZ 1988, 824, 825; BVerwG, Beschl. v. 21.03.1996, 7B 164/95, NVwZ-RR 1996, 498, 499.

7 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 299.

nenbezogenen Allgemeinverfügung klassifiziert.[8] Dem kann man zustimmen, da es letztendlich auf das Gleiche hinausläuft, ob der Eintritt gesetzlicher Rechtsfolgen durch die behördliche Feststellung bestimmter Tatsachen bedingt ist oder ob eine Behörde ermächtigt wird, bei Vorliegen bestimmter Tatsachen bestimmte Regelungen durch sich an jedermann richtende personenbezogene anlassbezogene Allgemeinverfügungen zu treffen. Es erscheint nicht sinnvoll, beide Maßnahmen unterschiedlich zu beurteilen.

Ein ähnliches Muster findet man auch in Art. 35 Abs. 1, 4 DS-GVO. Art. 35 Abs. 1 DS-GVO ordnet an, dass für Datenverarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, eine DSFA durchzuführen ist. In Art. 35 Abs. 4 DS-GVO werden die Behörden verpflichtet, durch Erstellung einer Liste verbindlich festzulegen, wann ein solch hohes Risiko besteht und somit in jedem Fall eine DSFA durchzuführen ist. Besonderheit ist in diesem Fall jedoch, dass nicht nur die Liste die Pflicht zur Durchführung begründet. Diese kann sich allein schon aus Art. 35 Abs. 1 DS-GVO ergeben. Der Verantwortliche muss also auch, wenn ein etwaiger Verarbeitungsvorgang nicht in der Liste aufgeführt ist, selbstständig anhand der Kriterien der Art. 35 Abs. 2 und 3 DS-GVO überprüfen, ob voraussichtlich ein hohes Risiko vorliegt.[9] Dies ändert aber nichts an der Einschätzung, die Listen als normumschaltende Verwaltungsmaßnahmen charakterisieren zu können, da die Aufsichtsbehörden durch die Bereitstellung der Listen Verarbeitungsvorgänge als verbindlichen Grund einstufen, der die Verpflichtung nach Art. 35 Abs. 1 DS-GVO auslöst.

III. Charakterisierungsmöglichkeit der Blacklist als Allgemeinverfügung

Fraglich ist, ob die momentan existierenden Blacklist als normumschaltende Verwaltungsmaßnahmen in der vorliegenden Variante als Allgemeinverfügung charakterisiert werden kann.

1. Materielle Voraussetzungen

Ein Verwaltungsakt (VA) ist jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist. Eine Allgemeinverfügung ist ein VA, der sich an einen nach allgemeinen Merkmalen bestimmten oder bestimmbaren Personenkreis richtet oder die öffentlich-rechtliche Eigenschaft einer Sache oder ihre Benutzung durch die Allgemeinheit betrifft.

Die Allgemeinverfügung als besondere Form des VA iSv § 35 S.1 VwVfG, existiert in drei Formen: als personenbezogene (Var. 1), sachbezogene (Var. 2) oder benutzungsregelnde (Var. 3) Allgemeinverfügung.

Ob eine Maßnahme als VA und im Speziellen als eine Allgemeinverfügung einzuordnen ist, bestimmt sich danach, ob sie die Merkmale des § 35 VwVfG erfüllt (sog. materieller VA-Begriff), unabhängig davon, in welcher Form sie ergeht.[10]

Für Allgemeinverfügungen als Unterfall des VA bedeutet dies, dass eine Allgemeinverfügung die Tatbestandsmerkmale des § 35 S. 1 VwVfG erfüllen muss, und S. 2 nur eine Teil-Legaldefinition des Merkmals „Einzelfall" enthält; alle anderen Tatbestandsmerkmale des S. 1 bleiben unberührt.[11] Maßgeblich ist somit letztlich, ob sich der Akt nach objektiver Betrachtung als verbindliche, auf Setzung einer Rechtsfolge gerichtete und auf Rechtsbeständigkeit hin abzielende und von der Behörde erkennbar gewollte Regelung darstellt oder nicht.

a) Maßnahme einer Behörde

Der Begriff der Behörde ist in § 1 Abs. 4 VwVfG legaldefiniert. Die Aufsichtsbehörden (Datenschutzbeauftragte der einzelnen Bundesländer) die die Positivlisten erstellt haben, sind unstreitig Behörden im Sinne dieser Vorschrift.

b) Verfügung, Entscheidung oder andere hoheitliche Maßnahme

Den Begriffen Verfügung, Entscheidung oder Maßnahme ist gemein, dass sie Formen der Willensbildung,[12] also verwaltungsrechtliche Willenserklärungen sind, die final auf eine Rechtsfolge gerichtet sind. Ob dies der Fall ist, ist durch Auslegung zu ermitteln.

Ob eine Rechtsgrundlage für den Erlass eines VA vorhanden ist, das heißt dafür, dass die Behörde sich zu einer Regelung der Rechtsform des VA bedienen durfte, ist für die Frage der Rechtsnatur nicht entscheidend.[13] Es kann jedoch trotzdem als Auslegungshilfe auf die Entscheidungskompetenz der Behörde abgestellt werden. Fehlt eine offensichtliche VA-Befugnis, kann nicht ohne weiteres unterstellt werden, die Behörde habe einen VA erlassen wollen.[14] Vorliegend sind die Aufsichtsbehörden verpflichtet, eine Liste mit Datenverarbeitungsvorgängen, die eine DSFA erfordern, zu erstellen („Die Aufsichtsbehörde erstellt eine Liste...", Art. 35 Abs. 4 DS-GVO), während hingegen die Erstellung einer Liste mit Datenverarbeitungsvorgängen, die keine DSFA erfordern, lediglich optional ist („Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist", Art. 35 Abs. 5 DS-GVO).

Dies sagt jedoch nichts darüber aus, ob diese Listen als Allgemeinverfügung erlassen werden können. Grundsätzlich muss die Verwendung der Handlungsform VA wegen des Vorbehalts des Gesetzes gesetzlich vorgeschrieben sein, wenn

8 Appel/Melchinger, VerwArch 84 (1993), 349, 376 ff.; Jacobs, NVwZ 1987, 100, 105; Jarass, NVwZ 1987, 95 ff.; a. A. Ehlers, DVBl 1987, 972, 973 ff.

9 Erläuternd: Baumgartner, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 35, Rn. 46.

10 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 16.

11 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 267.

12 BT-Drs. 7910 S. 57; Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 69.

13 BVerwG, Beschl. v. 09.11.1984, 7 C 5/84, NVwZ 1985, 264, 264.

14 VG München, Beschl. v. 24.05.2004, M 22 E 04.799, NVwZ 2005, 477, 478.

es sich um eine für den Adressaten ungünstige Entscheidung handelt. Da die Listen die Handlungsverpflichtung[15] der Verantwortlichen begründen, eine DSFA durchzuführen (und diese auch praktischen Aufwand bedeutet), handelt es sich um eine belastende Maßnahme. Dass die Befugnis besteht, diese Liste als Allgemeinverfügung zu erlassen, ergibt sich nicht direkt aus der Vorschrift. Allerdings würde, wenn man von einer fehlenden VA-Befugnis ausginge, dies nichts daran ändern, dass der VA „in der Welt ist" und angefochten werden muss, um ihn zu beseitigen – die Anfechtungslast trägt also in jedem Fall der von dem VA Betroffene.

In der Literatur wird bereits vertreten, dass, sofern der Adressatenkreis hinreichend bestimmbar ist (zum Beispiel jeder Verantwortliche, der Genomdaten von Deutschen verarbeitet), die Listen von den Aufsichtsbehörden in Form einer Allgemeinverfügung (§ 35 S. 2 VwVfG) erlassen werden können.[16] Nach dieser Ansicht könnte die Behörde also wählen, für welche Handlungsform sie sich entscheidet.

Aufschluss über den Willen der Behörde kann auch die Form der in Rede stehenden Maßnahme geben. Vergleicht man die Listen mit anderen im Internet veröffentlichen Allgemeinverfügungen,[17] sind diese klar als solche gekennzeichnet und folgen auch der geläufigen Struktur eines Verwaltungsaktes (Inhalt der Anordnung, Begründung, Gebührenregelung, Rechtsbehelfsbelehrung). Dies alles vermag man zumindest in der gemeinsamen Liste der Datenschutzkonferenz nicht zu erkennen. Sie erscheint vielmehr als schlichte Broschüre oder Information mit einer Tabelle. Es wird zwar darauf hingewiesen, dass die Durchführung der DSFA (siehe näheres unter c)), verpflichtend ist, jedoch enthält die Liste nicht die oft typische Überschrift „Allgemeinverfügung" wie bei sonstigen im Internet veröffentlichten Allgemeinverfügungen.[18] Auch erfolgt keine Rechtsbehelfsbelehrung im Sinne des § 58 VwGO, sondern nur der Hinweis, dass gegen eine Geldbuße, die verhängt wurde, weil keine DSFA durchgeführt wurde (was selbstverständlich einen Verwaltungsakt darstellt[19]), der Rechtsweg gemäß Art. 78 DS-GVO eröffnet ist. Auch die übrigen Listen der einzelnen Aufsichtsbehörden der Länder weisen diese Gestaltung auf. Man könnte dadurch den Eindruck gewinnen, die Aufsichtsbehörden wollten eben (noch) keine Allgemeinverfügung erlassen. Ob sie dies jedoch getan haben, ist, wie oben schon festgestellt, keine Frage der äußeren Form, sondern des Inhalts.

c) Regelung

Die Blacklist müsste, um als Allgemeinverfügung zu gelten, nach dem objektiven Sinngehalt auf eine unmittelbare, für die von ihr Betroffenen verbindliche Festlegung von Rechten und Pflichten gerichtet sein, das heißt einen Anspruch unmittelbarer Verbindlichkeit haben.[20] Sie muss also auf unmittelbare Rechtswirkung gerichtet sein. Dies wird man ohne Zweifel bejahen können, enthält die von der Datenschutzkonferenz herausgegebene Liste für Verarbeitungsvorgänge nicht öffentlicher Stellen doch folgenden Hinweis:

„Führt eine verantwortliche Stelle (Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO) Verarbeitungsvorgänge aus, die in Art. 35 Abs. 3 DS-GVO der Liste aufgeführt sind, ohne vorab eine DSFA durchgeführt zu haben, so kann die zuständige Aufsichtsbehörde wegen Verstoßes gegen Art. 35 Abs. 1 DS-GVO von ihren Abhilfebefugnissen gemäß Art. 58 Abs. 2 DS-GVO einschließlich der Verhängung von Geldbußen gemäß Art. 83 Abs. 4 DS-GVO Gebrauch machen. Gegen eine derartige Maßnahme der Aufsichtsbehörde steht der Rechtsweg gemäß Art. 78 DS-GVO offen."

Man könnte zwar die Ansicht vertreten, dass sich die Pflicht zur Durchführung der DFSA nicht erst aus der Liste ergibt, sondern bereits aus Art. 35 Abs. 1 DS-GVO, da es dort heißt: *„(…) so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch."* Das Unterlassen der Durchführung kann auch einen Verstoß gegen Art. 35 Abs. 1 DS-GVO begründen.[21] Verstöße gegen Art. 35 DS-GVO sind gem. Art. 83 Abs. 4 lit. a) DS-GVO bußgeldbewehrt. Im Grundsatz muss der Verantwortliche nach Art. 35 Abs. 1 DS-GVO selbst eine (Wertungs-)entscheidung treffen, ob „sein" Verarbeitungsvorgang nach seiner eigenen Prognose voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Er muss die Entscheidung über das „ob" einer DSFA also grundsätzlich selbst treffen. Im Unterschied hierzu wird durch die Positivlisten die Prognoseentscheidung durch die Aufsichtsbehörden bereits getroffen und dem Verantwortlichen kein Entscheidungsspielraum mehr eingeräumt. In der Zusammenschau aus gesetzlicher Regelung in Art. 35 Abs. 1 und 4 DS-GVO und der Positivliste ergibt sich mithin klar eine Handlungspflicht.

d) Regelung eines Einzelfalls

Da sich die Listen an alle richten, die die genannten Arten von Verarbeitungstätigkeiten vornehmen, kann es sich bei einer solchen Liste, wenn überhaupt, nur um eine generell-konkrete Maßnahme handeln. Für die Frage, ob die Maßnahme zur Regelung eines Einzelfalls erfolgt, kommt es nicht darauf an, ob auch die rechtlichen Voraussetzungen für eine solche Regelung vorliegen. Die Regelung eines Einzelfalls im Sinne einer hier in Betracht kommenden personenbezogenen Allgemeinverfügung wird man annehmen können, wenn sich die Allgemeinverfügung an einen nach

15 Vgl. wann ein belastender Verwaltungsakt vorliegt: Müller, in: BeckOK VwVfG, 45. Ed. 2019, VwVfG, § 48, Rn. 27.

16 Nolte/Werkmeister, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 35, Rn. 32.

17 Beispielhaft, eine Allgemeinverfügung der Stadt Cottbus: https://www.cottbus.de/aktuelles/allgemein/allgemeinverfuegung_der_stadt_cottbus_zum_alkoholverbot_gueltigkeitszeitraum_25_juni_bis_31_oktober_2019.html; Allgemeinverfügung des Eisenbahn-Bundesamtes: https://www.eba.bund.de/SharedDocs/Downloads/DE/TechnArbeitsschutz/33_Allgemeinverfuegung_Tunnelbaustellen_Grossbaumaschinen.pdf;jsessionid=F363E4852036CD471B29678D17729239.live21302?__blob=publicationFile&v=2.

18 Siehe Fn 17.

19 Gassner, in: Blum/Gassner/Seith, Ordnungswidrigkeitengesetz, 1. Aufl. 2016, § 65, Rn. 5; Kurz, in: Karlsruher Kommentar, OWiG, 5. Aufl., § 65, Rn. 8; OLG Schleswig, Urt. v. 10.09.1969, NJW 1970, 158, 159.

20 BVerwG, Urt. v. 22.05.1980, 2 C 30/78, NJW 1981, 67, 68; BVerwG, Urt. v. 25.03.1964, VI C 150/62, MDR 1964, 701, 702.

21 Baumgartner, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 35, Rn. 78.

22 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 282.

allgemeinen Merkmalen bestimmten Kreis von Adressaten aus Anlass einer bestimmten konkreten Situation richtet.[22] Der Unterschied zur Rechtsnorm ist nicht die Unbestimmtheit des Personenkreises, sondern die Konkretheit des geregelten Sachverhalts. Eine Allgemeinverfügung kann auch eine Regelung „für wen immer es angeht" bezüglich erst in der Zukunft liegender Konkretisierungsfälle sein.[23]

Personenbezogene Allgemeinverfügungen richten sich an einen bestimmten oder bestimmbaren Personenkreis. Der Umstand, dass der Adressatenkreis zur Zeit des Erlasses der Regelung objektiv nicht feststeht, spricht nicht gegen die Annahme einer Allgemeinverfügung.[24] Die betroffenen Personen werden nach allgemeinen Merkmalen gattungsmäßig bestimmt. Das Gattungsmerkmal, das den Personenkreis bestimmbar macht, kann durch ein konkretes Ereignis hergestellt werden, das Anlass für eine öffentlich bekannt gegebene Anordnung an einen näher umschriebenen Personenkreis ist. Maßgebliches Abgrenzungskriterium zur Rechtsverordnung ist die Konkretheit des Sachverhalts.[25] Die Rechtsprechung verfährt bei der Annahme einer personenbezogenen Allgemeinverfügung eher großzügig. Nach Auffassung des BGH schließt es die generelle Natur der Allgemeinverfügung sogar regelmäßig aus, dass der geregelte Sachverhalt sowohl sachlich als auch räumlich, zeitlich und hinsichtlich des betroffenen Personenkreises konkretisiert wird.[26]

Ein nach allgemeinen Merkmalen bestimmbarer Personenkreis liegt auch vor, wenn der Personenkreis nicht unabhängig von der in Frage stehenden Regelung einer bestimmten Gattung zugehört, sondern die Regelung diese Gattung erst begründet, indem Sie z.B. allen denjenigen, die etwas Bestimmtes tun wollen, dieses verbietet[27] oder etwas befiehlt[28], sich die Regelung also an jedermann wendet.

Die Verarbeitungsarten, die in der Liste genannt sind, dürften zumindest zu einem Großteil (insbesondere Nr. 1-3, 11-13, 15[29]) so beschrieben sein, dass jeder Adressat erkennen kann, ob er diese Art der Verarbeitung vornimmt und damit die DSFA durchführen muss. So muss zum Beispiel nach Nr. 1 eine DSFA vorgenommen werden, wenn eine Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen durchgeführt wird und mindestens ein weiteres Kriterium aus WP 248 Rev. 01 zutrifft. Dieser Verarbeitungsvorgang dürfte in jedem Fall so klar umgrenzt sein, dass sich für Verantwortliche ergibt, ob sie zum angesprochenen Adressatenkreis gehören oder nicht. Bei anderen Verarbeitungsvorgängen, wie der unter Nr. 4 genannten „umfangreichen" Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen, könnte man dies wohl auch mit dem Hinweis darauf, dass nicht klar definiert ist, was „umfangreich" bedeutet, anders sehen.

Der Adressatenkreis der Liste ist damit mindestens zum Teil hinreichend bestimmbar, denn jeder Verantwortliche, der eine in der Liste genannte Verarbeitungsart durchführt, muss ohne weitere Differenzierung (nach beispielsweise Zweck der Verarbeitung) die DSFA durchführen. Die in Spalte 2 und 3 genannten Einsatzfelder und Beispiele wie „Große Anwaltskanzlei" und „Carsharing und Mobilitätsdienste" bestimmen den Adressatenkreis keinesfalls abschließend, sondern dienen eben nur als Beispiel.

e) Außenwirkung

Die hoheitliche Maßnahme muss nach ihrem objektiven Sinngehalt darauf gerichtet sein, Außenwirkung zu entfalten.[30] Die getroffene hoheitliche Regelung darf nicht nur darauf abzielen, im Bereich der Behörden als verwaltungsinterne Anweisung Wirkungen zu zeigen.[31] Da die Positivlisten festlegen, wann die unbedingte Rechtspflicht der Verantwortlichen zur Durchführung einer DSFA besteht, liegt auch klar eine Außenwirkung vor. Die Listen dienen gerade nicht nur als behördeninterne Hinweise oder Anweisungen. In Kombination mit der gesetzlichen Pflicht aus Art. 35 Abs. 1 DS-GVO ergibt sich eine Wirkung in Richtung der außerhalb der Aufsichtsbehörden stehenden datenverarbeitenden Stellen.

f) Zwischenergebnis

Damit erfüllen die Positivlisten (mindestens partiell) die materiellen Voraussetzungen eines Verwaltungsaktes in Form einer personenbezogenen Allgemeinverfügung.

2. Form

Problematisch für die Klassifizierung der Positivlisten als Allgemeinverfügung könnte auf den ersten Blick erscheinen, dass die Listen nur auf der Homepage der jeweiligen Aufsichtsbehörden abgerufen werden können. Nach § 37 Abs. 2 VwVfG kann ein VA schriftlich, elektronisch, mündlich oder in anderer Weise erlassen werden. Man könnte überlegen, ob die Liste einen VA in Textform darstellt. Ein VA in Textform liegt vor, wenn der Inhalt in einer Urkunde oder in anderer dauerhafter Weise materialisiert ist. Das kann man bereits annehmen, wenn der VA auf einem Datenträger des Empfängers abgespeichert ist. Dazu würde es zum Beispiel genügen, wenn die Positivliste als PDF (in dieser Form ist sie veröffentlicht) auf dem PC bei dem Verantwortlichen abgespeichert wird.

In Betracht käme hier auch ein elektronischer VA. Ein elektronischer VA ist jeder textlich perpetuierte VA, der nur als elektronischer Speicherzustand auf einem (austauschba-

23 BVerfG, Beschl. v. 26.03.2001, 1 BvQ 15/01, NJW 2001, 1411, 1412.

24 VGH Mannheim, Urt. v. 22.05.2013, 9 S 1367/12, BeckRS 2013, 52330.

25 OVG Münster, Beschl. v. 20.07.2010, 2 A 61/08, BeckRS 2010, 51242.

26 BGH, Beschl. v. 29.04.2008, KVR 28/07, NJW-RR 2008, 1654, 1655.

27 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 37, Rn. 287.

28 Scheffczyk, in: von Alemann, BeckOK VwVfG, 45. Ed. 2019, § 35, Rn. 14, 257; OVG Lüneburg, Beschl. v. 18.10.2004, 1 ME 205/05, NVwZ-RR 2005, 93, 94.

29 Bei allen anderen Verarbeitungstätigkeit ist bis jetzt die Bedeutung des Wortes „umfangreich" noch nicht einheitlich geklärt. Grundlage ist Art. 35 Abs. 3 lit. b) DS-GVO. Zwar nennen die ErwG 75 bzw. 91 die Berücksichtigung zweier Einflussgrößen für die Bemessung, ob eine Verarbeitung umfangreich ist (Zahl der Personen und Menge der Daten).

30 BVerwG, Urt. v. 15.02.1989, 6 A 2/87, NVwZ 1989, 1055, 1055; BVerwG, Urt. v. 26.04.2012, 2 C 17/10, NVwZ 2012, 1483.

31 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 14.

ren) elektronischen Datenträger existiert und damit nicht unmittelbar wahrnehmbar ist.[32] Vom elektronischen VA ist der von § 41 Abs. 2 S. 2 VwVfG erwähnte „elektronisch übermittelte" VA zu unterscheiden. Dieser Begriff erfasst nicht nur elektronische VA, sondern auch schriftliche VA, soweit sie elektronisch übermittelt werden.[33]

Man könnte hier wohl einen VA-Erlass in Textform oder aber auch in elektronischer Form annehmen. In jedem Fall ist der VA aber auf „andere Weise" im Sinne des § 37 Abs. 2 S. 1 VwVfG dadurch erlassen worden, dass die Aufsichtsbehörden die Liste auf ihren Internetseiten veröffentlichen und sie zum Download bereitsteht.

3. Abgrenzung zu anderen Rechtsakten

a) öffentliche Bekanntgabe

Die Bekanntgabe ist zwar kein Tatbestandsmerkmal des VA im Sinne des § 35 VwVfG. Ob die Blacklist einen VA in Form einer Allgemeinverfügung im materiell-rechtlichen Sinn darstellt, ist mithin losgelöst von der Bekanntgabe zu beurteilen. Relevant ist die Bekanntgabe jedoch für die Rechtsschutzmöglichkeiten gegen die Blacklist.

Nach h.M. wird ein VA erst durch seine Bekanntgabe gemäß 41 VwVfG wirksam.[34] Unter Bekanntgabe versteht man allgemein die Eröffnung des VA gegenüber dem Betroffenen.[35] Ein Verwaltungsakt, der dem Betroffenen nicht ordnungsgemäß bekanntgegeben wurde, ist diesem gegenüber unwirksam, jedoch „in der Welt" und ggf. wirksam gegenüber den Betroffenen, denen er ordnungsgemäß bekanntgegeben wurde. Liegt gar keine wirksame Bekanntgabe vor, ist der betroffene VA ein bloßes Verwaltungsinternum.[36] Eine Sonderform der Bekanntgabe ist die öffentliche Bekanntgabe nach § 41 Abs. 3, 4 VwVfG. Die öffentliche Bekanntgabe unterscheidet sich von der Individualbekanntgabe dadurch, dass ihre Wirksamkeit nicht vom Zugang des VA beim Betroffenen abhängt.[37] Allgemeinverfügungen können öffentlich bekanntgegeben werden, wenn die Bekanntgabe an die einzelnen Beteiligten untunlich oder unmöglich ist, § 41 Abs. 3 S. 2 VwVfG. Untunlich ist die Individualbekanntgabe unter anderem auch, wenn nicht mit Sicherheit feststellbar ist, wer betroffen ist.[38]

Das Zugangserfordernis wird dann durch eine öffentliche Verlautbarung des VA ersetzt. Dadurch wird zwar jedermann die Kenntnisnahme ermöglicht, bei dieser hängt jedoch die Wahrnehmung der Kenntnisnahmemöglichkeit von der Aufmerksamkeit, dem Interesse und den tatsächlichen Möglichkeiten des Betroffenen ab.[39] Ob der Betroffene tatsächlich Kenntnis nimmt, ist keine Voraussetzung für die Wirksamkeit der öffentlichen Bekanntgabe. Nach dieser Logik würde die öffentliche Bekanntgabe grundsätzlich unbeschränkt gelten und folglich auch gegenüber erst später betroffenen Personen, die zur Zeit der Bekanntgabe noch nicht zum Adressatenkreis des VAs gehörten. Die Bekanntgabe setzt damit auch die Rechtsbehelfsfristen des § 58 VwGO in Gang (ein Monat bzw. ein Jahr bei fehlender Rechtsbehelfsbelehrung), was in letzter Konsequenz dazu führen würde, dass die Rechtsbehelfsfristen abgelaufen sein könnten, bevor eine Person, die erst später betroffen ist oder von der Verfügung Kenntnis genommen hat, Rechtsmittel einlegen kann. Unter Rechtsschutzgesichtspunkten des Art. 19 Abs. 4 GG müsste zumindest ein Wideraufgreifen des Verfahrens möglich sein.[40] In Anlehnung an die Rechtsprechung des Bundesverwaltungsgerichts zur selben Problematik bei Verkehrsschildern (die auch als Allgemeinverfügung gelten[41]), könnte man hier argumentieren, dass die Rechtsmittelfrist erst zu laufen beginnen kann, wenn der von Regelung Betroffene erstmals auch wirklich Adressat ist (und auch erst dann eine Beschwer im Sinne des § 42 Abs. 2 VwGO überhaupt vorliegt), da dies sonst den Rechtsschutz unzumutbar verkürzen würde.[42]

Bei der Blacklist kann die Aufsichtsbehörde vorher nicht wissen, wer die genannten Verarbeitungsvorgänge vornehmen wird. Deshalb bleibt ihr letztendlich nichts anderes übrig, als die Listen öffentlich bekanntzugeben. Aufgrund der erhöhten Sensibilität der Verantwortlichen für die Anforderungen der DS-GVO ist davon auszugehen, dass ein Besuch der Internetseiten der Aufsichtsbehörden nicht unwahrscheinlich ist und auch erwartet werden kann, so dass in jedem Fall von einer Kenntnisnahmöglichkeit der Verantwortlichen ausgegangen werden kann, auch wenn dies in der Praxis einen gewissen Aufwand für die Verantwortlichen begründet, gerade vor dem Hintergrund, dass es 17 Aufsichtsbehörden gibt und die Listen fortlaufend aktualisiert werden sollen. Daher ist es zu begrüßen, dass es zumindest eine gemeinsame Liste für nicht-öffentliche Stellen gibt. Dies würde im vorliegenden Fall bedeuten, dass Zeitpunkt der öffentlichen Bekanntgabe derjenige Zeitpunkt ist, ab dem die Liste im Netz abrufbar ist.

Bezüglich der Fristen für etwaige Rechtsbehelfe kann nach dem oben Dargestelltem argumentiert werden, dass diese erst dann anfangen zu laufen, wenn ein Verantwortlicher einen der in den Blacklists genannten Verarbeitungsvorgänge erstmalig vornimmt, da er auch erst dann von der Allgemeinverfügung und ihrem Regelungsgehalt betroffen ist.

b) Sich daraus ergebende Notwendigkeit der Abgrenzung

Mit der öffentlichen Bekanntgabe nach § 41 Abs. 3 VwVfG erlangt die Allgemeinverfügung allgemeine Wirksamkeit gegenüber jedem Adressaten, auch gegenüber solchen, die zum Zeitpunkt des Erlasses noch nicht von der Regelung

32 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 37, Rn. 65.

33 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 37, Rn. 67.

34 Ramsauer, in: Kopp/Ramsauer, VwVfG, 20. Aufl. 2019, § 41, Rn. 15.

35 Ramsauer, in: Kopp/Ramsauer, VwVfG, 20. Aufl. 2019, § 41, Rn. 6.

36 BVerwG, Urt. v. 21.11.1986, 8 C 127/87, NVwZ 1987, 330, 331; BVerwG, Urt. v. 09.01.1989, 6 C 47/86, NVwZ 1989, 1173.

37 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 41, Rn. 135.

38 BT-Drs. 7/910, S. 62.

39 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 41, Rn. 135.

40 Schmidt-Aßmann, in: Maunz/Dürig, Art. 19, Rn. 251; Stelkens, NJW 2010, 1184, 1186.

41 BVerwG, Urt. v. 23. 09.2010, 3 C 37/09, NJW 2011, 246, 246.

42 BVerwG, Urt. v. 23.09.2010, 3 C 37/09, NJW 2011, 246, 247.

betroffen waren, aber in Zukunft betroffen sind. Damit haben solche Regelungen Gemeinsamkeiten mit Rechtsnormen beziehungsweise normkonkretisierenden Verwaltungsvorschriften. Nach Auffassung der Autoren scheidet jedoch eine Einordnung der Blacklist in diesem Sinne aus. Dass ein Außenrechtssatz sui generis[43] vorliegt, erscheint aufgrund des Ausnahmecharakters relativ unwahrscheinlich. Die Annahme, Blacklists könnten normkonkretisierende Verwaltungsvorschriften darstellen, geht fehl, weil es nicht um die einheitliche Auslegung unbestimmter Rechtsbegriffe geht, sondern um eine Wertentscheidung der Behörde.

IV. Rechtsschutz gegen die Blacklist

Wenn man, nach hier vertretener Ansicht, die „Blacklist" als Allgemeinverfügung ansieht, kann gegen sie im Wege der Anfechtungsklage gemäß § 42 Abs. 1 VwGO vorgegangen werden.[44] Ein stattgebendes Anfechtungsurteil hebt die Allgemeinverfügung gemäß § 113 Abs. 1 VwGO „soweit" auf, wie sie den Kläger in seinen Rechten verletzt. Wenn die Regelung also teilbar ist, kann damit auch nur eine Aufhebung erfolgen, soweit der Kläger betroffen ist.[45] Es wäre also denkbar, dass nur bestimmte Verarbeitungsarten aus der Liste „gestrichen" werden. Die Liste könnte aufgrund bestimmter Mängel aber auch als Ganzes aufgehoben werden. In beiden Fällen wären aufgrund des Adressatenkreises jedoch weitere betroffene Verantwortliche, die nicht gerichtlich gegen die Liste vorgegangen sind, Nutznießer des erstrittenen Urteils.[46]

Nichts anderes ergibt sich aus dem Umstand, dass die Aufsichtsbehörden eventuell selbst nicht erkannt haben, dass es sich bei den Blacklists um eine Allgemeinverfügung handelt und sie eine solche gar nicht erlassen wollten. Wenn sich im Wege der Auslegung (durch ein Gericht) herausstellt, dass eine Erklärung als VA zu werten ist, obwohl die Behörde tatsächlich eine andere Erklärung abgeben wollte, weil sie diese Maßnahme nicht als VA ansah, liegt dennoch ein materieller und mit Anfechtungsklage anfechtbarer VA vor.[47] Wie bereits oben dargestellt, dürfte für Verarbeitungen, die nach Veröffentlichung der Blacklist begonnen werden, die Jahresfrist nach § 58 Abs. 2 VwGO gelten.

Unklar ist, wie es sich auf etwaige Rechtsschutzverfahren auswirkt, dass momentan das nach Art. 35 Abs. 6 DS-GVO erforderliche Kohärenzverfahren für die gemeinsame Liste der Aufsichtsbehörden für nicht-öffentliche Stellen noch nicht abgeschlossen ist. Die Stellungnahme des EDSA nach Art. 64 Abs. 1 lit. a) DS-GVO erfolgte am 25.09.2018,[48] die Liste wurde daraufhin mit Fassung vom 17.10.2019 angepasst und ergänzt, jedoch wurde die Liste nicht vollumfänglich in dem Maß geändert, wie der EDSA angeregt hatte. Hierbei geht es konkret um Standortdaten. Der EDSA bat darum, die Liste dahingehend zu ändern, dass bei der Verarbeitung von Standortdaten hinzugefügt wird, dass eine DSFA nur erforderlich ist, wenn diese Verarbeitung in Verbindung mit mindestens einem weiteren auf der Liste aufgeführten Kriterium erfolgt. Dies wurde bis jetzt nicht angepasst (siehe Nr. 4 auf der Liste). Eigentlich müsste jetzt nach Art. 64 Abs. 8, Art. 65 DS-GVO das Streitbeilegungsverfahren eingeleitet werden. Es findet sich auch kein finaler Beschluss des EDSA über die deutsche DSFA-Liste auf der Homepage des EDSA.[49] Es ist daher zum Zeitpunkt der Erstellung dieses Beitrages davon auszugehen, dass noch keine final mit dem EDSA abgestimmte Blacklist der deutschen Behörden veröffentlicht wurde. Diese würde aber auch bedeuten, dass die Jahresfrist nach § 58 Abs. 2 DS-GVO erst zu laufen beginnt, wenn diese (vorerst) finale Blacklist online gestellt wird.

V. Fazit

Nach der hier vertretenen Ansicht stellen die Blacklists nach Art. 35 Abs. 4 DS-GVO, da sie die materiellen Voraussetzungen des § 35 S. 1, 2 VwVfG erfüllen, Allgemeinverfügungen dar, gegen die im Wege der Anfechtungsklage vorgegangen werden kann.

Im Detail stellt sich die verwaltungsrechtliche Einordnung der Blacklist aber sicher noch als schwierig dar. Dies dürfte unter anderem auch dem Umstand geschuldet sein, dass hier unmittelbar anwendbares europäisches Recht (DS-GVO) und nationales Verwaltungs(verfahrens)recht in praktisch handhabbaren Einklang gebracht werden müssen.

Dr. Carlo Piltz
Dr. Carlo Piltz, Rechtsanwalt, reuschlaw Legal Consultants, Berlin

Carolin Lühe
Carolin Lühe hat ihr Zweites Juristisches Staatsexamen im Februar 2020 in Berlin abgeschlossen. Sie war wissenschaftliche Mitarbeiterin im Deutschen Bundestag und bei reuschlaw Legal Consultants und hat sich im Rahmen dieser Tätigkeiten vorrangig mit Datenschutzthemen befasst.

43 Da (untergesetzliche) Rechtssetzungsformen nach h. M. wohl keinen Numerus clausus kennen, liegt ein solcher vor, wenn die Exekutive eine generell abstrakte Regelung entwirft, die wie ein Parlamentsgesetz sowohl den Bürger unmittelbar berechtigt und verpflichtet, als auch von den Gerichten und Behörden zu beachten ist, ihm also gesetzesgleiche Bindungswirkung zukommt (so BVerwG, Urt. v. 20.11.2003, 4 CN 6/03, NVwZ 2004, 614, 615.).

44 BVerwG, Urt. v. 25.10.2018, 7 C 22/16, NVwZ, 2019, 574, 575.

45 Stelkens, in: Stelkens/Bonk/Sachs, VwVfG, 9. Aufl. 2018, § 35, Rn. 274.

46 OVG Berlin, Beschl. v. 20.02.2002, 2 S 6/01, NVwZ-RR 2002, 720 (im durch das Gericht zu entscheidendem Fall ging es um die Verpflichtung, Einweg-Getränkeverpackungen für Bier und Mineralwasser zurückzunehmen, für sie Pfand erheben, zu erstatten und einer Verwertung zuzuführen).

47 BVerwG, Urt. v. 21.11.1980, 7 C 1879, BeckRS 1980 30424776 (für Ablehnung eines Antrags); BVerwG, Urt. v. 26.06.1987, 8 C 21/86, NVwZ 1988, 51, 51 (für Rechnung); VGH München, Beschl. v. 20.12.1986, 9 B 1851/79, BayVBl 1987, 693 (für von der Behörde gewollte innerdienstliche Erklärung).

48 Abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25 opinion_2018_art_64_de_sas_dpia_list_de_0.pdf

49 Abrufbar unter: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions_de

Prof. Dr. Rolf Schwartmann/RA Steffen Weiß, LL.M.

Ein Entwurf für einen Code of Conduct zum Einsatz DS-GVO-konformer Pseudonymisierung

Die Pseudonymisierung personenbezogener Daten ist mangels gesetzlicher Konkretisierungen von unterschiedlichen und voneinander unabhängigen Ansätzen seitens Verantwortlichen oder Auftragsverarbeitern geprägt. Der Beitrag widmet sich einer Initiative der Fokusgruppe Datenschutz des Digital-Gipfels der Bundesregierung, um mittels eines Codes of Conduct die Pseudonymisierung anhand transparenter und standardisierter Vorgaben durchzuführen.

I. Die Pseudonymisierung in der DS-GVO

Die Pseudonymisierung personenbezogener Daten hat einen hohen Wiedererkennungswert in der Datenschutz-Grundverordnung: Sie tritt beispielsweise im Rahmen der kompatiblen Weiterverarbeitung über Art. 6 Abs. 4 DS-GVO in Erscheinung. Gleichzeitig wird sie bei den technisch-organisatorischen Maßnahmen zur Wahrung von Privacy by Design/by Default gem. Art. 25 DS-GVO genannt. Aber auch im Zuge der Meldepflichten von Datenschutzverletzungen gem. Art. 33/34 DS-GVO sowie als eine Maßnahme zur Datensicherheit gem. Art. 32 DS-GVO erfährt sie eine gesetzliche Erwähnung ebenso, wie im Zuge der Öffnungsklausel des Art. 89 Abs. 1 DS-GVO. Die Definition der Pseudonymisierung über Art. 4 Nr. 5 DS-GVO als eine Verarbeitung personenbezogener Daten in der Weise, dass ohne die Hinzuziehung von zusätzlichen Informationen eine Zuordnung dieser Daten zu einem Betroffenen nicht möglich ist, soweit diese zusätzlichen Informationen getrennt verarbeitet werden und technisch-organisatorischen Maßnahmen zum Schutz vor einer Zuordnung zu einer identifizierten oder identifizierbaren Person implementiert sind, offenbart erste Anforderungen an diese Rechtsfigur. Fundamentale Änderungen zur Rechtslage im BDSG a.F. sind mit dieser Definition nicht einhergegangen. Immerhin gehen DS-GVO und BDSG a.F.[1] von einem Zustand der anonymen Datenverarbeitung aus, nachdem Klartextdaten einer Pseudonymisierung unterzogen wurden. Mit Blick auf die Grundverordnung dürften sich die Pseudonymisierung und die Anonymisierung im Wesentlich dadurch unterscheiden, dass bei der Pseudonymisierung die Möglichkeit der Re-Identifizierung besteht, während die Anonymisierung ein Verarbeitungsvorgang „ohne Wiederkehr" ist.[2]

Abseits der gesetzlichen Definition und der exemplarischen Erwähnung finden sich in der Grundverordnung keine konkretisierenden Hinweise zur Pseudonymisierung. Weder zu Fragen ihrer technischen Erstellung noch zu den notwendigen technisch-organisatorischen Maßnahmen zur Absicherung der „zusätzlichen Informationen".

II. Ein Code of Conduct für die Pseudonymisierung

Fehlen gesetzliche Konkretisierungen, müssen Rechtsanwender bzw. die operativ mit dem Datenschutz betrauten Stellen für Rechtssicherheit sorgen. Dies kann wesentlich durch das Erarbeiten gemeinsamer Standards erfolgen, die einzelne Ansätze harmonisieren und Vorgaben oder Richtlinien einer breiten Öffentlichkeit in transparenter Weise zugänglich machen. Hier können Codes of Conduct einen wichtigen Beitrag leisten, in dem sie eine Sammlung von Verhaltensweisen darstellen, die in unterschiedlichsten Umgebungen und Zusammenhängen abhängig von der jeweiligen Situation angewandt werden können bzw. sollen.[3] Dabei sollen – ausweislich der Grundverordnung – die „Besonderheiten" einer Verarbeitung berücksichtigt werden.[4] Oder anders gesagt: Die in der DS-GVO nur unpräzise geregelten Rechtsfragen sollen für den konkreten Fall einer Institution oder einer Kategorie von Datenverarbeitern präzisiert worden.[5]

Um dem Wunsch eines standardisierten Vorgehens bei der Pseudonymisierung personenbezogener Daten nachzugehen, wurde im Zuge des Digital-Gipfels der Bundesregierung seitens der Fokusgruppe Datenschutz der Plattform 9 „Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft" die Entscheidung getroffen, einen Entwurf für einen Code of Conduct (CoC) zum Einsatz DS-GVO konformer Pseudonymisierung zu veröffentlichen.[6] Der Code basiert auf den Vorarbeiten der Gruppe in Gestalt eines Whitepapers[7] sowie darauf basierender Anforderungen an den Einsatz von Pseudonymisierungslösungen.[8] Der CoC wird im Folgenden einer Betrachtung unterzogen werden

1 Vgl. § 3 Abs. 6a BDSG a.F.

2 Zur Abgrenzung vgl. Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017 – Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung, Ziff. 3.2.

3 Vgl. https://de.wikipedia.org/wiki/Verhaltenskodex. Eine gesetzliche Definition existiert insofern nicht.

4 Vgl. Art. 40 Abs. 1.

5 Vgl. Reifert, ZD 2019, 305 (306).

6 Schwartmann/Weiß (Hrsg.), Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung – ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2019.

7 Schwartmann/Weiß (Hrsg.), Whitepaper zur Pseudonymisierung a.a.O.

8 Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen – ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2018.

1. Anwendungsbereich

Der CoC soll für Verantwortliche und Auftragsverarbeiter unabhängig ihres Sektors gelten. D.h. er beinhaltet universale, nicht sektorspezifische Anforderungen an datenverarbeitende Stellen, die eine Pseudonymisierung durchführen wollen, eine solche verantworten oder Produkte einsetzen, die die Anforderungen des Codes einhalten.[9]

Sollten Verantwortliche in ihren Diensten oder Produkten pseudonymisierte Daten einsetzen, können sie dem CoC dergestalt beitreten, als dass damit der Nachweis erbracht wird, dass die verwendeten Pseudonyme nach den dort definierten Regeln erstellt wurden. Der Code verpflichtet dabei nicht den Verantwortlichen oder Auftragsverarbeiter, jede Verarbeitung von pseudonymisierten Daten seinem Anwendungsbereich zu unterwerfen. Dem Betroffenen ist jedoch die jeweilige Einbeziehung des Codes kenntlich zu machen.[10]

2. Der Fachverantwortliche für Pseudonymisierung

Pseudonymisierungsprozesse innerhalb einer Stelle bedürfen einer Aufsichts- und Beratungsinstanz, die sich für die ordnungsgemäße Durchführung erforderlicher Maßnahmen verantwortlich zeigt. Hierzu führt der Code die Figur des Fachverantwortlichen für Pseudonymisierung (FvfP) ein. Der FvfP koordiniert lediglich die organisatorischen Verantwortlichkeiten im Zuge einer Pseudonymisierung. Eine Verantwortlichkeit für die datenschutzrechtliche Zulässigkeit einer Datenverarbeitung geht damit nicht einher. Diese organisatorische lediglich „interne Verantwortlichkeit" muss dabei nicht zwingend einer einzelnen Person zugeordnet werden. Auch Abteilungen können diese Rolle einnehmen, wobei die konkrete Ausgestaltung von Zuständigkeiten zwingend zu dokumentieren ist.[11] Der CoC versucht damit dem Umstand Rechnung zu tragen, dass Zuständigkeiten innerhalb einer datenverarbeitenden Stelle oftmals unterschiedlich verteilt sind. Gleichzeitig soll eine Verantwortlichkeit explizit auf die Pseudonymisierung bezogen werden, was in der Vergangenheit regelmäßig nicht ausdrücklich erfolgte, sondern in anderen Funktionen aufging. Zu begründen ist dies beispielsweise mit der Komplexität der Pseudonymisierung. Der Datenschutzbeauftragte kann dabei nicht die Rolle des FvfP einnehmen, da dies zu einem Interessenskonflikt mit seinen gesetzlich zugewiesenen Aufgaben führen würde, denn mit der Funktion des FvfP ist eine organisatorische Verantwortlichkeit verbunden, die nicht mit den Aufgaben des Datenschutzbeauftragen in Einklang zu bringen wäre (vgl. Art. 38 Abs. 6 S. 2 DS-GVO).

3. Die Festlegung der geeigneten Pseudonymisierung

Ein wesentliches Anliegen des CoC besteht darin, die Entscheidungsfindung eines Verantwortlichen oder Auftragsverarbeiters zu einer gewählten Pseudonymsierungsmethode transparent zu machen und hierbei entsprechende Kriterien vorzugeben. Als universaler Code of Conduct für die Pseudonymisierung können die konkreten Umstände einer Pseudonymsierung und Gründe für ihren Einsatz nicht vorausgesehen werden. Folglich kann eine Pseudonymisierungsmethode auch nicht abschließend durch einen CoC vorgegeben, sondern allenfalls empfohlen werden (vgl. II. 9.).

Zu den für die Ermittlung einer geeigneten Pseudonymisierungsmethode relevanten Kriterien gehören u.a. die Art und Risikoklasse der verarbeiteten personenbezogenen Daten, der Zweck der Verarbeitung sowie der Kontext der Pseudonymisierung, wobei dieser in rechtlicher Hinsicht gemeint ist. Die Durchführung einer Pseudonymisierung im Zuge einer Zweckänderung der Datenverarbeitung (vgl. Art. 6 Abs. 4 DS-GVO) kann eine andere Methode notwendig machen, als beispielsweise die Pseudonymisierung als rein technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO. An dieser Stelle wird deutlich, dass die Pseudonymisierung nur Teil einer Zulässigkeitsprüfung ist und eine Datenverarbeitung nur durch das Vorhandensein einer Pseudonymisierung nicht legitimiert werden kann.[12]

Ebenfalls müssen Verantwortliche oder Auftragsverarbeiter die erwartete Anzahl der verarbeiteten Datensätze berücksichtigen, bevor eine konkrete Pseudonyisierungmethode festgelegt wird. Dies sollte auch eine etwaige Dynamik beim Datenumfang berücksichtigen. Klassische Listenverfahren zur Erstellung von Pseudonymen eignen sich beispielsweise nicht für eine große Anzahl von Daten.

4. Geeignete Pseudonymisierugnsmethoden

Wie bereits erwähnt, vermeidet der CoC die Vorgabe einer bestimmten einzusetzenden Pseudonymisierungsmethode. Im Kontext der Auswahl einer Methode auf Basis der zu prüfenden Kriterien[13] erfolgt hingegen eine allgemeine Beschreibung verschiedener Arten von Pseudonymen, um den Anwender bei der Auswahl einer Methode zu unterstützen. Hierzu zählen:

- Personen-Pseudonyme, die an Stelle von Identitätsdaten wie z.B. Name, Ausweisnummer oder Mobiltelefonnummer stehen
- Rollen-Pseudonyme, bei denen eine oder ggf. mehrere Personen einem Pseudonym zugeordnet sind (z.B. IP-Nummer)
- Beziehungs-Pseudonyme, bei denen eine Person für jede (Kommunikations-) Beziehung ein anderes Pseudonym verwendet, z.B. unterschiedliche Spitznamen
- Rollen-Beziehungs-Pseudonyme, die eine Kombination der beiden Pseudonym-Arten sind
- Wechselnde Pseudonyme, bei denen z.B. für jede Transaktion oder jeden Eintrag ein neues Pseudonym genutzt wird, was z.B. beim Online-Banking zum Einsatz kommt

9 Vgl. CoC, Ziff. 1.1.
10 Vgl. CoC, Ziff. 1.1.
11 Vgl. CoC, Ziff. 2.1.1.
12 Vgl. Hansen/Walczak, RDV 2019,
13 CoC, Ziff. 2.1.2.1.-2.1.2.4.

Um dem Prinzip der Datenminimierung ausreichend Rechnung zu tragen, ist bei der Auswahl einer geeigneten Pseudonymisierungsart ein Verfahren vorzuziehen, das für den vorgesehenen Einsatzzweck geeignet ist, Betroffene aber gleichzeitig in größtmöglichem Umfang vor einer ungewollten Identifizierung schützt.[14]

Bei der konkreten Festlegung einer Methode stehen Anwendern grundsätzlich zwei Verfahren zur Verfügung: Pseudonymisierungslisten und Pseudonyme durch Berechnungsverfahren.[15] Pseudonymisierungslisten ordnen Identitätsdaten anhand einer Tabelle Pseudonymen zu. Im Rahmen von Berechnungsverfahren werden Pseudonyme aus Identitätsdaten algorithmisch berechnet. Die Stärke einer gewählten Methode muss ausweislich des Codes of Conduct unter Berücksichtigung aller objektiven Faktoren, Risiken für die Rechte und Freiheiten Betroffener sowie auch den Kosten einer Identifizierung bzw. der hierfür erforderliche Zeitaufwand unter Berücksichtigung der verfügbaren Technologien geprüft, festgelegt und dokumentiert werden.[16] Hier bietet es sich an, auf weitere technische Beschreibungen zu rekurrieren, die insbesondere Risiken bei der Erstellung von Pseudonymen adressieren und den Abwägungsprozess unterstützen.[17]

Grundsätzlich müssen Berechnungsverfahren einem State-of-the-Art-Transformationsverfahren zugrunde liegen. Aus Gründen des praktischen Einsatzes sollte ebenfalls eine effiziente Selektion und Löschung der Daten möglich sein. Unabhängig von der gewählten Methode hat eine Pseudonymisierung so früh wie möglich zu erfolgen[18] (vgl. auch Art. 5 Abs. 1 lit. c DS-GVO). Darüber hinaus spielt die Häufigkeit einer Re-Identifizierung eine Rolle bei der Auswahl einer geeigneten Pseudonymisierungsmethode.[19] Mit Blick auf die Aufsichts- und Beratungsfunktion des FvfP spielen Erkenntnisse über die Anzahl durchgeführter Re-Identifizierungen und die dabei eingehaltene Verzögerungstoleranzen eine Rolle bei der Evaluierung gewählter Methoden und Verfahren.

Abseits der Prüfkriterien zur Ermittlung einer geeigneten Pseudonymisierungsmethode enthält der CoC ferner allgemeine „Checkpoints“, die bei der Pseudonymisierung zu berücksichtigen sind. Hintergrund hierfür ist zum einen der Umstand, dass es sich bei pseudonymisierten Daten weiterhin um personenbezogene Daten handelt[20], so dass der Umstand einer Übermittlung personenbezogener Daten an Dritte[21] ebenso eine datenschutzrechtliche Implikation hat, wie die Übermittlung solcher Daten an Dritte in ein Drittland[22], eine Pflicht zur regelmäßigen Überprüfung der Erforderlichkeit der Verarbeitung[23], bestehende Informationspflichten gegenüber Betroffenen[24] oder etwaige Mitteilungspflichten gegenüber Aufsichtsbehörden in besonderen Fällen.[25]

5. Risikoadäquates Rechte- und Rollenkonzept

Ein Rechte- und Rollenkonzept ist Teil der gesetzlich vorgesehenen technisch-organisatorischen Maßnahmen zum Schutz der „zusätzlichen Informationen“, aber auch beachtenswert im Zuge des Schutzes von Pseudonymen. Durch ein Rechte- und Rollenkonzept wird fundamental die Zugriffsmöglichkeit auf Schlüssel oder Geheimnisse zur Re-Identifizierung Betroffener ebenso geregelt, wie der Zugriff auf erzeugte Pseudonyme bzw. der vorgelagerte Vorgang ihrer Erzeugung.

Die DS-GVO zeigt sich flexibel, was eine Rollenverteilung bei der Pseudonymisierung anbelangt. Insofern sieht sie ausdrücklich eine Pseudonymisierungsmöglichkeit bei demselben Verantwortlichen vor.[26] Besagte Rollenverteilung ist in der Praxis jedoch wesentlich komplexer ausgestaltet, weshalb der CoC die unterschiedlichen Beteiligten einer Pseudonymisierung über ein eigenes Kapitel adressiert. Hierbei hat die Rollenverteilung und die Berechtigungsvergabe das Risiko für Rechte und Freiheiten Betroffener zu berücksichtigen.[27] D.h. nach den Vorgaben des CoC ist das gesetzlich vorhandene Wahlrecht des Datenverarbeiters an dieser Vorgabe auszurichten. Der Code unterscheidet im Wesentlichen zwischen drei Modellen:

- „Alles-in-einer-Hand-Modell“: Der Verantwortliche oder Auftragsverarbeiter verfügt sowohl über die pseudonymisierten Daten als auch über die jederzeitige Möglichkeit der Re-Identifizierung. Hier müssen zumindest interne Vorgaben bestehen, aus denen sich eine Unterscheidung zwischen unzulässigen von zulässigen Re-Identifizierungen für Anwender ergeben kann. Ferner ergeben sich – je nach Risiko für Betroffene – Anforderungen an ein internes Rechte- und Rollenkonzept.
- Treuhändermodell: Beim klassischen Treuhändermodell besteht eine Vertrauensstelle, die räumlich und organisatorisch unabhängig vom Verantwortlichen oder Auftragsverarbeiter ist. Ob besagter Treuhänder bspw. mit der Schlüsselverwaltung als Ausprägung einer „zusätzlichen Information“ oder der Verarbeitung pseudonymisierten Daten betraut ist, unterliegt den Erwägungen des Verantwortlichen bzw. Auftragsverarbeiters. Beim Modell des Treuhänders können unterschiedliche Anforderungen an eine Re-Identifizierung von Betroffenen bestehen. Z.B. kann ein Treuhänder vorab der Verarbeitung in definierten Fällen mit der Re-Identifizierung beauftragt werden (ex ante). Ebenso kann eine Re-Identifizierung auf Basis einer Abwägung des Treuhän-

14 CoC, Ziff. 2.1.2.5.

15 Vgl. Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen a.a.O., D.2.2.

16 CoC, Ziff. 2.1.2.6.

17 Vgl. bspw. European Union Agency for Cybersecurity, Pseudonymisation techniques and best practices – Recommendations on shaping technology according to data protection and privacy provisions (November 2019); Schwartmann/Weiß (Hrsg.), Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen a.a.O., D.2.2. ff.

18 CoC, Ziff. 2.1.2.5.

19 CoC, Ziff. 2.1.2.9.

20 Vgl. ErwG 26 S. 2.

21 CoC, Ziff. 2.1.2.7. sowie II. 7.

22 CoC, Ziff. 2.1.2.8.

23 CoC, Ziff. 2.1.7.

24 CoC, Ziff. 2.1.5.

25 CoC, Ziff. 2.1.8.

26 ErwG 29 S. 1.

27 CoC, Ziff. 2.1.3.

ders selbst erfolgen, die nicht durch zuvor definierte Zwecke beschränkt ist, jedoch einer vorherigen Festlegung diesbezüglich geltender Kriterien bedarf (ad hoc). Letztlich ist auch eine Re-Identifizierung ex post denkbar, in der ein Treuhänder über Aufdeckungen im Nachgang informiert wird und er darauf basierend ggf. zusätzlich Schutzmaßnahmen ergreift.

- Mischmodelle adressieren die Trennung von pseudonymisierten Daten beim Verantwortlichen selbst, allerdings werden Informationen hinsichtlich der pseudonymisierten Daten über mehrere Hierarchieebenen oder unabhängige Abteilungen verteilt. Hierbei ist in größeren Organisationen der Aufbau einer eigenen vertrauenswürdigen „dritten Partei" denkbar, welche die getrennte Verwaltung der Daten und/oder Geheimnisse bzw. Schlüssel intern anbietet.

6. Vorgaben an die Re-Identifizierung

Der Pseudonymisierung personenbezogener Daten ist die Re-Identifizierung von Betroffenen immanent. Der CoC fordert insofern die Erarbeitung diesbezüglicher Vorgaben, sollte eine solche seitens eines Verantwortlichen oder Auftragsverarbeiters bezweckt sein. Die Zulässigkeit der Aufdeckung eines Pseudonyms ist hierbei abhängig vom rechtlichen Kontext der Verarbeitung. Mit Ausnahme der Pseudonymisierung als reine Schutzmaßnahme gem. Art. 32 DS-GVO hat sich der Verantwortliche die Frage zu stellen, ob die Rückführung in seinem Interesse oder in dem des Betroffenen erfolgen soll. Hiernach beurteilt sich die einschlägige Rechtsgrundlage.[28] Bei dynamischen Datensätzen ist im Übrigen regelmäßig zu prüfen, ob durch die Dynamik eine Re-Identifizierung von Betroffenen möglich ist.[29]

7. Geplante Weitergaben an Dritte

Die Zulässigkeit einer Weitergabe personenbezogener Daten an Dritte stellt eine allgemeine Prüfpflicht aus datenschutzrechtlicher Sicht dar. Der CoC konkretisiert diese Prüfpflicht im Zuge einer Übermittlung pseudonymisierter Daten. Hierbei fordert er angemessene Maßnahmen, so dass eine unzulässige Re-Identifizierung von Betroffenen im Zuge der Weitergabe möglichst ausgeschlossen ist. Zu eine dieser Maßnahmen aus organisatorischer Sicht können Bestätigungen in Schrift- oder Textform seitens des Datenempfängers gezählt werden, dass eine Re-Identifizierung nicht erfolgt. Fraglich ist, ob einer datenübermittelnden Stelle weitergehende Pflichten auferlegt werden sollen, immerhin entsteht im Zuge der Übermittlung regelmäßig eine neue Verantwortlichkeit für die Daten. Die datenübermittelnde Stelle hat grundsätzlich wenig Einsicht in eine Datenverarbeitung auf Seiten des Empfängers. Die bei einer Auftragsverarbeitung bestehenden Prüfpflichten beziehen sich auf technisch-organisatorische Maßnahmen, wobei die weisungsgebundene Datenverarbeitung eine der Kernpflichten des Auftragsverarbeiters ist. Besagte Pflichten beziehen damit regelmäßig nicht auf ein „Zusatzwissen" beim Datenempfänger. Der CoC entscheidet sich für die Vorgabe, dass die Datenweitergabe von einer Rechtsgrundlage abgedeckt sein muss. Zum anderen sind angemessene Maßnahmen zu treffen, um eine unzulässige Re-Identifizierung von Betroffenen durch den Empfänger möglichst auszuschließen. Dies beinhaltet ausweislich der Erläuterungen eine Prüfpflicht zumindest bezogen auf offensichtliche Identifizierungsmöglichkeiten auf Seiten des Empfängers, die bei deren Vorliegen durch ergänzende Maßnahmen begleitet werden müssen.[30]

8. Dokumentation und regelmäßige Evaluation der Prozesse, Abwägungen und tatsächlichen Maßnahmen

Ein wesentliches Anliegen des CoC stellt die besagte Transparenz in der Entscheidungsfindung als Bestandteil gesetzlich bestehender Rechenschaftspflichten dar. Der CoC bündelt die Kontrolle bzw. Überprüfung der Entscheidungsfindung sowie hiervon abgeleitete Maßnahmen beim FvfP. Hierdurch soll der FvfP einerseits in der Lage sein

- den Prozess oder die Maßnahme hinsichtlich der Wirksamkeit zu bewerten;
- die Implementierung der Prozesse oder der getroffenen Maßnahmen zu verifizieren;
- die Einhaltung der Prozesse oder der getroffenen Maßnahmen zu evaluieren.

Andererseits sollen der FvfP und alle mit der Umsetzung betrauten Personen in der Lage sein, den Prozess oder die Maßnahme zu verstehen und entsprechend der definierten Vorgaben umzusetzen.

Im Zuge der Entscheidungsfindung für eine geeignete Pseudonymisierungsmethode sind getroffene Abwägungen ebenfalls zu dokumentieren, wobei diese unter den Aspekten Stand der Technik sowie Zweckkonformität regelmäßig zu überprüfen sind. Freilich sind hierbei wesentlich die Vorgaben des CoC in die Abwägung einzubeziehen. Durch den Dokumentationsprozess werden Verantwortliche oder Auftragsverarbeiter gezwungen sein, sämtliche Anforderungen des CoC systematisch abzuarbeiten. Ferner wird es anderem Kontrollinstanzen in Organisationen dadurch ermöglicht, Kontrollhandlungen zur Pseudonymisierung vorzunehmen.[31]

9. Technische Fragen

Da einer Pseudonymisierung in vielen Fällen ein technischer Vorgang innewohnt, befasst sich der CoC dementsprechend mit den technischen Anforderungen an die Pseudonymisierung. Den Einstieg bilden allgemeine Anforderungen, die eine Rückkopplung mit dem FvfP auch hinsichtlich technischer Belange erfordern. Wichtig ist hierbei wiederum, dass es auch aus technischer Sicht nicht nur eine Pseudonymisierungsmethode zur Erreichung der Ziele einer Organisation gibt. Die gemeinsame Schnittmenge von Berechnungsverfahren zur Erstellung von Pseudonymen sowie den klassischen Listenverfahren bildet jedoch eine erzeugte ID: Daher

28 Vgl. CoC, Ziff. 2.1.4.

29 CoC, Ziff. 2.1.4.

30 CoC, Ziff. 2.1.7.

31 Vgl. CoC Ziff. 2.1.92.

beinhaltet der CoC allgemeine Anforderungen an solche IDs.[32] Diese Anforderungen werden durch spezifische Hinweise im Rahmen des Einsatzes von Berechnungsverfahren ergänzt.[33] Die ausgesprochene Empfehlung der Verwendung von kryptographischen Hash-Funktionen oder eines symmetrischen Blockchiffreverfahrens ist ein spezifischer Verweis auf eine bestimmte Technik der Erstellung eines Pseudonyms, vermeidet jedoch die Formulierung eine entsprechende Vorgabe. Bei der Verwendung von Hash-Funktionen bestehen im Übrigen verschiedene Empfehlungen, die an dieser Stelle nur exemplarisch genannt werden sollen.[34]

III. Fazit

Lässt man die Bemühungen der Fokusgruppe Datenschutz zur Erarbeitung eines CoC für die Pseudonymisierung Revue passieren, ist auffällig, dass sich der CoC als Querschnittsdokument wie ein roter Faden durch alle Aspekte einer Pseudonymisierung zieht. Er leistet seinen Beitrag als ein Leitfaden für Anwender der Pseudonymisierung unabhängig von ihrer Branche. Möchten Anwender wissen, ob das eingesetzte Pseudonymisierungsverfahren datenschutzkonform ist, werden sie im CoC keine Antwort hierzu finden. Denn die jeweiligen Umstände einer Datenverarbeitung sind zu spezifisch, als dass sie in einem CoC abschließend beurteilt werden könnten. Daher ist es für die Rechtsfortbildung umso wichtiger, dass „Insellösungen" für eine Pseudonymisierung personenbezogener Daten weiterentwickelt werden und sich an sektorspezifischen Anforderungen ausrichten. Daher ist für die Finalisierung dieses CoC zur Pseudonymisierung geplant, sog. „Good Practices" aufzunehmen, die bezogen auf spezifische Verarbeitungszwecke und -kontexte den Prozess der Pseudonymisierung anhand der Vorgaben des CoC beschreiben. Sollten diese Good Practices sodann um Governance- und Monitoring-Prozesse erweitert werden, steht eine Vorlage bei einer zuständigen Aufsichtsbehörde nichts mehr im Wege. Auch dies ist durch die Verfasser des CoC vorgesehen.

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

RA Steffen Weiß, LL. M.
Mitglied der Geschäftsführung für Internationales bei der Gesellschaft für Datenschutz und Datensicherheit e.V. und Sherpa der Fokusgruppe Datenschutz im Rahmen des Digital-Gipfels der Bundesregierung.

32 Vgl. Ziff. 2.2.2.

33 Vgl. CoC Ziff. 2.2.3.

34 Agencia Española de Protección de Datos/European Data Protection Supervisor, Introduction to the hash function as a personal data pseudonymisation technique (Oktober 2019).

Prof. Dr. Rolf Schwartmann/Prof. Dr. Bernd Grzeszick, LL.M.

Die datenschutzrechtliche Stellung von Abgeordneten und Fraktionen

Die DS-GVO enthält eine Vielzahl ungelöster Rechtsfragen. Kaum betrachtet wird dabei die Frage, ob und inwieweit Abgeordnete und Fraktionen unter die Datenschutz-Grundverordnung[1] (DS-GVO) sowie unter das Bundesdatenschutzgesetz[2] (BDSG) fallen. Bei Licht betrachtet, muss für sie ein differenziertes Sonderregime gelten.

A. Unmittelbare Anwendbarkeit der DS-GVO auf Abgeordnete und Fraktionen?

In diesem Zusammenhang stellt sich zunächst die Frage, ob die DS-GVO überhaupt auf Abgeordnete und Fraktionen Anwendung finden kann. Der sachliche Anwendungsbereich der DS-GVO wird in Art. 2 DS-GVO bestimmt.

I. Art. 2 Abs. 2 lit. a DS-GVO und Art. 16 AEUV

Nach Art. 2 Abs. 2 lit. a DS-GVO findet die DS-GVO aber keine Anwendung auf die Verarbeitung personenbezogener

1 ABl. 2016 L 119 vom 04.05.2016, S. 1 ff. sowie Corrigendum zu 2012/0011 (COD), Nr. 12399/16 vom 27.10.2016.

2 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch das zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU – vom 20.11.2019 (BGBl. I S. 1626).

Daten im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt. Der Begriff des „Anwendungsbereichs des Unionsrechts" im Sinne von Art. 2 Abs. 2 lit. a DS-GVO ist dabei unionsrechtlich determiniert und zu bestimmen. Die Begrenzung der Reichweite der DS-GVO in Art. 2 Abs. 2 lit. a DS-GVO beruht darauf, dass die Kompetenzen der EU i.S.d Grundsatzes der begrenzten Einzelermächtigung[3] begrenzt sind, weshalb bei einer zu weiten Auslegung des Anwendungsbereichs der DS-GVO diese den Rahmen der Unionskompetenzen überschreiten und rechtswidrig sein könnte. Die Begrenzung des Art. 2 Abs. 2 lit. a DS-GVO ist daher mit Blick auf die Regelung des Art. 16 Abs. 2 UAbs. 1 Satz 1 AEUV, der Kompetenzgrundlage für den Erlass der DS-GVO ist, zu verstehen. Art. 2 Abs. 2 lit. a DS-GVO hat insoweit lediglich deklaratorischen Charakter.[4] Ganz überwiegend wird zu Art. 16 Abs. 2 UAbs. 1 Satz 1 AEUV[5] darauf verwiesen, dass der Umfang der Gesetzgebungskompetenz weiter sein kann als der Umfang der Grundrechtsgewährung[6]. Art. 16 Abs. 2 AEUV – und daher auch Art. 2 Abs. 2 lit. a DS-GVO – können daher auch anwendbar sein auf nationale Datenverarbeitungen, die weder ein grenzüberschreitendes Element aufweisen noch mit der Ausübung einer der Grundfreiheiten der Verträge verbunden sind.[7]

1. Verständnis des „Anwendungsbereichs des Unionsrechts"

Mit Blick darauf ist der „Anwendungsbereich des Unionsrechts" weit zu verstehen. Im Grundsatz wird daher davon ausgegangen, dass die DS-GVO insofern zugunsten einer Kompetenz der EU weit auszulegen ist und nur wenige Bereiche nicht erfasst.[8] Der „Anwendungsbereich des Unionsrechts" umfasst somit alle unionsrechtlich geregelten Sachverhalte und damit auch Sachbereiche außerhalb der Legislativkompetenz der Union, sofern die Mitgliedstaaten bei der Ausübung ihrer Kompetenzen in diesem Bereich unionsrechtliche Vorgaben zu beachten haben.

2. Art. 18 Satz 1 AEUV und der „Anwendungsbereich der Verträge"

Als Orientierung kann ferner die Regelung des Art. 18 Satz 1 AEUV dienen, zu der – bzw. zu deren Vorläuferregelung im EGV – auch bereits einige Entscheidungen des EuGH vorliegen. Im Rahmen des Art. 18 AEUV bestimmt der EuGH in seinen Entscheidungen den „Anwendungsbereich" ebenfalls weit.[9] Danach ist maßgeblich, ob jeweils die Verwirklichung eines unionsrechtlich gewährten Rechts oder Grundsatzes betroffen ist. Dies ist regelmäßig der Fall bei Vollzug oder Durchführung des Unionsrechts sowie bei einem – auch mittelbaren – Zusammenhang mit der Ausübung der Grundfreiheiten.

II. Grundsätze zur Zuordnung von Tätigkeiten der Abgeordneten und Fraktionen

Dies ist bei Tätigkeiten der Abgeordneten und Fraktionen aber nicht der Fall. Zwar mag vor allem das Ergebnis der Legislativtätigkeit des Bundes- bzw. Landtags teilweise in den Anwendungsbereich des Unionsrechts fallen, soweit Gesetze Richtlinien umsetzen etc. Für das Verfahren der parlamentarischen Rechtsetzung und die – darauf bezogene – parlamentarisch-politische Tätigkeit der Abgeordneten und Fraktionen trifft dies allerdings nicht zu. Denn es sind keine unionsrechtlichen Vorgaben ersichtlich, die das parlamentarische Gesetzgebungsverfahren in den Mitgliedstaaten und die darauf bezogenen Tätigkeiten der Abgeordneten und Fraktionen regelten. Die Organisation der nationalen Parlamente sowie auch die Ausgestaltung des Abgeordnetenmandats fallen danach grundsätzlich nicht in den Anwendungsbereich des Unionsrechts; die Grundlagen der parlamentarischen Arbeit ergeben sich allein aus den jeweiligen nationalen Regelungen. Dies wird auch vom Unionsrecht respektiert, da nach Art. 4 Abs. 2 Satz 1 EUV die Union die nationale Identität achtet, die in ihren grundlegenden politischen und verfassungsgemäßen Strukturen zum Ausdruck kommt.

III. Zwischenergebnis zur DS-GVO und Tätigkeiten der Abgeordneten und Fraktionen

1. Parlamentarisch-politische Willensbildung nicht erfasst

Nach den vorstehenden Grundsätzen unterfallen Tätigkeiten der Abgeordneten und der Fraktionen, die Teil des parlamentarisch-politischen Willensbildungsprozesses sind, nach Art. 2 Abs. 2 lit. a DS-GVO grundsätzlich nicht der DS-GVO.[10] Dazu gehört neben der unmittelbaren Beteiligung an Verfahren der Gesetzgebung und Beschlussfassung u.a. auch die Entwicklung und Umsetzung eigener Standpunkte, Initiativen und Konzepte, die Zusammenarbeit mit anderen Abgeordneten und Fraktionen etc. sowie letztlich auch der Kontakt zum Bürger, da dies zentraler Teil der politischen Kommunikation und damit Teil der Willensbildung vom Bürger zum Staat hin ist.

2. Teilnahme am allgemeinen wirtschaftlichen Rechtsverkehr erfasst

Dagegen können Tätigkeiten der Abgeordneten und der Fraktionen in den Anwendungsbereich des Unionsrechts fallen, falls diese eine Teilnahme am allgemeinen wirtschaftli-

3 So von Lewinski, in: Auernhammer, BDSG DS-GVO, 6. Aufl., 2018, DS-GVO Art. 2 Rn. 3.

4 Albrecht, CR 2016, 88, 90; Kühling/Raab, in: Kühling/Buchner, DS-GVO, 2. Aufl., 2018, Art. 2 Rn. 21.

5 Wolff, in: Frankfurter Kommentar zu EUV, GRC und AEUV, Band II, 2017, Art. 16 AEUV Rn. 19.

6 Brühann, in: von der Groeben/Schwarze/Hatje, 7. Aufl., 2015, Art. 16 AEUV Rn. 65.

7 Brühann, in: von der Groeben/Schwarze/Hatje, 7. Aufl., 2015, Art. 16 AEUV Rn. 67 mit Verweis auf Rspr. des EuGH zur entsprechenden Regelung in Art. 3 Abs. 2 der RL 95/46/EG: EuGH, C-465/00 – Österreichischer Rundfunk –, Rn. 40 ff.; EuGH, Rs. C-101/01 – Lindqvist –, Rn. 37 ff.; EuGH, C-524/06, Huber –, Rn. 44 f.

8 So von Lewinski, in: Auernhammer, BDSG DS-GVO, 6. Aufl., 2018, DS-GVO Art. 2, Rn. 16 f.

9 Dazu sowie zum Folgenden Streinz, in: ders., EUV/AEUV, 3. Aufl., 2018, Art. 18 AEUV, Rn. 19 ff. m.N.

10 So auch Schröder, ZRP 2018, 129, 130; Grzeszick, NVwZ 2018, 1505 ff.

chen Rechtsverkehr darstellen. Wenn die Abgeordneten und die Fraktionen für ihre Tätigkeiten z.B. für die Erledigung der Büroarbeit nötige Gegenstände kaufen, Werke in Auftrag geben ober Mitarbeiter zur Erledigung allgemeiner Organisations- und Sekretariatsarbeit einstellen, nehmen sie am allgemeinen wirtschaftlichen Rechtsverkehr teil. Das entsprechende rechtsgeschäftliche Handeln kann insofern in den Anwendungsbereich des Unionsrechts fallen. Die Abgeordneten und Fraktionen sind dann an die Regelungen der DS-GVO gebunden. Denn diese Tätigkeiten sind nicht hinreichend auf die politische Willensbildung bezogen, sondern insoweit inhaltlich neutrale Hilfs- und Unterstützungstätigkeiten.

3. Keine Derogation der DS-GVO durch Art. 38 GG

Die Regelung des Art. 38 GG rechtfertigt dabei keine grundsätzliche Derogation der DS-GVO. Zwar könnte insbesondere mit Blick auf die Bedeutung des Art. 38 Abs. 1 S. 2 GG über eine Begrenzung der DS-GVO reflektiert werden, falls Art. 38 GG als integrationsfester Bestandteil der nationalen Verfassungsidentität verstanden wird. Die mit Blick auf Art. 38 Abs. 1 S. 2 GG spezifisch relevanten Tätigkeiten von Abgeordneten und Fraktionen werden aber von der DS-GVO ohnehin nicht erfasst, weshalb auch kein Bedürfnis nach einer verfassungsrechtlichen Reduktion bzw. Begrenzung des Anwendungsbereichs der DS-GVO besteht.

B. Verfassungsrechtliche Garantien für Abgeordnete und Fraktionen

Für den nicht unionsrechtlich determinierten Bereich sind die Tätigkeiten der Abgeordneten und Fraktionen verfassungsrechtlich besonders geschützt.

I. Abgeordnete

Verfassungsrechtliche Grundlage der Rechtsstellung der Abgeordneten sind vor allem die Art. 38, 46-48 GG. Die sich aus Art. 38, 46-48 GG ergebende Rechtsstellung des Abgeordneten als Mitglied des Bundestages wird vom BVerfG als „verfassungsrechtlicher Status“ bezeichnet.[11] Rechte und Pflichten des Abgeordneten fallen darin zusammen, dass er berufen ist, an der Arbeit des Bundestages, seinen Verhandlungen und Entscheidungen teilzunehmen.[12] Art. 38 Abs. 1 S. 2 GG umschreibt nach Ansicht des BVerfG die „organschaftliche Stellung der Abgeordneten“ und legt „ihnen Pflichten als Mitgliedern des Bundestages“ auf.[13] Was dem Abgeordneten sonst an Befugnissen zukommt oder an Verpflichtungen obliegt, ist funktional auf diese organschaftliche Stellung bezogen und dazu bestimmt, sie zu stützen und zu sichern.[14]

II. Fraktionen

Grundsätzlich ist anerkannt, dass in der Konsequenz auch den Fraktionen ein verfassungsrechtlicher Status zukommt.[15] In der Rspr. des BVerfG erfolgte eine ausdrückliche verfassungsrechtliche Verortung der Fraktionen zunächst zunächst in Art. 21 GG.[16] Fraktionen wurden dabei als notwendige Einrichtungen des Verfassungslebens bezeichnet, und mit der Anerkennung der Parteien in Art. 21 GG erkenne das Grundgesetz auch die Fraktionen an. Eine deutliche Hinwendung zu Art. 38 Abs. 1 GG erfolgte vor allem[17] in späteren Entscheidungen des BVerfG.[18] Darin wurde ausgeführt, dass für die Rechtsstellung der Fraktionen nicht Art. 3 i.V.m. Art. 21 GG maßgebend sei, sondern vielmehr die Rechtsstellung der Fraktionen wie der Status der Abgeordneten aus Art. 38 Abs. 1 GG abzuleiten sei. Der Bezug zu Art. 38 Abs. 1 GG wird dann in den folgenden weiteren Entscheidungen ausgebaut, der Bezug zu Art. 21 GG eingeschränkt bzw. aufgegeben.[19] Für die vorliegende Fragestellung ist somit davon auszugehen, dass Fraktionen verfassungsrechtlich zentral in Art. 38 Abs. 1 GG verankert sind; ergänzend kommt hinzu die Stellung der Parteien sowie – mit Blick auf die Konkretisierungen in der Geschäftsordnung – die Geschäftsordnungsautonomie des Parlaments.[20]

C. Anwendbarkeit der Regelungen des BDSG

Somit ist zu klären, ob die datenschutzrechtlichen Vorgaben des BDSG zur Anwendung kommen können. Dies hängt maßgeblich davon ab, ob Abgeordnete und Fraktionen als öffentliche Stellen, als nichtöffentliche Stellen oder als Datenschutzsubjekte sui generis anzusehen sind. Abgeordnete und Fraktionen müssen hierbei vor dem Hintergrund des verfassungsrechtlichen Gleichklangs auch in datenschutzrechtlicher Hinsicht einer einheitlichen Beurteilung unterliegen.

I. Unterscheidung zwischen parlamentarischer Kerntätigkeit und fiskalischen Hilfsgeschäften

Bezüglich der Festlegung des anwendbaren Datenschutzrechts ist zwischen der Wahrnehmung der parlamentarischen Kerntätigkeit und fiskalischen Hilfsgeschäften zu unterscheiden.[21]

II. Einordnung parlamentarischer Kerntätigkeit von Abgeordneten und Fraktionen

1. Einordnung als „öffentliche Stelle“ i.S.d. BDSG

Fraglich ist, ob Abgeordnete und Fraktionen im Rahmen ihrer parlamentarischen Kerntätigkeit als öffentliche Stelle

11 So etwa BVerfGE 20, 56, 103; 80, 188 Leitsatz 2, 217; 99, 19, 32.

12 BVerfGE 104, 310, 330.

13 BVerfGE 6, 445, 447 f.

14 So Klein, in: Maunz/Dürig, Art. 38 GG (88. EL August 2019) Rn. 193.

15 Zum Folgenden auch Grzeszick, NVwZ 2017, 985 ff. m.N.

16 BVerfGE 10, 4, 14.

17 Bereits zuvor, aber wenig beachtet BVerfGE 43, 142, 149.

18 Dazu sowie zum Folgenden BVerfGE 70, 324, 363 ff.

19 BVerfGE 80, 188, 189, 219 f., 241; 84, 304, 322, 324; 93, 195, 203 f.

20 Umfassende Darstellung bei Hölscheidt, Das Recht der Parlamentsfraktionen, 2001, S. 160 ff., 237 ff., 283 ff. et passim m.N.

21 Schröder, ZRP 2018, 129, 130; Grzeszick, NVwZ 2018, 1505, 1508; dazu auch DSK Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien v. 05.09.2018 unter 3.

im Sinne von §§ 1 Abs. 1 Nr. 1 und 2, 2 Abs. 1 und 2 BDSG anzusehen sind.

a) „öffentliche Stelle" nach §§ 1 Abs. 1 Nr. 1 und 2, 2 Abs. 1 und 2 BDSG

Der Begriff der öffentlichen Stelle ist dabei umfassend zu verstehen und erfasst alle öffentlich-rechtlich organisierten Einheiten ungeachtet ihrer Rechtsform, die dem Bund bzw. einem Land zuzurechnen sind.[22] § 2 Abs. 1 BDSG nennt insofern insbesondere Behörden und andere öffentlich-rechtlich organisierte Einrichtungen. Der Begriff der Behörde ist dabei weder im europäischen noch im nationalen Datenschutzrecht legaldefiniert.[23] Damit ist hinsichtlich des Behördenbegriffs vorrangig auf § 1 Abs. 4 VwVfG zu rekurrieren.[24] Hierbei hat das BDSG die Frage, ob der Behördenbegriff organisatorisch oder funktional zu verstehen ist,[25] im Sinne des Ansatzes der DS-GVO zugunsten eines funktionalen Behördenbegriffs entschieden.[26] Entscheidend ist daher ein aufgabenorientiertes Verständnis, wobei maßgeblich ist, ob öffentlich-rechtliche Verwaltungsaufgaben wahrgenommen werden.[27] Abgeordnete und Fraktionen nehmen im Rahmen ihrer parlamentarischen Kerntätigkeit keine Aufgaben der öffentlichen Verwaltung wahr. Vielmehr sind sie Teil der Legislative und insofern keine Behörde i.S.d. § 1 Abs. 4 VwVfG. Diese Annahme stützt auch § 46 Abs. 3 AbgG.

Einige Stimmen[28] nehmen demgegenüber dennoch an, dass Fraktionen als öffentlich-rechtlich organisierte Einrichtung einzustufen sind.[29] Eine uneingeschränkte Anwendung des Datenschutzrechts folgt daraus vor dem Hintergrund der verfassungsrechtlichen Stellung der Fraktionen sowie der Abgeordneten im Ergebnis freilich nicht.[30] Fraktionen als öffentlich-rechtliche Einrichtungen zu qualifizieren kann dabei bereits vor dem Hintergrund nicht überzeugen, dass wiederum Abgeordnete „im Hinblick auf [die] von Fremdbestimmung und öffentlich-rechtlicher Aufgabenbindung freie Mandatsausübung"[31] selbst als nicht-öffentliche Stelle angesehen werden können.[32] Da Fraktionen ihre Rechtsstellung aber ebenfalls aus Art. 38 GG ableiten, kann sich für Abgeordnete und Fraktionen im Hinblick auf ihre rechtliche Einordnung als Datenschutzsubjekte keine abweichende Beurteilung ergeben.[33]

Ferner ist es wertungswidersprüchlich, Fraktionen als öffentlich-rechtlich organisierte Einrichtung i.S.d. BDSG einzuordnen, gleichwohl aber die Anwendbarkeit des BDSG im Wege der verfassungskonformen Auslegung im parlamentarischen Kernbereich ohnehin wieder auszuschließen. Vielmehr zeigt sich an der verfassungsrechtlichen Stellung von Abgeordneten und Fraktionen, dass diese einer Zuordnung unter die Begriffe des BDSG nicht zugänglich sind.[34] Auch nach Ansicht des Wissenschaftlichen Dienstes des Bundestages[35] ist eine Einordnung von Fraktionen als öffentliche Stelle und eine Einstufung des einzelnen Abgeordneten als nichtöffentliche Stelle vor dem Hintergrund, dass Fraktionen ihren verfassungsrechtlichen Status aus demjenigen der Abgeordneten ableiten, „nur schwer begründbar"[36].

Der Wissenschaftliche Dienst sowie die Positionierung der Bundesbeauftragten für Datenschutz und Informationssicherheit[37] spricht sich im Ausgangspunkt (unabhängig von den damit einhergehenden Rechtsfolgen)[38] dafür aus, auch Abgeordnete als öffentliche Stelle zu qualifizieren, sei doch auch das Abgeordnetenmandat durch öffentlich-rechtliche Regelungen geprägt. Gegen eine derartige Sichtweise spricht zumindest im Hinblick auf die parlamentarische Kerntätigkeit, dass im Rahmen der Mandatsausübung nach Art. 38 GG eine Bindung an Aufträge und Weisungen gerade nicht vorliegt.[39] Zudem erfolgt die Qualifizierung als öffentlich-rechtlich organisierte Einrichtung nicht anhand der Frage, ob öffentlich-rechtliche Regelungen auf die jeweilige Tätigkeit Anwendung finden, sondern ob Aufgaben der öffentlichen Verwaltung wahrgenommen werden. Dies ist aber bei Abgeordneten und Fraktionen im Rahmen ihrer parlamentarischen Tätigkeit gerade nicht der Fall, vgl. § 46 Abs. 3 AbgG.

Im Ergebnis können also weder Fraktionen noch Abgeordnete als öffentliche Stellen i.S.d. BDSG angesehen werden. Nur so kann auch ein Verstoß gegen den Grundsatz der Gewaltenteilung nach Art. 20 Abs. 2 S. 2 GG vermieden werden, da andernfalls der Anwendungsbereich des BDSG eröffnet wäre und eine Kontrollzuständigkeit des Bundesbeauftragten für Datenschutz und Informationsfreiheit nach § 9 BDSG begründet würde. Dies würde aber die Regelungsbefugnis des

22 Gola/Heckmann-Schulz, § 2 Rn. 7; Taeger/Gabel-Arning/Rothkegel, DS-GVO/BDSG § 2 Rn. 13.

23 Gola/Heckmann-Schulz, § 2 Rn. 8.

24 Übereinstimmend BeckOK-Schild, § 2 Rn. 12; Gola/Heckmann-Schulz, § 2 Rn. 8; Taeger/Gabel-Arning/Rothkegel, DS-GVO/BDSG, § 2 Rn. 14; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG, § 2 Rn. 4.

25 Dazu insgesamt Gola/Heckmann-Schulz, § 2 Rn. 8; Simitis-Dammann, § 2 BDSG a.F. Rn. 15; Kühling/Buchner-Klar/Kühling, § 2 Rn. 4; Taeger/Gabel-Arning/Rothkegel, DS-GVO/BDSG, § 2 Rn. 15.

26 Simitis/Hornung/Spiecker gen. Döhmann-Petri, § 2 Rn. 16; Taeger/Gabel-Arning/Rothkegel, DS-GVO/BDSG, § 2 Rn. 15; HK-DS-GVO/BDSG, Schwartmann/Mühlenbeck, Art. 4 Nr. 7 Rn. 11; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG, § 2 Rn. 4.

27 Taeger/Gabel-Arning/Rothkegel, DS-GVO/BDSG, § 2 Rn. 15; Simitis/Dammann zu § 2 BDSG a.F. Rn. 15: kritisch wiederum Auernhammer/Eßer, DS-GVO/BDSG zu § 2 BDSF a.F. Rn. 6.

28 So etwa Paal/Pauly-Ernst, DS-GVO/BDSG, § 2 Rn. 5; Simitis-Dammann, § 2 BDSG a.F. Rn. 29; Auernhammer-Eßer, DS-GVO/BDSG zu § 2 BDSG a.F. Rn. 1; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG, § 2 Rn. 9; dazu auch Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2019, S. 6 und Fn. 6.

29 Vgl. etwa Paal/Pauly-Ernst, DS-GVO/BDSG, § 2 Rn. 5; Simitis-Dammann, § 2 BDSG a.F. Rn. 29; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG, § 2 Rn. 9.

30 Simitis-Dammann, § 2 BDSG a.F. Rn. 29 schlägt etwa eine verfassungskonforme Auslegung der Vorschriften des BDSG für parlamentarische Kernbereiche vor.

31 Simitis-Dammann, § 2 BDSG a.F. Rn. 29.

32 Simitis-Dammann, § 2 BDSG a.F. Rn. 29.

33 Zumindest im Hinblick auf die Notwendigkeit der einheitlichen rechtlichen Beurteilung von Fraktionen und Abgeordneten übereinstimmend Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6.

34 In diese Richtung LT-Drs. 21/11638, S. 17 zum HmbDSG.

35 Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6.

36 Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6.

37 Übereinstimmend BfDI Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 3.

38 Dazu Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6 f. sowie BfDI Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 4.

39 Simitis-Dammann, § 2 BDSG a.F. Rn. 29; Auernhammer-Eßer, DS-GVO/BDSG zu § 2 BDSG a.F. Rn. 10.

Parlaments im Rahmen ihrer legislativen Kerntätigkeit und die damit einhergehende selbstständige Ausübung von Untersuchungs- und Kontrollbefugnissen missachten.[40] Eine Aufsicht durch den BfDI kann auch nach Ansicht der vormaligen BfDI[41] und nach Auffassung des derzeitigen BfDI jedenfalls für den parlamentarischen Kernbereich nicht gelten[43]. Diese Ansicht teilt auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK)[44], die davon ausgeht, dass Abgeordnete und Fraktionen zumindest im Rahmen des parlamentarischen Kernbereichs nicht unter das Datenschutzrecht zu fassen sind und daher auch eine entsprechende Aufsicht nicht besteht. Eine Gleichsetzung von Abgeordneten und Fraktionen mit Behörden i.S.d. § 2 Abs. 1 BDSG ist insofern aufgrund der verfassungsrechtlichen Stellung von Abgeordneten und Fraktionen nicht gerechtfertigt.[45]

b) Rechtsfolgen im Hinblick auf BDSG und DS-GVO

Würden Abgeordnete und Fraktionen als öffentliche Stellen qualifiziert, so fände zumindest das BDSG Anwendung. Eine unmittelbare Anwendbarkeit der DS-GVO ist freilich nach den obigen Darlegungen zu Art. 2 DS-GVO ausgeschlossen, weshalb der Rückgriff über die Regelung des § 1 Abs. 8 BDSG zumindest fraglich erscheint. Jedenfalls ist zumindest eine verfassungskonforme Einschränkung der Vorschriften[46] erforderlich.

2. Einordnung als „nichtöffentliche Stelle" i.S.d. BDSG

Somit ist fraglich, ob Abgeordnete und Fraktionen im Rahmen ihrer parlamentarischen Tätigkeit als nichtöffentliche Stelle i.S.v. § 1 Abs. 1 S. 2, 2 Abs. 4 BDSG einzuordnen sind.

a) Abgeordnete und Fraktionen als nichtöffentliche Stellen

Teilweise[47] werden zumindest Abgeordnete – anders als Fraktionen[48] – als nichtöffentliche Stelle angesehen. Gegen diese Annahme sprechen insbesondere folgende Argumente: Die Einordnung als nichtöffentliche Stelle widerspräche zum einen dem Wesen der Tätigkeiten eines Abgeordneten als Teil des obersten Staatsorgans Bundestag bzw. Landtag.[49] Daneben sind Abgeordnete jedenfalls im Rahmen ihrer parlamentarischen Tätigkeit und im Rahmen ihrer Mandatsausübung nach Art. 38 GG keine natürlichen Personen.[50] Auch die BfDI-Position betont, „eine Einordnung als nichtöffentliche Stelle würde die Abgeordneten mit beliebigen Privatunternehmen gleichsetzen, was ihrer herausgehobenen Stellung nicht gerecht würde".[51] Gleiches gilt dabei für Fraktionen: Ihr besonderer verfassungsrechtlicher Status schließt eine Einordnung als juristische Person bzw. Personenvereinigung des Privatrechts i.S.d. §§ 21 ff. BGB aus, sind sie doch gerade keine Parteien. Dies zeigt sich auch an der jüngeren Rechtsprechung des BVerfG, die vermehrt Art. 38 GG anstelle von Art. 21 GG für Fraktionen heranzieht (vgl. dazu oben B. II). Zudem wäre die unterschiedliche Einordnung von Abgeordneten wiederum als nichtöffentliche Stelle auch in rechtspraktischer Hinsicht zweifelhaft, weil diese so letztlich anderen Datenschutzvorschriften als Fraktionen unterlägen.[52] Eine Trennung sowohl der rechtlich anwendbaren Regelungen als auch der jeweiligen zuständigen Aufsichtsbehörde für Abgeordnete und Fraktionen ist dabei nicht nur wegen der „engen Verknüpfung der Tätigkeitsbereiche",[53] sondern auch vor dem Hintergrund von Art. 38 GG wertungswidersprüchlich. Ferner hätte die Annahme, dass Abgeordnete und Fraktionen als nichtöffentliche Stelle anzusehen sind und damit der Datenschutzaufsicht unterfallen, einen Verstoß gegen den Grundsatz der Gewaltenteilung zur Folge (vgl. dazu oben unter II. 1. a).

b) Rechtsfolgen im Hinblick auf DS-GVO und BDSG

Eine Einordnung von Abgeordneten und Fraktionen als nichtöffentliche Stellen hätte zur Folge, dass auf den parlamentarischen Bereich zumindest die Regelungen des BDSG – vorbehaltlich einer verfassungskonformen Auslegung[54] – für nichtöffentliche Stellen Anwendung fänden.

3. Konsequenz: Abgeordnete und Fraktionen als Datenschutzsubjekte sui generis

Folglich können Abgeordnete und Fraktionen im Rahmen des parlamentarischen Kernbereichs weder als öffentliche noch als nichtöffentliche Stelle angesehen werden. Eine pauschale Einordnung von Abgeordneten und Fraktionen

40 Dazu Schröder, ZRP 05/2018, 129, 131.

41 Übereinstimmend BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S.4.

42 Dazu BfDI Kelber, Interview in der WELT v. 29.01.2020: „Der Twitteraccount von Bundestagsabgeordneten ist Teil von deren parlamentarischer Tätigkeit und unterliegt damit nicht meiner Aufsicht." Abrufbar unter https://www.welt.de/wirtschaft/article205402427/Datenschutz-Ulrich-Kelber-droht-mit-dem-Beispiel-von-1-1.html (zuletzt abgerufen am 04.02.2020).

43 Übereinstimmend BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 4; Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung, 39. Sitzung v. 25.04.2017, BT-Drs. 18/12144, S. 2 sowie dazu Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 7; dazu auch Schröder, ZRP 2018, 129, 131.

44 Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 05.09.2018.

45 20. Tätigkeitsbericht des Bundesbeauftragten für Datenschutz, BT-Drs. 15/5252, S. 117; Schröder, ZRP 2018, 129, 131.

46 In diese Richtung etwa Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6 f.; BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 4; Simits-Dammann, BDSG, zu § 2 BDSG a.F. Rn. 30.

47 Simitis-Dammann, BDSG, zu § 2 BDSG a.F. Rn. 29;

48 In diesem Sinne etwa Paal/Pauly-Ernst, DS-GVO/BDSG § 2 Rn. 5; Simitis-Dammann, § 2 BDSG a.F. Rn. 29; Auernhammer-Eßer, DS-GVO/BDSG zu § 2 BDSG a.F. Rn. 1; Kühling/Buchner-Klar/Kühling, DS-GVO/BDSG, § 2 Rn. 9. Dazu auch Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6 und Fn. 6.

49 HK-LDSG NRW-Pabst, § 5 Rn. 33.

50 HK-LDSG NRW-Pabst, § 5 Rn. 33.

51 BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 3.

52 Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6.

53 Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 6.

54 Vgl. dazu Fn. 33.

unter die Begriffsdefinitionen des BDSG verbietet sich dabei bereits schon vor dem Hintergrund der Notwendigkeit der Ausdifferenzierung zwischen parlamentarischer Kerntätigkeit und der außerhalb dieses Bereichs liegenden Teilnahme am allgemeinen wirtschaftlichen Rechtsverkehr. Eine pauschale Zuordnung unter eine der Begriffsdefinitionen des BDSG würde somit sowohl der verfassungsrechtlichen Stellung als auch den datenschutzrechtlichen Eigenarten der verschiedenen Tätigkeitsbereiche nicht gerecht.

Abgeordnete und Fraktionen können somit im Rahmen ihrer Kerntätigkeit nicht unter die Begriffsbestimmungen des BDSG subsumiert werden. Sie sind vielmehr vor dem Hintergrund ihres verfassungsrechtlichen Status als Datenschutzsubjekte sui generis anzusehen.[55] Sie unterfallen dabei weder den Regelungen des BDSG noch der DS-GVO.[56] In der Folge sind auch die tatbestandlichen Voraussetzungen des Rückverweises aus § 1 Abs. 8 BDSG auf die Vorschriften der DS-GVO nicht erfüllt, da weder Abgeordnete noch Fraktionen im Rahmen der parlamentarischen Kerntätigkeit als öffentliche Stellen anzusehen sind.

IV. Einordnung von Abgeordneten und Fraktionen jenseits des Kernbereichs

Die Besonderheiten im Hinblick auf die Tätigkeiten von Abgeordneten und Fraktionen können nur insoweit gelten, wie der parlamentarische Kernbereich betroffen ist, bei dem sich der besondere verfassungsrechtliche Status von Abgeordneten und Fraktionen realisiert. Sofern dieser Bereich verlassen wird, ist zumindest nicht ausgeschlossen, dass Abgeordnete und Fraktionen im Rahmen ihrer sonstigen Tätigkeit der öffentlichen Aufgabenerfüllung nachgehen und somit Verwaltungstätigkeiten ausüben.[57] Insoweit könnten Abgeordnete und Fraktionen als öffentliche Stelle i.S.d. §§ 1 Abs. 1 Nr. 1 und 2, 2 Abs. 1 und 2 BDSG anzusehen sein. Sofern also Abgeordnete und Fraktionen wie eine Behörde oder sonstige öffentlich-rechtlich organisierte Einrichtung am Rechtsverkehr teilnehmen, fallen diese Tätigkeiten auch in den Anwendungsbereich des BDSG bzw. der DS-GVO. Ob eine Einordnung von Abgeordneten und Fraktionen als nichtöffentliche Stelle i.S.v. § 2 Abs. 4 BDSG jedenfalls dann in Betracht kommt, wenn sie außerhalb der Mandatsausübung oder ihrer Verwaltungstätigkeit im Rahmen fiskalischer Geschäfte tätig werden, erscheint zweifelhaft. Denn Abgeordnete werden außerhalb ihrer Mandatsausübung im Rahmen sonstigen Verwaltungshandelns zumindest nicht zu einer natürlichen Person i.S.d. § 2 Abs. 4 BDSG, sondern handeln weiterhin im Rahmen ihrer Stellung als Abgeordnete. Gleiches gilt für Fraktionen. Diese werden im Rahmen fiskalischen Handelns durch dieses nicht zu einer privatrechtlichen Vereinigung im Sinne des BGB. Eine Einordnung als nichtöffentliche Stelle i.S.d. § 2 Abs. 4 BDSG außerhalb der parlamentarischen Kerntätigkeit liegt daher fern.

Letztlich ist im Sinne der DSK jeweils eine Bewertung im Einzelfall maßgeblich.[58] Demzufolge können Abgeordnete und Fraktionen außerhalb des parlamentarischen Kernbereichs als öffentliche Stelle den Regelungen des BDSG für öffentliche Stellen bzw. über § 1 Abs. 8 BDSG auch der DS-GVO unterfallen.

D. Ausblick

Es handelt sich bei der Frage nach der Anwendbarkeit des Datenschutzrechts auf Abgeordnete und Fraktionen, insbesondere im Hinblick auf den parlamentarischen Kernbereich, um eine Materie, die mit Blick auf die verfassungsrechtlichen Positionen spezifisch auszugestalten ist.[59] Letztlich besteht vor dem Hintergrund der Besonderheiten des Verfassungsrechts eine ähnliche Konstellation wie bei Kirchen, deren Status ebenfalls einen „Pendelblick"[60] zwischen Datenschutz- und Verfassungsrecht fordert.[61] Allerdings hat die DS-GVO dabei ausdrücklich in Art. 91 DS-GVO eine Öffnungsklausel geschaffen, wogegen für den parlamentarischen Kernbereich die DS-GVO unmittelbar nicht greift, und auch ein Rückverweis über § 1 Abs. 8 BDSG nicht überzeugt, v.a. aus verfassungsrechtlichen Gründen. Art. 20 Abs. 3 GG fordert gleichwohl auch im parlamentarischen Bereich eine Achtung des Rechts auf informationelle Selbstbestimmung.[62] Inwieweit diesem datenschutzrechtlich Rechnung getragen werden kann, bedarf einer genauen Untersuchung.

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Prof. Dr. Bernd Grzeszick, LL.M.
Lehrstuhl für Öffentliches Recht, Internationales Öffentliches Recht, Allgemeine Staatslehre und Rechtsphilosophie an der Universität Heidelberg, Direktor des Instituts für Staatsrecht, Verfassungslehre und Rechtsphilosophie, Direktor des Heidelberg Center for American Studies sowie Mitglied der Heidelberger Akademie der Wissenschaften.

55 In diesem Sinne vgl. auch HK-LDSG NRW-Pabst, § 5 Rn. 34.

56 Im Ergebnis übereinstimmend DSK Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien v. 05.09.2018 unter 1; Grzeszick, NZwZ 2018, 1505, 1508; BT-Drs. 18/12144; S. 2; BfDI, Datenschutz-Grundverordnung für Abgeordnete – Handreichung für die Mitglieder des Deutschen Bundestages v. 18.12.2018, S. 2; Schröder, ZRP 05/2018, 129, 131. Zur Anwendbarkeit des BDSG zumindest mit Einschränkungen, Simitis-Dammann, BDSG, zu § 2 BDSG a.F. Rn. 29 f.; Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 5 f.

57 In diesem Sinne wohl auch DSK, Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien v. 05.09.2018 unter 3; vgl. dazu auch Grzeszick, NZwZ 2018, 1505, 1508 sowie Schröder, ZRP 05/2018, 129, 131.

58 DSK Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien v. 05.09.2018 unter 3.

59 Vgl. etwa HK-LDSG NRW-Pabst, § 5 Rn. 35; DSK, Anwendung der DS-GVO im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien v. 05.09.2018 unter 4.; Schröder, ZRP 05/2018, 129, 131; Wissenschaftlicher Dienst des Deutschen Bundestages – Datenschutzrecht für Abgeordnete, WD 3 – 3010 – 056/18 v. 26.08.2018, S. 5 f.

60 HK-DS-GVO/BDSG-Thüsing/Rombey, Art. 91 Rn. 3.

61 Dazu ausführlich HK-DS-GVO/BDSG-Thüsing/Rombey, Art. 91 Rn. 3.

62 Schröder, ZRP 05/2018, 129, 131.

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (46): Einzelaspekte des Beschäftigtendatenschutzes im TB des Sächsischen Datenschutzbeauftragten

Zusammengestellt und erläutert von Prof. Peter Gola*

Vorbemerkung

Der am 19. 12. 2019 für die Jahre 2017 bis 2018 vorgelegte Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten gliedert sich in zwei Teile und zwar einen nach dem öffentlichen und privaten Bereich getrennten Einzelbericht für die Zeit vor Inkrafttreten der DS-GVO und einen gesonderten Bericht zur Datenschutz-Grundverordnung (EU) 2016/679 nebst der Richtlinie (EU) 2016/680 und sonstige Bereiche für den Berichtszeitraum vom 25.5. bis 31.12.2018.

I. Der Datenaustausch zwischen potentiellem Arbeitgebern und den Jobcentern

Verläuft eine Bewerbung auf ein Stellenangebot des Jobcenters negativ, so kann der potentielle Arbeitgeber dem Jobcenter Angaben zum Verlauf des Vorstellungsgesprächs machen und die SGB II-Behörde diese Daten erheben und verwerten.

Dies ergebe sich zum einen für das Jobcenter laut SächsDSB *(TB 2017/2018 Teil 1 Abschn. 2.7.3.1)* aus § 67 a Abs. 2 Nr. 2 Buchst. b aa SGB X in Verbindung mit § 31 Abs. 1 Nr. 2 SGB II. Das Jobcenter habe auch die Aufgabe zu überprüfen, ob der Leistungsberechtigte durch sein Verhalten ggf. die Anbahnung eines Arbeitsverhältnisses – zum Beispiel durch unzureichende Bewerbungen oder sein Verhalten im Vorstellungsgespräch – verhindere.

Die Rechtsgrundlage für die Auskunftserteilung und mithin für eine Datenübermittlung durch das Unternehmen, bei dem sich der Leistungsbezieher bewerben sollte bzw. beworben hatte, an den Leistungsträger leitete der SächsDSB noch aus § 28 Abs. 2 Nr. 2a BDSG a.F. ab, wobei u.a. Art. 6 Abs. 1 lit. f DS-GVO nunmehr eine Rechtfertigungsnorm sein kann. Das betroffene Unternehmen kann sich gegenüber der Behörde „entlasten" und kann nicht nur Angaben darüber machen, dass es zu keiner Einstellung gekommen sei, sondern auch zu den Gründen der fehlgeschlagenen Anstellung. Ggf. greift auch die Übermittlungsbefugnis des § 24 Abs. 1 Nr.- 1 BDSG. wenn die Übermittlung der Verfolgung einer Straftat, d.h. hier des Sozialbetrugs (§ 263 StGB) dienen soll.

II. Versand elektronischer Lohnbescheinigungen

Der SächsDSB stellt weiter fest *(TB 2017/2018 Teil 1 Abschn. 2.7.3.2)*, dass es nicht datenschutzkonform ist, Lohnsteuerbescheinigungen unverschlüsselt an die private E-Mail-Adresse der Arbeitnehmer zu versenden. Dieses Vorgehen scheitere zum einen daran, dass der unverschlüsselte Versand nicht der sich aus der besonderen Sensibilität der Lohn- und Gehaltsdaten ergebenden Pflicht, diese persönlichen Daten der Arbeitnehmer vor unberechtigten Zugriffen besonders zu schützen, gerecht werde. Zum anderen sei eine Übermittlung an private E-Mailadressen nur per Einwilligung zulässig, deren Freiwilligkeit aber in Frage stehe. Als Lösung empfiehlt der SächsDSB allen Mitarbeitern private, auf Firmenservern gehostete, durch individuelle Passwörter geschützte E-Mail-Postfächer zur Verfügung zu stellen.

III. Herausgabe von Personalunterlagen an ausgeschiedene Mitarbeiter

Die Auffassung eines Petenten, wonach der Arbeitgeber Personalunterlagen nach Ende der Beschäftigung unverzüglich herauszugeben habe, teilte der SächsDSB *(TB 2017/2018 Teil 1 Abschn. 2.7.3.4)* unter Beurteilung der vor dem 25.5.2018 geltenden Rechtslage aus folgenden Gründen nicht: „Das Datenschutzrecht kennt keinen Herausgabeanspruch, sondern nur den Anspruch auf Löschung (Vernichtung) oder Sperrung, also eine besonders geschützte und zweckbegrenzte Form der Aufbewahrung (§ 35 Abs. 2 Satz 1 bzw. § 35 Absatz 3 BDSG a.F.). Ein arbeitsrechtlicher oder allgemein zivilrechtlicher Herausgabeanspruch mag allenfalls bei Unterlagen in Betracht kommen, die dem Arbeitgeber vom Beschäftigten überlassen wurden und deren Verbleib vom Arbeitgeber über das Beschäftigungsende hinaus nicht länger beansprucht werden kann. Dies trifft auf Unterlagen, die im Rahmen ordnungsgemäßer Personalaktenführung rechtmäßig zur Personalakte genommen wurden, regel-

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

mäßig nicht zu. Vielmehr gilt – auch datenschutzrechtlich – der Grundsatz, dass Personalunterlagen so lange aufbewahrt werden dürfen, wie noch mit Ansprüchen des Beschäftigten zu rechnen ist. Da nach § 195 BGB die regelmäßige Verjährungsfrist von Ansprüchen ehemaliger Beschäftigter erst nach drei Jahren endet, können Personalakten dementsprechend gleichermaßen lange aufbewahrt werden. Zudem beginnt wegen § 199 BGB die Verjährungsfrist erst am Jahresende des Jahres, in dem der Beschäftigte das Unternehmen verlässt.

Ferner ist die Aufbewahrung von Personalunterlagen auch über diesen Zeitraum hinaus vielfach aus anderem Recht geboten und damit gestattet: So gibt es diverse gesetzliche Aufzeichnungs- und Aufbewahrungspflichten, teils mit Fristen bis zu 10 Jahren, um Steuerbehörden und den Sozialversicherungsträgern Prüfungen zu ermöglichen. Eine Darstellung aller hier möglicherweise einschlägigen Bestimmungen und Sachverhalte ist mir an dieser Stelle nicht möglich. Nur beispielhaft möchte ich das für Krankschreibungen relevante Aufwendungsausgleichsgesetz benennen. Nach § 6 Absatz 1 AAG besteht ein Erstattungsanspruch bis zu vier Jahren nach Ablauf des Kalenderjahrs, in dem er entstanden ist. Somit können Arbeitsunfähigkeitsbescheinigungen erst fünf Jahre nach Ablauf des Kalenderjahrs, in dem der Erstattungsanspruch entstanden ist, vernichtet werden."

Die Argumente gelten aber auch, wenn sich ein Beschäftigter insoweit nunmehr auf die DS-GVO berufen würde. Hier gewährt Art. 15 Abs. 3 DS-GVO dem Beschäftigten zwar ggf. ein Recht auf Erteilung von Kopien der zu seiner Person gespeicherten Daten, nicht aber einen Herausgabeanspruch von Originalunterlagen.

IV. Unzulässigkeit von Mailingaktionen einer Gewerkschaft an die gesamte Belegschaft

Der SächsDSB *(TB 2017/2018, Teil 1, Abschn. 2.7.3.5)* hatte sich damit zu befassen, dass eine Gewerkschaft zur Information der Beschäftigten und damit auch zu Werbezwecken für ihre Ziele nach Art. 9 Absatz 3 GG regelmäßig Mailing-Aktionen an alle Beschäftigten eines Unternehmens, mithin auch an Nicht-Mitglieder durchführte. Sie bezog sich dabei auf das Grundsatzurteil des BAG vom 20.01.2009 (1 AZR 515/08), wonach Arbeitgeber einer tarifzuständigen Gewerkschaft grundsätzlich nicht untersagen könnten, sich zu Werbe- und Informationszwecken per E-Mail an die Beschäftigten über deren betriebliche E-Mail-Adressen zu wenden.

Der SächsDSB konnte jedoch zu Recht in dem Urteil des BAG keine pauschale Erlaubnis für eine tarifzuständige Gewerkschaft entnehmen, alle Beschäftigten der betreffenden Arbeitgeber per betrieblicher E-Mail anzusprechen. Die bei Nichtmitgliedern als Rechtsgrundlage in Betracht kommende Interessenabwägung (nunmehr Art. 6 Abs. 2 lit. f DS-GVO) begründe die Zulässigkeit solcher Mailingaktionen nicht, so dass für eine rechtssichere Lösung nur eine Einwilligung möglich sei.

V. Übermittlung von Schuldnerdaten an Arbeitgeber

Der SächsDSB konnte berichten *(TB 2017/2018, Teil 1, Abschn. 2.7.5.1)* dass ein Gläubiger, der einen Vollstreckungsbescheid gegen einen Beschäftigten besaß, sich per E-Mail an dessen Arbeitgeber gewandt hatte. Unter Mitteilung konkreter Informationen über die Vermögenslage des Beschäftigten regte er an, dass der Arbeitgeber seinen Arbeitnehmer zur Vermeidung kostenträchtiger Pfändungsmaßnahmen zu freiwilligen Ratenzahlungen bewegen möge.

Der SächsDSB beanstandete das Vorgehen noch unter Betrachtung des BDSG a.F. Ohne Einwilligung des Betroffenen, die hier natürlich nicht vorlag, gestattet § 4 Absatz 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Daran fehlte es aber im konkreten Fall. Erst ein richterlicher Pfändungs- und Überweisungsbeschluss berechtigt zur Lohnpfändung und damit zum Herantreten an den Arbeitgeber des Schuldners. Liegt ein solcher Beschluss nicht vor, kann der Gläubiger sich nicht auf § 28 Abs. 1 Nr. 2 BDSG oder nunmehr Art. 6 Abs. 1 lit. f DS-GVO berufen. Gegenüber dem berechtigten Wunsch des Gläubigers an der zügigen Schuldenbegleichung überwiegen schutzwürdige Interessen des Beschäftigten. Negative Informationen über die Vermögens- und Verschuldungslage sind regelmäßig geeignet, die Reputation des Betroffenen zu beschädigen. Dies gilt auch bzw. gerade gegenüber der Personalabteilung, für die geordnete finanzielle Verhältnisse eines Beschäftigten gemeinhin auch eine Compliance-relevante Frage sind. Der mit der E-Mail verfolgte Zweck, der Arbeitgeber möge seinen Beschäftigten zu einer freiwilligen Begleichung seiner Schulden „bewegen", verfolge einen sozialen Druck jenseits gesetzlich erlaubter Instrumente zur Beitreibung finanzieller Forderungen.

Dass eine außergerichtliche Lösung zur Begleichung seiner Schulden möglicherweise auch im wirtschaftlichen Interesse des Betroffenen lag, legitimiert die Übermittlung an seinen Arbeitgeber nicht, denn Offerten dieser Art hätten dem Betroffenen auch unmittelbar unterbreitet werden können.

VI. Lohn und Gehaltsabrechnung durch Steuerberater – Frage der Auftragsverarbeitung

Nach der Spruchpraxis des Sächsischen Datenschutzbeauftragten ist die Lohn- und Gehaltsabrechnung, soweit sie durch Steuerberater erfolgt, kein Gegenstand einer Auftragsverarbeitung. Eine gemeinsame explizite Position der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu der Thematik stehe zwar aus; jedoch gebe das DSK-Kurzpapier Nr. 13 zur Auftragsverarbeitung diesbezügliche Hinweise. Danach liegt keine Auftragsverarbeitung vor, soweit die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss,

vorliegt. Beispielhaft genannt werden hierbei Berufsgeheimnisträger und auch Steuerberater.

Dies trifft ist aus Sicht des SächsDSB auf Steuerberater zu, die nach ihrem Berufsrecht eigene und damit originäre Verantwortung für den Inhalt der Lohn- und Gehaltsabrechnung zu leisten haben. Demgemäß werden bei der Einschaltung eines Steuerberaters steuerrechtliche Tatbestände offengelegt und übermittelt, zu denen neben möglichen Gesundheitsinformationen auch die Informationen zur Veranlagung und Abführung der Kirchensteuer, d.h. besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Absatz 1 DS-GVO gehören, wobei der SächsDSB in § 26 Absatz 3 BDSG die die Übermittlung rechtfertigende Erlaubnisnorm sieht.

VII. Datenschutzbeauftragte, Betriebsräte und Personalvertretungen

1. Die Mitarbeitervertretung als Verantwortlicher

Bei der Frage, ob Betriebsräte und Personalvertretungen eigenständige Verantwortliche im Sinne von Art. 4 Nummer 7 DS-GVO seien, hält der SächsDSB *(TB 2017/2018, Teil 2 Abschn. 2.1.1)* unter Berufung auf vor Inkrafttreten der DS-GVO ergangene Rechtsprechung (BAG, Beschl. v. 7. 2. 2012-1 ABR 46/10) daran fest, dass der Betriebsrat eine zum Unternehmen gehörende Einheit darstelle und dass Personalvertretungen unselbständiger Teil einer öffentlichen Stelle seien. Damit bestehe auch eine Benennungspflicht für einen Datenschutzbeauftragten nur für das Unternehmen bzw. die Behörde, nicht aber für die jeweiligen Beschäftigtenvertretungen. Der SächsDSB weist aber auf die insoweit bestehende Uneinigkeit zwischen den deutschen Datenschutzaufsichtsbehörden hin.

2. Kontrolle der Mitarbeitervertretung durch den DSB

Von der früheren BAG-Rechtsprechung abweichender Auffassung ist der SächsDSB jedoch hinsichtlich der Frage, inwieweit der betriebliche/behördliche Datenschutzbeauftragte befugt ist, die personenbezogenen Datenverarbeitung des Betriebsrats bzw. der Personalvertretung zu überwachen *(TB 2017/2018, Teil 2, Abschn. 4.8.8)* Auch oder gerade weil in der DS-GVO und dem diese ergänzenden Bundesdatenschutzgesetz keine Hinweise zur Reichweite der Überwachungsbefugnisse des Datenschutzbeauftragten getroffen sind, schließt sich der Sächsische Datenschutzbeauftragte der Meinung an, dass die Datenschutz-Grundverordnung von einer lückenlosen Kontrolle bei Verantwortlichen ausgeht. Da sich gegenüber der Datenschutz-Grundverordnung – im Gegensatz zum Bundesdatenschutzgesetz a. F. – auch das Betriebsverfassungsgesetz nicht mehr in einem gleichrangigen Verhältnis befinde, sei davon auszugehen, dass den Datenschutzbeauftragten Zugang zu (allen) personenbezogenen Daten und Verarbeitungsvorgängen zu gewähren sei und es keine kontrollfreie Datenverarbeitung gebe.

Die vollständige Überwachungsbefugnis bestehe ferner auch gegenüber anderen weisungsfrei und autonom entscheidenden funktionalen Stellen innerhalb von Verantwortlichen, wie zum Beispiel bei Schwerbehinderten- und Gleichstellungsbeauftragten. In allen Fällen hat der Datenschutzbeauftragte sich jedoch im Rahmen seiner Geheim-haltungs- und Vertraulichkeitspflicht zu bewegen, Art. 38 Absatz 5 DS-GVO.

Praxisfälle zum Datenschutzrecht IV: Musterfalllösungen zur Personalarbeit in Zeiten der Digitalisierung

Miriam Claus, LL.M./RAin Yvette Reif, LL.M.*

I. Sachverhalt

In einem Gespräch mit einem Mitarbeiter der Personalabteilung erfährt der Datenschutzbeauftragte (DSB), dass im Rahmen von Bewerbungsverfahren regelmäßig Informationen über die potenziellen Mitarbeiter/innen im Internet eingeholt werden. In diesem Zusammenhang wird zunächst eine „Google-Recherche“ durchgeführt. Des Weiteren werden eventuell vorhandene Profile in den Netzwerken XING und Facebook gelesen. Geprüft werden soll insbesondere, ob die dortige Selbstdarstellung mit derjenigen aus dem Lebenslauf bzw. Vorstellungsgespräch übereinstimmt. Muss der DSB die beschriebene Vorgehensweise der Personalabteilung beanstanden?

Im weiteren Verlauf des Gesprächs erfährt der DSB, dass die Vorstellungsgespräche zum Teil via Videochat durchgeführt und für eine spätere Auswertung gespeichert werden. Dadurch sollen Reisekosten eingespart und auch weiter entfernt wohnenden Bewerbern/Bewerberinnen ein zeitnahes Vorstellungsgespräch ermöglicht werden. Genutzt werden dafür handelsübliche Videochatprogramme. Muss der DSB die Videointerviews beanstanden?

* Miriam Claus, LL.M. ist Referentin bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.; RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der GDD und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl. 2016.

II. Musterfalllösung

1. Zulässigkeit von Internetrecherchen über Bewerber/innen

Es ist unbestreitbar, dass es sich bei den im Internet erhobenen Informationen um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO der potenziellen künftigen Mitarbeiter/innen handelt.

Die Erhebung von Bewerberdaten im Internet könnte über § 26 Abs. 1 S. 1 BDSG gerechtfertigt sein.

Dazu müsste es sich bei den Bewerbern/innen zunächst um Beschäftigte i.S.v. § 26 BDSG handeln. Der Begriff des Beschäftigten ist legaldefiniert in § 26 Abs. 8 BDSG. Gem. § 26 Abs. 8 S. 2 BDSG gelten danach auch Bewerber/innen für ein Beschäftigungsverhältnis als Beschäftigte. § 26 Abs. 1 S. 1 BDSG ist damit vorliegend anwendbar.

Nach § 26 Abs. 1 S. 1 BDSG dürfen Bewerberdaten in dem Umfang verarbeitet werden, wie dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist. Verarbeitet werden dürfen insbesondere Informationen zur Eignung, fachlichen Qualifikation und Ausbildung des/der Bewerbers/Bewerberin. Dem/der Arbeitgeber/in kann daran gelegen sein, die diesbezüglichen Angaben des/der Bewerbers/Bewerberin auch auf ihren Wahrheitsgehalt zu überprüfen bzw. überprüfen zu lassen. Gesprochen wird dann von sog. Background- oder Pre-Employment-Checks.

Die datenschutzrechtliche Zulässigkeit solcher Background- oder Pre-Employment-Checks ist umstritten. So rät der LfDI Baden-Württemberg[1], auf die Durchführung von Pre-Employment-Checks zu verzichten. Dem/der Arbeitgeber/in stünden genügend Möglichkeiten zur Verfügung, um die richtige Personalentscheidung zu treffen, insbesondere Vorstellungsgespräche, Assessment-Center und die Anforderung von Unterlagen im Original. Auch wenn die DS-GVO anders als das frühere nationale Recht den Grundsatz der Direkterhebung nicht mehr explizit regele, seien personenbezogene Daten im Grundsatz auch weiterhin beim Bewerber/bei der Bewerberin selbst zu erheben. Nur bei Online-Netzwerken wie XING oder LinkedIn, die Beschäftigte zur beruflichen Selbstdarstellung nutzen, soll nach Ansicht des LfDI ausnahmsweise das schutzwürdige Interesse des Bewerbers/der Bewerberin hinter dem Interesse des potenziellen Arbeitgebers an einer Datenerhebung ohne Mitwirkung desselben/derselben zurückstehen. Recherchen in sozialen Netzwerken wie Facebook oder Twitter hält der LfDI hingegen regelmäßig für datenschutzrechtlich unzulässig. Auch das „Googeln" von Bewerbern ist kritisch zu sehen.[2] Insofern stellt sich das Problem, dass bei Verwendung von Suchmaschinen wie z.B. Bing, Google, Yahoo regelmäßig überschießende Daten ausgeworfen werden, die für die Entscheidung über die Begründung des Beschäftigungsverhältnisses nicht von Relevanz sind. Auch bei Erhebung über das Internet darf der Arbeitgeber aber nur Daten sammeln, die von seinem Fragerecht gegenüber dem Bewerber/in erfasst sind.[3]

Rechtssicher auf § 26 Abs. 1 S. 1 BDSG gestützt werden kann damit im Ergebnis nur die Recherche in beruflichen Netzwerken, da hier die Darstellung der beruflichen Qualifikationen im Vordergrund steht.[4]

Fraglich ist, ob für Recherchen, die über berufliche Netzwerke hinausgehen, eine Einwilligung des Bewerbers/der Bewerberin als taugliche Rechtsgrundlage in Betracht kommt. Entscheidend sind insoweit die Umstände des Einzelfalls und die Reichweite der abgegebenen Erklärung. Aufgrund der besonderen Situation des Bewerbers/der Bewerberin bedarf es in jedem Fall einer besonderen Prüfung der Freiwilligkeit der Erklärung (§ 26 Abs. 2 S. 1 BDSG). Da ein Bewerber/eine Bewerberin, die einem Pre-Employment-Checks nicht zustimmt, möglicherweise im Auswahlverfahren benachteiligt wird, wird nur in besonderen Fällen von einer echten Freiwilligkeit ausgegangen werden können.[5]

Im Rahmen von Backgroundchecks können nicht nur „normale" personenbezogene Informationen über Bewerber/innen anfallen, sondern auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO. Praktisch relevant ist insofern z.B., dass sich bei einer Internetrecherche über den Bewerber/die Bewerberin diese/n betreffende Gesundheitsinformationen finden oder Informationen, die Rückschlüsse auf die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, eine Gewerkschaftszugehörigkeit oder die sexuelle Orientierung des Bewerbers/der Bewerberin zulassen. Für besondere Kategorien personenbezogener Daten sieht Art. 9 Abs. 1 DS-GVO grundsätzlich ein Verarbeitungsverbot vor.

In Umsetzung der Öffnungsklausel aus Art. 9 Abs. 2 lit. b DS-GVO regelt § 26 Abs. 3 BDSG die Verarbeitung von Daten nach Art. 9 Abs. 1 DS-GVO für Zwecke des Beschäftigungsverhältnisses. Diese ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Im Zusammenhang mit § 26 Abs. 3 S. 1 BDSG ist umstritten, ob eine Datenverarbeitung ausschließlich zur Ausübung bzw. Erfüllung gesetzlicher Rechte und Pflichten gestattet sein soll oder ob die Verarbeitung besonderer Kategorien personenbezogener Daten legitimierende Rechte und Pflichten auch aus dem Arbeitsvertrag bzw. der arbeitsrechtlichen Beziehung erwachsen können.[6] Für das Erfordernis einer Rechtsvorschrift spricht sich die Datenschutzkonferenz in

1 Ratgeber Beschäftigtendatenschutz, 3. Aufl. 2019, S. 22 f. (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/07/Arbeitnehmerdatenschutz-Handreichung.pdf).

2 Vgl. etwa D/W/W/S/Däubler, BDSG, § 26 Rn. 46; Däubler, Digitalisierung und Arbeitsrecht, § 4 Rn. 4 f.

3 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl., Rn. 596.

4 Vgl. Weth/Herberger/Wächter/Sorge/Weth, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2. Aufl. 2019, Rn. 102.

5 Schwarz, ZD 2018, 353, 355.

6 Vgl. hierzu bei Gola/Heckmann/Gola, § 26 BDSG Rn. 144 ff.

ihrem Kurzpapier Nr. 17 aus.[7] Ein solches Verständnis führt allerdings zu erheblichen Schwierigkeiten in der Praxis. So wäre etwa in Fällen, in denen das Fragerecht des Arbeitgebers auch besondere Kategorien personenbezogener Daten umfasst, die mit der Ausübung des Fragerechts verbundene Datenverarbeitung nicht legitimiert. Aus diesem Grunde sollte der Erlaubnisrahmen aus § 26 Abs. 3 S. 1 BDSG weitergezogen und nicht allein gesetzliche Rechte und Pflichten als ausreichend erachtet werden.[8]

Entscheidend für die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen von Backgroundchecks ist damit, ob die konkret erfassten Informationen vom Fragerecht des Arbeitgebers umfasst sind und kein Grund zur Annahme überwiegender Betroffeneninteressen am Ausschluss der Verarbeitung besteht. Gegen ein Überwiegen schutzwürdiger Betroffeneninteressen und für eine Zulässigkeit der Verarbeitung kann insbesondere sprechen, wenn die betroffene Person die sensiblen Informationen offensichtlich selbst online gestellt hat (Rechtsgedanke des Art. 9 Abs. 2 lit. e DS-GVO). Allein der Umstand, dass die sensiblen Daten vom Bewerber / von der Bewerberin online gestellt wurden, rechtfertigt die Verarbeitung durch den Arbeitgeber hingegen nicht. Es bedarf vielmehr stets des notwendigen Bezugs der Information zum Beschäftigungsverhältnis.

Der notwendige Zusammenhang im Internet über den Bewerber / die Bewerberin ermittelter Informationen zum Beschäftigungsverhältnis kann generell nur gewährleistet werden, wenn, wie bereits eingangs dargestellt, die Recherche von Anfang an auf den beruflich relevanten Kontext und die entsprechenden Netzwerke reduziert wird. Erst recht ist eine Kenntnisnahme nicht beruflich relevanter besonderer Kategorien personenbezogener Informationen über den Bewerber/die Bewerberin zu vermeiden.

Gemäß Art. 14 DS-GVO sind die betroffenen Bewerber/innen über die Durchführung von Backgroundchecks zu informieren. Nach Art. 14 Abs. 3 lit. a DS-GVO müssen die Informationen nach Abs. 1 der betroffenen Person innerhalb einer angemessenen Frist erteilt werden, jedoch spätestens innerhalb eines Monats. In der Praxis ist es sinnvoll, vor der Durchführung eines Pre-Employment-Checks hierauf hinzuweisen, z.B. im Rahmen eines Bewerberportals, und die gesetzlich geforderten Informationen bereitzuhalten.[9]

Soweit die Recherchen bei Facebook sowie das „Googeln" von Bewerbern/Bewerberinnen betroffen sind, sollte der DSB also die bestehende Praxis, im Internet über Bewerber zu recherchieren, beanstanden. Die Personalabteilung sollte zudem darauf hingewiesen werden, dass die Bewerber/innen über die Datenrecherche im Internet zu informieren sind.

2. Zulässigkeit von Videointerviews

Fraglich ist, ob die mit der Durchführung von Videointerviews verbundene personenbezogene Datenverarbeitung i.S.v. § 26 Abs. 1 S. 1 BDSG für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.

Nach dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)[10] können Videointerviews in Bewerbungsverfahren zulässig sein. Gerade bei einer großen Zahl von Bewerbern sei es oft nicht möglich, alle in Betracht kommenden Personen zu einem persönlichen Gespräch einzuladen, so das BayLDA. Insbesondere wenn Bewerber aus weiter Distanz anreisen müssten, könne eine digitale Lösung im beiderseitigen Interesse liegen. Der Einsatz von Videointerviews könne dazu führen, dass mehr Bewerber die Möglichkeit haben, sich persönlich darzustellen. Dadurch wiederum könne der Arbeitgeber im Interesse beider Beteiligten eine qualifiziertere Auswahlentscheidung treffen.

Zu beachten sei allerdings, dass nicht mehr Daten verarbeitet werden sollten als im Fall des persönlichen Gesprächs vor Ort, d.h., es sollte keine Aufzeichnung des Gesprächs erfolgen. Alternativ solle außerdem die Möglichkeit zum persönlichen Gespräch erhalten bleiben, sprich, der Bewerber sollte zwischen Videointerview und persönlichem Gespräch vor Ort wählen können. Auch Datensicherheitsaspekte dürften nicht außer Acht gelassen werden und die Kommunikation nur verschlüsselt erfolgen. Im Idealfall laufe das Videointerview über die unternehmenseigene Infrastruktur auf eigenen Servern. Im Hinblick auf Art. 13 DS-GVO sei der Bewerber über die vorgenannten Rahmenbedingungen des Videointerviews zu informieren. Unter Transparenzgesichtspunkten sei es schließlich geboten, dass die Bewerber während des Interviews sämtliche Gesprächspartner auf Seiten des Unternehmens sehen könnten, so das BayLDA.

Die Personalabteilung zeichnet die Interviews zur späteren Auswertung auf. Mithin nimmt sie eine Verarbeitung personenbezogener Daten vor, die das erforderliche Maß überschreitet. Auch werden keine besonderen Maßnahmen in Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten ergriffen.

Auch hier muss der DSB also das Vorgehen der Personalabteilung beanstanden. Eine Speicherung der Videointerviews zwecks späterer Auswertung ist abzustellen. Auch muss die Personalabteilung dem Bewerber die Wahl zwischen Videointerview und persönlichem Gespräch ermöglichen. Hinsichtlich der Datensicherheit muss der DSB auf die Etablierung geeigneter Maßnahmen hinwirken.

7 Datenschutzkonferenz, Kurzpapier Nr. 17: Besondere Kategorien personenbezogener Daten, Stand: 27.03.2018, S. 1 f.

8 So auch Piltz, BDSG – Praxiskommentar für die Wirtschaft, 2017, § 26 Rn. 84; Gola/Heckmann/Gola, § 26 BDSG Rn. 144 ff.

9 Schwarz, ZD 2018, 353, 356.

10 BayLDA, 8. Tätigkeitsbericht (2017/2018), Abschnitt 15.3., kritisch Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2016, Abschnitt 7.3.

DataAgenda.de

IHR PORTAL ZUM DATENSCHUTZ

Expertenwissen in GDD-Qualität

- detaillierte Arbeitspapiere, Checklisten uvm.
- Videos in TV-Qualität zur aktuellen Gesetzeslage mit Handlungsempfehlungen
- aktuelle Nachrichten zum Datenschutz: Urteile, Fallbeispiele, Entwicklungen
- Datenschutz Newsbox – aktuelle Themen monatlich im Überblick

+++ DS-GVO Bußgelder +++ Löschpflichten und Löschkonzepte +++ Stellung des Betriebsrates nach DS-GVO +++ Fotos und die DS-GVO +++ Datenschutz beim E-Mail-Versand +++ EuGH: Facebook Fanpages +++

Rechtsprechung

Beendigung der DSB-Benennung und Sonderkündigungsschutz bei Wegfall der Bestellvoraussetzungen

(**Bundesarbeitsgericht**, Urteil vom 5. Dezember 2019 – 2 AZR 223/19 –)

1. **Der Sonderkündigungsschutz des Beauftragten für den Datenschutz nach § 4f Abs. 3 Satz 5 BDSG in der bis zum 24. Mai 2018 geltenden Fassung (aF) endet mit Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF. Gleichzeitig beginnt der nachwirkende Sonderkündigungsschutz des § 4f Abs. 3 Satz 6 BDSG aF.**

2. **Mit Ende der Bestellpflicht erfolgt eine Abberufung. Der Begriff der „Abberufung" in § 4f Abs. 3 Satz 6 BDSG aF umfasst „jede Beendigung des Amtes, die durch ein Verhalten der verantwortlichen Stelle veranlasst wurde" (BAG 27. Juli 2017 – 2 AZR 812/16 –).**

3. **Für die Beschäftigung eines Datenschutzbeauftragten im Rahmen eines Arbeitsvertrages spricht, wenn die Parteien in einem schriftlichen Anstellungsvertrag ihr Vertragsverhältnis mehrfach als „Arbeitsverhältnis" und den Beauftragten als „Arbeitnehmer" bezeichnen sowie ein Recht des Verantwortlichen vereinbaren, dem Beauftragten ggf. auch eine andere angemessene Tätigkeit zuzuweisen.**

4. **Die Wirksamkeit der Bestellung als DSB wird nicht durch seine bereits zuvor erfolgte Bestellung zum Geschäftsleiter nach § 53 Abs. 2 Nr. 1 KWG in Frage gestellt. Das damit bedingte Fehlen der nach § 4f Abs. 2 Satz 1 BDSG aF erforderliche Zuverlässigkeit als DSB, führt nicht zur Nichtigkeit der Bestellung. Es bliebe ansonsten nur ein erheblich verringerter Anwendungsbereich für den in § 4f Abs. 3 Satz 4 BDSG aF vorgesehenen Widerruf der Bestellung, und das Recht der Aufsichtsbehörde, eine Abberufung wegen fehlender Zuverlässigkeit zu verlangen, liefe im Wesentlichen ins Leere (vgl. Gola/Schomerus BDSG 12. Aufl. § 4f Rn. 29b).**

(Leitsätze 2 bis 4 nicht amtlich)

Sachverhalt:

Die Parteien streiten über die Wirksamkeit zweier ordentlicher Kündigungen.

Der Kläger arbeitete bei der Beklagten – einem australischen Bankinstitut, das unter anderem in F eine Niederlassung unterhält – seit dem 1. April 2010 als Director Institutional Banking. Zu diesem Zeitpunkt waren in der Niederlassung neun Beschäftigte tätig, die alle ständig automatisiert personenbezogene Daten verarbeiteten. Am 8. April 2010 wurde der Kläger als einer von zwei Geschäftsleitern der Niederlassung nach § 53 Abs. 2 Nr. 1 KWG in das Handelsregister eingetragen. Mit Schreiben vom 1. Juni 2010 bestellte die Beklagte den Kläger gemäß § 4f BDSG in der bis zum 24. Mai 2018 geltenden Fassung (im Folgenden aF) zum Beauftragten für den Datenschutz. Ausweislich verschiedener „Organisation Charts" beschäftigte die Beklagte in den Jahren 2010 bis 2015 zwischen zehn und dreizehn, im Jahr 2016 neun Mitarbeiter in der Niederlassung in F.

Mit Schreiben vom 12. April 2017 kündigte die Beklagte das Arbeitsverhältnis des Klägers „ordentlich unter Einhaltung der gesetzlichen Kündigungsfrist" zum 31. Juli 2017, hilfsweise zum nächstzulässigen Termin. Mit weiterem Schreiben vom selben Tag kündigte sie es „ordentlich unter Einhaltung der vertraglichen Kündigungsfrist" zum 30. September 2017, hilfsweise zum nächstzulässigen Termin. Im Zeitpunkt des Zugangs der Kündigungen beschäftigte die Beklagte in der Niederlassung insgesamt acht Arbeitnehmer.

Der Kläger ist der Ansicht, die Kündigungen seien willkürlich, da die von der Beklagten behauptete Unternehmerentscheidung bankaufsichtsrechtlich nicht umsetzbar sei. Ferner habe ihm aufgrund des Sonderkündigungsschutzes nach § 4f Abs. 3 Satz 5 BDSG aF nur außerordentlich gekündigt werden können.

Der Kläger hat beantragt

1. festzustellen, dass das zwischen den Parteien bestehende Arbeitsverhältnis durch die seitens der Beklagten mit Schreiben vom 12. April 2017 ausgesprochene ordentliche Kündigung nicht zum 31. Juli 2017 aufgelöst worden ist;

2. festzustellen, dass das zwischen den Parteien bestehende Arbeitsverhältnis auch durch die seitens der Beklagten mit Schreiben vom 12. April 2017 ausgesprochene weitere ordentliche Kündigung nicht zum 30. September 2017 aufgelöst worden ist.

Die Beklagte hat Klageabweisung beantragt und gemeint, dem Kläger stehe kein Sonderkündigungsschutz zu. Sie sei eine Kapitalgesellschaft nach australischem Recht und habe im Zeitpunkt der Bestellung des Klägers zum Beauftragten für den Datenschutz dauerhaft nur neun Arbeitnehmer in der Niederlassung beschäftigt. Zudem habe der Kläger als Geschäftsleiter der Niederlassung gar nicht bestellt werden dürfen. Jedenfalls sei der Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF noch vor Ausspruch der Kündigungen unterschritten worden. Aufgrund einer Restrukturierung sei der Arbeitsplatz des Klägers spätestens zum 30. September 2017 weggefallen. In der Revisionsbegründung hat die Beklagte erstmals die Arbeitnehmereigenschaft des Klägers bestritten.

Das Arbeitsgericht hat festgestellt, dass das Arbeitsverhältnis der Parteien durch die Kündigungen nicht aufgelöst worden ist. Die dagegen gerichtete Berufung der Beklagten hat das Landesarbeitsgericht zurückgewiesen. Mit ihrer Revision verfolgt die Beklagte ihren Klageabweisungsantrag weiter.

Die Revision hat Erfolg. Mit der von ihm gegebenen Begründung durfte das Landesarbeitsgericht die Berufung der Beklagten gegen das der Klage stattgebende erstinstanzliche Urteil nicht zurückwei-

sen. Ob das Arbeitsverhältnis der Parteien aufgelöst worden ist, kann der Senat nicht selbst entscheiden. Dies führt zur Aufhebung des Berufungsurteils (§ 562 Abs. 1 ZPO) und zur Zurückverweisung der Sache an das Landesarbeitsgericht zur neuen Verhandlung und Entscheidung (§ 563 Abs. 1 ZPO).

I. Der Kläger hat Klage nach § 4 Satz 1 KSchG erhoben. Er wendet sich trotz seiner auf konkret genannte Zeitpunkte bezogenen Anträge nicht allein gegen die Beendigung des Arbeitsverhältnisses zu bestimmten Daten, sondern insgesamt gegen dessen Auflösung. So haben auch die Vorinstanzen seine Klageanträge verstanden.

II. Das Landesarbeitsgericht hat zu Unrecht angenommen, die ordentlichen Kündigungen seien wegen des Sonderkündigungsschutzes gemäß § 4f Abs. 3 Satz 5 BDSG aF unwirksam. Der Kläger kann sich nicht auf diesen Sonderkündigungsschutz berufen, da die Beklagte bei Zugang der Kündigungen nicht in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigte.

1. Das Landesarbeitsgericht hat zutreffend geprüft, ob ein Anwendungsfall des § 4f Abs. 3 Satz 5 BDSG aF vorliegt.

a) Die Zuständigkeit deutscher Gerichte für die Entscheidung des Rechtsstreits ist gegeben (Art. 6 Abs. 1 iVm. Art. 20 Abs. 2, Art. 21 Abs. 1 Buchst. a EuGVVO, § 21 Abs. 1 ZPO bzw. § 29 Abs. 1 ZPO bzw. § 48 Abs. 1a Satz 1 iVm. § 2 Abs. 1 Nr. 3 Buchst. b ArbGG). Es ist nicht zu prüfen, ob der beschrittene Rechtsweg zulässig ist (§ 73 Abs. 2 iVm. § 65 ArbGG). Die Parteien haben wirksam die Anwendbarkeit deutschen Rechts vereinbart (Art. 3 Abs. 1, Abs. 2 Satz 1 Alt. 1, Art. 8 Rom I-VO). Auf die Möglichkeit einer konkludenten Rechtswahl kommt es nicht an, da die Parteien in Nr. 23 des Anstellungsvertrags vom 26. Februar 2010 ausdrücklich eine solche getroffen haben. § 4f Abs. 3 Satz 5 BDSG aF ist im Übrigen bereits deshalb anwendbar, weil die Beklagte ein privater Arbeitgeber ist, für den nach dem im internationalen Arbeitsrecht geltenden Territorialitätsprinzip grundsätzlich die nationale Rechtsordnung des Aufnahmestaats gilt (vgl. BVerfG 8. Oktober 1996 – 1 BvL 15/91 – zu B II 1 b der Gründe, BVerfGE 95, 39; BAG 11. Dezember 2007 – 1 ABR 67/06 – Rn. 41, BAGE 125, 122).

b) Die Niederlassung der Beklagten in F gehört als nichtöffentliche Stelle iSv. § 4f Abs. 1 Satz 4 BDSG aF zum Adressatenkreis der Norm.

aa) Gemäß § 2 Abs. 4 Satz 1 BDSG aF sind nicht-öffentliche Stellen natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 der Norm fallen. Letzteres ist bei der Beklagten offenkundig nicht der Fall. Die Aufzählung von natürlichen und juristischen Personen, Gesellschaften und anderen Personenvereinigungen verdeutlicht den Willen des Gesetzgebers, unabhängig von Rechtsform oder Rechtsfähigkeit jede „Stelle" zu erfassen, die personenbezogene Daten verarbeitet (vgl. Simitis, in: Simitis BDSG 8. Aufl. § 2 Rn. 118 ff.; Gola/Schomerus BDSG 12. Aufl. § 2 Rn. 20; ErfK/Franzen 19. Aufl. BDSG § 2 Rn. 2 f.).

bb) Nach Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46/EG (RL 95/46/EG) wendet jeder Mitgliedstaat die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt (zur einheitlich richtlinienkonformen Auslegung auch bei überschießender Umsetzung einer Richtlinie: vgl. EuGH 10. Dezember 2009 – C-323/08 – [Rodriguez Mayor ua.] Rn. 27; BAG 29. Juni 2017 – 2 AZR 597/16 – Rn. 37, BAGE 159, 278). Die Wendung „im Rahmen der Tätigkeiten einer Niederlassung" kann im Hinblick auf das Ziel der Richtlinie, bei der Verarbeitung personenbezogener Daten einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere des Rechts auf Privatleben, zu gewährleisten, nicht eng ausgelegt werden. Voraussetzung ist lediglich die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung (vgl. EuGH 1. Oktober 2015 – C-230/14 – Rn. 24 f., 28 mwN).

cc) Die Niederlassung der Beklagten in F ist eine nicht-öffentliche Stelle im vorbezeichneten Sinn. Sie betreibt eine Bank mit mehreren Mitarbeitern in festen Räumlichkeiten.

c) Zwischen den Parteien ist ein Arbeitsverhältnis iSv. § 4f Abs. 3 Satz 5 BDSG aF begründet worden. Der von der Beklagten erstmals im Revisionsverfahren gehaltene Vortrag, der Kläger sei kein Arbeitnehmer, ist wegen der den Senat nach § 559 Abs. 2 ZPO bindenden entgegenstehenden Feststellung des Landesarbeitsgerichts unbeachtlich.

aa) Der Arbeitnehmerstatus des Klägers steht zwar nicht schon deshalb fest, weil ersichtlich beide Parteien bis zur Entscheidung des Landesarbeitsgerichts vom Bestehen eines Arbeitsverhältnisses ausgegangen sind. Der Senat ist an die übereinstimmende Rechtsauffassung von Parteien nicht gebunden. Die Gerichte können auch zugunsten einer Partei von deren Rechtsmeinung abweichen (BAG 31. Juli 2014 – 2 AZR 422/13 – Rn. 21, BAGE 149, 18).

bb) Die Parteien können aber bestimmte Tatsachen durch allgemein gebräuchliche, einfache rechtliche Ausdrücke in den Rechtsstreit einführen, wenn diese den Teilnehmern des Rechtsverkehrs geläufig sind und das Vorliegen entsprechender tatsächlicher Umstände mit ihnen in Verbindung gebracht wird. Die Parteien lösen auch auf diese Weise eine Erklärungspflicht der Gegenseite gemäß § 138 Abs. 2 ZPO aus (BAG 6. November 2007 – 1 AZR 862/06 – Rn. 13, BAGE 124, 323; vgl. BGH 19. März 2004 – V ZR 104/03 – zu II 1 aa der Gründe, BGHZ 158, 295). Im Gebrauch des betreffenden Rechtsbegriffs durch das Landesarbeitsgericht kann dann die komprimierte Feststellung der mit ihm regelmäßig verbundenen Tatsachen iSv. § 559 Abs. 2 ZPO zu erblicken sein (BAG 31. Juli 2014 – 2 AZR 422/13 – Rn. 22, BAGE 149, 18).

cc) Das Landesarbeitsgericht hat im Tatbestand und in den Entscheidungsgründen des angefochtenen Urteils mehrfach das Vertragsverhältnis der Parteien als „Arbeitsverhältnis" sowie den Kläger als „Arbeitnehmer" bezeichnet. Es handelt sich hierbei um einfache Rechtsbegriffe und damit um Rechtstatsachen (zum Begriff „Arbeitsverhältnis" vgl. BAG 26. Juni 2019 – 5 AZR 178/18 – Rn. 19 f.). Der Kläger hat den Ausdruck „Arbeitnehmer" zur Beschreibung seines Rechtsstatus auch in einem tatsächlichen Sinn gebraucht, indem er vor einem Arbeitsgericht den Sonderkündigungsschutz für Arbeitnehmer nach § 4f Abs. 3 Satz 5 BDSG aF in Anspruch genommen und zudem die Rüge fehlender sozialer Rechtfertigung der Kündigung erhoben hat, die nur für Arbeitnehmer in einem Arbeitsverhältnis erfolgversprechend ist. Die Beklagte ist dem vorinstanzlich nicht entgegengetreten. Das Nichtbestreiten von Rechtstatsachen hat die Geständnisfiktion des § 138 Abs. 3 ZPO zur Folge (BAG 16. Dezember 2010 – 6 AZR 487/09 – Rn. 38, BAGE 136, 340).

dd) In dem Hinweis der Beklagten auf das Fehlen konkreter Feststellungen liegt keine zulässige Verfahrensrüge iSv. § 551 Abs. 3 Nr. 2 Buchst. b ZPO. Die Beklagte bezeichnet kein tatsächliches Verhalten des Landesarbeitsgerichts, das einen Verfahrensmangel ergäbe (vgl. BAG 6. November 2007 – 1 AZR 862/06 – Rn. 14, BAGE 124, 323).

ee) Darüber hinaus haben die Parteien im schriftlichen Anstellungsvertrag vom 26. Februar 2010 ihr Vertragsverhältnis mehrfach als „Arbeitsverhältnis" und den Kläger als „Arbeitnehmer" bezeichnet sowie in Nr. 2 des Vertrags ein Recht der Beklagten vereinbart, dem Kläger ggf. auch eine andere angemessene Tätigkeit zuzuweisen. Schon deshalb ist der Kläger als Arbeitnehmer anzusehen (vgl. BAG 25. Januar 2007 – 5 AZB 49/06 – Rn. 12; 21. April 2005 – 2 AZR 125/04 – zu II 2 c der Gründe).

d) Die Beklagte bestellte den Kläger mit Schreiben vom 1. Juni 2010 in der von § 4f Abs. 1 Satz 1 BDSG aF gebotenen Form (vgl.

BAG 27. Juli 2017 – 2 AZR 812/16 – Rn. 19, BAGE 160, 1) zum Beauftragten für den Datenschutz.

e) Die Wirksamkeit der Bestellung des Klägers wird nicht durch seine bereits zuvor erfolgte Bestellung zum Geschäftsleiter nach § 53 Abs. 2 Nr. 1 KWG in Frage gestellt. Die Feststellung des Landesarbeitsgerichts, der Kläger habe aufgrund eines Interessenkonflikts nicht die nach § 4f Abs. 2 Satz 1 BDSG aF erforderliche Zuverlässigkeit, ist zwar revisionsrechtlich nicht zu beanstanden. Eine Nichtigkeit der Bestellung folgt daraus aber nicht.

aa) Die Zuverlässigkeit eines Beauftragten für den Datenschutz kann in Frage stehen, wenn Interessenkonflikte drohen. Eine Überschneidung von Interessensphären kann die von § 4f Abs. 2 Satz 1 BDSG aF geforderte Zuverlässigkeit beeinträchtigen. Mit der Stellung und Funktion des Datenschutzbeauftragten ist es nicht zu vereinbaren, wenn er in erster Linie seine eigene Tätigkeit kontrollieren muss (vgl. BAG 23. März 2011 – 10 AZR 562/09 – Rn. 24; 22. März 1994 – 1 ABR 51/93 – zu B IV der Gründe, BAGE 76, 184). Das Landesarbeitsgericht hat einen solchen Interessenkonflikt im Fall des Klägers festgestellt.

bb) Aus der fehlenden Zuverlässigkeit einer zum Beauftragten für den Datenschutz bestellten Person folgt nach dem BDSG aF indes nicht die Nichtigkeit der Bestellung. Das Gesetz ordnet diese Rechtsfolge nicht selbst an (zur Unergiebigkeit der Formulierung „darf nicht" für die Frage nach der Nichtigkeitsfolge: vgl. BGH 30. April 1992 – III ZR 151/91 – zu II 3 b der Gründe, BGHZ 118, 142; Palandt/Ellenberger 78. Aufl. § 134 Rn. 6a). Es kann offenbleiben, ob es sich bei § 4f Abs. 2 Satz 1 BDSG aF um ein Verbotsgesetz iSv. § 134 BGB handelt. Ebenso wenig bedarf der Entscheidung, ob selbst bei Annahme einer Verbotsgesetzeigenschaft des § 4f Abs. 2 Satz 1 BDSG aF schon deshalb gemäß § 134 Halbs. 2 BGB nicht die Nichtigkeit der Bestellung die Folge ist, weil es sich um ein ausschließlich einseitig gegen die datenverarbeitende Stelle gerichtetes Verbot handelt (zu einseitigen Verbotsgesetzen: vgl. BGH 12. Mai 2011 – III ZR 107/10 – Rn. 12; Palandt/Ellenberger 78. Aufl. § 134 Rn. 9). Jedenfalls ergibt die systematische Auslegung, dass der Gesetzgeber keine Nichtigkeit der Bestellung des Beauftragten für den Datenschutz im Fall fehlender Zuverlässigkeit iSv. § 4f Abs. 2 Satz 1 BDSG aF anordnen wollte. Es bliebe ansonsten nur ein erheblich verringerter Anwendungsbereich für den in § 4f Abs. 3 Satz 4 BDSG aF vorgesehenen Widerruf der Bestellung, und das Recht der Aufsichtsbehörde, eine Abberufung wegen fehlender Zuverlässigkeit zu verlangen (§ 38 Abs. 5 Satz 3 BDSG aF), liefe im Wesentlichen ins Leere (vgl. Gola/Schomerus BDSG 12. Aufl. § 4f Rn. 29b).

cc) Ob etwas anderes gelten kann, wenn die Bestellung eines Beauftragten für den Datenschutz an einem so schwerwiegenden und offenkundigen Fehler leidet, dass sie ihre Unwirksamkeit „auf der Stirn geschrieben" trägt (zu diesem Maßstab für die Nichtigkeit der Wahl der Vertrauensperson der schwerbehinderten Menschen vgl. BAG 25. Oktober 2017 – 7 ABR 2/16 – Rn. 15), bedarf vorliegend keiner Entscheidung. Ein solcher Fall liegt hier nicht vor.

f) Der Kläger wurde als verpflichtender Beauftragter für den Datenschutz iSv. § 4f Abs. 1 Satz 4 BDSG aF bestellt und zählte zu den nach § 4f Abs. 3 Satz 5 BDSG aF geschützten Personen. Zum Zeitpunkt seiner Bestellung beschäftigte die Beklagte in der Regel mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten.

aa) Mit der Voraussetzung, dass ein Beauftragter „nach Abs. 1 … zu bestellen (ist)", knüpft § 4f Abs. 3 Satz 5 BDSG aF nach dem eindeutigen Gesetzeswortlaut an die grundsätzliche (allgemeine) Bestellpflicht der verantwortlichen Stelle nach § 4f Abs. 1 BDSG aF an (BAG 27. Juli 2017 – 2 AZR 812/16 – Rn. 13, BAGE 160, 1).

bb) Zum Zeitpunkt der Bestellung des Klägers zum Beauftragten für den Datenschutz am 1. Juni 2010 bestand für die Beklagte die Pflicht zu einer solchen Bestellung. Das Landesarbeitsgericht hat mit bindender Wirkung für den Senat gemäß § 559 Abs. 2 ZPO festgestellt, dass im Zeitpunkt der Bestellung der Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF von in der Regel neun Personen überschritten und er damit nicht ein bloß „freiwilliger" Beauftragter für den Datenschutz war.

(1) Da § 4f Abs. 1 Satz 4 BDSG aF auf die „in der Regel" ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen abstellt, kommt es für die Größe der nichtöffentlichen Stelle nicht auf die zufällige tatsächliche Anzahl der Beschäftigten im Zeitpunkt der Bestellung an. Maßgebend ist die Beschäftigungslage, die im Allgemeinen für die Stelle kennzeichnend ist. Zur Feststellung der regelmäßigen Beschäftigtenzahl bedarf es deshalb eines Rückblicks auf die bisherige personelle Stärke der Stelle und einer Einschätzung ihrer zukünftigen Entwicklung; Zeiten außergewöhnlich hohen oder niedrigen Verarbeitungsanfalls sind dabei nicht zu berücksichtigen (zu § 23 Abs. 1 Satz 3 KSchG vgl. BAG 24. Januar 2013 – 2 AZR 140/12 – Rn. 24, BAGE 144, 222; zu § 38 Abs. 1 Satz 1 BetrVG vgl. BAG 2. August 2017 – 7 ABR 51/15 – Rn. 25).

(2) Beim Begriff der „in der Regel" Beschäftigten handelt es sich um einen unbestimmten Rechtsbegriff. Die revisionsgerichtliche Kontrolle seiner Anwendung ist eingeschränkt. Das Revisionsgericht kann nur prüfen, ob das Berufungsgericht den unbestimmten Rechtsbegriff richtig erkannt, bei der Subsumtion des Einzelfalls beibehalten, nicht gegen Denkgesetze und allgemeine Erfahrungssätze verstoßen und alle erheblichen Umstände berücksichtigt hat (vgl. BAG 24. Februar 2005 – 2 AZR 207/04 – zu B III 3 der Gründe).

(3) Nach diesen Grundsätzen ist die Feststellung des Landesarbeitsgerichts, die Beklagte habe zum Zeitpunkt der Bestellung des Klägers zum Beauftragten für den Datenschutz am 1. Juni 2010 in ihrer Niederlassung in F in der Regel mehr als neun Personen iSv. § 4f Abs. 1 Satz 4 BDSG aF beschäftigt, revisionsrechtlich nicht zu beanstanden. Das Berufungsgericht ist zutreffend davon ausgegangen, dass maßgeblich die für die Stelle im Allgemeinen oder typischerweise kennzeichnende Anzahl der mit automatisierter Datenverarbeitung ständig beschäftigten Personen ist. Vor diesem Hintergrund hat es nicht allein auf die im Zeitpunkt der Bestellung des Klägers beschäftigten neun Personen abgestellt, sondern die vom Arbeitgeber vorgesehene Beschäftigtenzahl im September 2009 und die tatsächliche Beschäftigtenzahl im September 2010 in seine Betrachtungen eingestellt. Revisionsrechtlich erhebliche Fehler hat die Beklagte diesbezüglich nicht aufgezeigt. Soweit sie in der Revisionsbegründung neuen Vortrag zum Wegfall und zu der Besetzung bestimmter Stellen hält, kann das nach § 559 Abs. 1 ZPO nicht berücksichtigt werden.

2. Das Landesarbeitsgericht hat rechtsfehlerhaft angenommen, die gegenüber dem Kläger ausgesprochenen ordentlichen Kündigungen seien nach § 4f Abs. 3 Satz 5 BDSG aF unzulässig und damit nach § 134 BGB nichtig, obwohl die Beklagte bei Zugang der Kündigungen in ihrer Niederlassung nicht in der Regel mehr als neun Personen iSv. § 4f Abs. 1 Satz 4 BDSG aF beschäftigte.

a) Die Feststellung des Berufungsgerichts, die Beklagte habe zum Zeitpunkt des Zugangs der Kündigungen in ihrer Niederlassung in F in der Regel nicht mehr als neun Personen iSv. § 4f Abs. 1 Satz 4 BDSG aF beschäftigt, ist revisionsrechtlich nicht zu beanstanden.

b) Ein Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF während der Tätigkeit als Beauftragter für den Datenschutz führt dazu, dass dessen Sonderkündigungsschutz nach § 4f Abs. 3 Satz 5 BDSG aF entfällt, ohne dass es eines Widerrufs der Bestellung durch den Arbeitgeber bedarf. Das folgt aus der Auslegung der Norm.

aa) Der Wortlaut der Regelung spricht stark für die Annahme, dass ein Sonderkündigungsschutz nur besteht, wenn im Zeitpunkt des Zugangs der Kündigung die Voraussetzungen für die verpflichtende Bestellung eines Beauftragten für den Datenschutz vorliegen.

§ 4f Abs. 3 Satz 5 BDSG aF knüpft nicht vergangenheitsbezogen an die ursprüngliche Bestellung an, sondern an eine gegenwärtige Pflicht zur Bestellung („Ist nach Abs. 1 ein Beauftragter für den Datenschutz zu bestellen“).

´bb) Für dieses Verständnis spricht auch die sich aus der Gesetzesbegründung ergebende gesetzesübergreifende Systematik.

´(1) Maßgebliche Beurteilungsgrundlage für die Rechtmäßigkeit einer Kündigung sind die objektiven Verhältnisse im Zeitpunkt des Zugangs der Kündigungserklärung (für die soziale Rechtfertigung vgl. BAG 24. März 2011 – 2 AZR 790/09 – Rn. 17). Das gilt auch für die Frage, ob Sonderkündigungsschutz besteht (für § 15 Abs. 1 Satz 1 KSchG iVm. § 103 Abs. 1 BetrVG vgl. BAG 27. September 2012 – 2 AZR 955/11 – Rn. 20).

(2) Der Gesetzgeber hat sich bei der Einführung des Sonderkündigungsschutzes in § 4f BDSG aF ausdrücklich darauf bezogen, dass Abs. 3 Satz 5 der Norm den Kündigungsschutz für den Datenschutzbeauftragten an denjenigen für vergleichbare Funktionsträger wie Betriebsratsmitglieder nach § 15 Abs. 1 Satz 1 und Satz 2 KSchG anpasst (vgl. BT-Drs. 16/12011 S. 30). Das spricht für die Übertragbarkeit entsprechender Wertungen.

(a) Das Amt des Betriebsrats endet, wenn die Zahl der ständig beschäftigten Arbeitnehmer des Betriebs nicht nur vorübergehend auf unter fünf Arbeitnehmer absinkt und damit die Voraussetzungen für die Bildung eines Betriebsrats entfallen (BAG 7. April 2004 – 7 ABR 41/03 – zu B II 1 b der Gründe mwN, BAGE 110, 159; ErfK/Koch 19. Aufl. BetrVG § 1 Rn. 21; Fitting 29. Aufl. § 1 Rn. 269; KR/Rinck 12. Aufl. § 103 BetrVG Rn. 27; Richardi/Maschmann, in: Maschmann BetrVG 16. Aufl. § 1 Rn. 143).

(b) Der besondere Kündigungsschutz nach § 15 Abs. 1 Satz 1 KSchG besteht nur während der Amtszeit des Betriebsrats (APS/Linck 5. Aufl. KSchG § 15 Rn. 75; ErfK/Kiel 19. Aufl. KSchG § 15 Rn. 18; LSSW/Wertheimer 11. Aufl. § 15 Rn. 15 f.). Der Begriff „Beendigung der Amtszeit“ in § 15 Abs. 1 Satz 2 KSchG erfasst alle Fälle, in denen das Gesetz ihn ausdrücklich verwendet (zB in § 21 BetrVG) und in denen sich entweder aus dem Gesetz selbst oder aus allgemeinen Rechtsgrundsätzen ergibt, dass das betreffende Gremium die ihm obliegenden Aufgaben auf Dauer nicht mehr wahrnehmen darf (KR/Kreft 12. Aufl. § 15 KSchG Rn. 79). Mit dem Ende der Amtszeit beginnt der nachwirkende Kündigungsschutz des § 15 Abs. 1 Satz 2 KSchG (LKB/Bayreuther 16. Aufl. § 15 Rn. 65). Das ist beispielsweise der Fall, wenn die Zahl der wahlberechtigten Personen unter fünf sinkt (ErfK/Kiel 19. Aufl. KSchG § 15 Rn. 32).

(3) Da der Gesetzgeber den besonderen Kündigungsschutz des § 4f Abs. 3 Satz 5 BDSG aF an den des § 15 Abs. 1 Satz 1 KSchG „anpassen“ wollte, ist es folgerichtig, dass auch beim Beauftragten für den Datenschutz der Sonderkündigungsschutz mit Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF endet und der nachwirkende Kündigungsschutz des § 4f Abs. 3 Satz 6 BDSG aF beginnt. Es gibt gesetzessystematisch keinen Anlass, bei der dem Sonderkündigungsschutz für Mitglieder des Betriebsrats nachgebildeten kündigungsrechtlichen Regelung andere Maßstäbe anzulegen. Zwar beruht das Betriebsratsamt nicht auf einer Bestellung durch den Arbeitgeber. Es gibt aber auch keine mit § 18 Abs. 3 BetrVG vergleichbare zwingende Publizität, ob der Beauftragte für den Datenschutz verpflichtend oder freiwillig bestellt ist. Für die Beendigung des Amts des verpflichtend bestellten Beauftragten für den Datenschutz bedarf es nicht zwingend eines Widerrufs der Bestellung (zum Fall der Fusion zweier Krankenkassen vgl. BAG 29. September 2010 – 10 AZR 588/09 – Rn. 23 und Rn. 27, BAGE 135, 327; so auch Simitis, in: Simitis BDSG 8. Aufl. § 4f Rn. 200; ausdrücklich für den Fall des Absinkens unter den Schwellenwert: Gola/Schomerus BDSG 12. Aufl. § 4f Rn. 45a; wohl auch Gehlhaar NZA 2010, 373; aA Taeger/Gabel/Scheja § 4f BDSG Rn. 53; Auernhammer/Raum BDSG 4. Aufl. § 4f Rn. 150 f.; mit einer Einschränkung für den Fall, dass die Voraussetzungen der Bestellpflicht offenkundig nicht mehr vorliegen: Däubler, in: Däubler/Klebe/Wedde/Weichert BDSG 5. Aufl. § 4f Rn. 64; unentschieden zur Frage des Widerrufserfordernisses v. d. Bussche in Plath BDSG/DS-GVO 2. Aufl. § 4f Rn. 67).

cc) Sinn und Zweck der gesetzlichen Regelung stehen dieser Lesart nicht entgegen.

(1) Durch die im Jahr 2009 erfolgte Änderung des § 4f BDSG aF sollte die Position des Beauftragten für den Datenschutz gestärkt werden, insbesondere durch den besonderen und nachwirkenden Kündigungsschutz in § 4f Abs. 3 Satz 5 und Satz 6 BDSG aF (BT-Drs. 16/12011 S. 30). Die Änderung bezog sich nach der Gesetzesbegründung ausdrücklich nur auf den nach § 4f Abs. 1 BDSG aF verpflichtend bestellten Beauftragten für den Datenschutz, nicht auf einen freiwillig bestellten Beauftragten, da dies die Stellen davon abhalten könne, auch freiwillig Beauftragte zu bestellen, was ein ungewolltes Ergebnis wäre. Könnte der Arbeitgeber bei einem Absinken der Beschäftigtenzahl unter den Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF nur durch einen Widerruf der Bestellung ein Fortbestehen des Sonderkündigungsschutzes nach § 4f Abs. 3 Satz 5 BDSG aF vermeiden, führte dies zu dem gesetzgeberisch nicht gewollten Anreiz, damit zugleich das Fortbestehen der Bestellung auf freiwilliger Basis zu beenden.

(2) Wenn keine Verpflichtung mehr zur Bestellung eines Beauftragten für den Datenschutz besteht, bedarf es außerdem nicht mehr des Schutzes der Unabhängigkeit seiner Stellung. Der Schutz des § 4f Abs. 3 Satz 5 BDSG aF erfolgt vorrangig im Interesse eines effektiven Datenschutzes. Der Beauftragte für den Datenschutz soll in die Lage versetzt werden, seine sich aus § 4g BDSG aF ergebenden Aufgaben und Befugnisse selbstbewusst gegenüber dem Arbeitgeber durchzuführen und einzufordern. Dadurch soll seine Unabhängigkeit gestärkt werden. Wenn ihm diese gesetzlichen Befugnisse nicht mehr zustehen, bedarf es dieses besonderen Schutzes seiner Unabhängigkeit nicht mehr. Der persönliche Schutz des Funktionsträgers wird ausreichend über den nachwirkenden Kündigungsschutz gemäß § 4f Abs. 3 Satz 6 BDSG aF gewährleistet. Das Benachteiligungsverbot des § 4f Abs. 3 Satz 3 BDSG aF und das Maßregelungsverbot des § 612a BGB ergänzen diesen Schutz.

dd) Probleme bei der Bestimmung des genauen Zeitpunkts, ab dem der Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF unterschritten ist, haben bei der Auslegung, die allerdings auch zu praktikablen Ergebnissen führen soll, kein ausschlaggebendes Gewicht.

(1) Es kommt auf die Zahl der „in der Regel“ mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen an, so dass kurzfristige Schwankungen ohnehin nicht von Bedeutung sind. Probleme bei der Feststellung des Unterschreitens eines Schwellenwerts kann es im Übrigen ebenso bei § 23 Abs. 1 KSchG, § 1 Abs. 1 BetrVG oder § 5 Abs. 1 iVm. § 3 Abs. 1 PflegeZG geben. Der Beauftragte für den Datenschutz wird dabei sogar weniger als Arbeitnehmer in den vorgenannten Fällen im Ungewissen über die Zahl der in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen sein, da dies seinen eigenen Aufgabenbereich und der Schwellenwert eine überschaubare Beschäftigtenzahl betrifft.

(2) Der vorliegende Fall gibt keinen Anlass zur Entscheidung, ob der Beauftragte wieder als verpflichtend bestellter Beauftragter iSv. § 4f Abs. 3 Satz 5 BDSG aF anzusehen ist, wenn der Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF zunächst – ggf. von den Beteiligten unerkannt – unterschritten und später erneut überschritten wird (vgl. Gehlhaar NZA 2010, 373). Dafür könnte sprechen, dass der Gesetzgeber zwischen dem Oberbegriff „Abberufung“ (vgl. § 4f Abs. 3 Satz 6 BDSG aF) und dem „Widerruf der Bestellung“ (vgl. § 4f Abs. 3 Satz 4 BDSG aF) unterscheidet. Solange der Arbeitgeber die Bestellung des Beauftragten nicht widerruft, hinderte auch nicht das Schriftformerfordernis des § 4f Abs. 1 Satz 1 BDSG aF ein erneutes Einrücken in die zuvor übertragene Funktion eines verpflichtend bestellten Beauftragten für den Datenschutz.

ee) Endet durch ein Unterschreiten des Schwellenwerts des § 4f Abs. 1 Satz 4 BDSG aF die Funktion als verpflichtender Beauftragter für den Datenschutz, beginnt der nachwirkende Sonderkündigungsschutz des § 4f Abs. 3 Satz 6 BDSG aF. Es handelt sich auch insoweit um eine Abberufung im Sinne der Bestimmung (vgl. APS/Greiner 5. Aufl. BDSG § 4f Rn. 17). Der Begriff der „Abberufung" in § 4f Abs. 3 Satz 6 BDSG aF umfasst „jede Beendigung des Amtes, die durch ein Verhalten der verantwortlichen Stelle veranlasst wurde" (BAG 27. Juli 2017 – 2 AZR 812/16 – Rn. 25, BAGE 160, 1). Darunter fällt auch das Absinken der Beschäftigtenzahl aufgrund von Personalentscheidungen des Arbeitgebers.

III. Der Senat kann nicht selbst entscheiden, ob die Kündigungen wirksam sind (§ 563 Abs. 3 ZPO). Dem Kläger könnte ein nachwirkender Kündigungsschutz nach § 4f Abs. 3 Satz 6 BDSG aF zustehen. Zur Frage, wann der Schwellenwert des § 4f Abs. 1 Satz 4 BDSG aF nicht mehr überschritten war, hat das Landesarbeitsgericht keine ausreichenden Feststellungen getroffen. Es hat nur ausgeführt, dass zu einem Zeitpunkt zwischen dem 1. Oktober 2015 und dem 30. November 2016 die Beschäftigtenzahl der Beklagten auf neun gesunken sei und sich ab Januar 2017 auf acht Beschäftigte weiter reduziert habe. Ob zum Zeitpunkt des Zugangs der Kündigungen am 12. April 2017 die Jahresfrist des § 4f Abs. 3 Satz 6 BDSG aF abgelaufen war, lässt sich den Feststellungen nicht entnehmen.

IV. Der Rechtsstreit ist an das Landesarbeitsgericht zurückzuverweisen (§ 563 Abs. 1 Satz 1 ZPO), damit es die erforderlichen Feststellungen zum Zeitpunkt des Unterschreitens des Schwellenwerts des § 4f Abs. 1 Satz 4 BDSG aF trifft. Sollte das Landesarbeitsgericht zu dem Ergebnis kommen, dem Kläger habe wegen Zeitablaufs kein nachwirkender Sonderkündigungsschutz nach § 4f Abs. 3 Satz 6 BDSG aF zugestanden, wird es sich insbesondere mit dessen Rüge einer Unwirksamkeit der Kündigung wegen Verstoßes gegen das Willkürverbot auseinanderzusetzen haben. Hierauf ist es bislang – aus seiner Sicht konsequent – nicht eingegangen. Ferner wird das Berufungsgericht aufzuklären haben, welches Verhältnis die beiden Kündigungen vom 12. April 2017 zueinander haben. Nach der Senatsrechtsprechung können mehrere vom Arbeitgeber zu unterschiedlichen Zeitpunkten ausgesprochene Kündigungen in einem Hilfsverhältnis zueinander stehen, dh. die weitere Kündigung kann nur für den Fall ausgesprochen sein, dass sich nicht schon die frühere Kündigung als wirksam erweist (vgl. BAG 18. Juni 2015 – 2 AZR 480/14 – Rn. 15, BAGE 152, 47). Die Beklagte hat zwar die Kündigung zum 31. Juli 2017 ausdrücklich auf die gesetzliche und die Kündigung zum 30. September 2017 auf die vertragliche Kündigungsfrist bezogen, gleichzeitig aber jeweils „hilfsweise zum nächstzulässigen Termin" gekündigt.

Kein Anspruch auf Zugang zu Informationen über Aufsichtsmaßnahmen bei Tiertransporten (Ls)

(**Bundesverwaltungsgericht**, Urteil vom 30. Januar 2020 – 10 C 11.19 –)

1. **Ein Anspruch auf Zugang zu Informationen über behauptete Verstöße gegen tierschutzrechtliche Bestimmungen besteht weder nach dem Umweltinformationsrecht noch nach dem Verbraucherinformationsgesetz.**
2. **Bei den Informationen handelt es sich nicht um Umweltinformationen im Sinne des Umweltinformationsrechts. Das Merkmal der Umwelt erfasst u.a. Tiere als Teil der natürlichen Lebensräume und die Artenvielfalt, tierschutzrechtliche Belange aber nicht.**
3. **Das Verbraucherinformationsgesetz berücksichtigt Verstöße gegen tierschutzrechtliche Vorschriften ebenfalls nicht. Sein Zweck ist der Verbraucherschutz und nicht der Tierschutz. Ein Informationszugang nach diesem Gesetz wegen Abweichungen vom Lebensmittel- und Futtermittelgesetzbuch scheidet aus, weil lebende Tiere regelmäßig keine Lebensmittel sind.**

(Nicht amtliche Leitsätze)

Beginn der allgemeinen archivrechtlichen Schutzfrist bei Personenakten des Bundesamtes für Verfassungsschutz (Ls)

(**Bundesverwaltungsgericht**, Urteil vom 11. Dezember 2019 – 6 C 21.18 –)

1. **Das einzelne in einer Akte enthaltene Schriftstück ist eine Unterlage im Sinne von § 11 Abs. 6 und § 1 Nr. 9 BArchG.**
2. **Der in § 1 Nr. 5 BArchG genannte Begriff des Vorgangs ist materiell zu bestimmen. Er erfasst einzelne Unterlagen, die als inhaltlich zusammengehörende Teile einer Gesamtakte abgetrennt werden können. Dies gilt auch in Bezug auf die vom Bundesamt für Verfassungsschutz zu einem Beobachtungsobjekt geführten Akten.**
3. **Die allgemeine archivrechtliche Schutzfrist von 30 Jahren nach § 11 Abs. 1 und 6 BArchG beginnt bei den vom Bundesamt für Verfassungsschutz geführten Akten nicht erst mit der letzten inhaltlichen Bearbeitung der Gesamtakte. Wird ein Schriftstück nach inhaltlicher Prüfung ohne weitere Bearbeitungsschritte in die Akte aufgenommen, ist bereits der Zeitpunkt der „zdA"-Verfügung als letzte inhaltliche Bearbeitung der Unterlagen eines Vorgangs im Sinne der Bestimmung des Begriffs der Entstehung in § 1 Nr. 5 BArchG maßgeblich.**

Streitwert bei Auskunftsklagen nach Art. 15 DS-GVO

(**Oberlandesgericht Köln**, Beschluss vom 6. Februar 2020 – 20 W 9/10 –)

1. **Maßgeblich für die Höhe des festzusetzenden Streitwertes ist in Bezug auf den jeweiligen Antrag das "Angreiferinteresse", d.h. dasjenige des Klägers, Widerklägers oder Rechtsmittelführers, der den Antrag anhängig macht, und zwar zur Zeit der Einreichung (§ 4 ZPO).**

2. Der Streitwert einer Auskunftsklage gem. Art. 15 DS-GVO ist angesichts der hierdurch geschützten grundrechtlichen Position bereits dann mit pauschal 5.000 zu bewerten, wenn sich der Kläger durch die erstrebten Auskünfte zumindest auch mittelbare wirtschaftlichen Vorteile verspricht.

(Leitsätze des Einsenders)

Aus den Gründen:

Das Landgericht hat den Streitwert für den Klageantrag zu 1 mit 500,00 € zu gering bewertet. Maßgeblich für die Höhe des festzusetzenden Streitwertes ist in Bezug auf den jeweiligen Antrag das ,,Angreiferinteresse", d. h. des Klägers, Widerklägers oder Rechtsmittelführers, der den Antrag anhängig macht, und zwar zur Zeit der Einreichung (S 4 ZPO). Der vom Landgericht festgesetzte Wert dürfte sich dagegen am lnteresse der Beklagten orientieren, die Vorlagen der begehrten Auskünfte und Belege nicht leisten zu müssen, was sich rechtlich nach dem für die Auskunftserteilung und Belegvorlage erforderlichen Aufwand bemisst.

Der Bedeutung des mit der Klage verfolgten Anspruchs aus Art. 15 DS-GVO und der hierdurch geschützten grundrechtlichen Position der Klägerin wie auch dem Umstand, dass sich die Klägerin im konkreten Fall durch die erstrebten Auskünfte mittelbare wirtschaftlichen Vorteile verspricht, wird nach Einschätzung des Senats eine Festsetzung des Werts auf 5.000,00 € gerecht. (vgl. Beschluss des Senats vom 3.9.2019 -20 W 10/18).

(Eingereicht von RA Dr. Martin Riemer)

Änderung der Nutzungsbedingungen eines sozialen Netzwerks

(**Oberlandesgericht Dresden**, Beschluss vom 19. November 2019 – 4 U 1471/19 –)

1. Die Änderung der Nutzungsbedingungen eines sozialen Netzwerkes kann wirksam durch Anklicken einer Schaltfläche in einem „pop-up"-Fenster erfolgen; ob eine daneben bestehende Änderungsklausel wirksam in den zugrunde liegenden Nutzungsvertrag einbezogen wurde, ist dann ohne Belang. Eine solche Zustimmung ist auch dann nicht als sittenwidrig anzusehen, wenn sie dem Nutzer nur die Alternative lässt, entweder zuzustimmen oder das Nutzungsverhältnis zu beenden.

2. Die Sanktionierung eines Verstoßes gegen das in den Nutzungsbedingungen eines sozialen Netzwerks enthaltene Verbot der „Hassrede" mit einer zeitlich begrenzten Sperre (hier: Versetzung für 30 Tage in den sog. read-only modus) ist in der Regel verhältnismäßig.

Sachverhalt

Der Kläger betreibt auf dem von der Beklagen angebotenen sozialen Netzwerk XXX ein Nutzerkonto. Er nimmt die Beklagte wegen einer behaupteten Sperrung und Löschung der Äußerung „Wo lebst denn du, von den 1300 Kinderehen, Morden, Ehrenmorden, Vergewaltigungen von Goldstücken, Kinderarmut und Altersarmut hast Du noch nichts mitbekommen?" u.a. auf Wiederfreischaltung in Anspruch. Das Landgericht hat den Antrag abgelehnt, weil in der streitgegenständlichen Äußerung eine Hassbotschaft im Sinne der Gemeinschaftsstandards der Beklagten zu sehen sei. Dem tritt der Kläger mit der Berufung entgegen. Die aktuellen Nutzungsbedingungen und Gemeinschaftsstandards der Beklagten seien nicht wirksam in das Nutzungsverhältnis einbezogen worden, weil das ihr eingeräumte Recht, diese Bedingungen einseitig zu ändern, zu unbestimmt und nach § 307 BGB unwirksam sei.

Aus den Gründen

Der Senat beabsichtigt, die zulässige Berufung nach § 522 Abs. 2 ZPO ohne mündliche Verhandlung durch – einstimmig gefassten – Beschluss zurückzuweisen. Die zulässige Berufung des Klägers bietet in der Sache offensichtlich keine Aussicht auf Erfolg. Die Rechtssache hat auch weder grundsätzliche Bedeutung noch erfordert die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts durch Urteil. Auch andere Gründe gebieten eine mündliche Verhandlung nicht. Zu Recht und mit zutreffenden Erwägungen hat das Landgericht die Klage abgewiesen. Die hiergegen gerichteten Berufungsangriffe begründen keine konkreten Zweifel an der Richtigkeit und Vollständigkeit der entscheidungserheblichen Feststellungen (§ 529 Abs. 1 Nr. 1 ZPO) und sind auch in rechtlicher Hinsicht nicht geeignet, das angefochtene Urteil in Zweifel zu ziehen.

Die vom Kläger behaupteten Sanktionen der Beklagten wegen des streitgegenständlichen Posts sind an den Nutzungsbedingungen und Gemeinschaftsstandards der Beklagten in der geänderten Fassung vom 19.04.2018 (Anlagen K 1 und K 3) zu messen. Diese Nutzungsbedingungen sind wirksam in den zwischen den Parteien bestehenden Vertrag einbezogen worden. Es kann in diesem Zusammenhang dahinstehen, ob dies auf der Grundlage der Änderungsklausel in Ziff. 13. der Nutzungsbedingungen (alt) i.V.m. der Zusatzklausel für Deutschland möglich gewesen wäre oder ob diese Klausel gegen § 307 BGB i.V.m. den aus § 308 Nr. 4 und 5 BGB abzuleitenden Wertungen verstößt (in diesem Sinne etwa KG Berlin, Urteil vom 24. Januar 2014 – 5 U 42/12 –, juris). Die geänderten Nutzungsbestimmungen sind hier nämlich ausschließlich aufgrund der Zustimmung des Klägers durch Anklicken der Schaltfläche entsprechend der Anlage B5 wirksam geworden. Die allen Nutzern als „pop-up" bei Aufruf des Dienstes der Beklagten zugegangene Mitteilung über die beabsichtigte Änderung der Nutzungsbedingungen (B3) in Verbindung mit der Aufforderung, die „ich stimme zu"-Schaltfläche anzuklicken, ist dabei als an den einzelnen Nutzer gerichtetes Angebot auf Abschluss eines Änderungsvertrages im Sinne von § 145 BGB zu sehen. Ein durch Anklicken erfolgter Vertragsabschluss hat grundsätzlich individuellen Charakter, auch wenn die Willenserklärungen, aus denen er sich zusammensetzt, vorformulierte Bestandteile besitzen. Die Neufassung der AGB wird in einen solchen Fall nicht aufgrund einer vorformulierten Änderungsklausel, sondern aufgrund eines nach allgemeinen Regeln über Willenserklärungen und Rechtsgeschäfte zwischen den Parteien geschlossenen Änderungsvertrages einbezogen (Münchener Kommentar – Basedow, BGB 8. Aufl. 2019, § 305, Rn 86; 90 m.w.N.; JurisPK -BGB – Lapp, 2. A. § 305, Rz. 57). Daher kommen solche Erklärungen als Gegenstand einer AGB-rechtlichen Prüfung nicht in Betracht (BGH, Urteil vom 07. November 2001 – VIII ZR 13/01 –, Rn. 42 – 43, juris; ebenso BGH, Urteil vom 13. Februar 1985 – IVb ZR

72/83 juris). Ebenso wenig ist für die Wirksamkeit dieser Individualvereinbarung von Belang, dass nach Ziff. 5 der Sonderbedingungen für Nutzer in Deutschland auf einseitige Änderungen der Nutzungsbedingungen durch E-Mail innerhalb einer 30 – Tagesfrist hätte hingewiesen werden müssen, der Kläger eine solche E-Mail jedoch nicht erhalten haben will.

Dieses individuelle Angebot im Sinne des § 145 BGB hat er unstreitig durch Anklicken der Schaltfläche angenommen. Dass in den Anlagen B3 und B4 die „neue Datenschutzgrundverordnung" als Grund für die Änderung benannt und lediglich verklausuliert darauf hingewiesen wird, dass neben der Datenschutzrichtlinie der Beklagten auch die Nutzungsbedingungen von XXX aktualisiert wurden um „zu erklären, ... was wir von allen Nutzern erwarten", steht einer wirksamen Annahme dieser Nutzungsbedingungen, die über den am Ende der Anlage B3 eingebetteten Link Bestandteil des Angebots der Beklagten auf Abschluss eines Änderungsvertrages geworden sind, nicht entgegen. Ob der Kläger seine Annahmeerklärung wegen eines Inhaltsirrtums nach § 119 BGB hätte anfechten können, bedarf hier keiner Entscheidung. Eine solche Anfechtung hat er unstreitig nicht erklärt, auf einen Willensmangel hat er sich nicht berufen. Entgegen der Auffassung des Klägers ist das ihm durch die Anlagen B3/B4 aufgezwungene Angebot, entweder die Nutzungsbedingungen zu akzeptieren oder seinen Vertrag mit der Beklagten zu beenden, auch nicht als sittenwidrig anzusehen. Auch wenn die Beklagte im Bereich der sozialen Netzwerke in Deutschland eine überragend wichtige Stellung einnimmt (vgl. Senat, Beschluss vom 08. August 2018 – 4 W 577/18 –, Rn. 24, juris), unterliegt sie zum einem keinem Kontrahierungszwang, sondern ist bei der Auswahl ihrer Vertragspartner im Rahmen allgemeiner Diskriminierungsverbote frei. Zum anderen ist aber auch nicht ersichtlich, weshalb die Annahme der geänderten Bedingungen für den Kläger so unzumutbar sein sollte, dass eine de-facto erzwungene Zustimmung als sittenwidrig anzusehen sein sollte. Die mit der Änderung erfolgte Präzisierung u.a. des Begriffes der Hassrede und des bei Verstößen geltenden Sanktionsregimes begünstigt im Gegenteil die Nutzer, weil sie das zuvor bestehende uferlose und damit rechtlich bedenkliche (vgl. hierzu OLG München, Beschluss vom 17.7.2018 – 18 W 858/18) Sanktionsermessen auf eine AGB- rechtlich unbedenkliche (vgl. hierzu Senat, Beschluss vom 8.8.2018 – 4 W 577/18 – juris) Form zurückführt. Aus welchen Gründen er sich durch die von ihm beklagte „Friss-oder-Stirb-Auswahl" in einer rechtswidrigen Zwangslage befunden haben will, trägt auch der Kläger nicht vor. Es ist daher – soweit ersichtlich – in der Rechtsprechung auch allgemein anerkannt, dass die Änderungen der Nutzungsbedingungen durch die derzeit geltende Fassung keinen Bedenken unterliegen (vgl. OLG Karlsruhe, Beschluss vom 18.12.2018 – 7 W 66/18; LG Bremen, Urteil vom 20. Juni 2019 – 7 O 1618/18 –, juris; so auch Kaufhold, IWRZ 2019, 38ff. dort Nr. 3).

Dass sich das Verbot von Hassrede in Ziff. 12 der Gemeinschaftsstandards auf die Meinungsfreiheit der Nutzer auswirkt, jedoch weder eine überraschende Klausel im Sinne des § 305c BGB noch eine unangemessene Benachteiligung der Nutzer im Sinne des § 307 BGB darstellt, hat der Senat in der Entscheidung vom 8. August 2018, auf die sich auch das Landgericht bezogen hat (Beschluss vom 08. August 2018 – 4 W 577/18 –, Rn. 22, juris), näher ausgeführt. Hieran ist auch im Anschluss an die Berufungsbegründung, die insofern keine neuen Gesichtspunkte aufzeigt, festzuhalten. Zur Vermeidung von Wiederholungen nimmt der Senat insbesondere auf die Rz 20 bis 25 dieser Entscheidung bei juris Bezug. Die Auffassung des Klägers, jeder Mensch dürfe „hassen und hetzen", solange er dabei keine Straftatbestände verwirkliche (Berufungsbegründung, S. 23), trifft schon für das allgemeine Äußerungsrecht nicht zu. Für die hier in Rede stehende Frage, unter welchen Bedingungen der Betreiber eines sozialen Netzwerkes unter Bezug auf seine AGB Meinungsäußerungen löschen und Nutzer sperren darf, verkennt sie die anzuwendenden Maßstäbe grundlegend. Sie wird in der obergerichtlichen Rechtsprechung so auch nirgends vertreten (OLG Karlsruhe, Beschl. v. 28.02.2019 – 6 W 81/18 – Leitsatz 2; Beschl. v. 25.06.2018 – 15 W 86/18 – juris Rn. 21; OLG Stuttgart, Beschl. v. 06.09.2018 – 4 W 63/18 – Rn. 74). Der Entscheidung des OLG München vom 17.7.2018 (18 W 858/18), die der Kläger für seine Auffassung in Anspruch nimmt, lässt sich dies in dieser Schärfe ebenfalls nicht entnehmen. Das OLG München betont dort vielmehr ausdrücklich – ebenso wie der Senat – das Gebot der praktischen Konkordanz, die Entscheidung ist zudem noch zu den alten Nutzungsbedingungen der Beklagten ergangen. In einer neueren als Anlage B 19 vorgelegten Entscheidung hat das OLG München überdies klargestellt, dass es gerade nicht der Auffassung ist, die Gemeinschaftsstandards und Nutzungsbedingungen müssten gewährleisten, dass Beiträge, die vom Grundrecht der Meinungsfreiheit gedeckt seien, in keinem Fall von der Kommunikationsplattform der Beklagten entfernt werden dürften (Beschluss vom 30.11.2018, 24 W 1771/18, dort S. 7). Dies lässt sich auch dem Beschluss des Kammergerichts vom 22.3.2019 (10 W 172/18 – juris) nicht entnehmen. Das Kammergericht hat dort vielmehr ausdrücklich offengelassen, ob die Gemeinschaftsstandards von ZZZ, soweit sie „hasserfüllten Inhalt" sanktionieren, mit § 307 BGB vereinbar sind und hat im Übrigen lediglich ausgeführt, diese müssten einen „zulässigen Inhalt" haben, ohne indes die Anforderungen an diesen Inhalt näher zu umreißen. Grundsätzliche Bedeutung dieser Frage im Sinne des § 522 Abs. 2 Nr. 2 ZPO, die einer Entscheidung nach § 522 Abs. 2 ZPO entgegenstünde und die Zulassung der Revision geböte, sieht der Senat nach alledem nicht.

Der streitgegenständliche Post beinhaltet Hassrede im Sinne von Nr. 12 der Gemeinschaftsstandards, wie das Landgericht zutreffend ausgeführt hat. Zur Vermeidung von Wiederholungen nimmt der Senat auf die Gründe der angegriffenen Entscheidung, dort insbesondere Seiten 12 und 13, Bezug.

Die Auffassung des Klägers, das Landgericht habe die Äußerung „Wo lebst denn du, von den 1300 Kinderehen, Morden, Ehrenmorden, Vergewaltigungen von Goldstücken, Kinderarmut und Altersarmut hast Du noch nichts mitbekommen?" hierbei in nicht mehr vertretbarer Weise ausgelegt und sei erst aufgrund dessen zu einem „Angriff auf Personen aufgrund geschützter Eigenschaften" gelangt, teilt der Senat nicht. Sie beruht ersichtlich darauf, dass der Kläger den Begriff der Hassrede auf Angriffe gegen eine bestimmte Person verengt, während Ziff. 12 der Gemeinschaftsstandards hierunter bereits jede Art von „entmenschlichender" Sprache in Bezug auf eine konkrete Personengruppe fasst. Dass die streitgegenständliche Äußerung sich gegen die Gruppe der verächtlich als „Goldstücke" titulierten Asylbewerber richtet, lässt der Kläger gegen sich gelten, auch wenn er nachträglich seine Äußerung nur auf Personen bezogen haben will, die „als Flüchtlinge nach Deutschland kommen und hier gegen Strafvorschriften verstoßen und teilweise.. grausame Gewalttaten begehen". Diese Unterscheidung findet jedoch im Wortlaut und Sinnzusammenhang des Posts, bei dem es sich um eine Stellungnahme zur „Einwanderungs- und Flüchtlingspolitik" handeln soll, keine Stütze. Trotz des fehler-

haften Gebrauchs der Präposition „von“ kann der Satz nur so verstanden werden, dass „Goldstücke“ für die aufgeführten Straftaten verantwortlich gemacht werden. Da sich dieser Begriff in der rechten Szene aus der Verdrehung eines Zitats des ehemaligen YYY-Vorsitzenden und Kanzlerkandidaten M... S... entwickelt hat, das sich auf die seit 2015 nach Deutschland eingereisten Flüchtlinge in ihrer Gesamtheit bezieht (vgl. auch https://www.spiegel.de/netzwelt/web/rechte-sprache-deutschrechts-rechts-deutsch-a-1221185.html; LG Bremen Urteil vom 20. Juni 2019 – – 7 O 1618/18 – –, juris), wird der Durchschnittsempfänger, dem dieser szenetypische Sprachgebrauch geläufig ist und der zur Kenntnis nimmt, dass der Kläger damit auf den Kommentar eines anderen Nutzers (“Mit Merkel geht es den Menschen hier in Deutschland noch nie so gut wie jetzt.“) reagiert hat, dem Post auch nicht lediglich entnehmen, dass der Kläger eine „Ablehnungshaltung gegenüber straffälligen Ausländern“ einnimmt. Die Einleitung „wo lebst denn du“ verdeutlicht vielmehr, dass der Kläger die Auffassung des Nutzers, auf den er Bezug nimmt, nicht teilt, sondern der Meinung ist, dass sich die Situation in Deutschland seit 2005 allgemein verschlechtert habe, wofür er neben „Kinderarmut und Altersarmut“ auch „1300 Kinderehen, Morde, Ehrenmorde und Vergewaltigungen“ anführt, die er pauschal allen Flüchtlingen in Deutschland anlastet. Diese, den einzelnen Flüchtlingen jede Individualität absprechende Einstellung hat das Landgericht zutreffend als „entmenschlichende“ Sprache im Sinne von Ziff. 12 der Gemeinschaftsstandards eingestuft, die ebenso „Menschen ausschließt“ wie sie „ein Umfeld der Einschüchterung schafft“ (vgl. die Aufzählung in Ziff. 12. der Gemeinschaftsstandards unter „Angriffe mit Schweregrad 1“). In diesem für den Durchschnittsrezipienten erkennbaren Sinn stellt die Äußerung zugleich eine Aufstachelung zum Hass gegen Teile der Bevölkerung im Sinne des § 130 StGB dar, denn als Teile der Bevölkerung i.S. dieser Vorschrift können auch Asylbewerber oder allgemein in Deutschland lebende Ausländer angesehen werden (BGH, Urt. v. 20.09.2011 – 4 StR 129/11; Kammergericht Berlin, Urt. v. 26.11.1997 – (5) 1 Ss 145/94 (30/94); OLG Frankfurt, Urt. v. 15.08.2000 – 2 Ss 147/2000; OLG München, Beschl. v. 17.09.2018 – 18 W 1383/18 – Rn. 47 m.w.N.). Ob sie damit zugleich den Straftatbestand der Volksverhetzung gem. § 130 StGB verwirklicht, kann wegen des ohnehin gegebenen Verstoßes gegen die Gemeinschaftsstandards indes offen bleiben.

Vor diesem Hintergrund ist die 30-tägige Versetzung in den read only-Modus auch nicht als unverhältnismäßig anzusehen. Sie ist weder willkürlich festgesetzt worden noch wird der Kläger hierdurch vorschnell oder dauerhaft gesperrt (vgl. hierzu Senat, Beschluss vom 08. August 2018 – 4 W 577/18 –, Rn. 25, juris). Die Sanktionierung eines klaren Verstoßes gegen Ziff. 12 der Gemeinschaftsstandards mit einer zeitlich begrenzten Sperre für die aktive Nutzung hat der Senat aaO. als in der Regel verhältnismäßige Sanktion angesehen. Aus welchen Gründen vorliegend hiervon abzuweichen wäre, hat der Kläger nicht vorgetragen. Weder lässt sich seinem Vorbringen entnehmen, dass er hierdurch einen wirtschaftlichen Schaden erlitten haben will, noch ist eine wirkliche Beeinträchtigung seiner Kommunikationsfreiheit erkennbar geworden. Dass das Landgericht sich gem. § 286 ZPO davon überzeugt gesehen hat, dass der Kläger überhaupt eine solche Sperre hinnehmen musste, obwohl die Beklagte dies in erster Instanz bestritten und der Kläger hierfür keinen Beweis angetreten hat, kann unter diesen Umständen dahinstehen.

Kein DS-GVO-Schadensersatzanspruch bei bloßen Bagatellverstößen

(**Oberlandesgericht Dresden**, Beschluss vom 11. Juni 2019 – 4 U 760/19 –)

Bei bloßen Bagatellverstößen im Datenschutzrecht ohne ernsthafte Beeinträchtigung für das Selbstbild oder Ansehen einer Person besteht kein Schadensersatzanspruch nach Art. 82 Abs.1 DS-GVO

Sachverhalt:

Der Kläger war bei Facebook Mitglied. Wegen eines umstrittenen Postings sperrte ihn Facebook und löschte auch seinen Text. Der Kläger sah hierin eine unerlaubte Datenschutzverletzung und verlangte nach Art. 82 Abs.1 DS-GVO Schadensersatz iHv. 150,– EUR.

Aus den Gründen:

Dass dem Kläger durch die Sperrung ein materieller oder immaterieller Schaden im Sinne des Art. 82 DS-GVO entstanden wäre, kann der Senat überdies nicht erkennen. Die bloße Sperrung seiner Daten stellt ebenso wie der Datenverlust noch keinen Schaden im Sinne der DS-GVO dar (Wybitul/Haß/Albrecht, NJW 2018 S. 113 (114)). Die behauptete Hemmung in der Persönlichkeitsentfaltung durch die dreitägige Sperrung hat allenfalls Bagatellcharakter (s.o.).

Auch wenn in der Literatur unter Bezug auf Erwägungsgrund 146 der DS-GVO vereinzelt die Auffassung vertreten wird, eine wirksame Durchsetzung europäischen Datenschutzrechts erfordere einen Abschreckungseffekt und den Verzicht auf die nach bisherigem Recht (vgl. hierzu BGH, Urteil vom 29.11.2016 – VI Z 530/15) geltende Erheblichkeitsschwelle (Gola, DS-GVO, 2. Aufl. Art 82 Rn 13 m.w.N.; so auch AG Dietz, Urteil vom 7.11.2018 – 8 C 130/18 –)) rechtfertigt dies keinen Ausgleich immaterieller Bagatellschäden. Das Datenschutzrecht schützt zwar per se ein subjektives Recht, das einen starken Bezug zum persönlichen Empfinden des Einzelnen hat. Dennoch ist Art. 82 nicht so auszulegen, dass er einen Schadensersatzanspruch bereits bei jeder individuell empfundenen Unannehmlichkeit oder bei Bagatellverstößen ohne ernsthafte Beeinträchtigung für das Selbstbild oder Ansehen einer Person begründet (Becker in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 82 DSGVO, Rn. 4c). Insbesondere kann der Hinweis auf einen „vollständigen und wirksamen Schadensersatz“ in Erwägungsgrund 146 der DSGVO nicht in diesem Sinne verstanden werden (so auch Lach, jurisPR-ITS 5/2019 Anm. 3). Die Wahrung des Rechts auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG und des Schutzes personenbezogener Daten nach Art. 8 GRC gebieten einen solchen Ausgleich regelmäßig nicht. Anders mag dies in den Fällen sein, in denen der datenschutzrechtliche Verstoß eine Vielzahl von Personen in gleicher Weise betrifft und Ausdruck einer bewussten, rechtswidrigen und im großen Stil betriebenen Kommerzialisierung ist (Becker, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 82 DSGVO, Rn. 4d). So liegen die Dinge hier indes nicht. Zwar gehört die Kommerzialisierung von Nutzerdaten zum Geschäftsmodell der Beklagten; die Sperrung des klägerischen Accounts befördert jedoch diese Kommerzialisierung nicht, sondern behindert sie vielmehr, weil der Kläger in dieser Zeit keine Daten „produziert“, die die Beklagte verwerten könnte. Gegen eine Ausdehnung des immateriellen Schadenser-

satzes auf Bagatellschäden spricht auch das erhebliche Missbrauchsrisiko, das mit der Schaffung eines auf Rechtsfolgenseite nahezu voraussetzungslosen Schmerzensgeldanspruchs gerade im Bereich des Datenschutzrechts einherginge. Angesichts dessen sowie der damit einhergehenden vollständigen Abkehr von der bisher geltenden Rechtslage wäre zu erwarten gewesen, dass eine solche Änderung im Verordnungstext oder in den Erwägungsgründen einen deutlichen Ausdruck gefunden hätte. Dies ist jedoch nicht der Fall.

Zum datenschutzrechtlichen Widerspruchrecht gegenüber der Erhebung von Sozialdaten

(**Landessozialgericht Hessen**, Beschluss vom 29. Januar 2020 – L 4 SO 154/19 B –)

1. **Bei der Erhebung von Sozialdaten bei der betroffenen Person im Rahmen der Amtsermittlung im Verwaltungsverfahren zur Bewilligung von Sozialleistungen (§ 20 SGB X, § 67a Abs. 2 SGB X) mittels eines Überprüfungsbogens ist keinem Widerspruch nach Art. 21 Abs. 1 DS-GVO zugänglich, da diese Verarbeitung im konkreten Fall nach Art. 6 Abs. 1 lit. c DS-GVO zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.**
2. **Zur einschränkenden Auslegung von § 56a SGG wegen Art. 19 Abs. 4 GG und Art. 47 GrCh.**

Aus den Gründen:

Gemäß § 73a Abs. 1 Satz 1 Sozialgerichtsgesetz (SGG) i.V.m. § 114 S. 1 Zivilprozessordnung (ZPO) ist einem Beteiligten auf Antrag Prozesskostenhilfe zu bewilligen, wenn er nach seinen persönlichen und wirtschaftlichen Verhältnissen die Kosten der Prozessführung nicht, nur zum Teil oder nur in Raten aufbringen kann, die beabsichtigte Rechtsverfolgung oder Rechtsverteidigung hinreichende Aussicht auf Erfolg bietet und nicht mutwillig erscheint. Der Maßstab für die insoweit geforderten Erfolgsaussichten ist im Licht der grundrechtlich garantierten Rechtsschutzgleichheit zu bestimmen. … (wird ausgeführt)

Gemessen an diesem Maßstab fehlt es an der hinreichenden Erfolgsaussicht der sozialgerichtlichen Klage, gerichtet auf die strafbewehrte Unterlassung, vom Kläger einmal jährlich mittels eines „sogenannten Überprüfungsbogens einen verkappten Weiterbewilligungsantrag zu fordern".

Soweit der Kläger unmittelbar einen Verstoß gegen Verwaltungsverfahrensrecht nach dem Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) durch die Übersendung des Fragebogens mit Anschreiben vom 24. April 2019 rügen will, ist die Klage bereits unzulässig. Ihr steht § 56a Satz 1 SGG entgegen. Rechtsbehelfe gegen behördliche Verfahrenshandlungen können hiernach nur gleichzeitig mit den gegen die Sachentscheidung zulässigen Rechtsbehelfen geltend gemacht werden. Soweit es um die Reichweite zulässiger Amtsermittlung geht, ist es dem Kläger zuzumuten, gegebenenfalls gegen eine ablehnende Sachentscheidung zu klagen und inzident – ggf. im Eilrechtsschutz – klären zu lassen, ob zur weiteren Leistungsgewährung die entsprechenden Angaben erforderlich sind.

Dies gilt allerdings nicht hinsichtlich des gerügten Verstoßes gegen Rechte aus 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 (DS-GVO).

Wegen des Gebots der Gewährung effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG ist § 56a SGG einschränkend auszulegen. Die Vorschrift darf der Zulässigkeit einer Klage nicht entgegenstehen, wenn die betroffene Verfahrenshandlung unmittelbare Rechtswirkungen zu Lasten des Betroffenen über das Verwaltungsverfahren hinaus entfaltet und insoweit Rechtsschutz gegen die Sachentscheidung zu spät käme (vgl. Axer, SGb 2013, 669 <673 f.> m.w.N.). Entsprechendes gilt auf der Grundlage von Art. 47 der Charta der Grundrechte der Europäischen Union (GrCh) für vergleichbare Rechtswirkungen bei Verstößen gegen Unionsrecht. Nach Auffassung des Senats handelt es sich jedenfalls bei dem Betroffenenrecht zum Widerspruch nach Art. 21 DS-GVO um ein Recht, dem ein wirksamer Rechtsbehelf zur Seite stehen muss, wie sich auch aus Art. 79 DS-GVO ergibt (wie hier zu Art. 21 DS-GVO Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 21 Rn. 41; Herbst, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 21 Rn. 60; vgl. auch Leopold, ZESAR 2018, 326 <330 f.>).

Der Kläger trägt bei verständiger Würdigung der Klagebegründung vor, er habe u.a. mit der E-Mail seiner Betreuerin vom 26. April 2019 dem Beklagten mitgeteilt, dass er keinen Weiterbewilligungsantrag zu stellen und keine Unterlagen vorzulegen habe. Da dies eine Reaktion auf die Übersendung des Überprüfungsbogens mit Anschreiben vom 24. April 2019 war und der Kläger auch in der Vergangenheit schon ein datenschutzwidriges Vorgehen gerügt hat, kann diese E-Mail nur so verstanden werden, dass der Erhebung von Daten mittels des Überprüfungsbogens (und damit einer Verarbeitung im Sinne von Art. 4 Nr. 2 DS-GVO) auch gegenüber dem Beklagten (als Verantwortlichen i.S.d. Art. 4 Nr. 7 DS-GVO) widersprochen wird, weil er die Erhebung dieser Daten auf der Grundlage der DS-GVO nicht als rechtmäßig erachtet. Damit ist die rechtliche Überprüfung eröffnet, ob der Beklagte auf den Widerspruch hin die Erhebung von Daten mittels des Überprüfungsbogens einstellen musste. Ob die Tatbestandsvoraussetzungen von Art. 21 DS-GVO vorliegen, ist Frage der Begründetheit.

Da die Ausübung des Widerspruchsrechts nur eine einseitige empfangsbedürftige, formfreie Willenserklärung ist und die Rechtsfolge auf eine wiederum formlose Prüfung des Verantwortlichen ex nunc eintritt (Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 21 Rn. 17 m.w.N.), ist die Durchführung eines Vorverfahrens entbehrlich.

Soweit die Klage zulässig ist, bestehen mangels Begründetheit keine hinreichenden Erfolgsaussichten.

Als Rechtsgrundlage für das Klagebegehren kommt wegen der Unzulässigkeit der Klage im Übrigen allein Art. 21 Abs. 1 DS-GVO in Betracht. Die betroffene Person hat hiernach das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen (Art. 21 Abs. 1 Satz 1 1. Hs. DS-GVO). Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 Abs. 1 Satz 2 DS-GVO).

Dieses Widerspruchsrecht steht der betroffenen Person nur zu, wenn die Verarbeitung ausschließlich auf der Grundlage von Art. 6 Abs. 1 lit. e oder lit. f DS-GVO erfolgt. Dem entspricht § 84 Abs. 5 SGB X, wonach das Widerspruchsrecht aus Art. 21 Abs. 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle u.a. nicht besteht, soweit eine Rechtsvorschrift zur Verarbeitung von Sozialdaten verpflichtet.

Im Falle des Klägers erfolgt die Erhebung der Sozialdaten aber auf der Grundlage von Art. 6 Abs. 1 lit. c DS-GVO, so dass das Widerspruchsrecht nicht besteht, worüber der Beklagte den Kläger auch zutreffend bereits mit Schreiben vom 2. August 2018 (Bl. 167 ff. der Verwaltungsakte) unter Hinweis auf § 84 Abs. 5 SGB X informiert hat. Die Verarbeitung ist nach Art. 6 Abs. 1 lit. c DS-GVO rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Die Voraussetzung der Erforderlichkeit stellt sicher, dass der Verantwortliche ein vorgegebenes Ziel nicht zum Anlass nimmt, überschießend personenbezogene Daten zu verarbeiten (Buchner/Petri, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 81).

Der Beklagte unterliegt im Verwaltungsverfahren zur Bewilligung von Leistungen als örtlicher Sozialhilfeträger einer solchen rechtlichen Verpflichtung, nämlich der Pflicht zur Amtsermittlung nach § 20 SGB X. Das Formular wurde dem Kläger im Rahmen eines Verwaltungsverfahrens der Weiterbewilligung von Leistungen nach dem Vierten Kapitel des SGB XII mit der Aufforderung ausgehändigt, es ausgefüllt und unterschrieben unter Beifügung von Unterlagen zurückzusenden (vgl. z.B. Schreiben vom 24. April 2019, Bl. 17 der Gerichtsakte S 11 SO 12/19 ER). Verpflichtende Datenverarbeitung im Rahmen der Erledigung öffentlicher Aufgaben wird sowohl lit. c als auch lit. e zugeordnet (siehe Albers/Veit, BeckOK Datenschutzrecht, Stand 1. November 2019, Art. 6 Rn. 35; wohl auch Bieresborn, NZS 2018, 10 <13>, der auf die Folgen für das Widerspruchsrecht hinweist). Auch der deutsche Gesetzgeber ging bei der Änderung von § 84 Abs. 5 SGB X ersichtlich davon aus, dass die verpflichtende Verarbeitung von Sozialdaten durch Sozialleistungsträger Art. 6 Abs. 1 lit. c DS-GVO unterfällt und daher kein Widerspruchsrecht besteht (vgl. BT-Drs. 18/12611, S. 132). Die „rechtliche Verpflichtung" ist dadurch gekennzeichnet, dass sich die in einer Vorschrift des objektiven Rechts normierte Verpflichtung unmittelbar auf die Datenverarbeitung bezieht; allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus (vgl. Buchner/Petri, in: Kühling/Buchner, DS-GVO BDSG, 2. Aufl. 2018, Art. 6 Rn. 76; Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 43). Diesen Anforderungen genügt die Pflicht nach § 20 SGB X. Wie § 20 Abs. 1 Satz 1 und Abs. 2 SGB X deutlich machen, handelt es sich bei der Amtsermittlung um eine Pflichtaufgabe, sobald ein Verwaltungsverfahren eingeleitet ist (§ 8 SGB X). Diese Aufgabenzuweisung findet ihre Entsprechung in den Befugnisnormen zur datenschutzrechtlich relevanten Amtsermittlung nach §§ 67 ff. SGB X und der DS-GVO. Die Übersendung eines Überprüfungsbogens an den Betroffenen erfolgt auf der Grundlage der Pflicht des § 67a Abs. 2 SGB X, Sozialdaten vorrangig beim Betroffenen zu erheben. Diese Vorschrift zeigt auch, dass sich die Pflichtenstellung der Amtsermittlung – soweit sie wie hier mit der Datenverarbeitung verbunden ist – unmittelbar auf die Datenverarbeitung bezieht. Folglich unterliegt die durch die Erforderlichkeit begrenzte Pflicht zur Amtsermittlung nach § 20 SGB X ggf. in Verbindung mit speziellen Befugnisnormen aus §§ 67 ff. SGB X oder besonderen Normen der DS-GVO nicht dem Widerspruchsrecht des Art. 21 Abs. 1 DS-GVO (so wohl auch Bieresborn, NZS 2018, 10 <13>).

Die Verarbeitung der Daten des Klägers ist auch erforderlich.

Für Leistungen nach dem Vierten Kapitel des Sozialgesetzbuches Zwölftes Buch –- Sozialhilfe – (SGB XII) muss in dem sich an die Erstbewilligung anschließenden Zeitraum zwar kein Folgeantrag gestellt werden (BSG, Urteil vom 29. September 2009 – B 8 SO 13/08 R –, BSGE 104, 207, zitiert nach juris Rn. 11 f. zum Grundsicherungsgesetz). Diese Rechtsauffassung entspricht der ganz vorherrschenden Ansicht auf der Grundlage von §§ 41, 44 SGB XII n.F. (Blüggel, in: Schlegel/Voelzke, jurisPK-SGB XII, § 44 SGB XII Rn. 31 ff.; Krauß, in: Knickrehm/Kreikebohm/Waltermann, Kommentar zum Sozialrecht, 6. Aufl. 2019, § 44 Rn. 1) und wird auch vom erkennenden Senat vertreten. Hiervon zu unterscheiden ist jedoch die Frage, welchen Umfang die notwendige Amtsermittlung nach Ablauf des Bewilligungszeitraums hat. Hier begegnet es keinen Bedenken, dass die wesentlichen Informationen routinemäßig neu abgefragt werden, insbesondere deshalb, weil der Umfang des Fragenkatalogs des vom Beklagten verwendeten Überprüfungsbogens (eine Seite) erheblich von dem des Erstantrages (vier Seiten) abweicht. In Abhängigkeit des Bewilligungszeitraums (hier: ein Jahr) ist es auch nicht zu beanstanden, nach einer gewissen Dauer des Leistungsbezuges auch die Kontoauszüge der letzten drei Monate anzufordern. Die vom Bundessozialgericht im Urteil vom 19. September 2008 – B 14 AS 45/07 R –, BSGE 101, 260, zitiert nach juris Rn. 16 f., angestellte Überlegung, dass es im Rahmen eines aus Steuermitteln finanzierten Fürsorgesystems, das strikt an die Hilfebedürftigkeit der Leistungsempfänger als Anspruchsvoraussetzung anknüpft, keine unzumutbare und unangemessene Anforderung darstellt, Auskunft über den Bestand an Konten und die Kontenbewegungen (durch die Vorlage von Kontoauszügen) zu geben, jedenfalls soweit die Einnahmeseite betroffen ist, hat auch ihre Berechtigung bei Folgezeiträumen.

Ungeachtet dessen trägt der Kläger auch keine Gründe vor, die sich aus seiner besonderen Situation i.S.d. Art. 21 Abs. 1 Satz 1 DS-GVO ergeben und den Widerspruch tragen sollen. Nicht zuletzt wegen der Normstruktur des Art. 21 Abs. 1 Satz 2 DS-GVO, die eine Abwägung erfordert, müssen konkrete Tatsachen zu dieser besonderen Situation vorgetragen werden, die ausnahmsweise das Unterlassen der Erhebung rechtfertigen sollen (Gola/Schulz, DS-GVO, 2. Aufl. 2018, Art. 21 Rn. 9). Hieran fehlt es, der Kläger verweist zunächst auf die nach seiner Auffassung der Rechtsprechung des Bundessozialgerichts widersprechende Verwaltungspraxis. Soweit er allgemein auf seinen Gesundheitszustand verweist, sind dies keine Gründe, die einen Bezug zu Datenschutzbelangen haben. Auch kann daraus nicht abgeleitet werden, seine Betreuerin sei mit dem Ausfüllen des Überprüfungsbogens und dem Vorlegen der Unterlagen unverhältnismäßig belastet.

Wegen der eindeutigen gesetzgeberischen Wertung des § 84 Abs. 5 SGB X und zwei voneinander unabhängigen Gründen, die gegen hinreichende Erfolgsaussichten sprechen, ist die Bewilligung von Prozesskostenhilfe auch nicht aus dem Grund angezeigt, dass es sich bei der Bestimmung des Anwendungsbereichs des Art. 21 DS-GVO noch nicht um eine obergerichtlich oder höchstrichterlich geklärte Rechtsfrage handelt.

Löschung von personenbezogenen Daten aus dem polizeilichen Vorgangs- und Bearbeitungssystem (VBS) NIVADIS (Ls)

(**Oberverwaltungsgericht Lüneburg**, Urteil vom 14. Januar 2020 – 11 LC 191/17 –)

1. **Nach Umsetzung der Richtlinie (EU) 2016/680, mit der für den Datenschutz in den Bereichen Justiz und Polizei eine Mindestharmonisierung innerhalb der Europäischen Union herbeigeführt werden soll, richtet sich im Landesrecht der Anspruch auf Löschung personenbezogener Daten aus dem polizeilichen Vorgangs- und Bearbeitungssystem VBS NIVADIS nach § 52 Abs. 2 des Niedersächsischen Datenschutzgesetzes – NDSG – in der Fassung vom 16. Mai 2018.**
2. **Personenbezogene Daten, die sich bereits anonymisiert im Archiv des VBS NIVADIS befinden, können nicht mehr zum Zweck der Verhütung von Straftaten genutzt werden. Sie dienen nur noch dem Zweck der Vorgangsverwaltung und Dokumentation behördlichen Handelns. Insoweit ist ihre Kenntnis für einen gewissen Zeitraum zur Erfüllung polizeilicher Aufgaben weiterhin erforderlich.**
3. **Die als Polizeibehörde für den Datenschutz zuständige Stelle hat geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch der verarbeiteten personenbezogenen Daten zu ergreifen.**

Zur Reichweite von Auskünften nach dem Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation (Verbraucherinformationsgesetz – VIG) (Ls)

(**Verwaltungsgerichtshof Baden-Württemberg**, Beschluss vom 13. Dezember 2019 – 10 S 2614/19 –)

1. **Das individuelle Informationsrecht nach § 2 Abs. 1 Satz 1 VIG ist ein „Jedermannsrecht", das von keinem besonderen Interesse oder einer Betroffenheit abhängig ist. Unbeachtlich ist für das Informationszugangsrecht die Unterstützung des Antragstellers (z. B. durch eine Internet-Plattform).**
2. **§ 2 Abs. 1 Satz 1 VIG ist mit Unionsrecht vereinbar. Die Verbraucherinformation unterhalb der Gefahrenschwelle auf der Grundlage innerstaatlichen Rechts ist unionsrechtlich nicht ausgeschlossen.**
3. **§ 2 Abs. 1 Satz 1 Nr. 1 VIG erfasst jede objektive Abweichung von Rechtsvorschriften. Eine „nicht zulässige Abweichung" im Sinne dieser Bestimmung muss nicht durch Verwaltungsakt festgestellt werden; ausreichend ist die entsprechende abschließende aktenkundige Feststellung der zuständigen Behörde unter Würdigung des Sachverhalts und der einschlägigen Rechtsvorschriften (wie BVerwG, Urteil vom 29.08.2019 – 7 C 29/17 – Leitsätze 4 und 5).**
4. **Eine mutmaßliche Weiterverwendung rechtmäßig erlangter Informationen durch den Antragsteller ist für das VIG-Verfahren rechtlich unerheblich. Die Informationsweiterverwendung bestimmt sich vornehmlich nach § 2a IWG; dabei sind die unionsrechtlichen Vorgaben nach der Richtlinie 2013/37/EU zu beachten.**
5. **Die für § 40 Abs. 1a LFGB geltenden Standards zur Grundrechtsbindung der öffentlichen Hand sind auf den individuellen Informationszugang nach § 2 Abs. 1 VIG nicht zu übertragen. Der Gesetzgeber unterscheidet bewusst zwischen der von Amts wegen erfolgenden Information der Öffentlichkeit und dem antragsabhängigen individuellen Zugang zu Verbraucherinformationen (BT-Drs. 16/5404, S. 8: „zwei Säulen, die sich ergänzen").**
6. **Die EU-Grundrechte-Charta steht dem Informationszugang nach dem VIG nicht entgegen. Dieses Gesetz ist – auch in Bezug auf die unternehmerische Freiheit (Art. 16 GRCh) – durch den Schrankenvorbehalt des Art. 52 Abs. 1 GRCh gedeckt.**

Sorgfaltspflichten vor Klageeinreichung; zur Kenntnisnahmepflicht von Erklärungen über „WhatsApp"

(**Landgericht Bonn**, Urteil vom 31. Januar 2020 – 17 O 323t19)

1. **Zur Vermeidung einer Kostentragungspflicht gem. § 93 ZPO ist der Kläger vor Einreichung einer Antrags- oder Klageschrift auch verpflichtet, einen etwaigen Nachrichteneingang bei "WhatsApp" zur Kenntnis zu nehmen und daraufhin zu kontrollieren, ob der Beklagte bereits anerkannt oder sich der geforderten Verpflichtung unterworfen hat.**
2. **Haben die Parteien bereits im Vorfeld Kommunikationen über "WhatsApp" geführt, ist es zulässig, dass weitere rechtserhebliche Erklärungen ebenfalls über diesen Kommunikationskanal abgegeben werden, soweit das Textformerfordernis ausreicht.**

3. **Bei einer derart weit verbreiteten Applikation wie "WhatsApp" kann aus einer Phase ohne Kommunikation nicht der Schluss gezogen werden, der andere Teil habe diesen eröffneten Kommunikationskanal wieder aufgegeben.**
4. **Gemäß § 291 ZPO ist als allgemeinbekannt anzunehmen, dass bei der Anzeige von zwei blauen Haken die Nachricht auf dem Endgerät des Empfängers eingegangen und auch von diesem geöffnet worden ist. Insoweit kann offen bleiben, ob von dieser WhatsApp-Nachricht tatsächlich erst später Kenntnis genommen wurde.**

(Einsender: RA Konstantin Mertsiotis, der auch Verfasser der Leitsätze ist)

Streitwert bei Tracking-E-Mails

(**Landgericht Wiesbaden**, Beschluss vom 22. August 2019 – 8 O 94/19 (rechtskr.) –)

Der Streitwert für die datenschutzrechtliche Unterlassung des Versands unzulässiger Werbe-E-Mails an einen Verbraucher, wobei 62 solcher E-Mails versandt wurden und einige davon Tracking-Pixel von Google Analytics enthielten, um dem Absender Aufschluss über das Leseverhalten des Empfängers zu verschaffen, beträgt 30.000 EUR.

(Nicht amtlicher Leitsatz)

Anmerkung von RA Jonas Breyer, Wiesbaden:

Bekanntlich stellt unerlaubte E-Mail-Werbung abgesehen von wettbewerbsrechtlichen Implikationen auch einen unterlassungspflichtige Verletzung des allgemeinen Persönlichkeitsrechts dar, da der Empfänger als Ausfluss seiner privaten Lebensgestaltung grundsätzlich selbst entscheiden kann, mit wem er Kontakt haben möchte und in welchem Umfang.[1] Große Unterschiede bestehen dagegen in Bezug auf den Streitwert. Maßgeblich hierfür ist das Interesse des Klägers an der Unterbindung weiterer gleichartiger Verstöße.[2] Handelt es sich beim Empfänger um einen Unternehmer, werden häufig höhere Werte angenommen, etwa 3.000 €[3] oder auch 10.000 €.[4] Ist der Empfänger ein Verbraucher, liegt der Wert häufig mit 500 €[5] bis 3.000 €[6] darunter.

Eine neue Entscheidung hat uns nun das Landgericht Wiesbaden beschert. Im dortigen Fall nahm ein Unternehmen Online-Bestellungen von Verbrauchern zum Anlass, deren E-Mail-Adressen in seinen Newsletter-Verteiler aufzunehmen. Die E-Mails erwiesen sich als rechtswidrig, weil sie – wie zumeist – weder durch eine wirksame Einwilligung gedeckt war noch die Informationspflichten nach Art. 6 Abs. 1 Buchst. f DS-GVO i.V.m. § 7 Abs. 3 UWG erfüllt waren. Diese sind Voraussetzung für einen Opt-out-Versand.[7] Mehrere der insgesamt 62 E-Mails enthielten im Quellcode Tracking-Pixel von Google-Analytics, sodass beim Öffnen der E-Mails eine Reihe personenbezogener Daten wie die IP-Adresse an US-amerikanische Google-Server zur zweck- und seitenübergreifenden Auswertung übermittelt wurde, um das Leseverhalten des Empfängers auszuforschen. Auch kam es im Rahmen von Google Analytics zum Setzen von Cookies zu Marketing-Zwecken ohne Einwilligung.

Google Analytics wird als so invasiv beurteilt, dass es auch unabhängig vom Cookie nur durch eine Einwilligung gerechtfertigt werden kann.[8] Auch die angebliche IP-Anonymisierung von Google vermag daran nichts zu ändern, zumal diese erst von Google vorgenommen wird; im Übrigen ist auch ohne IP-Adresse eine Personenbeziehbarkeit anhand des Browser-Fingerprints und ähnlicher Daten möglich.[9] Entgegen landläufiger Meinung stellt es auch keinen Erlaubnistatbestand dar, auf Google Analytics in der Datenschutzerklärung oder via Pop-up hinzuweisen. Leider bleibt auch eine Einwilligung eine bloß theoretische Möglichkeit, da eine Einwilligung unter anderem informiert zu formulieren wäre (Art. 4 Nr. 11 DS-GVO), was wegen Googles weithin intransparenter Datenverarbeitung aber nicht möglich ist. Auch verwendet Google Daten seines Diensts Analytics laut eigener Datenschutzerklärung zu seitenübergreifenden und eigenen Zwecken, sodass jedenfalls ein Vertrag nach Art. 26 DS-GVO notwendig wäre.[10] Einen solchen bietet Google aber nicht an, und die irische Aufsichtsbehörde handelt nicht. Hinzu kommt neben der erwähnten Cookie-Problematik der Komplex „Cloud Act versus Art. 48 DS-GVO".[11] Zu Recht hat sich die DSK gegen derlei invasive Tracker ausgesprochen, insbesondere Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage verneint.[12]

Aus den von der DSK ausgeführten Gründen kann eine Widerspruchslösung auch nicht auf § 15 Abs. 3 TMG gestützt werden. Selbst wenn man diese Vorschrift entgegen ihrem Wortlaut für europarechtskonform auslegbar hält,[13] stellt nach der Rechtsprechung des Europäischen Gerichtshofs eine Widerspruchslösung keine Einwilligung dar, und zwar nicht nur bei Cookies.[14] Immerhin hat der Bundesgerichtshof mit seiner „europarechtskonformen Auslegung" des § 15 Abs. 3 TMG[15] den Weg zum Europäischen Gerichtshof geebnet. Nachdem sich die Europäische Kommission auf den bemerkenswerten Standpunkt gestellt hatte, dass die deutsche Widerspruchslösung in Marketingfällen gemäß § 15 Abs. 3 TMG als Einwilligung gewertet werden könne, kam das Bemühen des deutschen Gesetzgebers endgültig zum Erliegen, § 15 Abs. 3 TMG an europäisches Recht anzupassen – sei es an die Cookie- bzw. die Datenschutz-Richtlinie oder an die DS-GVO –, wohl wissend, dass eine direkte Anwendung von Richtlinien zu Lasten nichtstaatlicher Verantwortlicher regelmäßig nicht in Betracht kommt und ihm die Unterstützung der deutschen Wirtschaft sicher ist. In dieser Konstellation wäre die Herstellung eines europarechtskonformen Zustands schwierig gewesen.

Einen Unsubscribe-Link klickte der Empfänger nicht an, da die Widerspruchsbelehrung unvollständig und die Unsubscribe-Seite ihrerseits mit unzulässigen Trackern kontaminiert war, sodass es zu 62 E-Mails kam. Schriftsätzlich wurde auf den Effektivitätsgrundsatz unter anderem im Sinne von Art. 83 DS-GVO sowie auf bereits verhängte DS-

GVO-Bußgelder verwiesen; deren Bemessung schlägt im Übrigen auf zivilrechtliche Ansprüche nach Art. 82 DS-GVO durch.[16] So bewertete das Gericht das Unterlassungsinteresse des Empfängers mit 30.000 €.

(Hinweis: Der Autor ist am Rechtsstreit auf Seiten des Unterlassungsklägers beteiligt.)

1 BGH, Urt. v. 10.07.2018 – VI ZR 225/17, Rn. 14, NJW 2018, 3506.
2 BGH, Beschl. v. 26.04.1990 – I ZR 58/89, NJW-RR 1990, 1322.
3 BGH, Beschl. v. 30.11.2004 – VI ZR 65/04, BeckRS 2004, 12785.
4 KG, Beschl. v. 09.08.2013 – 5 W 187/13, BeckRS 2015, 18410.
5 OLG Hamm, Urt. v. 17.10.2013 – 6 U 95/13, NJW-RR 2014, 613.
6 OLG Frankfurt/Main, Beschl. v. 02.03.2016 – 6 W 9/16, MMR 2016, 454.
7 OLG Jena, Urt. v. 21.04.2010 – 2 U 88/10, MMR 2011, 101.
8 LG Dresden, Urt. v. 11.01.2019 – 1a O 1582/18, ZD 2019, 416.
9 Brehm, Verräterische Merkmale, c't 11/2016, S. 144 f.
10 Vgl. EuGH, Urt. v. 05.06.2018 – C-210/16, Rn. 25 ff., NJW 2018, 2537, Facebook; EuGH, Urt. v. 29.07.2019 – C-40/17, Rn. 64 ff., NJW 2019, 2755, Fashion ID.
11 Vgl. Stellungnahme des EDSA an den LIBE-Ausschuss v. 10.07.2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en, siehe auch das zugehörige Rechtsgutachten im Anhang, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf, jeweils abgerufen am 27.09.2019; Pressemeldung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen v. 09.07.2019, https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%Bcr-datenschutz-und, abgerufen am 27.09.2019; zu rechtlichen Einzelheiten Gausling, MMR 2018, 578.
12 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien v. März 2019, Anhang I, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf, abgerufen am 27.09.2019.
13 Zweifelnd auch Spittka, DB 2019, 2850, 2853.
14 EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 44 ff., NJW 2019, 3433 – Planet49.
15 BGH, Beschl. v. 05.10.2017 – I ZR 7/16, Planet49.
16 Wybitul/Haß/Albrecht, NJW 2018, 113, 115.

Kein Schadensersatz-Anspruch nach der DS-GVO wegen fehlerhaften Basisscores

(**Landgericht Karlsruhe**, Urteil vom 2. August 2019 – 8 O 26/19 –)

Ein DS-GVO-Schadensersatzanspruch gegen eine Auskunftei kommt nicht bereits schon dann in Betracht, wenn ein Kreditinstitut aufgrund eines von der Auskunftei bezogenen fehlerhaften Basisscores einen Kreditvertrag mit dem Verbraucher ablehnt.

Aus den Gründen:

Die Ablehnung eines Kreditvertrags durch ein Kreditinstitut, die auch auf der Mitteilung einer unzutreffenden Einschätzung der Bonität der Kläger durch eine Auskunftei beruht, begründet nicht ohne weiteres eine entschädigungspflichtige Persönlichkeitsverletzung, da es zum einen dem Kreditsuchenden selbst obliegt, seine Bonität im direkten Kontakt zu belegen, und zum anderen ein Anspruch auf Abschluss eines Kreditvertrags zum Zwecke des Konsums nicht besteht.

Zum Anspruch eines Polizeibeamten auf Akteneinsicht nach § 3 Abs. 1 Satz 1 des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin – IFG Berlin

(**Verwaltungsgericht Berlin**, Urteil vom 31. Januar 2020 – 2 K 182.19 –)

Jeder Mensch hat nach Maßgebe des IFG Berlin gegenüber den in § 2 IFG Berlin genannten öffentlichen Stellen nach seiner Wahl ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten auch soweit sie Personalangelegenheiten betreffen.

Tatbestand:

Der Kläger begehrt Auskunft über die zu seiner Person abgefragten Datensätze in Datenbanken des Landes Berlin.

Der Kläger ist als Polizeivollzugsbeamter beim Beklagten tätig. Im Rahmen von dienstrechtlichen Auseinandersetzungen wurde ihm bekannt, dass über ihn Auskünfte in Datenbanken des Beklagten abgefragt wurden. Mit Schreiben vom 29. März 2015 beantragte der Kläger u.a. Auskunft zu der Frage, welche Polizeibeamten ihn aus welchem Anlass innerhalb der letzten zwei Jahre „im Poliks bzw. EWW" abgefragt hätten. Daraufhin veranlasste der Beklagte am 14. April 2015 eine Protokolldatenauswertung.

Mit Schreiben vom 25. Januar 2018 beantragte der Kläger erneut Akteneinsicht in die vom Beklagten vorgenommene „Protokollbandabfrage" und nahm Bezug auf das Informationsfreiheitsgesetz Berlin. Mit Bescheid vom 14. Februar 2018 lehnte der Beklagte den Antrag auf Einsicht in die Protokolldatenauswertung vom 14. April 2015 ab und bezog sich auf zu schützende personenbezogene Daten derjenigen Personen, die im Auswertezeitraum eine Abfrage in polizeilichen Datenbanken zum Kläger vorgenommen hatten. Außerdem bestünden Anhaltspunkte dafür, dass der Kläger mit seinem Antrag überwiegend Privatinteressen verfolge.

Mit seiner am 12. Juni 2019 erhobenen Klage verfolgt der Kläger sein Begehren weiter und trägt vor: Er verfolge nicht überwiegend Privatinteressen, sondern dienstliche Interessen. Gegen ihn werde sowohl ein gerichtliches Disziplinarverfahren als auch ein weiteres behördliches Disziplinarverfahren geführt. In diesen Verfahren habe der Beklagte regelmäßig Poliks-Abfragen vorgenommen, ohne dass ein Sachgrund vorgelegen hätte und ohne dass diese Anfragen aktenmäßig dokumentiert worden seien.

Entscheidungsgründe:

Der Klageantrag ist ausgehend vom objektivierten Empfängerhorizont dahingehend auszulegen, dass der Kläger der Sache nach den Zugang zu der vom Beklagten am 14. April 2015 veranlassten Protokolldatenauswertung begehrt.

Die Klage mit diesem Antrag ist zulässig und begründet. Der angegriffene Bescheid des Beklagten vom 14. Februar

2018 in der Gestalt des Widerspruchsbescheides vom 14. Mai 2019 ist rechtswidrig und verletzt den Kläger in seinen Rechten (vgl. § 113 Abs. 5 VwGO). Der Kläger hat einen Anspruch auf Zugang zur begehrten Information.

Rechtsgrundlage für das Begehren des Klägers ist § 3 Abs. 1 Satz 1 des Gesetzes zur Förderung der Informationsfreiheit im Land Berlin – IFG Berlin. Danach hat jeder Mensch nach Maßgabe dieses Gesetzes gegenüber den in § 2 IFG Berlin genannten öffentlichen Stellen nach seiner Wahl ein Recht auf Einsicht in oder Auskunft über den Inhalt der von der öffentlichen Stelle geführten Akten. Diese Voraussetzungen sind hier gegeben (dazu 1.). Das Vorliegen von Ausschlussgründen hat der Beklagte nicht plausibel dargelegt (dazu 2.).

1. Der Kläger gehört als natürliche Person zum anspruchsberechtigten Personenkreis. Der Polizeipräsident ist als Behörde des Landes Berlin informationspflichtige Stelle gemäß § 2 Abs. 1 IFG Berlin. Die Protokolldatenauswertung ist als schriftlich bzw. elektronisch festgehaltene sonstige Aufzeichnung auch Akte im Sinne des § 3 Abs. 2 IFG Berlin.

2. Der Beklagte muss das Vorliegen von Ausschlussgründen plausibel darlegen. Hieran fehlt es.

a) Soweit der Beklagte sich auf § 62 des Gesetzes zum Schutz personenbezogener Daten in der Berliner Verwaltung – BlnDSG – beruft, folgt hieraus kein spezialgesetzlicher Ausschlussgrund für Informationsansprüche nach dem Informationsfreiheitsgesetz. Vielmehr enthält insbesondere § 62 Abs. 3 BlnDSG nur Regelungen dazu, in welchen Fällen Protokolle, die im Rahmen automatisierter Verarbeitungssysteme erstellt wurden, durch Behörden genutzt werden dürfen. Die Vorschrift schützt indes nicht die die Daten abfragenden Amtsträger.

b) Auch § 6 IFG Berlin steht dem Informationszugangsanspruch des Klägers nicht entgegen. Nach § 6 Abs. 1 IFG Berlin besteht das Recht auf Akteneinsicht oder Aktenauskunft nicht, soweit durch die Akteneinsicht oder Aktenauskunft personenbezogene Daten veröffentlicht werden und tatsächliche Anhaltspunkte dafür vorhanden sind, dass überwiegend Privatinteressen verfolgt werden oder der Offenbarung schutzwürdige Belange der Betroffenen entgegenstehen und das Informationsinteresse (§ 1 IFG Berlin) das Interesse der Betroffenen an der Geheimhaltung nicht überwiegt. Die Norm enthält zwei Varianten, in denen die Veröffentlichung personenbezogener Daten ausgeschlossen ist, einerseits dann, wenn tatsächliche Anhaltspunkte dafür vorhanden sind, dass überwiegend Privatinteressen verfolgt werden (dazu aa)) und andererseits der Offenbarung schutzwürdige Belange der Betroffenen entgegenstehen (dazu bb)).

aa) Das Gesetz enthält mit der primär zu prüfenden ersten Variante (überwiegendes Verfolgen von Privatinteressen) eine abstrakte Interessenabwägung, die dem Schutz personenbezogener Daten vor dem Informationsinteresse den Vorrang einräumt und den Anspruch auf Informationszugang ausschließt. Diese erste Variante des Ausschlussgrundes setzt voraus, dass tatsächliche Anhaltspunkte dafür bestehen, dass überwiegend private Interessen verfolgt werden (OVG Berlin-Brandenburg, Urteil vom 14. Juli 2016 – OVG 12 B 24.15 – juris Rn. 20). Dies ist hier indes nicht der Fall. Denn im Hinblick auf die gegen den Kläger geführten Disziplinarverfahren, mit denen die begehrten protokollierten Poliks-Abfragen in Zusammenhang stehen, steht auch die Kontrolle staatlichen Handelns im Raume (vgl. insoweit OVG Berlin-Brandenburg, Urteil vom 14. Juli 2016 – OVG 12 B 24.15 – juris Rn. 20 a.E.). Darüber hinaus betrifft die Frage nach der Rechtmäßigkeit von Poliks-Abfragen durch einzelne Polizeibeamte auch die Rechtmäßigkeit staatlichen Handelns, so dass mit dem Informationsbegehren nicht überwiegend Privatinteressen verfolgt werden.

bb) Es bestehen auch keine tatsächlichen Anhaltspunkte dafür, dass der Offenbarung schutzwürdige Belange der Betroffenen entgegenstehen und das Informationsinteresse das Interesse der Betroffenen an der Geheimhaltung nicht überwiegt. Denn gemäß § 6 Abs. 2 Satz 1 Nr. 2 IFG Berlin stehen der Offenbarung personenbezogener Daten schutzwürdige Belange der Betroffenen in der Regel nicht entgegen, soweit sich aus einer Akte die Mitwirkung eines bestimmten Amtsträgers oder einer bestimmten Amtsträgerin an Verwaltungsvorgängen, dessen oder deren Name, Titel, akademischer Grad, Beruf, innerdienstliche Funktionsbezeichnung, dienstliche Anschrift und Rufnummer ergeben.

Bei den in der Protokolldatenauswertung enthaltenen personenbezogenen Daten handelt es sich um Daten im Sinne des § 6 Abs. 2 Satz 1 Nr. 2 IFG Berlin, insbesondere um Namen und innerdienstliche Funktionsbezeichnungen der in Poliks abfragenden Polizeibeamten und -beamtinnen, die damit als Amtsträger bzw. Amtsträgerinnen an Verwaltungsvorgängen mitgewirkt haben.

Die Regelvermutung, dass in diesem Fall die schutzwürdigen Belange der Betroffenen nicht entgegenstehen, hat der Beklagte auch nicht entkräftet. Soweit er sich in diesem Zusammenhang wiederum auf § 62 Abs. 3 BlnDSG bezieht, folgt hieraus keine Beschränkung der Kontrollmöglichkeiten des (von Poliks-Abfragen betroffenen) Bürgers über das Informationsfreiheitsgesetz. Vielmehr dürfen gemäß § 62 Abs. 3 BlnDSG die Protokolle für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung gerade auch durch die betroffene Person – also die Person die Gegenstand der Datenabfrage war (s. insoweit § 31 Nr. 1 BlnDSG) – verwendet werden (vgl. zur entsprechenden Regelung im Bundesdatenschutzgesetz Schwichtenberg, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018, § 76 BDSG Rn. 5). Außerdem hat der Beklagte auch nicht im Ansatz dargelegt, warum die in der Protokolldatenauswertung enthaltenen personenbezogenen Daten der die Datenbanken abfragenden Personen so sensibel sind, dass abweichend von der Regelvermutung des § 6 Abs. 2 Satz 1 Nr. 2 IFG Berlin ihrer Offenbarung schutzwürdige Belange entgegenstehen sollen.

Einführung in den Datenschutz

Mitarbeiter schulen via E-Learning.

E-Learning in TV-Studioqualität

- ✓ Rechtssicher gemäß DS-GVO
- ✓ von einem Experten entwickelt
- ✓ Dauer: 45 Minuten
- ✓ animierte Schaubilder und Grafiken
- ✓ interaktive Quizfolgen
- ✓ Abschlusszertifikat
- ✓ auch in englischer Sprache verfügbar

Jetzt informieren:
datakontext.com/eLearning

DATAKONTEXT

Berichte, Informationen, Sonstiges

Ein Leben für den Datenschutz

Interview mit dem Datenschutz-Experten Professor Peter Gola zu seinem vier Jahrzehnte währenden Einsatz für den Datenschutz, den Herausforderungen der DS-GVO und zu seinem neuen Handbuch zum Beschäftigtendatenschutz.

Mit freundlicher Genehmigung entnommen: HR-Performance 1/2020, Datakontext-Verlag

Professor Gola 1999 auf dem Datenschutz-Colloquium in Frankfurt/M.

HRP: Sie befassen sich seit den Anfängen der Datenschutzgesetzgebung mit der Materie. Was war der Auslöser für die Gesetzesinitative?

Professor Peter Gola: Meine berufliche Laufbahn begann nach dem 2. Juristischen Staatsexamen 1969 bei der damals als eine neue Bundesforschungseinrichtung gegründeten Gesellschaft für Mathematik und Datenverarbeitung. Anlass für ihre Gründung und für die gleichzeitig geführte Diskussion, inwieweit automatisierter Verarbeitung personenbezogener Daten persönlichkeitsrechtliche Grenzen zu ziehen sind, war der Folgende: Zum einen wurde die Entwicklung der Auftragsdatenverarbeitung als noch in den Anfängen befindliche unverzichtbare Zukunftstechnologie staatlich gefördert und zum anderen wurden gleichzeitig ihre Gefahren für die Freiheitsrechte der Bürger mehr erahnt als erkannt. Mit der damals übernommenen Vorreiterrolle im Bereich der Datenschutzgesetzgebung haben Wissenschaft und Politik in Deutschland zweifelsohne ein wichtiges Zeichen gesetzt.

Professor Gola 2004 (1. v. r.) auf der DAFTA mit Bernd Hentschel (2. v. r.), dem verstorbenen Inhaber von DATAKONTEXT, und Peter Schaar (4. v. r.), dem ehemaligen Bundesdatenschutz-Beauftragten

HRP: Was sind für Sie seit der DS-GVO die zentralen Herausforderungen für die Personaler und ihre IT-Landschaft?

Prof. Gola: Eine Aufgabe wird es sein, einerseits gesetzeskonforme und gleichzeitig praktikable Wege zur Erfüllung der Transparenzpflichten gegenüber den Beschäftigten bezüglich der sie betreffenden Datenverarbeitung zu finden. Aufsichtsbehörden und die Rechtsprechung sollten klare Linien zwischen den Rechten auf Einsicht, Auskunft, Aushändigung von Kopien und Datentransfer ziehen. Auch für die Verwendung von im Rahmen von algorithmischen Verfahren und künstlicher Intelligenz gewonnenen Erkenntnissen müssen, wenn sie zu beschäftigtenbezogenen Ergebnissen führen, klare Grenzlinien gezogen werden.

HRP: Braucht zukünftig jede Software, die mit personenbezogenen Daten hantiert, ein „Datenschutz-Gen"?

Prof. Gola: Die DS-GVO fordert bei jeder neuen (und, soweit noch nicht geschehen, auch bestehenden) Verarbeitungen von personenbezogenen Daten die Prüfung ihrer Auswirkungen auf den Schutz personenbezogener Daten bzw. besser: die Persönlichkeitsrechte der Betroffenen. Bestehenden Risiken ist durch angemessene Schutzmaßnahmen zu begegnen. Bei einem hohen Risiko bedarf es einer formalen Datenschutz-Folgenabschätzung (DSFA), d.h. eines Checks nach der bereits erfolgten oder der noch zu vollziehenden Implementation des angesprochenen „Datenschutz-Gens". Die Folgenabschätzung hat sich mit den Maßnahmen, Garantien und Verfahren zu befassen, durch die dieses Risiko für die Persönlichkeitsrechte eingedämmt, der Schutz personenbezogener Daten sichergestellt, und die Einhaltung der Bestimmungen der DS-GVO nachgewiesen werden kann.

HRP: Die HR-Software-Entwickler und auch die Personalverantwortlichen haben in all den Jahren keine wirkliche Affinität zum Thema Datenschutz entwickelt. Woran liegt das Ihrer Einschätzung nach?

Prof. Gola: Die in der Frage enthaltene Pauschalaussage trifft wohl zumindest bedingt zu. Das mag daran liegen, dass von beiden genannten Seiten der Datenschutz oft als ein Hindernis gesehen wird, das einem angestrebten Ziel zumindest erschwerend im Wege steht. Ein wenig aber vielleicht auch daran, dass auch die betroffenen Beschäftigten von ihren datenschutzrechtlichen Rechtspositionen nur selten Gebrauch machen. Allein die in den letzten Jahrzehnten ergangene Rechtsprechung belegt, dass zwar die kollektive Seite des Datenschutzes, d.h. die Mitbestimmung der Mitarbeitervertretungen, nicht aber

von einzelnen Beschäftigten geltend gemachte individuelle Datenschutz-Rechtspositionen Konflikte bereiteten; und dies u.a. eben deshalb, weil auch hier die erwähnte Affinität zum eigenen Datenschutz größer sein müsste.
Man mag sich nur vorstellen, vor welchem Problemen viele Personalabteilungen ständen, wenn Beschäftigte ihre zum Teil neuen Rechte auf Einsicht, Auskunft, Aushändigung von Kopien- und Datentransfer mehrheitlich und „routinemäßig" wahrnehmen würden. Jedenfalls muss man jetzt wissen, wie man einer solchen Situation gerecht werden kann, denn die Nicht-Erfüllung obiger Pflichten ist mit einem nicht mehr zu vernachlässigendem Bußgeldkatalog belegt, und fehlende, weil bisher nicht relevant gewordene, Datenschutzorganisation und diesen Problemen nicht Rechnung tragende IT-Technik sind kein Entschuldigungsgrund.

HRP: Die Nutzung personenbezogener Daten treibt das Geschäft im Internet. Sehen Sie das als Geburtsfehler oder als notwendiges Übel an?
Prof. Gola: Zu Beginn der Datenschutzdiskussion wurden die Gefahren für die Freiheitsrechte des Einzelnen in den wachenden Kontrollmöglichkeiten des Staates gesehen. Inzwischen nehmen vornehmlich international aufgestellte Konzerne, deren Geschäft die Vermarktung der Daten ihrer Nutzer ist, die Rolle des „großen Bruders" ein. Informationelle Selbstbestimmung heißt natürlich auch, dass man sich bzw. seine Daten im Internet vermarkten kann. Aufgabe des Datenschutzes ist es, den Nutzern bewusst zu machen, worauf sie sich einlassen. Das nachgefragte notwendige Übel ist, dass das für viele ohne Belang ist.

HRP: Sie sind dem Datenschutz von Beginn an eng verbunden geblieben. Was ist Ihrer Meinung nach bei Thema Datenschutz rückblickend gut und was ist schlecht verlaufen?
Prof. Gola: Betrachtet man die Entwicklung, so wurde aus der marginalen nationalen Einzelregelung des BDSG eine umfassende europaweite, verfassungsrechtlich abgesicherte Rechtsordnung, die durch die Rechtsprechung des EuGH ständig fallbezogen konkretisiert wird. Datenschutz bzw. der Persönlichkeitsschutz des Einzelnen bei der Verarbeitung der ihn betreffenden Daten hat zumindest in Europa eine angemessene Grundlage.

Diese Regeln bedürfen jedoch angesichts der Schnelligkeit der Entwicklung der diesbezüglichen Techniken ständiger Überprüfung. Wobei sich auch abzeichnet, dass den Möglichkeiten der mit dem schon wieder aus der Mode gekommenen Begriff Big Data bezeichneten allumfassenden Datenauswertung und den Möglichkeiten, mittels Künstlicher Intelligenz dem Betroffenen selbst nicht bekannte sensible Informationen zu gewinnen, nicht nur durch unbestimmte Rechtsbegriffe der DS-GVO, sondern durch

Professor Gola (2. v. r.) im Jahr 2012 auf seiner letzten Mitglieder versammlung als Vorsitzender

konkrete Verbote Grenzen gezogen werden müssen.
HRP: Im vorherigen Jahr ist Ihr Handbuch Beschäftigtendatenschutz in der 8. Aufl. erschienen. Welchen Handlungsbedarf sehen Sie hier beim Gesetzgeber?
Prof. Gola: Seit Beginn der allgemeinen Datenschutzgesetzgebung steht die Schaffung eines speziellen Beschäftigtendatenschutzgesetzes für die Privatwirtschaft im Raum. Verschiedene Anläufe sind gescheitert. Allein mit § 32 BDSG a.F. bzw. § 26 BDSG n.F. wurde ein Anlauf gemacht. Art. 88 Abs. 1 DS-GVO eröffnet einen erheblich weiteren Regelungsspielraum. Er könnte genutzt werden, um von der Rechtsprechung und den Aufsichtsbehörden fallbezogen erfolgte Konkretisierungen der Arbeitnehmerrechte in Gesetzesform zu verallgemeinern. Nicht erkennbar ist, dass der

Professor Gola nach der Verleihung des Bundesverdienstkreuzes im Gespräch mit Andreas Jaspers, Geschäftsführer der GDD

Bundesgesetzgeber hiervon in absehbarer Zeit Gebrauch machen wird.
HRP: Wie fühlt sich für Sie ein Leben für den Datenschutz nach mehr als vier Jahrzehnten an?
Prof. Gola: Es war eher ein Leben mit dem Datenschutz, wobei insbesondere die 20 Jahre Lehrtätigkeit an der Hochschule auch andere Schwerpunkte hatten. Es war jedenfalls eine Zeit, in der sich technische Entwicklungen vollzogen, die früher mehrere Generationen gedauert hätten. Zu Beginn meiner beruflichen Tätigkeit gab es kein Mobiltelefon, keinen Laptop, kein Internet. Ob man bei der Beobachtung und juristischen Kommentierung dieser neuen Formen des menschlichen Zusammenlebens allgemein und in der Arbeitswelt im Besonderen etwas für den Datenschutz bewirkt hat, mögen andere beurteilen. Zumindest einige Auszeichnungen belegen das, wozu auch der Ehrenvorsitz der GDD gehört.

HRP: Sie haben das Bundesverdienstkreuz am Bande und 1. Klasse für Ihr vielfältiges Engagement erhalten. Gibt es Anlässe, wo Sie diese Auszeichnung tragen?
Prof. Gola: Ich trage das kleine Abzeichen des Verdienstkreuzes 1. Klasse bei passenden, aber seltenen Anlässen. Mein im Mai des Jahres anstehender 80. Geburtstag wird ein solcher sein.

HRP: Herr Gola, wir danken Ihnen sehr für das Gespräch.

Qualifizierte Mitarbeiter sind der beste Schutz vor Sabotage, Datendiebstahl oder Spionage

Bitkom veröffentlicht Studienbericht zu Wirtschaftsschutz in der digitalen Welt

Wenn es künftig um den Schutz vor Sabotage, Datendiebstahl oder Spionage geht, braucht es vor allem qualifizierte IT-Sicherheitsspezialisten. Praktisch alle Unternehmen (99 Prozent) sehen dies als geeignete Sicherheitsmaßnahme an, 69 Prozent halten sie sogar für sehr geeignet. Knapp dahinter rangieren Mitarbeiterschulungen zu Sicherheitsthemen.

Neben personellen Sicherheitsmaßnahmen spielen für Unternehmen in Zukunft auch technologische Lösungen eine wichtige Rolle. Künstliche Intelligenz und maschinelles Lernen hält fast die Hälfte (47 Prozent) für sehr geeignete Sicherheitsmaßnahmen, etwa wenn es um das Erkennen von Auffälligkeiten in Netzwerkdaten geht. Weitere 46 Prozent finden dies eher geeignet (93 Prozent gesamt). Den Ansatz von ‚Security by Design' in Bezug auf Geräte für das Internet der Dinge halten insgesamt 86 Prozent der Unternehmen für sinnvoll. Das bedeutet, dass Sicherheitsaspekte schon bei der Entwicklung von Geräten mit bedacht werden. Und 8 von 10 (80 Prozent) geben an, dass die Blockchain-Technologie künftig zweckmäßig ist, um sich vor Sabotage, Datendiebstahl oder Spionage zu schützen.

Zu beachten ist, dass der deutschen Wirtschaft durch Sabotage, Datendiebstahl oder Spionage jährlich ein Schaden von mehr als 100 Milliarden Eur entsteht. Drei von vier Unternehmen (75 Prozent) sind in den vergangenen zwei Jahren Opfer geworden, jedes achte Unternehmen (13 Prozent) vermutet dies.

Die gesamten Ergebnisse der Studie „Wirtschaftsschutz in der digitalen Welt" sind nun zum Download verfügbar: https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-in-der-vernetzten-Welt

EDSA: Europäische Leitlinie zur Videoüberwachung beschlossen

Mit Wirksamwerden der DS-GVO hat der Europäische Datenschutzausschuss (EDSA) seine Arbeit aufgenommen. In diesem Gremium sind Datenschutzaufsichtsbehörden aller europäischer Mitgliedstaaten sowie der Europäische Datenschutzbeauftragte und die Europäische Kommission vertreten. Eine wichtige Aufgabe besteht darin, allgemeine Leitlinien zur Interpretation der DS-GVO herauszugeben. Damit soll Klarheit hinsichtlich der Begriffe in den europäischen Datenschutzgesetzen im Sinne einer einheitlichen Auslegung geschaffen werden. Am 28./29. Januar 2020 tagte der EDSA zum 17. Mal und beschloss mit großer Mehrheit eine Leitlinie zum datenschutzkonformen Einsatz von Videoüberwachung.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit nimmt in einer Pressemittelung hierzu Stellung:

„Die seit Mai 2018 wirksame Datenschutz-Grundverordnung (DS-GVO) enthält keine speziellen Regeln zur Videoüberwachung. Deswegen müssen die datenschutzrechtlichen Anforderungen an den Einsatz von Videoüberwachung aus den allgemeinen Regelungen des Gesetzeswerks abgeleitet werden. Dies fordert nicht nur die Unternehmen, die Videotechnik rechtskonform einsetzen möchten, heraus. Auch die europäischen Aufsichtsbehörden stehen vor der Herausforderung, eine europaweit einheitliche Handhabung im Bereich der Videoüberwachung zu schaffen. Die nun beschlossene europäische Leitlinie ist ein wichtiger Beitrag in diesem Prozess. Dem Beschluss gingen intensive Verhandlungen zwischen den europäischen Aufsichtsbehörden im Datenschutzausschuss voraus. Zudem erfolgte eine großangelegte Beteiligung der Öffentlichkeit, bei der sich Interessenvertreterinnen und -vertreter aus Wirtschaft, Politik, Zivilgesellschaft wie auch Privatpersonen einbringen konnten.

Die Leitlinie betont den Grundsatz der Verhältnismäßigkeit. Da jede Videoüberwachung mit einem Eingriff in die Persönlichkeitsrechte verbunden ist, muss ihr stets ein berechtigtes Interesse des Kamerabetreibers zugrunde liegen. Dieses Interesse muss objektiv vorliegen, das heißt, bei einer Videoüberwachung aus Sicherheitsgründen müssen stets auch tatsächliche Anhaltspunkte für eine Gefahr für Leib, Leben oder Sachgüter vorliegen. Die Leitlinie stellt klar, dass ein rein subjektives Sicherheitsgefühl nicht genügt, um eine Videoüberwachung zu rechtfertigen. Auch mit Blick auf die Verarbeitung biometrischer Daten bietet die Leitlinie Klarheit. Gemäß der DS-GVO ist es privaten Unternehmen ohne ausdrückliche Einwilligung der Betroffenen grundsätzlich verboten, solche Daten zum Zwecke der Identifizierung bestimmter Personen zu verarbeiten. Die Leitlinie konkretisiert nunmehr die strengen Anforderungen der DS-GVO an die Wirksamkeit solcher Einwilligungen. Außerdem bietet sie Hilfestellungen zu Fragen der Transparenz bei Videoüberwachungsmaßnahmen."

Die Europäische Leitlinie zur Videoüberwachung wird in Kürze veröffentlicht und auf den Webauftritten der Berliner Beauftragten für Datenschutz und Informationsfreiheit (www.datenschutz-berlin.de) sowie des Europäischen Datenschutzausschusses (https://edpb.europa.eu/edpb_de) abrufbar sein.

Literaturhinweise

Utz Kramer (Hrsg.), **Sozialdatenschutzrecht**, Nomos Verlag, Baden-Baden, 4. neu bearbeitete Aufl., 2020, 488 S., € 78,00

Das Sozialgesetzbuch ist in der Bundesgesetzgebung eine eigenständige, umfangreiche Materie, die dem Umstand Rechnung trägt, dass das Sozialstaatsprinzip in unserem Grundgesetz nach ausgewogenen Regelungen verlangt, die zwischen dem Funktionieren der staatlichen Fürsorge und den Persönlichkeitsrechten der betroffenen Menschen unter Beachtung des überwiegenden Allgemeininteresses einen sachgerechten und angemessenen Ausgleich herstellen. Insbesondere der Datenschutz ist im Sozialbereich als bereichsspezifisches Normengeflecht gewachsen, der das komplette öffentliche Datenschutzrecht über die allgemeinen Bestimmungen hinaus nochmals eigenständig abbildet und für die besondere Situation im sozialen Kontext modifiziert.

Diesem Komplex widmet sich der vorliegende Handkommentar. Nach Inkrafttreten und Wirksamwerden der europäischen Datenschutzgrundverordnung ergab sich die Notwendigkeit, das eingeführte und bereits in der Vorauflage (3. Aufl. 2011) vielbeachtete Werk vollkommen neu zu bearbeiten, da die bereichsspezifischen Regelungen im Lichte des europäischen Datenschutzrechts verändert gelten und zuletzt durch das 2. Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679, vom 20.11.2019, BGBl. I, S. 1626, Artt. 119 ff., angepasst wurden. Dem Herausgeber ist es gelungen, für diese Aufgabe ein hochqualifiziertes Verfassergremium zu gewinnen, das aus Wissenschaftlern, renommierten Datenschützern und Praktikern im Sozialrecht besteht und damit die Voraussetzungen erfüllt, um das Thema von allen einschlägigen Seiten zu beleuchten.

Gerade die Kommunale Praxis hat sehnsüchtig auf diesen handlichen Band gewartet, der sichtlich einen guten Eindruck hinterlässt. Neben einer – nützlichen – Übersicht über die aktuelle Literatur ist dem Band eine Einführung vorangestellt, die besonders dem neu mit Sozialdatenschutzrecht befassten Leser hilfreiche Dienste leistet. Der Standort des Sozialdatenschutzrechts im Kontext der Datenschutzgrundverordnung, seine Struktur und Regelungssystematik sowie ein Überblick über die Inhalte vertiefen das Verständnis des Lesers, ohne ihn mit der Komplexität der Einzelnormen zu überfordern. Denn die Paragraphen haben aufgrund ihrer gedrängten nachträglichen Einfügung den Rahmen einer normalen Nummerierung des SGB X gesprengt und konnten – gleich mehrfach – nur unter Hinzufügung von Buchstaben und Buchstabenreihen zur laufenden Nummer die korrekte Reihenfolge behalten. Umso wichtiger war es, dass sich das vorliegende Werk vorgenommen hat, Struktur und Systematik für den Nutzer begreifbar zu ordnen, wozu diese Einführung zweifellos wesentlich beigetragen hat.

Die eigentliche Kommentierung zunächst des grundlegenden § 35 SGB I und danach der §§ 67 bis 85a SGB X enthält durchgehend vor jeder Norm eine ausführliche Kommentierungsgliederung mit dem Hinweis auf die die Auffindung der Bemerkungen erleichternden Randnummern. Der Abdruck der Gesetzesmaterialien zu den einzelnen Normen ist dem Nutzer sofort verfügbar und erleichtert ihm in Zweifelsfällen die (historische und systematische) Auslegung. Ein besonderes Alleinstellungsmerkmal des Werkes sind die zahlreichen Schaubilder, die schon die Vorauflage auszeichnete und gute Vorbilder für Schulungsfolien boten. Sie vereinfachen wie lehrbuchartige Übersichten, die unter didaktischen Aspekten erarbeitet sind, die korrekte Anwendung für den Praktiker im einzelnen Fall. Hervorzuheben ist zudem, dass der Bezug zur europäischen Datenschutzgrundverordnung immer wieder deutlich gemacht und – als Beispiel im Anhang nach § 79 SGB X durch einen Exkurs zur Datenschutz-Folgeabschätzung nach Art. 35 DS-GVO – bisweilen ausführlich erläutert wird, wo und inwiefern auf die Beziehung des Sozialdatenschutzes zum übergeordneten europäischen Recht besonders zu achten ist.

Ein ausführliches Stichwortverzeichnis – das in einer guten Kommentierung bekanntlich nicht fehlen darf – rundet dieses handliche Werk ab.

Das Buch ist insgesamt gesehen eine höchst nützliche Fundgrube für die korrekte Anwendung der sozialdatenschutzrechtlichen Bestimmungen in der Praxis. Alle öffentlichen Leistungserbringer, ob in Kommunen oder anderswo, die Träger der freien Wohlfahrtspflege, die Justiz, Rechtsanwälte und rechtsberatende Stellen sowie jeder, der auf der Seite Betroffener mit dem Thema befasst ist, sie alle finden in dieser Kommentierung die notwendige Unterstützung für ihre Arbeit. Auch Lernenden ist das Buch unentbehrlich; es sollte in keiner Bibliothek fehlen.

(Dr. Martin Zilkens)

Michael Nitsch (Hrsg.), **Compliance und soziale Verantwortung im Unternehmen,** Tagungsband 4. Wiesbadener Compliance-Tag der EBS Law School – Center for corporate Compliace, Schriften der EBS-Law School, Bd. 12, Nomos Verlag, Baden-Baden, 2019, 129 S., € 49,00

In der 4. Aufl. des Wiesbadener Compliance Tages widmen sich die Vorträge aktuellen Entwicklungen der Compliance. Allen voran geht es um die Neuerungen des Datenschutzrechts durch die DS-GVO und deren Auswirkungen auf unternehmensinterne Prozesse. Weiter wird die Entwicklung der sozialen Verantwortung von Unternehmen, die mit der Umsetzung der CSR-Richtlinie nunmehr Verbindlichkeit im deutschen Recht hat, näher beleuchtet. Schließlich stehen Pflichten von Gesellschaftsorganen im Focus mit ihrer strafrechtlichen Haftung und der Möglichkeit der Versicherbarkeit von Complianceverstößen. Zu den Autoren zählen Micheal Nietsch, Peter Gola, Birgit Spießhofer, Jürgen Tascke, Frank Salinger und Horst Ihlas.

(Redaktion)

Katharina Höhne, **Auswirkungen der unionsrechtlichen Öffnungsklausel nach Art. 88 DS-GVO auf den Beschäftigtendatenschutz nach deutschem Recht,** Beiträge zu Datenschutz und Informationsfreiheit, Bd. 28, Verlag Dr. Kovac, Hamburg 2019, 236 S., € 88,90

Die Publikation, die die Dissertation der Verfasserin wiedergibt, gliedert sich in mehrere Schritte.

Zur Bestimmung der Auswirkung der Öffnungsklausel gem. Art. 88 DS-GVO wird schrittweise vorgegangen. Zunächst wird ein Überblick über die Entwicklung des Beschäftigtendatenschutzes gegeben sein. Hierbei wird mit einem Abriss über die Entwicklung des Beschäftigtendatenschutzes auf nationaler und europäischer Ebene begonnen, der sich in die zwei Zeitabschnitte „bis zur Reform durch die DS-GVO" (1. Kapitel) und „im Licht der DS-GVO" (2. Kapitel) gliedert. Der erste Zeitabschnitt dieses Abrisses thematisiert schwerpunktmäßig die nationalen Forderungen an den Beschäftigtendatenschutz und den Einfluss des Unionsrechts auf das nationale Beschäftigtendatenschutzrecht. Der zweite Zeitabschnitt widmet sich den Hintergründen der DS-GVO und des Art. 88 DS-GVO. Auf diese Grundlagen wird im Laufe dieser Arbeit immer wieder zurückzukommen sein. Anschließend (3. Kapitel) soll die Legitimation des Beschäftigtendatenschutzes, die Digitalisierung illustriert werden, indem die wichtigsten technischen Neuerungen mit Relevanz für den Beschäftigtendatenschutz dargestellt wird.

In einem weiteren Schritt soll der Rechtsrahmen des Art. 88 DS-GVO festfelegt werden (2. Teil). Begonnen wird mit einer rechtlichen Einordnung des Ar. 88 DS-GVO (4. Kapitel). Der Schwerpunkt liegt hierbei auf der Untersuchung der Primärrechtmäßigkeit und der Rechtsnatur des Art. 88 DS-GVO. Hierauf folgt das Herzstück dieser Arbeit, eine Analyse des Regelungsgehalts des Art. 88 DS-GVO (5. Kapitel). Dem ist zunächst ein Abschnitt zur Methodik vorangestellt, in dem die Spezifika der Auslegung unionsrechtlicher Vorschriften wie dem hier einschlägigen Art. 88 DS-GVO herausgearbeitet werden (Abschnitt A). Art. 88 DS-GVO wird sodann sowohl auf seine zwingenden Vorgaben als auch auf die Regelungsspielräume an die Mitgliedstaaten untersucht. Immense Bedeutung kommt hierbei dem persönlichen Anwendungsbereich, konkret der Auslegung des Beschäftigtenbegriffs (Abschnitt B. III.), und dem Grad der Regelungstiefe des Art. 88 DS-GVO (Abschnitt F) zu.

Die in Kapitel 5 erreichten Ergebnisse stellen die Basis für die Beurteilung der Zukunft von Gesetzgebung und Betriebsvereinbarungen im Beschäftigungskontext nach deutschem Recht dar. Analysiert wird der Gestaltungsspielraum, den Art. 88 DS-GVO den Mitgliedstaaten lässt (6. Kapitel). Nachgegangen werden soll neben der Darstellung des Regelungsgehalts zunächst der Frage, ob § 26 BDSG-neu den von Art. 88 DS-GVO vorgegebenen Rahmen einhält. Zudem werden die Änderungen § 26 BDSG-neu gegenüber der bisherigen Rechtslage beleuchtet. In einem weiteren Schritt wird das Verhältnis des BDSG-neu zu Rechtsvorschriften und Gesetzten außerhalb des BDSG mit Relevanz für den Beschäftigtendatenschutz dargestellt. (8. Kapitel). Das Kapitel der Zukunft des deutschen Beschäftigtendatenschutzes endet mit einer Untersuchung des Schicksals von Kollektivvereinbarungen, wobei der Schwerpunkt auf Betriebsvereinbarungen aufgrund ihrer praktischen Relevanz gelegt werden soll (9. Kapitel). Zu guter Letzt werden die wesentlichen Ergebnisse der Arbeit zusammengefasst (4. Teil).

(Schriftleitung)

13. GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.
Sommer-Workshop
FÜR DATENSCHUTZBEAUFTRAGTE UND -BERATER SOWIE DATENSCHUTZDIENSTLEISTER
Timmendorfer Strand
3. bis 5. August 2020
Jetzt informieren und anmelden unter datakontext.com
DATAKONTEXT GmbH
Postfach 41 28 · 50217 Frechen
Tel.: +49 2234 98949-40 · Fax: + 49 2234 98949-44
tagungen@datakontext.com
DATAKONTEXT-Repräsentanz
Postfach 20 03 03 · 08003 Zwickau
Tel.: +49 375 291728 · Fax: + 49 375 291727
zwickau@datakontext.com
GDD Gesellschaft für Datenschutz und Datensicherheit e.V.
DATAKONTEXT

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegen genommen.

Geminn, Christian L., **Menschenwürde und menschenähnliche Maschinen und Systeme**, DÖV 2020, S. 172
Gefordert wird die Beachtung von Menschenwürde und Persönlichkeitsrechten bei der Konzeption von IT-Produkten.

Gola, Peter, **Der betriebliche Datenschutzbeauftragte als „Geheimnisträger" – Ein Überblick**, PinG 2020, S. 84
Bei der Wahrnehmung ihrer Aufgaben unterliegen Datenschutzbeauftragte im Interesse der Betroffenen als auch des Verantwortlichen bestehenden zahlreichen, sich nicht nur aus der DS-GVO ergebenden Vertraulichkeits- und Geheimhaltungspflichten.

Gola, Peter/Klug, Christoph, **Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2019**, NJW 2020, S. 660
Die Autoren setzen ihre halbjährliche Berichterstattung über die Entwicklung des Datenschutzrechts fort.

Gostomzyk, Tobias, **Veröffentlichung von Zitaten aus anwaltlichem Schriftsatz in einer Zeitschrift**, NJW 2020, S. 770
Der Autor erörtert in einer Anmerkung zum Urteil des BGH vom 26.11.2019 – VI ZR 12/19 – inwieweit Zitate aus anwaltlichen Schriftsätzen in Zeitschriften zitiert werden dürfen. Auch wenn sich Anwälte in Antwortschreiben auf Presseanfragen nicht einlassen, dürfen die Medien nach dem BGH ggf. trotzdem daraus zitieren. Soweit es um öffentliche Kommunikation geht, ist das Datenschutzrecht nicht anwendbar.

Karg, Marlies, **Passgenauer Schutz von Mandantendaten in der Steuerkanzlei**, NWB 2020 S. 654
Karg untersucht die besonderen Anforderungen an den Schutz von Mandantendaten.

Kirchert, Katrin, **Die Abkehr vom Schriftformerfordernis bei Einwilligungen im Beschäftigungskontext – Die Einwilligungen von Beschäftigten – nun auch als E-Mail möglich?** PinG 2020, S. 82
Die Autorin beantwortet die gestellte Frage positiv und gibt Handlungshinweise.

Kolmar, Frederike, **Umfang und Reichweite gemeinsamer Verantwortlichkeiten im Datenschutz**, NVwZ 2019, S. 1740
Die Autorin legt dar, wie seit der EuGH-Entscheidung in Sachen „Google Spain" (Urteil vom 13.05.2014 – C-131/12) der Begriff des (gemeinsam) Verantwortlichen als Adressat datenschutzrechtlicher Pflichten kontinuierlich erweitert worden ist.

Paal, Boris, **Meldepflicht bei Datenschutzverstößen nach Art. 33 DS-GVO**, ZD 2020, S. 119
Der Beitrag geht der Frage nach, welche Maßstäbe an das Vorliegen einer Datenschutzverletzung und die Beurteilung des erforderlichen Risikos zu stellen sind und gibt Empfehlungen betreffend des Eintritts der Meldepflicht.

Specht-Riemenschneider, Louisa, **Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!**, MMR 2020, S. 73
Die Autorin sieht den Hersteller in der Haftung für nicht den Datenschutzanforderungen entsprechende Produkte.

Strassemeyer, Laurenz, **Die Transparenzvorgaben der DSGVO für algorithmische Verarbeitungen**, K&R 2020, S. 176
Personenbezogene Daten werden zunehmend mit immer komplexeren technischen Systemen verarbeitet, wie beispielsweise künstlichen neuronalen Netzen. Dies erschwert die Einhaltung von Transparenzanforderungen der DS-GVO fortlaufend.

Taeger, Jürgen/Schweda, Sebastian, **Die gemeinsam mit anderen Erklärungen erteilte Einwilligung**, ZD 2020, S. 124
Der Beitrag erörtert das Urteil des EuGH zu Rechtsprechung Planet49 mit der im Aufsatztitel genannten Thematik, der Wirksamkeit von Cookie-Einwilligungen sowie Aspekten des Koppelungsverbots.

Wolff, Heinrich Amadeus, **Die Relativität des Personalaktenbegriffs**, ZBR 2019, S. 325
Wolff zeigt, dass die Regelungen zu den Personalakten der Beamten ein Sonderrechtsgebiet bilden, das sich mit der Zeit wandelt, aber über dessen Reichweite bis heute Unsicherheit besteht.

„Datenspenden“ gegen Corona

In der digitalisierten Welt hinterlässt jeder eine Vielzahl von persönlichen Daten. Häufig verbietet es der Datenschutz, diese Informationen zu nutzen. Das ist oft schade, denn es gibt Zwecke, für die so mancher seine Daten vielleicht gerne teilen würde. Denken wir an die Pandemiebekämpfung. Das Robert Koch-Institut könnte etwa Bewegungsdaten aus Mobiltelefonen gut verwenden, um Kontaktpersonen von mit dem Corona-Virus infizierten Personen oder Risikogebiete innerhalb Deutschlands zu ermitteln, um dessen Ausbreitung zu verlangsamen. Ob der Staat einen derart intensiven Eingriff anordnen dürfte, ist datenschutzrechtlich zu bezweifeln. Aber jeder Einzelne könnte seine zeitlich begrenzte Überwachung doch nach eigenem Ermessen und freiwillig erlauben, um durch seine „Bewegungsdatenspende“ einen Beitrag zur Sicherung der Gesundheit der Bevölkerung zu leisten. Entscheidend ist dann, dass die Daten nur zu den erlaubten Zwecken genutzt werden. Dazu müsste die Erhebung und Verarbeitung der Daten staatlich reglementiert und organisiert werden. Es müsste klargestellt werden, wer zu welchen Zwecken Zugriff auf die Daten hat und dass sie nach dem Ende der Pandemie gelöscht oder aber zu statistischen Zwecken oder für die Schaffung eines Warnsystems mit entsprechender Einwilligung weiterverwendet werden dürfen. Diese Aufgabe könnte ein Datentreuhänder übernehmen, der als „Sachwalter der Privatsphäre“ die Datenspenden organisiert. Der Staat kann das selbst übernehmen oder die Aufgabe einem privaten Treuhänder überlassen, der nach engen Regeln Rechenschaft über die Verwendung der Daten geben müsste.

WIR VERSCHAFFEN HANDLUNGSFREIHEIT.

Bereit, um etwas zu bewegen?

CBH
RECHTSANWÄLTE

CBH ist eine der führenden Wirtschaftskanzleien in Deutschland und berät in den strategischen Schwerpunkten Geistiges Eigentum, Medien und IT, Unternehmen und Finanzen, Personal und Sozialwesen, Bau und Immobilien sowie Verwaltung und Wirtschaft.

Im Fachbereich IT-Recht decken wir das gesamte Spektrum IT-rechtlicher Angelegenheiten ab und konzentrieren uns unter anderem auf datenschutzrechtliche Fragen. Datenschutz-Compliance verstehen wir dabei nicht nur als Pflichtaufgabe unserer Mandaten, sondern auch als Chance.

Unsere Ansprechpartner für IT- und Datenschutzrecht, Dr. Sascha Vander, LL.M. (s.vander@cbh.de) und Niklas Kinting (n.kinting@cbh.de), unterstützen Sie gerne.

Mehr Infos unter www.cbh.de

JUVE 2019 AWARDS
Kanzlei des Jahres für Vergaberecht

JUVE TOP 50
Wirtschaftskanzlei Deutschland
2019|2020

KÖLN BERLIN HAMBURG MÜNCHEN STUTTGART COTTBUS

Ihre DS-GVO Umsetzung smart auditiert und visualisiert.

DS-GVO Compliance Check

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit dem neuen Excel-Tool »DS-GVO Compliance Check«!

weitere Informationen unter:
www.datakontext.com/compliancecheck

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT