

Zeitschrift für
Datenschutz-,
Informations- und
Kommunikationsrecht

RDV

6/2020

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

DAMMANN, Alexa Skills auf dem Prüfstand der DS-GVO

LIESEM, Hohes Risiko oder doch nicht?

SCHULZ, Cookies, Schrems & Co. – Webseitengestaltung
zwischen rechtlichen Vorgaben und Businessperspektive

ZIEBARTH, Gesetzliche Strukturänderungen bei
Datenschutz-Aufsichtsbehörden in EU, Bund und Ländern

Kurzbeiträge

GOLA, Aus den aktuellen Berichten und Informationen der
Aufsichtsbehörden (50): Verarbeitungen zur Vertragserfüllung
und Benennung von Datenschutzbeauftragten
(u.a. im 25. TB der LfDI Niedersachsen (2019) vom 03.09.2020)

SUNDERMANN, Sperrt Art. 79 Abs. 1 DS-GVO Unterlassungsklagen
gegen Verantwortliche?

CLAUS/REIF, Praxisfälle zum Datenschutzrecht VII:
Musterfalllösung zur Heimarbeit

Rechtsprechung

Aus dem Inhalt

EUGH, Persönlichkeitsgutachten auf einer Partnervermittlungs-
Website ist keine Lieferung „digitaler Inhalte“

EUGH, Rechtsbehelf gegen ein Auskunftersuchen in Steuersachen (Ls)

BGH, Zu den Voraussetzungen eines Auslistungsanspruchs gegen den
Verantwortlichen eines Internet-Suchdienstes nach Art. 17 DS-GVO

BAG, Benachteiligung wegen der Religion bei Kopftuchverbot einer
Lehrerin (Ls)

BAG, Anspruch des Betriebsrats auf Einsicht und Auswertung
von Entgeltlisten nach EntgTranspG

36. Jahrgang
Dezember 2020
Seiten 287–348



Gesellschaft für Datenschutz
und Datensicherheit e.V.


DATAKONTEXT
www.rdv-online.de

mit Muster
Löschkonzept
zum
Download



Löschen nach DS-GVO in der Praxis
Sascha Kremer

1. Auflage 2020
122 Seiten / DIN A 4
ISBN: 978-3-89577-851-3
99,99 € inkl. E-Book und
Arbeitshilfen (PDF)

Bestellen Sie direkt unter:
datakontext.com/loeschkonzepte

Inhaltsverzeichnis

Editorial	287	Entschädigung bei Benachteiligung wegen Schwerbehinderung (Ls) (BAG, Urteil vom 28.05.2020)	338
Veranstaltungen	288	Auskunft hinsichtlich anderweitigen Erwerbs (Ls) (BAG, Urteil vom 27.05.2020)	338
Aufsätze			
Wiebke DAMMANN, LL.M. Alexa Skills auf dem Prüfstand der DS-GVO	289	Zum Umfang der Unterrichtung des Betriebsrats bei außerordentlicher Kündigung (BAG, Urteil vom 07.05.2020)	338
Kerstin LIESEM Hohes Risiko oder doch nicht?	297	Kündigungsschutz einer Schwangeren vor Arbeitsantritt (BAG, Urteil vom 27.02.2020)	339
RA Sebastian SCHULZ Cookies, Schrems & Co. – Webseitengestaltung zwischen rechtlichen Vorgaben und Businessperspektive	302	Keine Abhängigkeit des Inkrafttretens einer Betriebsvereinbarung von einem Belegschaftsquorum (Ls) (BAG, Beschluss vom 28.07.2019)	341
Dr. Wolfgang ZIEBARTH Gesetzliche Strukturänderungen bei Datenschutz-Aufsichtsbehörden in EU, Bund und Ländern	309	Tätowierungsverbot für Bayerische Polizeivollzugsbeamte (Ls) (BVerwG, Urteil vom 14.05.2020)	341
Kurzbeiträge			
Prof. Peter GOLA Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (50): Verarbeitungen zur Vertragserfüllung; Informationspflichten und Benennung von Datenschutzbeauftragten im Gesundheitsbereich (u.a. im 25. Tätigkeitsbericht der LfDI Niedersachsen (2019) vom 03.09.2020)	314	Rechtsweg zu den Arbeitsgerichten bei einem Rechtsstreit um Datenschutz eines Angestellten der Erzdiözese (LAG Nürnberg, Beschluss vom 29.05.2020)	342
Steffen SUNDERMANN Sperrt Art. 79 Abs. 1 DS-GVO Unterlassungsklagen gegen Verantwortliche?	317	Bestattungsgesetz hat Vorrang vor Informationsfreiheitsgesetz (Ls) (VerwGH Mannheim, Beschluss vom 06.08.2020)	342
Miriam CLAUS, LL.M./ RAin Yvette REIF, LL.M. Praxisfälle zum Datenschutzrecht VII: Musterfalllösung zur Heimarbeit	321	Zum Auskunftsanspruch gegenüber einer Bank (AG Bonn, Urteil vom 30.07.2020)	342
Rechtsprechung			
Persönlichkeitsgutachten auf einer Partnervermittlungs-Website ist keine Lieferung „digitaler Inhalte“ (EuGH, Urteil vom 08.10.2020)	324	Personalratswahl mit Corona-Einschränkungen (Ls) (VerwG Köln, Beschluss vom 07.10.2020)	344
Rechtsbehelf gegen ein Auskunftersuchen in Steuersachen (Ls) (EuGH, Urteil vom 06.10.2020)	327	Anforderungen an eine Beschwerde bei der Aufsichtsbehörde (Ls) (VerwG Mainz, Urteil vom 22.07.2020)	344
Zu den Voraussetzungen eines Auslistungsanspruchs gegen den Verantwortlichen eines Internet-Suchdienstes nach Art. 17 DS-GVO (BGH, Urteil vom 27.07.2020)	327	Berichte, Informationen, Sonstiges	
Benachteiligung wegen der Religion bei Kopftuchverbot einer Lehrerin (Ls) (BAG, Urteil vom 27.08.2020)	334	BayLDA: Typische Fehler bei Auskunftersuchen	345
Anspruch des Betriebsrats auf Einsicht und Auswertung von Entgeltlisten nach EntgTranspG (BAG, Beschluss vom 28.07.2020)	334	Datenverarbeitungen des Betriebsarztes	345
Auskunftsberechtigte nach dem Entgelttransparenzgesetz (Ls) (BAG, Urteil vom 25.06.2020)	338	Literaturhinweise	
		<i>Buchbesprechungen</i>	
		Alexander Roßnagel/Christian Geminn, DS-GVO verbessern – Änderungsvorschläge aus Verbrauchersicht	346
		Sebastian Buten, Die Betroffenenrechte nach der DS-GVO und ihre Umsetzung in der kommunalen Praxis	346
		Tassilo-Rouven König, Beschäftigtendatenschutz in der Beratungspraxis	346
		Thomas Götz, Big Data im Personalmanagement: Datenschutzrecht und betriebliche Mitbestimmung Theorie und Praxis des Arbeitsrechts	346
		<i>Neuerscheinungen</i>	
		Aufsätze	347
		Nachgefasst	348

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 LINNENKOHLE, Universität Kassel

Prof. Dr. Boris PAAL, M. Jur. (Oxford), Universität Freiburg

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. Irimi VASSILAKI, Athen/München

Prof. Dr. Wolfgang ZÖLLNER, Universität Tübingen

Beilagenhinweis: GDD-Mitteilungen 6/2020; 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 € 155,-

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

Grafisches Centrum Cuno GmbH & Co. KG

Gewerbering West 27, 39240 Calbe (Saale)

Anzeigenverwaltung

DATAKONTEXT GmbH, Frechen

Wolfgang Scharf

Telefon: (0 22 34) 9 89 49-60

wolfgang.scharf@datakontext.com

www.datakontext.com

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 6

Seiten 287–348

RDV

Recht der Datenverarbeitung

36. Jahrgang · Dezember 2020 · Seiten 287–348

Editorial

Das EntgTransG – ein Gesetz auf dem Prüfstand

Das seit dem 6. Juli 2017 in Kraft befindliche Gesetz zur Förderung der Transparenz von Entgeltstrukturen (EntgTranspG) soll Beschäftigte bei der Durchsetzung ihres Anspruchs auf gleiches Entgelt bei gleicher oder gleichwertiger Arbeit unterstützen und enthält ein weiteres Mal ein Verbot der Entgeltbenachteiligung (§ 3) bzw. ein Entgeltgleichheitsgebot (§ 7) für Frauen. Basis für die Durchsetzung der Entgeltgleichheit bildet ein datenschutzkonform ausgestalteter individueller, sich auf anonymisierte Vergleichsentgelte erstreckender Auskunftsanspruch. Begrenzt ist der individuelle Auskunftsanspruch auf Beschäftigte in Betrieben mit mehr als 200 Mitarbeitern (§§ 11 bis 16 EntgTranspG). Bei Bewerbern bestehen Ansprüche zur Überprüfung der angebotenen Vergütung nicht.

Der von der Bundesregierung nunmehr pflichtgemäß vorgelegte Evaluationsbericht bestätigt, dass das Gesetz bislang – u.a. mangels Nutzung des Auskunftsrechts durch die Betroffenen – Arbeitgeber vor keine Probleme gestellt hat. Des Weiteren führten Auskunftsbegehren häufig nicht zu einer Anpassung des Gehaltes (7 Prozent) oder der Entgeltregelungen (6 Prozent). Die Bundesregierung will daher die Praktizierung des EntgTransG durch die Bereitstellung von Informations-

und Beratungsangeboten gezielt unterstützen und insbesondere prüfen, wie der Auskunftsanspruch zu vereinfachen und zu verbessern wäre und hierbei die Erfahrungen europäischer Staaten mit vergleichbaren Regelungen prüfen (vgl. hierzu u.a. BT-Drs. 19/18043 v. 18.03.2020).

Ein Grund für die geringe Resonanz des EntgTranspG bei den Beschäftigten wird auch darin vermutet, dass das Gesetz lediglich einen Auskunftsanspruch, aber keinen Durchsetzungsanspruch oder diesbezügliche Unterstützung gewährt. Will der Arbeitgeber das „Vergleichsentgelt“ nicht ermitteln bzw. nicht zahlen, müssen die Betroffenen gegen den Arbeitgeber gerichtlich vorgehen. Das im Gesetzgebungsverfahren erörterte Verbandsklagerecht für Gewerkschaften oder zertifizierte Antidiskriminierungsverbände oder zumindest die Ermöglichung einer Prozessstandschaft wurde nicht vorgesehen (BT-Drs. 18/4321, S. 2; BT-Drs. 18/6550, S. 6), was sich nunmehr als Manko erweist (Hinrichs, in: Däubler/Bertzbach, AGG, EntgTranspG § 10 Rn. 4 m.w.N.).

Der Gesetzgeber wird also hinsichtlich der Effektivität des Gesetzes nachjustieren müssen. Vorgaben hierzu will bzw. wollte die EU-Kommission bis Ende 2020 mit neuen Regelungen zur Entgelttransparenz machen (vgl. Mitteilung der EU-Kommission vom 05.03.

2020: „Eine Union der Gleichheit: Strategie für die Gleichstellung der Geschlechter 2020 – 2025“). Auf die Bedenken der Wirtschaft, die weitere legislative Maßnahmen zu verpflichtender Lohntransparenz als nicht zielführend und notwendig bewertet, da sie die Ursachen für Entgeltunterschiede nicht angehen, sei hingewiesen (Verband der Bayerischen Wirtschaft, Die Aktionsfelder und Handlungsthemen der vbw).

<https://www.vbw-bayern.de/vbw/Aktionsfelder/index.jsp> Aktionsfelder/Europa, EU-Recht; EU-Richtlinie Entgelttransparenzgesetz.

Prof. Peter Gola



Prof. Peter Gola

Mitherausgeber und federführender Schriftleiter der Fachzeitschrift RDV sowie Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

Termin	Thema	Ort	Kontakt
12.01.21	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Stuttgart	GDD e.V. und DATAKONTEXT
04.02.21	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Online-Schulung	GDD e.V. und DATAKONTEXT
08.02.21	Datenschutz in medizinischen Einrichtungen	Köln	GDD e.V. und DATAKONTEXT
09.02.21	Grundlagen der Auftragsverarbeitung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
23.02.21	Datenschutz International	Berlin	GDD e.V. und DATAKONTEXT
25.02.21	Videoüberwachung nach BDSG und DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
02.03.21	Basiswissen IT-Sicherheit	Online-Schulung	GDD e.V. und DATAKONTEXT
03.03.21	Grundlagen der Auftragsverarbeitung	Online-Schulung	GDD e.V. und DATAKONTEXT
04.03.21	Mobile Endgeräte im Zeitalter von DS-GVO und ePrivacy-Verordnung	München	GDD e.V. und DATAKONTEXT
08.03.21	Konzerndatenschutz	Köln	GDD e.V. und DATAKONTEXT
09.03.21	ISO 27001 und Datenschutz	Berlin	GDD e.V. und DATAKONTEXT
10.03.21	Onlinedatenschutz auf dem Weg zur ePrivacy-Verordnung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
11.03.21	Datenschutz International	Online-Schulung	GDD e.V. und DATAKONTEXT
16.03.21	Datenschutz und Betriebsrat unter der DS-GVO	Frankfurt/M.	GDD e.V. und DATAKONTEXT
23.03.21	Datenschutz-Management light	Stuttgart	GDD e.V. und DATAKONTEXT
24.03.21	Löschen nach DS-GVO	Berlin	GDD e.V. und DATAKONTEXT
25.03.21	Onlinedatenschutz auf dem Weg zur ePrivacy-Verordnung	Online-Schulung	GDD e.V. und DATAKONTEXT
25.03.21	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Online-Schulung	GDD e.V. und DATAKONTEXT
30.03.21	Datenlöschung und andere SAP-Funktionen für den Datenschutz	Frankfurt/M.	GDD e.V. und DATAKONTEXT
31.03.21	Compliance-Tests und Schwachstellenscannen	Köln	GDD e.V. und DATAKONTEXT
13.04.21	ISO 27001 und Datenschutz	Online-Schulung	GDD e.V. und DATAKONTEXT
13.04.21	Verzeichnis von Verarbeitungstätigkeiten	Frankfurt/M.	GDD e.V. und DATAKONTEXT
15.04.21	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Online-Schulung	GDD e.V. und DATAKONTEXT
15.04.21	Websites datenschutzkonform gestalten	Köln	GDD e.V. und DATAKONTEXT
20.04.21	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
21.04.21	Planung und Umsetzung der Überwachungsaufgaben des DSB	Köln	GDD e.V. und DATAKONTEXT

Aufsätze

Wiebke Dammann, LL.M.

Alexa Skills auf dem Prüfstand der DS-GVO

Die Verbreitung von Smart-Home-Komponenten in deutschen Haushalten steigt stetig.¹ Auch die gängigen Sprachassistentendienste erfreuen sich trotz anfänglicher Skepsis zunehmender Beliebtheit. Für Unternehmen gehen mit der neuen Technik interessante Marketingansätze zur Kundenbindung einher. Der US-Konzern Amazon ermöglicht Unternehmen, sich mit eigenen Anwendungen, sogenannten Skills, an den Sprachassistentendienst Alexa anzubinden. Unternehmen, die untereinander im Wettbewerb stehen, können sich dieser neuen Form der

Kundenansprache nur schwer entziehen. Der Marketingmaßnahme stehen jedoch erhebliche datenschutzrechtliche Bedenken gegenüber. Dienste wie Alexa dringen tief in die Privat- und Intimsphäre ihrer Nutzer sowie unbeteiligter Dritter ein. Es liegt auf der Hand, dass es bei der Nutzung von Alexa zwangsläufig zu Verstößen gegen die geltenden datenschutzrechtlichen Vorschriften kommt. Der vorliegende Beitrag geht am Beispiel von Alexa Skills der Frage nach, wo die datenschutzrechtlichen Risiken bei Sprachassistentendiensten wie Alexa liegen.

I. Einleitung

Gemäß Art. 24 Abs. 1 DS-GVO müssen Unternehmen (nachfolgend „Drittanbieter“) vor Bereitstellung ihres Skills prüfen, welche Risiken mit dessen Nutzung unter Berücksichtigung des Umfangs, der Umstände und des Zwecks einer jeden Verarbeitung für die Rechte und Freiheiten der betroffenen Personen einhergehen. Die Durchführung der Prüfung ist z.B. durch die Erstellung von Verarbeitungsverzeichnissen und Datenschutz-Folgeabschätzungen zu dokumentieren. Die Drittanbieter benötigen für die von ihnen geforderte Prüfung jedoch ausreichende Kenntnis über die Risiken, die mit dem Einsatz von Sprachassistentendiensten wie Alexa für die betroffenen Personen einhergehen. Sie müssen das komplexe Zusammenspiel des Skills mit Alexa durchdringen und insbesondere über Zweck und Umfang aller in ihrer Verantwortung liegenden Verarbeitungsvorgänge informiert sein. Drittanbieter sehen sich hier jedoch mit einer Technik konfrontiert, die nur schwer durchschaubar ist und über deren Funktionsweise noch vieles im Dunkeln liegt. Bisher gibt es mit dem Einsatz von Systemen, die durch Zuführung immer neuer Datenströme ein selbstlernendes System bilden, kaum Erfahrungen. Es ist derzeit schwer abzuschätzen, welche Auswirkungen der Einsatz und der Ausbau KI-basierter Systeme für jeden Einzelnen und unsere Gesellschaft haben werden.² Hinzu kommt, dass US-Unternehmen wie Amazon zum Schutz ihres Know-hows nur wenige Informationen über das System, die tatsächlichen Datenströme und ihre Verwendung(-sabsichten) zur Verfügung stellen.

Eine eingehende Prüfung durch Aufsichtsbehörden und Gerichte, ob und inwieweit Sprachassistentendienste datenschutzrechtlichen Anforderungen genügen, ist bislang kaum erfolgt.³ Ein Umstand, der in Anbetracht der Vielzahl gegebenenfalls nicht datenschutzkonform verarbeiteter Daten verwundert.

Nachfolgend soll am Beispiel von Alexa Skills herausgearbeitet werden, dass es für Drittanbieter aufgrund der vorgenannten Unsicherheiten mit erheblichen datenschutzrechtlichen Risiken verbunden ist, Alexa Skills anzubieten.

II. Funktionsweise des Sprachassistentendienstes

Zum besseren Verständnis der im Beitrag angesprochenen Rechtmäßigkeitsprobleme soll im Folgenden die Funktionsweise des Sprachassistentendienstes Alexa und dessen Zusammenspiel mit Alexa Skills skizziert werden.

1. Alexa

Bei Alexa handelt es sich um einen cloudbasierten Sprachassistentendienst des US-Konzerns Amazon.com, Inc.. Auf dem deutschen Markt wird Alexa von Amazon Europe⁴ angebo-

1 Vgl. etwa Smart-Home-Studie der Bitkom, abrufbar unter: <https://www.bitkom.org/Bitkom/Publikationen/Smart-Home-Studie-2020>, zuletzt abgerufen am 14.10.2020.

2 Die Wissenschaftler Kate Crawford und Vladan Joler geben mit einer visuellen Übersicht und einem ausführlichen Essay einen Einblick in den Lebenszyklus einer Alexa Echo-Einheit. Sie zeigen auf, dass es für den Betrieb dieses komplexen Systems des Zusammenspiels dreier Komponenten bedarf: menschliche Arbeitskraft, materielle Ressourcen und Daten. Die Studie ist abrufbar unter: <https://anatomyof.ai>, zuletzt abgerufen am 13.10.2020.

3 Im Juli 2019 teilte der Bundesdatenschutzbeauftragte Prof. Dr. Kelber auf Anfrage von Abgeordneten des Bundestags mit, dass die Prüfung der datenschutzrechtlichen Zulässigkeit von Sprachassistentendiensten auf EU-Ebene bei den zuständigen Behörden in Luxemburg, Irland, München und Hamburg noch nicht abschließend geklärt sei, vgl. Art. „Datenschutzbeauftragter will Alexa und Siri prüfen“ auf f.A.Z. net. vom 26.07.2019, abrufbar unter: <https://www.faz.net/aktuell/wirtschaft/digitec/datenschutzbeauftragter-will-alexa-und-siri-pruefen-16303644.html>, zuletzt abgerufen am 14.10.2020.

4 Amazon Europe steht in diesem Beitrag für die Amazon Media S. à. r. l. und die mit Amazon Media S. à. r. l. verbundenen Unternehmen, alleamt Tochterunternehmen von Amazon.com, Inc. Der Begriff „Amazon“ bezieht sich in diesem Beitrag auf den Konzernverbund.

ten.⁵ Der Funktionsumfang des Sprachassistenten reicht von der Beantwortung allgemeiner Fragen über das Abspielen von Musik bis hin zur Übernahme organisatorischer Aufgaben, z.B. die Steuerung angeschlossener Geräte, die Auslösung von Bestellungen oder die Verwaltung von Terminen. Die Nutzer von Alexa benötigen für den Einsatz eine spezielle Hardware, insbesondere mit Mikrofonen ausgestattete Lautsprecher (z.B. Alexa Echo) sowie ein Nutzerkonto. Die Beantwortung einer Nutzeranfrage läuft grob skizziert in folgenden Schritten ab: Die Aufnahmefunktion von Alexa wird mit Ausspruch des Aktivierungsworts „Alexa“ oder durch Betätigung der Aktivierungstaste gestartet. Die Sprachbefehle der Nutzer werden über die mit Mikrofonen ausgestatteten Lautsprecher aufgenommen und als Audio-Dateien in der Amazon-Cloud gespeichert. Die Amazon-Cloud ist ein Service des US-amerikanischen Unternehmens Amazon Webservices, Inc. (nachfolgend nur „AWS“).⁶ Die Audio-Dateien werden in der Amazon-Cloud mittels einer speziellen Software in Transkripte, ein computerlesbares Textformat, übersetzt.⁷ Diese Transkripte werden an die passenden Datenbanken und Anwendungen zur Umsetzung der Anfrage weitergeleitet und bearbeitet, je nach Anfrage durch das Rückspielen einer Antwort auf eine Frage oder das Auslösen eines Dienstes. Sowohl die Audio-Dateien als auch die Transkripte werden auf unbestimmte Zeit auf den Servern von Amazon gespeichert, es sei denn, ein Nutzer löscht die Daten. Amazon schließt nicht aus, dass Audio-Dateien und Transkripte auch nach Löschung durch den Nutzer auf den Speichersystemen von Alexa verbleiben.⁸ Seit kurzem sollen Nutzer die Speicherung der Sprachbefehle deaktivieren können.⁹

2. Alexa Skills

Nutzer von Alexa können die Funktionen der Sprachsoftware durch die Aktivierung von Alexa Skills erweitern. Amazon stellt Drittanbietern für die Entwicklung eigener Skills ein „Skills Kit“ zur Verfügung, welches eine Sammlung von Schnittstellen, Tools, Dokumentationen und Codebeispielen für die Entwicklung der Skills vorhält. Fragt ein Nutzer den Skill eines Drittanbieters an, wird der Sprachbefehl zunächst cloudbasiert im Organisationsbereich von Amazon verarbeitet und in transkribierter Form über die gemeinsame Schnittstelle an die Server des Drittanbieters weitergeleitet. Der Drittanbieter verarbeitet die Nutzeranfrage dann mit seiner eigenen Software auf eigenen Servern und spielt die vom Nutzer angeforderte Aktion an die Amazon-Cloud zurück, wo sie, wie bereits unter Ziffer II.1. dargestellt, verarbeitet wird. Es kommt mithin zu einem Datenaustausch zwischen Amazon und dem Drittanbieter. Ausweislich der Datenschutzhinweise von Amazon werden an die Drittanbieter jedoch keine Audio-Dateien übermittelt. Die Drittanbieter erhalten die Sprachbefehle ausschließlich in transkribierter Form mit einem Zahlencode zur Nutzererkennung. Allein anhand dieses Zahlencodes soll der Drittanbieter den Nutzer nicht identifizieren können. Etwas anderes gilt dann, wenn ein Nutzer dem Drittanbieter den Zugriff auf weitere personenbezogene Daten gestattet, z.B. auf eine bei Amazon hinterlegte Anschrift.

3. Skill Metrics

Drittanbieter können über die Entwicklerplattform zudem Berichte und Auswertungen über das Verhalten ihrer Nutzer abrufen, sogenannte „Skill Metrics“. Skill Metrics wertet insbesondere die Anzahl der Nutzer eines Skills, Informationen zum Ablauf einer Nutzersession sowie Kennzahlen zum Nutzerverhalten aus, z.B. die regionale Verteilung der Nutzer.¹⁰

III. Information der Nutzer durch Amazon

Da die Rechtmäßigkeit von Angeboten wie Alexa maßgeblich von der ordnungsgemäßen Information der Nutzer abhängt und die Intentionen von Amazon mangels konkreter Verarbeitungsverzeichnisse aus öffentlichen Quellen gewonnen werden müssen, soll kurz auf den Informationsprozess von Amazon eingegangen werden. Amazon informiert die Nutzer über die mit Alexa einhergehenden Datenverarbeitungen unter anderem in seinen Nutzungsbedingungen¹¹ sowie über eine Datenschutzerklärung.¹² In der Datenschutzerklärung wird auf eine Hilfsseite mit der Überschrift „Alexa, Echo-Geräte und Ihre Privatsphäre“¹³ verlinkt. Auf dieser Seite werden die Nutzer unter dem Punkt „Was passiert, wenn ich mit Alexa spreche?“ darüber informiert, dass ihre Anfragen mit den Daten ihres Amazon-Kontos verknüpft werden und dass Amazon neben den Sprachbefehlen auch Informationen über sämtliche Geräte und Dienste, die mit Alexa verbunden sind, erhebt. Unter dem Punkt „Wie verbessern meine Sprachaufnahmen Alexa?“ wird den Nutzern mitgeteilt, dass die Nutzeranfragen auch zur Verbesserung der „Systeme zur Spracherkennung“ verwendet werden. Der maschinelle Lernprozess soll teilweise von Mitarbeitern begleitet und durch Stichproben überprüft werden. Diese Praxis

5 Alexa Nutzungsbedingungen, <https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740>, zuletzt abgerufen am 12.10.2020.

6 AWS betreibt Rechenzentren weltweit, in Deutschland z.B. in Frankfurt am Main.

7 Amazon bietet Entwicklern unter dem Namen „Amazon Transcribe“ die Übersetzungssoftware als separaten Service an. Die Software soll mit einem „Deep-Learning-Prozess“ (Automatische Spracherkennung) Sprache schnell und präzise in Text umzuwandeln, <https://aws.amazon.com/de/transcribe/?nc=sn&loc=1>, zuletzt abgerufen am 12.10.2020.

8 Auf eine Anfrage des US-Senators Chris Coons teilte Amazon im Juni 2019 mit, dass die mit Alexa verarbeiteten Daten erst nach Aufforderung der Nutzer gelöscht werden. Selbst nach Löschung der Daten könne jedoch nicht sichergestellt werden, dass die Audio-Dateien und die Transkripte auch weiterhin in den Speichersystemen von Alexa verbleiben. Antwort von Amazon abrufbar unter: <https://www.coons.senate.gov/download/amazon-response>, zuletzt abgerufen am 12.10.2020.

9 Vgl. Beitrag von Daniela Windelband vom 30.09.2020: „Amazon Alexa – endlich können Nutzer die Speicherung ihrer Sprachbefehle verhindern“, abrufbar unter: <https://www.datenschutz-notizen.de/amazon-alexa-endlich-koennen-nutzer-die-speicherung-ihrer-sprachbefehle-verhindern-3327291/>, zuletzt abgerufen am 14.10.2020.

10 Vgl. die englischsprachige Übersichtsseite von Amazon: „View Skill Metrics“, abrufbar unter: <https://developer.amazon.com/en-US/docs/alexa/devconsole/measure-skill-usage.html>, zuletzt abgerufen am 14.10.2020.

11 Nutzungsbedingungen abrufbar unter: <https://www.amazon.de/gp/help/customer/display.html?nodeId=201809740>, zuletzt abgerufen am 13.10.2020.

12 Datenschutzerklärung abrufbar unter: https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010 (zuletzt abgerufen am 12.10.2020).

13 Hilfsseite „Alexa, Echo-Geräte und Ihre Privatsphäre“, abrufbar unter <https://www.amazon.de/gp/help/customer/display.html?nodeId=GA7E98TJFEJLYSFR>, zuletzt abgerufen am 12.10.2020.

wurde von Datenschützern scharf kritisiert, als bekannt wurde, dass Amazon Sprachmitschnitte von Zeitarbeitern in Heimarbeit auswerten lässt.¹⁴ Amazon reagierte hierauf, so dass Nutzer jetzt dieser Form der Auswertung in den Einstellungen ihrer Alexa-App widersprechen können. Stimmt ein Nutzer über die Verwaltungseinstellungen seiner Alexa-App zu, nutzt Amazon die Audiodateien auch zur Erstellung eines Stimmprofils. Dieses soll der Spracherkennungssoftware zukünftig ermöglichen, den Nutzer allein anhand seiner Stimme zu identifizieren. Nach Angaben von Amazon sei Alexa so entwickelt worden, dass so wenige Informationen wie möglich aufgenommen werden. Die Sprachaufnahmen starten angabegemäß erst nach Ausspruch des Aktivierungsworts „Alexa“. Verbraucherschützer beklagten in der Vergangenheit, dass Alexa die Sprachaufnahme auch bei ähnlich klingenden Wörtern, z.B. „Alexander“, startet und der Dienst somit ungefragt Einblick in die Privatsphäre der Nutzer nehme.¹⁵

IV. Verantwortlichkeit der Drittanbieter

Aus dem unter Ziffer II. erläuterten Zusammenspiel von Alexa und Alexa Skills wird ersichtlich, dass es bei Verarbeitung der Sprachbefehle zu komplexen Verarbeitungsprozessen kommt. Drittanbieter sind mit ihren Skills eng in das System Alexa eingebunden. Es stellt sich daher die aus Sicht der Drittanbieter essentielle Frage der datenschutzrechtlichen Verantwortlichkeit.

Da weder Amazon noch Drittanbieter für den jeweils anderen weisungsgebunden Datenverarbeitungen durchführen, ist die Annahme eines Auftragsverarbeitungsverhältnisses nach Art. 28 DS-GVO fernliegend. Amazon und Drittanbieter könnten jedoch für ausgewählte Verarbeitungsvorgänge über den jeweils eigenen Organisationsbereich hinaus gemeinsam Verantwortliche i.S.d. Art. 26 Abs. 1 DS-GVO sein. Eine gemeinsame Verantwortlichkeit könnte sich hinsichtlich Aufnahme und Verarbeitung der Sprachbefehle zur Bearbeitung der Nutzeranfrage sowie bezüglich der Analysetätigkeit für Skill Metrics ergeben. Gemäß Art. 4 Nr. 7 DS-GVO i.V.m. Art. 26 DS-GVO setzt die Annahme einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit voraus, dass ein Beteiligter gemeinsam mit einem anderen eine Entscheidung über die Zwecke und Mittel der konkreten Datenverarbeitung trifft.

Die unbestimmten Rechtsbegriffe Festlegung, Zwecke und Mittel bedürfen in erster Linie einer Auslegung anhand der bislang zu dieser Thematik ergangenen Rechtsprechung.¹⁶ Der EuGH hat in drei wesentlichen Entscheidungen¹⁷ die Voraussetzungen für eine gemeinsame Verantwortlichkeit geprüft. Anhand der Entscheidungskriterien der Fashion-ID-Entscheidung¹⁸ soll nachfolgend geprüft werden, ob Drittanbieter durch Anbindung ihres Skills an Alexa die Kriterien für eine gemeinsame Verantwortlichkeit erfüllen.

1. Sachverhalt und Entscheidungskriterien der Fashion ID – Entscheidung

Der Entscheidung des EuGH lag folgender Sachverhalt zugrunde: Ein Website-Betreiber hatte in seine Website ein Social Plugin, den „Gefällt-mir-Button“ eingebunden. Durch Einbindung des Social Plugins wurden von den Besuchern

der Website ohne deren vorherige Information und Einwilligung personenbezogene Daten erhoben und an Facebook Ireland weitergeleitet. Der EuGH hatte über die Frage zu befinden, ob in einem Fall, bei dem jemand einen Programmcode in seine Website einbindet, der den Browser des Website-Besuchers veranlasst, Inhalte von einem Dritten anzufordern und hierzu personenbezogene Daten an den Dritten zu übermitteln, „für die Verarbeitung Verantwortlicher“ im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 sein kann, wenn er selber diesen Datenverarbeitungsvorgang nicht beeinflussen kann.¹⁹ Die Entscheidung ist für das System Alexa interessant, weil sie sich der Frage widmet, ob ein Dritter auch dann für Datenverarbeitungen verantwortlich ist, wenn er diese nicht steuern kann, die er aber (mit-)veranlasst und die ihm auch wirtschaftlich nutzen.

Der EuGH stellt in den Entscheidungsgründen zunächst fest, dass eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DS-GVO nicht voraussetzt, dass jeder Beteiligte gleichwertig für dieselbe Verarbeitung verantwortlich ist. Eine Datenverarbeitung könne aus mehreren Vorgängen bestehen, in deren Phasen die Beteiligten in unterschiedlichem Ausmaß eingebunden sind.²⁰ Für eine gemeinsame Entscheidung über die Mittel der Verarbeitung sprach aus Sicht des EuGH, dass der Website-Betreiber das Social Plugin in Kenntnis der Datenerhebung in seine Website eingebunden hat.²¹ Die gemeinsame Festlegung des Zwecks der Datenverarbeitung erkannte der EuGH darin, dass Facebook Ireland und der Website-Betreiber jeweils wirtschaftliche Zwecke mit der Einbindung des Plugins verfolgten. Es komme hierbei nicht darauf an, dass die beteiligten Akteure den gleichen wirtschaftlichen Zweck anstreben.²² Der Website-Betreiber ist aufgrund der gemeinsamen Festlegung von Zweck und Mittel der Datenverarbeitung gemeinsam mit Facebook Ireland verantwortlich, auch wenn er keinen Zugriff auf die relevanten Daten hat. Der EuGH weist in den Entscheidungsgründen je-

14 Vgl. Pressebericht des ZDF vom 04.08.2019, welcher auf einer Quelle der Nachrichtenagentur AFP basiert, abrufbar unter: <https://www.zdf.de/nachrichten/heute/sprachassistent-von-amazon-alexa-auswertung-in-heimarbeit-100.html>, zuletzt abgerufen am 12.10.2020.

15 Bericht der Verbraucherzentrale vom 20.12.2017: „Digitaler Sprachassistent: Alexa reagiert auch ungefragt“, abrufbar unter: <https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/digitaler-sprachassistent-alexa-reagiert-auch-ungefragt-21363>, zuletzt aufgerufen am 13.10.2020.

16 Daneben kann auch auf die Stellungnahme der Art. 29-DS-Gruppe zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ zurückgegriffen werden (WP 169 vom 16. Februar 2010). Die Stellungnahme erging noch zur alten Rechtslage, hat jedoch wegen Beibehaltung der Begriffe nach wie vor Gültigkeit. Die EDSK arbeitet aktuell an einer aktualisierten Leitlinie. Der Entwurf der Leitlinie kann abgerufen werden unter: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_de, zuletzt abgerufen am 14.10.2020.

17 Es handelt sich hierbei um die Entscheidungen vom 10.07.2018 – C 25/17 (Zeugen Jehovas), vom 05.06.2018 – C-210/16 (Wirtschaftsakademie Schleswig-Holstein) und vom 29.07.2019 – C-40/17 (Fashion-ID).

18 EuGH, Urteil vom 29.07.2019 – C-40/17.

19 Die Entscheidung erging noch zu der vor Inkrafttreten der DS-GVO geltenden Richtlinie 95/46. Da sich an der Definition der gemeinsamen Verantwortlichkeit mit Inkrafttreten der DS-GVO nichts geändert hat, können die zur Richtlinie 95/46 ergangenen Entscheidungen auch zur Auslegung von Art. 4 Nr. 7 DS-GVO herangezogen werden.

20 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 72.

21 Wie vor, Rn. 77 f.

22 Wie vor, Rn. 80.

doch einschränkend darauf hin, dass sich die Verantwortlichkeit des Website-Betreibers auf Vorgänge der Datenverarbeitung beschränke, für die er tatsächlich über die Zwecke und Mittel entscheidet. Der EuGH hatte dies für die Erhebung der in Rede stehenden Daten sowie deren Weitergabe und Übermittlung an Facebook Ireland angenommen.²³

2. Auswirkungen der Fashion ID – Entscheidung auf Alexa

Legt man die Auslegungskriterien der Fashion ID – Entscheidung der Situation der Drittanbieter zugrunde, bestimmen die Drittanbieter mit der Anbindung der Skills an Alexa gemeinsam mit Amazon über die Mittel der Bearbeitung der Nutzeranfrage. Die Drittanbieter programmieren mit dem von Amazon zur Verfügung gestellten Skills Kit ihre Skills und binden diese bewusst in das System Alexa ein. Einer gemeinsamen Verantwortlichkeit steht nicht entgegen, dass die Drittanbieter die Aufnahme und Umwandlung der Sprachbefehle sowie die Verarbeitung der Transkripte in der Amazon-Cloud nicht beeinflussen können und in der Regel auch keinen Zugriff auf die Daten der Nutzer sowie die Audio-Dateien haben. Sowohl Amazon als auch Drittanbieter verfolgen mit ihren Angeboten wirtschaftliche Zwecke, die sich nach der zitierten Entscheidung des EuGH nicht decken müssen. Unter Zugrundelegung der Kriterien aus der Fashion-ID-Entscheidung ist somit von einer gemeinsamen Verantwortlichkeit der Drittanbieter mit Amazon auszugehen.

Dabei werden die zukünftige Rechtsprechung und die Praxis der Aufsichtsbehörden zeigen, für welche konkreten Verarbeitungsvorgänge eine gemeinsame Verantwortlichkeit anzunehmen ist. Drittanbieter müssen infolgedessen vor Bereitstellung ihres Skills sicherstellen, dass sie die Anforderungen der DS-GVO an eine gemeinsame Verarbeitung erfüllen. Sie sind gemäß Art. 26 Abs. 1 Satz 2 DS-GVO mit Amazon zum Abschluss einer Vereinbarung zur gemeinsamen Verarbeitung verpflichtet. Ein Verstoß gegen diese Verpflichtung kann gemäß Art. 83 Abs. 4 DS-GVO gegenüber jedem Verantwortlichen mit empfindlichen Bußgeldern geahndet werden. Amazon bietet Drittanbietern bislang keine standardisierte Vereinbarung an. Dies kann sich ändern, wenn Gerichte und Aufsichtsbehörden den Dienst verstärkt in ihren Fokus nehmen. So hat Facebook Ireland den Betreibern einer Fanpage erst als Reaktion auf eine Entscheidung des EuGH²⁴ und den Beschluss der DSK vom 05.09.2018 eine standardisierte Vereinbarung angeboten, wenngleich diese nach Auffassung vieler Seitenbetreiber nicht den gesetzlichen Anforderungen entsprach.²⁵ Aufgrund der derzeitigen Untätigkeit von Amazon müssten Drittanbieter bereits wegen des Verstoßes gegen Art. 26 Abs. 1 Satz 2 DS-GVO vom Einsatz eines Alexa Skills absehen. Alternativ wäre Amazon direkt auf Abschluss einer Vereinbarung in Anspruch zu nehmen. Ein Anspruch auf Abschluss einer Vereinbarung zur gemeinsamen Verarbeitung ergibt sich unmittelbar aus Art. 26 DS-GVO.²⁶

Aus der gemeinsamen Verantwortlichkeit folgt für Drittanbieter auch die Pflicht, gegenüber den betroffenen Personen die Rechtmäßigkeit der relevanten Datenverarbeitungen sicherzustellen. Soweit den Drittanbietern für die Prüfung der Rechtmäßigkeit der Verarbeitung Informationen fehlen, z.B.

konkrete Verarbeitungsverzeichnisse, müssen diese bei Amazon angefragt werden. Etwaige Auskunftsansprüche können aufgrund der zwischen den gemeinsam Verantwortlichen bestehenden gesetzlichen Sonderverbindung aus einer analogen Anwendung von § 242 BGB hergeleitet werden.²⁷ Verstoßen die Mitverantwortlichen bei der Datenverarbeitung gegen die DS-GVO, können die Aufsichtsbehörden gegenüber jedem Verantwortlichen ein Bußgeld in beträchtlicher Höhe verhängen.

Die Prüfung der Rechtmäßigkeit der Verarbeitung ist für Drittanbieter daneben auch deshalb von erheblicher Bedeutung, weil sie den betroffenen Personen im Außenverhältnis gemäß Art. 82 Abs. 4 DS-GVO gesamtschuldnerisch mit Amazon haften.

V. Ausgewählte Probleme der Rechtmäßigkeit des Sprachassistentendienstes

Neben der aktuell nicht rechtskonform erfolgenden gemeinsamen Verarbeitung ergeben sich aus dem Einsatz von Alexa weitere Rechtmäßigkeitsprobleme, auf die nachfolgend exemplarisch eingegangen wird. Dabei beschränkt sich die Darstellung auf die im Organisationsbereich von Amazon erfolgenden Datenverarbeitungen.

1. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Amazon führt die Sprachbefehle der registrierten Nutzer mit deren Daten aus den Nutzerkonten, etwa Name und Anschrift, zusammen. Die Informationen aus den Audio-Dateien können somit einem konkreten Nutzer im Sinne von Art. 4 Nr. 1 DS-GVO zugeordnet werden. Für die Verarbeitung personenbezogener Daten bedarf es aufgrund des datenschutzrechtlichen Verbots mit Erlaubnisvorbehalt einer wirksamen Rechtsgrundlage. Gemäß Art. 5 und 6 DS-GVO kommen hierfür z.B. die Erteilung einer Einwilligung nach Art. 6 Abs. 1 S. 1 lit a i.V.m. Art. 7 DS-GVO sowie das Vorliegen eines Erlaubnistatbestands nach Art. 6 Abs. 1 S. 1 lit b bis f DS-GVO in Betracht. Die Erlaubnistatbestände stehen gleichwertig nebeneinander.²⁸ Für die Verarbeitung personenbezogener Daten einer besonderen Kategorie, z.B. Gesundheitsdaten oder biometrische Daten, ist gemäß Art. 9 DS-GVO zudem eine ausdrückliche Einwilligung zwingend erforderlich. Es soll nachfolgend auf die in Betracht kommenden Erlaubnistatbestände eingegangen werden.

a) Art. 6 Abs. 1 S. 1 lit b DS-GVO

aa) Die Verarbeitungsvorgänge zur Beantwortung einer Nutzeranfrage könnten auf Art. 6 Abs. 1 S. 1 lit b DS-GVO gestützt werden, der die Verarbeitung personenbezogener

23 Wie vor, Rn. 85.

24 EuGH, Urteil vom 05.06.2018 – Az.: C-210/16.

25 Vgl. Klageschrift der Bundestagsfraktion Bündnis 90/ Die Grünen gegen Facebook Ireland Limited, abrufbar unter: <https://www.gruene-bundestag.de/themen/netzpolitik/klage-gegen-facebook>, zuletzt abgerufen am 13.10.2020.

26 Instrukтив hierzu: Specht-Riemenschneider/Schneider, MMR 2019, 503, 506.

27 Wie vor.

28 Schulz, in: Gola, DS-GVO, 2. Aufl. 2018, Rn. 10.

Daten zur Erfüllung eines Vertrags gestattet. Amazon steht mit den Nutzern durch den Abschluss eines Nutzungsvertrags in einer vertraglichen Beziehung. Art. 6 Abs. 1 S.1 lit b DS-GVO ist jedoch nur auf Verarbeitungsvorgänge anwendbar, die zur Erfüllung des Vertragszwecks erforderlich sind und für welche keine weniger eingriffsintensiven Alternativen bestehen. Inwieweit diese Voraussetzungen erfüllt sind, kann nur anhand konkreter Verarbeitungsverzeichnisse geprüft werden. Vorbehaltlich der Ergebnisse einer Einzelfallprüfung kann Art. 6 Abs. 1 S. 1 lit b DS-GVO jedoch gegenüber volljährigen Nutzern als Erlaubnistatbestand für Verarbeitungen herangezogen werden, die zur Bearbeitung der Nutzeranfrage erforderlich sind.

bb) Alexa wird auch von Kindern genutzt. Amazon bietet z.B. sogenannte Kid Skills an, deren Aktivierung der Nutzer in der Alexa-App zustimmen muss. Es stellt sich die Frage, ob Art. 6 Abs. 1 S. 1 lit b DS-GVO auch gegenüber Minderjährigen als Erlaubnistatbestand herangezogen werden darf.²⁹ Da Art. 6 Abs. 1 S. 1 lit b DS-GVO tatbestandlich einen wirksamen Vertragsschluss voraussetzt, ist der Erlaubnistatbestand bei Kindern unter sieben Jahren wegen §§ 104 f. BGB nicht anwendbar. Der Abschluss des Nutzungsvertrags mit einem beschränkt Geschäftsfähigen, mithin einem Kind über 7 Jahren, bedarf gemäß § 107 BGB der Zustimmung der Sorgeberechtigten, soweit das Rechtsgeschäft nicht ausschließlich rechtlich vorteilhaft ist. Bei der Prüfung des ausschließlich rechtlichen Vorteils ist dabei allein auf die rechtlichen und nicht auf die wirtschaftlichen Wirkungen des Vertrags abzustellen.³⁰ Selbst wenn die Nutzung von Alexa und Alexa Skills überwiegend kostenlos ist, geht sie für die minderjährigen Nutzer mit rechtlichen Nachteilen einher. Zum einen ergeben sich aus dem Nutzungsvertrag zahlreiche Pflichten, etwa die Pflicht zum vertragsgemäßen Umgang mit der Software. Zum anderen akzeptieren die Nutzer mit Abschluss des Nutzungsvertrags die Verarbeitung ihrer personenbezogenen Daten, was einen Eingriff in das Recht auf informationelle Selbstbestimmung und somit einen rechtlichen Nachteil darstellt.³¹ Ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit b DS-GVO gegenüber beschränkt Geschäftsfähigen setzt daher die Zustimmung der Sorgeberechtigten zum Abschluss des Nutzungsvertrags voraus. In der Praxis dürfte das Vorliegen einer Zustimmung nur schwer prüfbar sein.

b) Art. 6 Abs. 1 S. 1 lit f DS-GVO

Der Anwendungsbereich von Art. 6 Abs. 1 S. 1 lit f DS-GVO ist weit gefasst und ermöglicht eine Datenverarbeitung auch über das vertraglich erforderliche Maß hinaus, wenn seitens der Verantwortlichen berechnete wirtschaftliche oder ideelle Interessen vorliegen, welche nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Zur Prüfung der Voraussetzungen von Art. 6 Abs. 1 S. 1 lit f DS-GVO ist zwingend die Vorlage der einschlägigen Verarbeitungsverzeichnisse erforderlich, da bereits bei Feststellung der berechtigten Interessen auf die mit der Verarbeitung verfolgten Zwecke und die zur Zweckerreichung erforderlichen

Mittel abzustellen ist. In jedem Fall stehen den Interessen von Amazon, etwa an der Fortentwicklung der Spracherkennungssoftware, die Interessen der betroffenen Personen auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation nach Art. 7 GRCh sowie hinsichtlich des Schutzes personenbezogener Daten nach 8 GRCh gegenüber. Da bei der Interessenabwägung unter anderem die Eingriffsintensität in die betroffenen Grundrechte zu beachten ist,³² kann auf die Rechtsprechung des EuGH und des BVerfG zu vergleichbaren Sachverhalten abgestellt werden. Alexa nimmt von den betroffenen Personen über einen langen Zeitraum hinweg die private Kommunikation auf und erhält somit sehr konkrete Rückschlüsse auf die Lebensweise, die Verhältnisse und das Kommunikationsverhalten der Nutzer. Der EuGH hat in seinem Urteil vom 13.05.2014 entschieden, dass die Grundrechte auf Achtung des Privatlebens und der Schutz personenbezogener Daten erheblich beeinträchtigt werden, wenn eine Verarbeitung einer Vielzahl von Personen einen strukturierten Überblick über die betroffene Person ermöglicht, die Informationen potentiell zahlreiche Aspekte über das Privatleben der Person geben und somit ein detailliertes Profil der Person erstellt werden kann.³³ Auch das BVerfG entschied in seinem Urteil vom 27.02.2008 über die verfassungsrechtliche Zulässigkeit der Onlinedurchsuchung, dass die Erhebung umfassender Persönlichkeitsprofile einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.³⁴ Gegenüber Kindern wird ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit f DS-GVO aufgrund des schwerwiegenden Grundrechtseingriffs somit von vornherein ausscheiden. Auch hinsichtlich der registrierten Nutzer dürfte es nur sehr schwer sein, eine konkrete Datenverarbeitung unter Berufung auf ein überwiegendes Interesse von Amazon auf Art. 6 Abs. 1 S. 1 lit f DS-GVO zu stützen.

c) Rechtsgrundlage Einwilligung

Die Daten minderjähriger Nutzer dürfen mithin in der Regel nur verarbeitet werden, wenn die Sorgeberechtigten gemäß Art. 6 Abs. 1 S. 1 lit a DS-GVO i.V.m. Art. 7 und 8 DS-GVO in die Datenverarbeitung eingewilligt haben. Das Erfordernis einer ausdrücklichen Einwilligung besteht zudem bei der Verarbeitung besonders sensibler Daten im Sinne von Art. 9 DS-GVO, z.B. Gesundheitsdaten oder biometrische Daten. Amazon hat bereits den Einsatz einer patentierten Software angekündigt, mit deren Hilfe Alexa den Gesundheitszustand eines Nutzers erkennen kann. Alexa soll bei Bedarf gute Besserung wünschen und dem Nutzer gezielt Medikamente an-

29 Art. 8 DS-GVO schließt nicht aus, dass eine Datenverarbeitung auch auf andere Erlaubnistatbestände im Sinne von Art. 6 Abs. 1 DS-GVO gestützt wird, vgl. Schulz, a.a.O., Art. 8 Rn. 3

30 Ellenberger, in: Palandt, Bürgerliches Gesetzbuch, 79. Aufl. 2020, § 107, Rn. 2.

31 Bräutigam, MMR 2012, 635, 638.

32 Schulz, a.a.O., Art. 6 Rn. 59.

33 EuGH, Urteil vom 13.05.2014 – C-131/12, Rn. 80.

34 BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, Rn. 237.

35 Amazon Watchblog.de: „Gute Besserung“ – Alexa erkennt Gesundheitszustand und spielt passende Werbung aus“; Beitrag vom 15.10.2018, abrufbar unter: <https://www.amazon-watchblog.de/technik/1510-alexa-erkennt-gesundheitszustand-spielt-passende-werbung.html>, zuletzt abgerufen am 12.10.2020.

bieten.³⁵ Hier wäre zweifellos der Anwendungsbereich von Art. 9 DS-GVO eröffnet. Gleiches trifft zu, wenn Nutzer über ihre Sprachbefehle oder die Inanspruchnahme konkreter Dienste, z.B. eine Gesundheits-App, sensible Daten offenbaren. Auch die Sprachbefehle unterfallen als biometrische Daten dem Anwendungsbereich von Art. 9 DS-GVO, soweit Amazon diese zur Identifizierung eines Nutzers erhebt. Da es technisch aktuell noch nicht möglich ist, die Sprachaufnahmen auf bestimmte Nutzer oder bestimmte Kategorien von Daten zu beschränken, kann der Einsatz der Sprachassistenten derzeit nur durch die Erteilung informierter Einwilligungen abgesichert werden.³⁶ Drittanbieter müssen somit sicherstellen, dass für alle in ihrem Verantwortungsbereich liegenden Datenverarbeitungen wirksame Einwilligungserklärungen der Nutzer vorliegen. Für diese Prüfung benötigen sie neben den einschlägigen Nutzungsbedingungen und Datenschutzerklärungen auch Screenshots, welche den Prozess der Einwilligungserteilung dokumentieren.

Es stellt sich in diesem Zusammenhang die Frage, inwieweit das Rechtsinstitut der Einwilligung als einzig taugliche Rechtsgrundlage zur Wahrung der Betroffenenrechte tatsächlich geeignet ist. Sprachassistentendienste wie Alexa sind auf Komfort und Schnelligkeit angelegt. Die datenschutzrelevanten Verarbeitungsvorgänge sind komplex und können von den meisten Nutzern nicht nachvollzogen werden. Die von Amazon zur Verfügung gestellten Informationen sind so umfangreich, dass es selbst Juristen schwerfällt, diese in einem angemessenen Zeitrahmen zur Kenntnis zu nehmen. Amazon informiert die Nutzer über die Datenverarbeitung und etwaige Widerspruchsrechte an vielen unterschiedlichen Stellen, etwa in den Nutzungsbedingungen, den Datenschutzzinformationen, auf diversen Hilfe-Seiten und im Bereich „Kundenservice“. Gerade die Vielzahl an Informationen und die Notwendigkeit, diese an den richtigen Stellen zusammenzuführen, dürften dem Nutzer eine transparente und präzise Information erheblich erschweren. Da die hinter Alexa stehende Technik sowie die mit den Daten verfolgten Zwecke nicht durchschaubar sind, ist fraglich, wer anhand welcher Kriterien überprüfen soll, welche Informationen Nutzern beim Einsatz von Systemen wie Alexa für eine informierte Einwilligung zur Verfügung gestellt werden müssen. Die Drittanbieter werden dies im Zweifel nicht beurteilen können. Es ist auch zweifelhaft, ob die Nutzer, die praktisch bei jeder Interaktion im Internet eine Zustimmung teilen müssen, die Informationen überhaupt noch zur Kenntnis nehmen oder in Anbetracht der Fülle täglich zu erteilender Zustimmungen bereits kapituliert haben. Trotz der vorgenannten Probleme stellt die Einwilligung nach der DS-GVO jedoch die einzige Möglichkeit dar, Angebote wie Alexa zumindest gegenüber den Nutzern zu legitimieren.

2. Sonderproblem: Verarbeitung von Daten unbeteiligter Dritter

a) Eröffnung des Anwendungsbereichs der DS-GVO

Zunächst soll der Frage nachgegangen werden, ob die Sprachaufnahmen unbeteiligter Dritter überhaupt in den sachlichen Anwendungsbereich der DS-GVO fallen.

aa) Alexa wird hauptsächlich in privaten Haushalten eingesetzt und nimmt nach Ausspruch des Aktivierungsworts „Alexa“ die Kommunikation sämtlicher im Aufstellraum befindlicher Personen auf. Der Start und die Durchführung der Aufnahme werden durch Lichteffekte kenntlich gemacht. Damit die Sprachaufnahmen eines Dritten dem Anwendungsbereich der DS-GVO unterfallen, müssen die Audio-Dateien Informationen enthalten, die gemäß Art. 4 Nr. 1 DS-GVO einer identifizierbaren natürlichen Person zugeordnet werden können. Ausweislich der Stellungnahme der Art. 29-DS-Gruppe im WP 136 sind Informationen über natürliche Personen: *Informationen, die das Privat- und Familienleben der Person im strengen Sinn berühren, aber auch Informationen über alle Arten von Aktivitäten der Person, etwa im Zusammenhang mit Arbeitsbeziehungen oder ihrem ökonomischen oder sozialen Verhalten.*³⁷ Die Sprachaufnahmen können solche Informationen enthalten, insbesondere dann, wenn die Aufnahme versehentlich startet und die im Raum anwesenden Personen nicht mit einem Mitschnitt ihrer Gespräche rechnen oder aber ein Besucher gar nicht weiß, dass sich ein Aufnahmegerät im Raum befindet.

Die in den Sprachaufnahmen enthaltenen Informationen müssen einer natürlichen Person zuordenbar sein. Diese Voraussetzung wäre bereits dann erfüllt, wenn der Dritte im Gespräch durch Nennung seines Namens oder andere unmissverständliche Zuordnungskriterien, etwa ein Verwandtschaftsverhältnis zum Nutzer, identifizierbar wird. Fehlen solche Zuordnungskriterien, könnte ein Dritter zukünftig auch anhand der Stimme identifiziert werden. Da die Treffsicherheit von Stimmgutachten aktuell jedoch noch begrenzt ist,³⁸ kann derzeit nicht sicher davon ausgegangen werden, dass Amazon oder ein Dritter eine natürliche Person allein anhand der Stimme identifiziert.

Ausweislich Erwägungsgrund 26 der Richtlinie sind bei Beurteilung der Frage der Zuordenbarkeit bestimmter Informationen zu einer natürlichen Person jedoch alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine natürliche Person direkt oder indirekt zu identifizieren. Hypothetische oder eher unwahrscheinliche Mittel zur Identifizierung sind nicht zu berücksichtigen, wohl aber der beabsichtigte Zweck der Verarbeitung und die auf dem Spiel stehenden Interessen für die betroffenen Personen.

36 Zu den Anforderungen an eine Einwilligung: Conrad, DuD 2020, 611 ff..

37 Stellungnahme „4/2007 zum Begriff „personenbezogene Daten““ der Art. 29-DS-Gruppe, abrufbar unter: https://www.bfdi.bund.de/Shared-Docs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP136_Opinion42007ConceptPersonalData.html, zuletzt abgerufen am 14.10.2020.

38 Angelika Braun im Gespräch mit Monika Seynsche, Interview im Rahmen der Sendung „Forschung aktuell“ des Deutschlandfunks zum Thema „Stimm-Datenbank zur Verbrecherjagd“ vom 30.04.2019, abrufbar unter: https://www.deutschlandfunk.de/forensische-gutachten-stimm-datenbank-zur-verbrecherjagd.676.de.html?dram:article_id=447594, zuletzt abgerufen am 09.10.2020.

39 Der Clarifying Lawful Overseas Use of Data Act, kurz „CLOUD-Act“ wurde im Frühjahr 2018 vom US Congress beschlossen und verpflichtet US-Unternehmen personenbezogene Daten an Strafverfolgungsbehörden herauszugeben, auch wenn diese auf Servern außerhalb der USA gespeichert werden.

Amazon ist aufgrund des CLOUD-Acts³⁹ zur Herausgabe der mittels Alexa erlangten Daten an US-Strafverfolgungsbehörden verpflichtet. Die Anzahl der behördlichen Datenabfragen von US-Behörden steigt, wobei aktuell unklar ist, welche Daten im Fall einer Anfrage an die Behörden übermittelt werden.⁴⁰ In Deutschland haben die Innenminister der Länder im Juni 2019 auf der Innenministerkonferenz erörtert, inwieweit die deutschen Strafverfolgungsbehörden die Daten von Smart-Home-Geräten bei der Strafverfolgung nutzen dürfen.⁴¹ In Anbetracht der geltenden Rechtslage ist es somit nicht unwahrscheinlich, dass Strafverfolgungsbehörden den Versuch unternehmen, auch unbeteiligte Dritte auf Basis einer Audio-Datei zu identifizieren.

bb) Amazon könnte hier jedoch einwenden, dass der Anteil der Personen, die nicht als Nutzer registriert sind und von Amazon oder durch eine behördliche Maßnahme identifiziert werden, sehr gering ist, mithin eine pauschale Eröffnung des Anwendungsbereichs der DS-GVO nicht gerechtfertigt wäre. Die Situation der unbeteiligten Dritten bei Alexa ist mit der Situation von Personen vergleichbar, die in den Aufnahmebereich eines privaten Videoüberwachungssystems gelangen. Die Art.-29-DS-Gruppe hatte hier auf den Einwand, dass nur ein geringer Anteil der aufgenommenen Personen tatsächlich identifiziert werde, im WP 136 festgestellt, dass bezüglich der Überwachungseinrichtung auf den Zweck der Verarbeitung abgestellt werden müsse. Wenn der Zweck eines Videoüberwachungssystems in der Bestimmung von Personen bestehe, sei es unerheblich, wenn eine Identifizierung nur in wenigen Ausnahmefällen erfolge.⁴²

Amazon verfolgt mit den Sprachaufnahmen nicht primär den Zweck, alle von der Aufnahme umfassten Personen zu identifizieren. Ausweislich der Nutzungsbedingungen und Datenschutzinformationen sollen die Sprachbefehle nur den Nutzern zugeordnet werden. Auch wird man nicht unterstellen können, dass Amazon mit der Speicherung der Audio-Dateien Strafverfolgungsbehörden bei deren Ermittlungsarbeiten unterstützen möchte.⁴³

Wie der Umstand, dass gegebenenfalls nur wenige unbeteiligte Dritte anhand ihrer Sprachaufnahmen identifiziert werden, von den zuständigen Aufsichtsbehörden gewertet werden wird, kann aktuell nicht abgeschätzt werden. Für eine solche Einschätzung wären vor allem detaillierte Informationen über die Anzahl der tatsächlich identifizierten unbeteiligten Dritten sowie die seitens Amazon mit den Sprachaufnahmen verfolgten Zwecke erforderlich. Es könnte zudem von Relevanz sein, welche technischen Maßnahmen Amazon unternimmt, um eine Identifizierung unbeteiligter Dritter zu verhindern. Der Wissenschaftliche Dienst des Bundestags kommt in einem Gutachten zur „Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa“ zu dem Schluss, dass „*offen bleibt, wie unbeteiligte Dritte und Minderjährige von der Datensammlung ausgeschlossen werden können.*“⁴⁴ Eine nähere Prüfung der Rechtmäßigkeit der Verarbeitung dieser Daten erfolgt jedoch nicht. Für die erforderliche Rechtssicherheit könnte vorliegend eine abschließende Stellungnahme des Europäischen Datenschutzausschusses sorgen. Grundsätzlich sollte aufgrund der beste-

henden Möglichkeiten einer Identifizierung jedoch davon ausgegangen werden, dass der Anwendungsbereich der DS-GVO für die Verarbeitung der Daten Dritter eröffnet ist.

b) Rechtsgrundlage für die Verarbeitung der Daten unbeteiligter Dritter

Für die Verarbeitung personenbezogener Daten unbeteiligter Dritter ist keine Rechtsgrundlage ersichtlich, so dass die Verarbeitung dieser Daten, soweit man die Eröffnung des Anwendungsbereichs der DS-GVO grundsätzlich bejaht, aktuell nicht rechtskonform erfolgt.

3. Datentransfer in die USA

Alexa und Alexa Skills werden auf dem europäischen Markt von Amazon Europe angeboten, deren Verbundunternehmen Konzerntöchter des US-Konzerns Amazon.com, Inc. sind. Die mit Alexa verarbeiteten Daten speichert Amazon auf Servern von AWS, ebenfalls einem Tochterunternehmen des US-amerikanischen Mutterkonzerns Amazon.com, Inc.. Amazon Europe gibt in seinen Nutzungsbedingungen an, dass sämtliche personenbezogene Daten an Amazon.com, Inc. und alle verbundenen Unternehmen weitergegeben werden. Es besteht mithin die Möglichkeit, dass personenbezogene Daten in die USA transferiert werden. Für Drittanbieter ist dieser Umstand insofern relevant, als dass der Datentransfer in die USA nach der derzeitigen Rechtslage nur sehr eingeschränkt datenschutzkonform möglich ist.

a) CLOUD Act

Amazon und AWS unterliegen, wie bereits unter Ziffer V.2.

a) aa) ausgeführt, dem CLOUD Act, der Unternehmen verpflichtet, personenbezogene Daten an US-Behörden herauszugeben, auch wenn diese Daten auf Servern außerhalb der USA gespeichert werden.⁴⁵ Die Regelungen des CLOUD-Acts

40 Amazon Information Request Report vom 31.07.2020, abrufbar unter: <https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF>, zuletzt abgerufen am 10.10.2020.

41 Den Meinungsstand der deutschen Innenminister gibt etwa der Art. 29-DS-Gruppe auf Smart-Home-Geräte löst Diskussionen aus“ wieder, abrufbar unter „Redaktion beck-aktuell, Nachrichten, Pressemitteilungen, Fachnews“, [becklink 2013361](https://becklink.com/2013361).

42 In der Stellungnahme „4/2007 zum Begriff „personenbezogene Daten““ der Art. 29-DS-Gruppe, Seite 19, heißt es konkret: „Da der Zweck eines Videoüberwachungssystems jedoch darin besteht, die Personen zu bestimmen, die auf den Videobildern zu sehen sind, wenn der für die Verarbeitung Verantwortliche ihre Identifizierung für notwendig hält, ist das gesamte System als Mittel zur Verarbeitung von Daten über bestimmbare Personen anzusehen, auch wenn einige aufgezeichnete Personen in der Praxis nicht bestimmbar sind.“ Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Stellungnahmen/WP136_Opinion42007ConceptPersonalData.html, zuletzt abgerufen am 14.10.2020.

43 So teilt AWS auf seiner Homepage zum CLOUD-Act mit: „AWS ist bekannt für seine ablehnende Haltung gegenüber Behördenanfragen nach Kundeninformationen, von denen wir meinen, dass sie zu weit gefasst oder unangemessen sind.“, abrufbar unter: <https://aws.amazon.com/de/compliance/cloud-act>, zuletzt abgerufen am 14.10.2020.

44 Gutachten des Wissenschaftlichen Dienst des Bundestags vom 29.05.2019, Seite 29, abrufbar unter: <https://netzpolitik.org/2019/alexa-gutachten-des-bundestages-amazon-hoert-auch-kindern-und-gaesten-zu>, zuletzt abgerufen am 14.10.2020.

45 Zum CLOUD-Act etwa: Spies, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, VI.2, Rn. 34.

stehen im Widerspruch zu Art. 48 DS-GVO, der bestimmt, dass eine Herausgabe personenbezogener Daten an die Behörde eines Landes außerhalb der Europäischen Union nur auf Grundlage einer internationalen Übereinkunft, etwa einem Rechtshilfeersuchen, herausgegeben werden dürfen. Ein zwischenstaatliches Übereinkommen mit den USA, welches einen unmittelbaren Datentransfer erlaubt, liegt aktuell nicht vor. Amazon und AWS müssten mithin bei jeder Anfrage einer US-Behörde, der kein Rechtshilfeersuchen zugrunde liegt, die Frage beantworten, ob sie den Bestimmungen der DS-GVO oder der behördlichen Anordnung nachkommen wollen. Entscheiden sich die US-Unternehmen für eine Herausgabe der Daten, könnte dies von einer Aufsichtsbehörde als Verstoß gegen die DS-GVO qualifiziert werden.

b) EU-US-Privacy-Shield-Abkommen

Ungeachtet der mit dem CLOUD-Act einhergehenden Risiken konnten Unternehmen einen Datentransfer in die USA bislang auf das zwischen der EU und den USA ausgehandelte EU-US-Privacy-Shield-Abkommen stützen. Die Angemessenheit des Abkommens wurde von der EU-Kommission mit Beschluss vom 12.7.2016 bestätigt. Der EuGH hat das EU-US-Privacy-Shield-Abkommen am 16.07.2020 jedoch für ungültig erklärt.⁴⁶ Unternehmen, die personenbezogene Daten in die USA transferieren, müssen nunmehr gemäß Art. 46 Abs. 1 DS-GVO selbst sicherstellen, dass geeignete Sicherheitsinstrumente zur Wahrung eines dem EU-Standard vergleichbaren Datenschutzniveaus vorgehalten werden und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Als geeignete Garantien kommen gemäß Art. 46 Abs. 2 lit c DS-GVO die EU-Standardvertragsklauseln in Betracht. Die EU-Kommission hat noch unter Geltung der alten Rechtslage mehrere Standardvertragsklauseln für die Datenübermittlung in Drittländer erlassen.⁴⁷ Ausweislich der Entscheidung des EuGH vom 16.07.2020 behalten die EU-Standardvertragsklauseln ihre Gültigkeit und können von den Verantwortlichen weiterhin verwendet werden.⁴⁸ Der EuGH hat in seiner Entscheidung jedoch klargestellt, dass die Verantwortlichen mangels eines verbindlichen Angemessenheitsbeschlusses verpflichtet sind, die Angemessenheit des Schutzstandards im Drittland im Verhältnis zum Schutzstandard in der EU zu prüfen und gegebenenfalls als „Ausgleich für den im Drittland bestehenden Mangel an Datenschutz“ z.B. durch weitere vertragliche Vereinbarungen oder weitere Garantien für eine Angleichung des Datenschutzniveaus zu sorgen.⁴⁹ Wie die Verantwortlichen angesichts der vom EuGH festgestellten datenschutzrechtlichen Defizite in den USA, unter Umgehung der weitgehenden Befugnisse des NSA, für einen solchen Ausgleich sorgen sollen, ist derzeit nicht geklärt. Der Europäische Datenschutzausschuss forderte die EU-Kommission bereits zum Abschluss einer neuen Vereinbarung

mit den USA auf.⁵⁰ Den Verantwortlichen bleibt angesichts der unsicheren Rechtslage aktuell nur, den Datentransfer in die USA gemäß Art. 49 Abs. 1 lit a DS-GVO durch die Einholung ausdrücklicher Einwilligungen abzusichern.

VI. Fazit

Der Einsatz von Alexa Skills mag unter Marketingaspekten attraktiv sein. Für Drittanbieter gehen mit der Zurverfügungstellung des Dienstes jedoch erhebliche datenschutzrechtliche Risiken einher. Drittanbietern sollte bewusst sein, dass sie gemeinsam mit Amazon auch für Verarbeitungsvorgänge verantwortlich sind, die Amazon im eigenen Organisationsbereich vornimmt. Infolge der gemeinsamen Verantwortlichkeit müssen sich Drittanbieter mit der Rechtmäßigkeit von Alexa beschäftigen. Diese Prüfung ist schwierig, weil den Drittanbietern weder eine Vereinbarung zur gemeinsamen Verarbeitung, noch konkrete Verarbeitungsverzeichnisse, etwa zur Vornahme der gebotenen Datenschutz-Folgeabschätzung, vorliegen. Die zuständigen Datenschutzbeauftragten der Drittanbieter werden wegen der erheblichen Risiken von der Verwendung eines Alexa Skills abraten. Mangels vergleichbarer Alternativen stellt dies aus Sicht der Drittanbieter jedoch keine befriedigende Lösung dar. Mehr Rechtssicherheit könnte hier die vom Bundesdatenschutzbeauftragten in Aussicht gestellte abschließende Beurteilung der Sprachassistentendienste durch den Europäischen Datenschutzausschuss verschaffen.



Wiebke Dammann, LL.M.

ist als Rechtsanwältin in den Bereichen IT-Recht und Datenschutz für die Kanzlei esb Rechtsanwälte Strewe und Partner mbB in Dresden tätig.

⁴⁶ EuGH, Urteil vom 16.07.2020 – C-311/18.

⁴⁷ Etwa: Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1487056769872&uri=CELEX:32004D0915>, zuletzt abgerufen am 14.10.2020.

⁴⁸ EuGH, Urteil vom 16.07.2020 – C-311/18, Rn. 128.

⁴⁹ EuGH, Urteil vom 16.07.2020 – C-311/18, Rn. 131 f..

⁵⁰ Statement des Europäischen Datenschutzausschusses vom 17.07.2020, abrufbar unter: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_de, zuletzt abgerufen am 14.10.2020.

Kerstin Liesem

Hohes Risiko oder doch nicht?

Ein Vorschlag zur Risikobestimmung innerhalb der Vorprüfung nach Art. 35 Abs. 1 DS-GVO zur Erforderlichkeit einer Datenschutz-Folgenabschätzung

Zentrales Element einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist die Risikoprognose. Der europäische Normgeber ordnet sie sowohl innerhalb der Vorprüfung nach Art. 35 Abs. 1 S. 1 DS-GVO als auch im Rahmen der eigentlichen Datenschutz-Folgenabschätzung (Art. 35 Abs. 7 lit c DS-GVO) an. Somit stellt sich für den Verantwortlichen die Frage, ob und wenn ja, wie sich diese beiden Risikoprognosen voneinander unterscheiden. Der Beitrag nimmt die Risikoabschätzung innerhalb der Vorprüfung in den Blick. Er plädiert dafür, bei der Schwellwertanalyse innerhalb des Art. 35 Abs. 1 S. 1 DS-GVO die Determinante Eintrittswahrscheinlichkeit außen vor zu lassen, da diese lediglich in Relation zu

den geplanten technischen und organisatorischen Maßnahmen zu bestimmen ist. Stattdessen schlägt er vor, ausschließlich die Schwere der Auswirkungen zu berücksichtigen. Die Determinante Eintrittswahrscheinlichkeit in Abhängigkeit von den technischen und organisatorischen Maßnahmen bliebe der Risikoprognose innerhalb der eigentlichen Datenschutz-Folgenabschätzung vorbehalten. Dieser Vorschlag würde zu einer trennscharfen Abgrenzung der Risikoabschätzungen innerhalb der Vorprüfung und der eigentlichen Datenschutz-Folgenabschätzung führen. Schlagworte: hohes Risiko, Risikoprognose, Risikoabschätzung, Risikoniveau, Schwellwertanalyse, Datenschutz-Folgenabschätzung.

I. Einleitung

Mit der Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 Datenschutzgrundverordnung (DS-GVO) hat der europäische Gesetzgeber ein neues Instrument geschaffen, das den Schutz personenbezogener Daten bei hoch riskanten Datenverarbeitungsvorgängen, insbesondere bei der Verwendung neuer Technologien, sicherstellen soll.¹ Als „eine der wenigen echten regulatorischen Innovationen der DS-GVO“² ist die DSFA als eine Ausformung der Technikfolgenabschätzung zu qualifizieren, deren Ziel es ist, die Auswirkungen neuer Technologien auf Umwelt und Gesellschaft zu beobachten und zu analysieren. Die DSFA dient als „Frühwarnmechanismus“³ und hat deshalb schon vor Inangriffnahme des geplanten Datenverarbeitungsvorgangs zu erfolgen.⁴ Art. 35 DS-GVO ist vom Grundgedanken durchdrungen, dass ein angemessenes Datenschutzregime nur dann etabliert werden kann, wenn auch die Folgen von Datenverarbeitungsvorgängen für die Rechte und Freiheiten⁵ der betroffenen Personen frühzeitig in den Blick genommen werden. Denn erst die kontinuierliche Analyse möglicher Konsequenzen ermöglicht es dem Verantwortlichen, risikominimierende Gegenmaßnahmen zu ergreifen.⁶ Die DSFA ist das Instrument innerhalb der DS-GVO, das den Verantwortlichen zu einer aktiven und kontinuierlichen Risikobewertung und -steuerung der eigenen Datenverarbeitungsvorgänge verpflichtet.⁷ Sie ist ein zentrales Element des risikobasierten Ansatzes⁸ der DS-GVO, wonach der Verantwortliche verpflichtet wird, dem Risiko für die Rechte und Freiheiten natürlicher Personen adäquate technische und organisatorische Maßnahmen (TOMs) entgegenzusetzen. Entscheidend ist dabei der Blickwinkel der betroffenen Personen, nicht der Organisation. Mithin kann auch vermeintlich geringfügigen datenschutzrechtlichen Verstößen Relevanz zukommen.⁹ Ziel der DSFA ist es, Datenverarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen und damit nach Erwägungsgrund¹⁰

(ErwG) 2 S. 1 insbesondere für das Grundrecht auf den Schutz personenbezogener Daten mit sich bringen, bereits vor Beginn der Datenverarbeitung zu identifizieren. Die Ergebnisse der Prognose sollen nach ErwG 84 berücksichtigt werden, wenn darüber entschieden wird, welche risikominimierende Maßnahmen der Verantwortliche implementieren muss.

- 1 Jandt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 1.
- 2 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 2.
- 3 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 8.
- 4 Laufende Datenverarbeitungsvorgänge hingegen sind nur dann einer DSFA zu unterziehen, wenn sich die Risiken aus den Verarbeitungsvorgängen ändern (Art. 35 Abs. 11 DS-GVO). Eine Veränderung der Risiken ist beispielsweise möglich durch Zweckänderungen oder Erweiterungen von Technologien, z.B. durch neue Funktionalitäten, Reibach, in: Taeger/Gabel, DS-GVO/BDSG, 3. Aufl. 2019, DS-GVO Art. 35 Rn. 28. Lässt sich keine Risikoveränderung konstatieren, dann bleiben gemäß ErwG 171 S. 3 die nach der Richtlinie 95/46/EG, Datenschutzrichtlinie (DS-RL), getroffenen Entscheidungen in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.
- 5 Mit Rechten und Freiheiten für den Betroffenen meint die DS-GVO vor allem das Recht auf Datenschutz, daneben jedoch auch andere in ErwG 4 S. 2 genannte Grundrechte wie Rede- und Gedankenfreiheit, Freizügigkeit, Benachteiligungsverbot, Recht auf Freiheit, Gewissens- und Religionsfreiheit.
- 6 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 6.
- 7 Damit unterscheidet sich die DSFA deutlich von der Vorabkontrolle nach Art. 20 Abs. 1 DS-RL, die durch die DS-GVO abgelöst wurde. Denn die DS-RL hatte die Mitgliedstaaten in die Pflicht genommen, konkrete Verarbeitungsvorgänge zu benennen, die wegen ihrer spezifischen Risiken für die Rechte und Freiheiten von Personen vorab überprüft werden mussten.
- 8 Ausführlich zum risikobasierten Ansatz: Piltz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 24 Rn. 19 ff.; Entstehungsgeschichte und Bewertung des risikobasierten Ansatzes, Schröder, ZD 2019, 503 (503 ff.).
- 9 Die DSFA ist also keine Maßnahme des Risikomanagements, deren Ziel es ist, Risiken für die Organisation so weit zu senken, dass der mit ihnen verbundene Schaden noch als hinnehmbar eingestuft werden kann, Nolte/Werkmeister, in: Gola, DS-GVO, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 4.
- 10 Zwar entfalten die Erwägungsgründe keine rechtsverbindliche Wirkung, allerdings spielen sie eine wichtige Rolle bei der Ermittlung des objektiven Telos der Vorschriften der DS-GVO, Ehmann/Selmayr, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Einführung, Rn. 97.

Aus der Konstruktion des Art. 35 DS-GVO ergibt sich für den Verantwortlichen eine zweistufige Prüfpflicht: Diese besteht auf der ersten Stufe in einer Vorprüfung nach Art. 35 Abs. 1 S. 1 DS-GVO zur Ermittlung der Erforderlichkeit einer DSFA. In ihrem Mittelpunkt steht die Frage, ob die Relevanzschwelle überschritten ist und damit ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt („Schwellwertanalyse“).

Erst wenn die Erforderlichkeit einer DSFA festgestellt ist, muss der Verantwortliche eine DSFA nach Maßgabe des Art. 35 DS-GVO durchführen (zweite Stufe).

Bei genauer Betrachtung der Anforderungen, die auf beiden Stufen an den Verantwortlichen gestellt werden, fällt eine Besonderheit ins Auge: Sowohl im Rahmen der Schwellwertanalyse (Art. 35 Abs. 1 S. 1 DS-GVO) als auch im Rahmen der eigentlichen DSFA (Art. 35 Abs. 7 Ziff. c) obliegt dem Verantwortlichen eine Prognose hinsichtlich des Risikoniveaus des beabsichtigten Datenverarbeitungsvorgangs. Auf beiden Stufen muss er nämlich – noch vor Beginn des Datenverarbeitungsvorgangs – abschätzen, ob voraussichtlich eine Hochrisikodatenverarbeitung vorliegt.

Aus dieser zweistufigen Konstruktion des Art. 35 DS-GVO erwachsen zwei Herausforderungen, mit denen der Verantwortliche bei seiner praktischen Arbeit konfrontiert ist:

Erstens muss er eigenständig beurteilen, ob sein geplanter Datenverarbeitungsvorgang voraussichtlich zu einem „hohen Risiko“ für Rechte und Freiheiten von natürlichen Personen führt oder ob das Risiko als „normal“ einzustufen ist. Diese Risikoabschätzung wird in der Praxis umso schwerer fallen, als weder die DS-GVO selbst eine Legaldefinition enthält, wann ein hohes Risiko anzunehmen ist,¹¹ noch der europäische Gesetzgeber klargestellt hat, wo die Trennlinie zwischen einem „normalem Risiko“, das jeder Verarbeitung personenbezogener Daten innewohnt,¹² und einem „hohen Risiko“ zu ziehen ist.¹³

Zweitens bleibt für den Verantwortlichen unklar, ob und wenn ja, wie sich die Risikoprognose in der Vorprüfung (Art. 35 Abs. 1 S. 1 DS-GVO) von der von ihm geforderten Abschätzung im Rahmen der eigentlichen DSFA (Art. 35 Abs. 7 Ziff. c DS-GVO) unterscheidet. In der Praxis stellt sich somit die Frage nach den Anforderungen an die jeweiligen Risikoabschätzungen, insbesondere im Hinblick auf ihre Determinanten.

Diese beiden Fragen beleuchtet der vorliegende Beitrag. Dabei nimmt er insbesondere die Risikobestimmung innerhalb der Vorprüfung in den Blick und entwirft einen praxisorientierten Vorschlag für eine trennscharfe Abgrenzung von der Risikoprognose innerhalb der eigentlichen DSFA.

II. Die Risikoprognose im Rahmen der Vorprüfung

Nach Art. 35 Abs. 1 S. 1 DS-GVO steht die Risikoprognose des Verantwortlichen im Zentrum der Vorprüfung. Sie ist – bildlich gesprochen – das Nadelöhr, das zur eigentlichen DSFA führt. Allerdings definiert die DS-GVO nicht legal, wann von einem „hohen Risiko“ auszugehen ist.

1. Regelbeispielskatalog nach Art. 35 Abs. 3 DS-GVO

Immerhin nennt die DS-GVO in Art. 35 Abs. 3 DS-GVO drei Regelbeispiele,¹⁴ bei deren Vorliegen eine DSFA obligatorisch ist. Das bedeutet, dass der europäische Gesetzgeber bei den in lit a – c beschriebenen drei Typen von Verarbeitungstätigkeiten generell hohe Risiken sieht, und zwar unabhängig vom konkreten Einzelfall und den dafür bereits geplanten risikominimierenden Maßnahmen. Aus der Zusammenschau von Art. 35 Abs. 3 DS-GVO und ErwGr 91 S. 2 ergibt sich, dass eine DSFA in folgenden Fallkonstellationen obligatorisch ist:

Erstens bei systematischen und umfassenden Bewertungen natürlicher Personen, die auf automatisierten Verarbeitungen und Profilbildungsmaßnahmen gründen und rechtliche oder ähnlich intensive Folgen für den Betroffenen haben (Art. 35 Abs. 3 DS-GVO lit a i.V.m. ErwG 91 S. 2 Var. 1).

Zweitens bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DS-GVO oder von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 (Art. 35 Abs. 3 lit b DS-GVO i.V.m. ErwG 91 S. 2 Var. 2).

Daneben erachtet der europäische Normgeber eine DSFA in Fällen systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche als zwingend. Dies geht aus Art. 35 Abs. 3 lit c DS-GVO i.V.m. ErwG 91 S. 3 Var. 1 hervor.

Die Regelbeispiele des Art. 35 Abs. 3 DS-GVO bilden ErwG 91 S. 1 ab, in dem es heißt: „Dies [die Durchführung einer Datenschutz-Folgenabschätzung] sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und – beispielsweise aufgrund ihrer Sensibilität – wahrscheinlich ein hohes Risiko mit sich bringen [...]. Allerdings ist Art. 35 Abs. 3 DS-GVO nicht abschließend. Das bedeutet, dass auch außerhalb dieser Fallkonstellationen DSFAs erforderlich sein können.“

2. Negativ- und Positivlisten der Aufsichtsbehörden

Außerhalb des Regelbeispielskatalogs nach Art. 35 Abs. 3 DS-GVO überträgt der europäische Normgeber die Konkreti-

11 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 15 a.

12 Piltz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 24 Rn. 45 mit Verweis auf Ratsdokument 12312/1/14 REV 1 v. 17.9.2014, S. 2. Der EuGH betont in ständiger Rechtsprechung, dass jede Verarbeitung von personenbezogenen Daten eine Beeinträchtigung des Grundrechts auf Datenschutz nach Art. 8 GRCh darstellt, die jedoch nach Art. 52 GRCh gerechtfertigt sein kann (EuGH v. 09.11.2010 – C-92/09 und C-93/09 (Schecke und Eifert)). Damit kann in jeder Verarbeitung von personenbezogenen Daten ein Risiko für die Rechte und Freiheiten natürlicher Personen gesehen werden, Bieker/Hansen/Friedewald, RDV 2016, 188 (190). Voraussetzung für eine Rechtfertigung ist, dass die Beeinträchtigung durch entsprechende Abhilfemaßnahmen auf ein Maß reduziert wird, das ein angemessenes Schutzniveau sicherstellt, Bieker/Bremert, ZD 2020, 7 (8).

13 Eine Unterscheidung zwischen „Risiko“ und „hohem Risiko“ wird lediglich in ErwG 76 S. 2 kurz angedeutet.

14 Zu den Schwierigkeiten bei der Auslegung der Tatbestandsmerkmale, Krings, DSB 2019, 193 (193)

sierungsbefugnis bzw. -pflicht den Aufsichtsbehörden. So eröffnet Art. 35 Abs. 5 DS-GVO den Aufsichtsbehörden die Möglichkeit, selbst eine Liste der Arten von Verarbeitungsvorgängen zu erstellen und zu veröffentlichen, für die keine DSFA erforderlich ist (so genannte „Negativlisten“ oder „Whitelists“). Das bedeutet: Die Aufsichtsbehörden können selbst Verarbeitungstätigkeiten definieren, bei denen sie generell keine hohen Risiken sehen. Allerdings haben die Aufsichtsbehörden in Deutschland – anders als beispielsweise in Österreich¹⁵ – (derzeit) noch keinen Gebrauch von dieser Möglichkeit gemacht.¹⁶

Daneben bestimmt Art. 35 Abs. 4 DS-GVO, dass die Aufsichtsbehörde eine Liste von Verarbeitungsvorgängen zu erstellen habe, für die eine DSFA zwingend erforderlich ist (so genannte „Positivliste“ oder „Blacklist“). Sowohl Positiv- als auch Negativlisten sollen zur Rechtssicherheit und -klarheit beitragen.¹⁷

Während die Erstellung von Negativlisten nach Art. 35 Abs. 5 DS-GVO fakultativ ist, ist die Vorlage von Positivlisten für die Aufsichtsbehörden verpflichtend. So hat die Datenschutzkonferenz (DSK) eine gemeinsame Liste aller Aufsichtsbehörden¹⁸ in Deutschland für den nichtöffentlichen Bereich¹⁹ verabschiedet, in der auch das Working Paper 248 rev.01 „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) (WP 248) der Art. 29-Gruppe der Europäischen Kommission berücksichtigt wurde. Diese gemeinsame Liste enthält 16 Verarbeitungstätigkeiten, für die eine DSFA obligatorisch ist. Das bedeutet, dass die Aufsichtsbehörden der Bundesländer für diese Verarbeitungstätigkeiten generell ein hohes Risiko annehmen. Diese gemeinsame Liste enthält die maßgebliche Beschreibung der Tätigkeit, typische Einsatzfelder und Beispiele. Allerdings ist auch diese Liste nicht abschließend und somit lediglich als „ausdifferenzierte Exemplifizierung solcher Verarbeitungsvorgänge, die in jedem Fall einer Datenschutz-Folgenabschätzung unterliegen“²⁰ zu verstehen. Auch wenn sie durch die Beschreibung von Typologien zur Rechtssicherheit und -klarheit²¹ beiträgt, so entbindet sie den Verantwortlichen dennoch nicht von einer eigenständigen Risikoprognose, zumindest in den Fällen, die nicht in der Positivliste aufgeführt sind.²²

3. Eigene Risikoprognose des Verantwortlichen

Ist die vom Verantwortlichen konkret geplante Verarbeitungstätigkeit weder im Regelbeispielskatalog des Art. 35 Abs. 3 DS-GVO noch auf der Liste der Aufsichtsbehörden nach Art. 35 Abs. 4 DS-GVO enthalten, so kommt der Verantwortliche nicht umhin, eine eigene Risikoabschätzung hinsichtlich der Rechte und Freiheiten natürlicher Personen vorzunehmen. An dieser Stelle wird der Verantwortliche wieder mit dem Ausgangsproblem konfrontiert. Er muss den unbestimmten Rechtsbegriff „hohes Risiko“ definieren und für die eigene datenschutzrechtliche Tätigkeit operationalisieren. Denn die DS-GVO definiert nicht legal, was unter einem „hohen Risiko“ zu verstehen ist. Auch die Erwägungsgründe enthalten lediglich abstrakte Hinweise, wie eine Risikobestimmung zu erfolgen habe. So lässt sich aus ErwG 75 entnehmen, dass der europäische Gesetzgeber für die Bestimmung des Risikos die Determinanten Eintrittswahr-

scheinlichkeit und Schwere (der Auswirkungen) herangezogen wissen wollte. Risiko im Sinne der DS-GVO kann also als das Produkt aus Eintrittswahrscheinlichkeit und Schwere der Auswirkungen für substanzielle Freiheitsrechte natürlicher Personen verstanden werden.²³ Auch wenn die Determinanten für die Risikobestimmung aus den Erwägungsgründen zur DS-GVO hervorgehen, so schweigen sich jedoch auch die Erwägungsgründe darüber aus, welche graduellen Abstufungen die Determinanten haben und ab welchen Stufen von einem „hohen Risiko“ ausgegangen werden muss.

a) Die Leitlinien der Art. 29-Datenschutzgruppe als Orientierungshilfe

Obleich eine verbindliche Auslegung des unbestimmten Rechtsbegriffs „hohes Risiko“ endgültig nur vom Europäischen Gerichtshof²⁴ vorgenommen werden kann – was bisher noch nicht geschehen ist – versuchen an dieser Stelle die Beauftragten für den Datenschutz der Länder Handreichungen und Orientierungshilfen zu geben.²⁵ Als Auslegungshilfe des unbestimmten Rechtsbegriffs „hohes Risiko“ verweisen sie auf die Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) im WP 248 Rev. 01 der europäischen Datenschutzgruppe nach Art. 29.²⁶ Danach sind bei der Beurteilung der Frage, ob ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko mit sich bringt, folgende neun Kriterien²⁷ zu berücksichtigen:

1. Bewertung und Einstufung,

15 Österreich hat im Mai 2018 eine Whitelist vorgelegt, abrufbar unter: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.pdf.

16 Kritisch zu Whitelists: Hansen, DuD 2016, 587 (588).

17 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 38.

18 Positivliste der DSK, abrufbar unter: https://www.la.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

19 Für den öffentlichen Bereich gibt es noch keine gemeinsame Liste der Aufsichtsbehörden der Länder, so dass es den einzelnen Bundesländern obliegt, eigene Listen vorzuhalten. Exemplarisch für den öffentlichen Bereich: Der Bayerische Landesbeauftragte für den Datenschutz, Datenschutz-Folgenabschätzung – Orientierungshilfe, Version 2.0, Stand: März 2019, abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf.

20 Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 37.

21 Kritisch dazu: Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 37.

22 Jandt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 17.

23 So auch Martini, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Rn. 15 b.

24 Über die Auslegung der DS-GVO als Bestandteil des Unionsrechts entscheidet letztverbindlich allein der EuGH (Art. 267, 344 AEUV). Dieser hat eine autonome Auslegungsmethode entwickelt, bei der das Primat der teleologischen Auslegung gilt, Ehmann/Selmayr, in: Ehmann/Selmayr, Datenschutzgrundverordnung, 2. Aufl. 2018, Einführung, Rn. 91.

25 Exemplarisch für den öffentlichen Bereich: Der Bayerische Landesbeauftragte für den Datenschutz, Datenschutz-Folgenabschätzung – Orientierungshilfe, Version 2.0, Stand: März 2019, abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/oh_dsfa.pdf; für den nicht-öffentlichen Bereich: Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich, Art. 35 DS-GVO, Stand: September 2019, abrufbar unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/handreichung_ds-fa.pdf.

26 Die Leitlinien sind in deutscher Sprache beispielsweise abrufbar unter: <https://www.datenschutz-bayern.de/technik/orient/wp248.pdf>.

27 Ausführliche Beschreibung der Kriterien in den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) im WP 248 Rev. 01 der Art. 29-Datenschutzgruppe, S. 10 ff.

2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung,
3. Systematische Überwachung,
4. Vertrauliche Daten oder höchst persönliche Daten,
5. Datenverarbeitung in großem Umfang,
6. Abgleichen oder Zusammenführen von Datensätzen,
7. Daten zu schutzbedürftigen Betroffenen (Erwägungsgrund 75 DS-GVO),
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,
9. Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“ (Art. 22 und ErwG 91 DS-GVO).

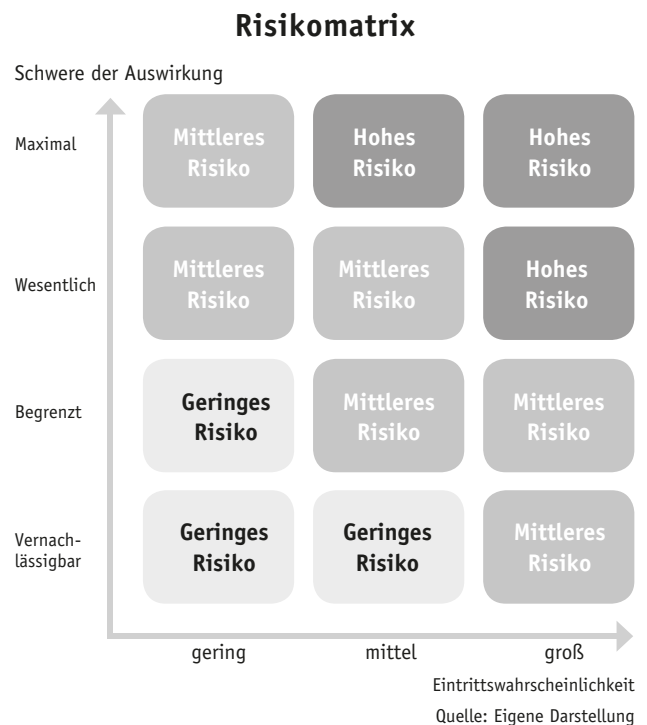
Zur Illustration hat die Art. 29-Datenschutzgruppe eine Liste²⁸ mit Beispielen für hochriskante Verarbeitungstätigkeiten erstellt und diese unter oben genannte neun Kriterien subsumiert. Flankierend gibt sie den Verantwortlichen für die eigene Risikoprognose folgende Orientierungshilfen²⁹ an die Hand: Erfüllt ein Verarbeitungsvorgang mindestens zwei der oben genannten neun Kriterien, so müsse der Verantwortliche in den meisten Fällen zu dem Schluss kommen, dass eine DSFA obligatorisch ist. Dabei nehme die Wahrscheinlichkeit, dass ein Verarbeitungsvorgang ein hohes Risiko für die Rechte und Freiheiten von Betroffenen mit sich bringt und somit eine DSFA erforderlich ist (und zwar unabhängig von den Maßnahmen, die der für die Verarbeitung Verantwortliche ins Auge fasst), im Allgemeinen immer weiter zu, je mehr Kriterien der Verarbeitungsvorgang erfüllt. Allerdings gilt diese Orientierungshilfe nach Ansicht der Art. 29-Datenschutzgruppe nicht uneingeschränkt. So könne es auch Fälle geben, in denen der Verantwortliche bei Erfüllung nur eines Kriteriums von der Notwendigkeit einer DSFA ausgehen müsse. Andererseits könne es auch vorkommen, dass ein Verantwortlicher einen Verarbeitungsvorgang, der den vorgenannten Kriterien entspricht, nicht als Vorgang bewertet, der „wahrscheinlich ein hohes Risiko mit sich bringt“. In einem solchen Fall müsse er begründen und dokumentieren, warum er keine DSFA durchführt und dabei den Standpunkt des Datenschutzbeauftragten mit einbeziehen bzw. festhalten.

Aus diesen einschränkenden Anmerkungen wird ersichtlich, dass das Vorliegen von zwei oder mehreren der von der Art. 29-Datenschutzgruppe benannten Kriterien allenfalls als Indiz für die Wahrscheinlichkeit eines hohen Risikos gelten kann. Absolut setzen sollte der Verantwortliche nach Meinung der europäischen Datenschutzgruppe diese Orientierungshilfe jedoch nicht. Damit wird ihm die eigene Risikoprognose allenfalls erleichtert, jedoch keinesfalls abgenommen. Mit der Darstellung der Vorschläge der Art. 29-Datenschutzgruppe enden auch die Orientierungshilfen der Beauftragten für den Datenschutz der Länder.

b) Die selbstgestaltete Risikomatrix als Leitplanke

Der Verantwortliche bleibt weiterhin mit der Aufgabe konfrontiert, für jeden konkreten Einzelfall eine eigenständige Risikoprognose durchzuführen. Aus ErwG 75 kann er ent-

nehmen, dass sich das Risikoniveau aus dem Verhältnis von Schwere der Auswirkungen auf den Betroffenen und Eintrittswahrscheinlichkeit ergibt. Nun kann er sich die – im Risikomanagement verwendete – Risikomatrix zu Nutze machen und auf der Abszisse die „Eintrittswahrscheinlichkeit“ und auf der Ordinate die „Schwere der Auswirkungen“ abtragen. Nun muss er die graduellen Abstufungen der Eintrittswahrscheinlichkeit (hier beispielhaft: gering, mittel, groß) als auch der Schwere der Auswirkungen (hier beispielhaft: vernachlässigbar, begrenzt, wesentlich und maximal) selbst bestimmen. Außerdem muss der Verantwortliche selbst die Risikoniveaus definieren.



In dieser Matrix wird in den folgenden drei Fällen von einem hohen Risiko ausgegangen:

1. Eintrittswahrscheinlichkeit MITTEL und Auswirkungen MAXIMAL,
2. Eintrittswahrscheinlichkeit GROSS und Auswirkungen MAXIMAL,
3. Eintrittswahrscheinlichkeit GROSS und Auswirkungen WESENTLICH.

Nun obliegt es dem Verantwortlichen, den jeweiligen Schweregrad der Auswirkungen sowie die Eintrittswahrscheinlichkeit inhaltlich mit Leben zu füllen. Bei Ersterem kann er sich an der Definition des Schweregrads der Auswirkungen des Privacy Impact Assessments (PIA)³⁰ orientieren. Da in oben aufgeführter Risikomatrix ein hohes Risiko nur vorliegen kann, wenn die Auswirkungen entweder wesentlich oder maximal sind, beschränken sich die hiesigen Aus-

²⁸ WP 248 Rev. 01, S. 13 ff.

²⁹ WP Paper 248 Rev. 01, S. 12 f.

³⁰ Privacy Impact Assessment, S. 4 f., abrufbar unter: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>.

fürungen auf diese beiden Abstufungen. Nach PIA sind Auswirkungen dann als wesentlich zu qualifizieren, wenn Betroffene eventuell signifikante Konsequenzen erleiden, die sie nur mit ernsthaften Schwierigkeiten überwinden können. Als Beispiele nennt PIA den Entgang nicht wiederkehrender Möglichkeiten (z.B. hinsichtlich der Kreditvergabe, der Zulassung zum Studium, des Praktikums, der Arbeitsstelle oder der Prüfungszulassung). Als maximal stuft PIA Auswirkungen ein, wenn Betroffene eventuell signifikante oder sogar unumkehrbare Konsequenzen erleiden, die sie nicht überwinden können.

Nach der Definition der einzelnen Abstufungen des Schweregrads der Auswirkungen muss der Verantwortliche nun den jeweiligen Grad der Eintrittswahrscheinlichkeit im Einzelfall definieren. Er muss also festlegen, wann geringe, mittlere oder große Eintrittswahrscheinlichkeiten anzunehmen sind. Auch wenn abstrakte Definitionen möglich sind (etwa geringe Eintrittswahrscheinlichkeit = Eintritt einmal im Jahr; mittlere Eintrittswahrscheinlichkeit = zwei- bis fünfmal im Jahr; große Eintrittswahrscheinlichkeit = mehr als fünfmal pro Jahr), so stellt die konkrete Bestimmung der Eintrittswahrscheinlichkeit den Verantwortlichen vor große Herausforderungen. Denn während er den Schweregrad der Auswirkungen der Datenverarbeitung – beispielsweise mithilfe der Abstufungssystematik von PIA (vernachlässigbar, begrenzt, wesentlich, maximal) – auch ohne Berücksichtigung der konkret getroffenen risikominimierenden Maßnahmen prognostizieren kann, gelingt ihm dies hinsichtlich der Eintrittswahrscheinlichkeiten nicht. Denn konkrete Eintrittswahrscheinlichkeiten lassen sich grundsätzlich erst dann bestimmen, wenn die Ereignisse, die zu Auswirkungen der Datenverarbeitung führen können, mit den geplanten Abhilfemaßnahmen in Beziehung gesetzt sowie bewertet worden sind.³¹ Denn für die Eintrittswahrscheinlichkeit macht es durchaus einen Unterschied, ob beispielsweise Krankenakten in Sicherheitsschranken in mit Alarmanlagen und Sicherheitskameras versehenen abgeschlossenen Räumen verwahrt werden oder offen im Regal in für jedermann zugänglichen Räumen stehen.

Berücksichtigt jedoch der Verantwortliche bereits bei der Risikoprognose im Rahmen der Vorprüfung die vorgesehenen risikominimierenden technischen und organisatorischen Maßnahmen (TOMs), dann nimmt er die Risikoprognose im Rahmen der eigentlichen DSFA nach Art. 35 Abs. 7 lit c DS-GVO vorweg. Eine gesonderte Risikoabschätzung im Rahmen der DSFA wäre somit redundant.³² Fraglich ist, ob dieses Ergebnis der Intention des europäischen Normgebers entspricht. Aus dem Normtext des Art. 35 Abs. 3 DS-GVO lässt sich keine konkrete Antwort entnehmen. So wendet sich der Blick zu den Fallkonstellationen nach Art. 35 Abs. 3 DS-GVO, für die der europäische Gesetzgeber exemplarisch hohe Risiken für die Rechte und Freiheiten natürlicher Personen angenommen hat. Hier hat sich der Normgeber eine generelle Sichtweise zu Eigen gemacht. So stellt er bei der Beurteilung, ob ein hohes Risiko vorliegt, ausschließlich auf potentiell schwerwiegende Auswirkungen ab. Keine Rolle bei der Be-

urteilung spielt hingegen, ob risikominimierende Maßnahmen vorgesehen waren.

Auch beim Blick auf die Positivlisten der Aufsichtsbehörden zeigt sich im Grunde dasselbe Bild. Auch hier werden Beispiele aufgeführt, die nach Ansicht der Aufsichtsbehörden generell zu gravierenden Konsequenzen für die Rechte und Freiheiten der Betroffenen führen können. Somit läge die Idee nahe, sich dieser Vorgehensweise auch bei der eigenen Risikoprognose im Rahmen der Vorprüfung zu bedienen. Damit müsste der Verantwortliche bei der Prüfung der Frage, ob eine Verarbeitung voraussichtlich mit einem hohen Risiko einhergeht, ausschließlich das Kriterium heranziehen, ob mittels der Verarbeitung maximale/wesentliche Auswirkungen für den Betroffenen zu befürchten sind. Die Eintrittswahrscheinlichkeit, die ohnehin nur in Verbindung mit den konkret geplanten TOMs prognostiziert werden könnte, bliebe im Rahmen der Vorprüfung unberücksichtigt. Sie würde erst auf der Ebene der eigentlichen DSFA bewertet werden. Die Fokussierung auf das Bruttoisiko³³ der Datenverarbeitungsvorgänge im Rahmen der Vorprüfung und auf das Nettoisiko im Rahmen der eigentlichen DSFA würde zu einer trennscharfen Abgrenzung der beiden Risikobestimmungen führen. Daneben würde diese Vorgehensweise in der Praxis zu einer leichteren Handhabung des ohnehin komplex angelegten Art. 35 DS-GVO führen. Und schließlich würde sich die vorgeschlagene Risikobestimmung auf der Linie der vom europäischen Normgeber in Art. 35 Abs. 3 DS-GVO, der Positivlisten der nationalen Aufsichtsbehörden sowie der Orientierungshilfe der Art. 29-Datenschutzgruppe zum Vorschein gekommenen Intention bewegen.³⁴ Auch die Gefahr, dass die Vorprüfung ihrer Filterwirkung nicht gerecht würde, besteht nicht. Vielmehr ist eher das Gegenteil der Fall: Das Nadelöhr des Art. 35 Abs. 1 S. 1 DS-GVO würde weiter, stellte man bei der Vorprüfung auf das Bruttoisiko ab.

III. Fazit und Ausblick

Im Zentrum der Prüfung, ob eine DSFA erforderlich ist, steht die Frage, ob es sich bei dem beabsichtigten Datenverarbeitungsvorgang um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt. Diese Einschätzung obliegt zuvörderst dem Verantwortlichen. In der Praxis kann die Risikoprognose zur Herausforderung werden, insbesondere, weil die DS-GVO selbst keine Legaldefinition des unbestimmten Rechtsbegriffs „hohes Risiko“, sondern allenfalls Beispiele enthält, die jedoch nicht abschließend sind. Aus ErwG 75 geht jedoch hervor, dass sich das Risiko aus dem Produkt der

31 Insofern ist der Argumentation von Syckor, Strufe und Rösberg zuzustimmen (Syckor/Strufe/Rösberg, ZD 2019, 390 (391)).

32 Diese Ansicht vertreten auch Syckor, Strufe und Rösberg (Syckor/Strufe/Rösberg, ZD 2019, 390 (391)).

33 Von Brutto- und Nettoisiken spricht auch Jung, CB 2018, 170 (173).

34 Auch Jung, CB 2018, 170 (174) konstatiert, dass der Ordnungsgeber bei Art. 35 Abs. 3 DS-GVO den ansonsten eingeschlagenen Pfad der Bestimmung des Risikoniveaus durch Eintrittswahrscheinlichkeit und Schaden verlassen hat und eine absolute Festlegung trifft. In derselben Absolutheit wirkten auch die Positivlisten nach Art. 35 Abs. 4 DS-GVO.

Determinanten „Schwere der Auswirkungen“ und „Eintrittswahrscheinlichkeit“ zusammensetzen soll. Wie das Risikoniveau konkret graduell bestimmt werden soll, darüber schweigen sich die DS-GVO und die Erwägungsgründe jedoch aus.

Jedoch hat der europäische Normgeber in Art. 35 Abs. 3 DS-GVO drei Fallkonstellationen bezeichnet, bei denen er generell, das bedeutet, unabhängig vom konkreten Einzelfall, ein hohes Risiko annimmt. Das bedeutet, dass der Normgeber ausschließlich darauf abstellt, ob der geplante Datenverarbeitungsvorgang potenziell schwerwiegende Auswirkungen für die Rechte und Freiheiten natürlicher Personen hat. Dabei ist die Eintrittswahrscheinlichkeit für die Annahme eines hohen Risikos unerheblich. Auch wenn der Verantwortliche – wegen geplanter risikominimierender TOMs – von einer geringen Eintrittswahrscheinlichkeit ausginge, die das Risiko auf ein Normalmaß reduzierte, so müsste er nach dem Willen des europäischen Gesetzgebers dennoch eine DSFA durchführen.

Ebenfalls ausschließlich auf potenziell schwerwiegende Auswirkungen stellen die Positivliste der Datenschutzbeauftragten der Länder sowie die Orientierungshilfe im Working Paper 248 der Art. 29-Datenschutzgruppe ab.

Vor diesem Hintergrund plädiert der vorliegende Beitrag dafür, bei der Risikobestimmung innerhalb der Vorprüfung nach Art. 35 Abs. 1 DS-GVO die Determinante „Eintrittswahrscheinlichkeit“ außen vor zu lassen und sich ausschließlich auf die Determinante „Schwere der Auswirkungen“ zu fokussieren. Dieses Vorgehen entspricht der Linie, die der europäische Normgeber in Art. 35 Abs. 3 DS-GVO vorgegeben hat und würde zu einer trennscharfen Abgrenzung der Risikoprognosen innerhalb der Vorprüfung (Art. 35 Abs. 1 S. 1 DS-GVO) und der eigentlichen DSFA (Art. 35 Abs. 7 DS-GVO) führen.



Prof. Dr. Kerstin Liesem

ist Professorin an der Hochschule für Polizei und öffentliche Verwaltung NRW.

RA Sebastian Schulz

Cookies, Schrems & Co. – Webseitengestaltung zwischen rechtlichen Vorgaben und Businessperspektive

Ein Leitfaden für Praktiker

Mit dem Einsatz von Cookies und vergleichbaren Skripten auf Webseiten und in Apps sind zahlreiche Fragestellungen verbunden. Einige davon werden bereits seit Jahren kontrovers diskutiert. Andere sind erst mit den jüngsten Verlautbarungen der Datenschutzaufsichtsbehörden, spätestens aber mit den Urteilen in der Rechtssache Planet 49, in den Fokus einer breiteren (Fach-)Öffentlichkeit gerückt. Allgemeingültige Aussagen sind gleichwohl weiterhin kaum erkennbar. Auch im Anschluss an die Urteile des EuGH und des BGH sind zahlreiche Fragen wei-

terhin offen, neue wurden aufgeworfen. Soweit überhaupt Aussagen der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten existieren, weichen diese mitunter erheblich voneinander ab. Die folgenden Ausführungen fassen die wesentlichen rechtlichen Herausforderungen zusammen, die sich bei der Einbindung von Cookies und anderen Skripten auf Webseiten stellen und unternehmen den Versuch, ein möglichst ausgewogenes Verhältnis zwischen rechtlichen Anforderungen und den Belangen von Webseitenbetreibern herzustellen.

I. Einleitung

Der BGH hat mit seinem Urteil vom 28.5.2020¹ einen Schlussstrich unter einen mehr als sechs Jahre andauernden Rechtsstreit gezogen. Zu den Kernaussagen des Gerichts zählt, dass auch deutsche Webseitenbetreiber für den Einsatz von Cookies, die werblichen Zwecken dienen, ein Opt-In der Webseitenbesucher benötigen. Für den BGH ergibt sich diese Aussage aus einer „Kombination“ aus dem in Art. 5 Abs. 3 S. 1 RL 2002/58/EG (E-Privacy-Richtlinie) normierten Einwilligungserfordernis für den Einsatz von Co-

kies einerseits und § 15 Abs. 3 TMG andererseits. Dass die Normen unterschiedlichen Schutzgütern dienen und zudem § 15 Abs. 3 TMG expressis verbis ein Widerspruchsverfahren vorsieht, ficht den BGH nicht an. Im Gegenteil: Im Fehlen einer wirksamen Einwilligung könne ein der Erstellung von Nutzungsprofilen entgegenstehender Widerspruch erblickt werden. Der gebotenen richtlinienkonformen Auslegung von § 15 Abs. 3 Satz 1 TMG stehe es nicht entgegen, dass der deutsche Gesetzgeber bisher keinen Akt der Umsetzung der

1 I ZR 7/16 – Cookie-Einwilligung II.

E-Privacy-Richtlinie vorgenommen habe. Es sei anzunehmen, dass der deutsche Gesetzgeber die bestehende Rechtslage in Deutschland für richtlinienkonform erachtete.

Ob sich der BGH mit solchen Aussagen noch innerhalb der Grenzen zulässiger „Im-Lichte“-Auslegung bewegt hat, mag die Rechtswissenschaft beantworten. Eleganter wäre es wohl gewesen, § 15 Abs. 3 TMG dem Anwendungsvorrang der DSGVO zum Opfer fallen zu lassen. § 15 Abs. 3 TMG ist, ebenso wie die praktisch wortgleiche Vorgängernorm des im Jahr 1997 in Kraft getretenen § 6 Abs. 3 Teledienstedatenschutzgesetz (TDDSG) originäres mitgliedstaatliches Datenschutzrecht ohne jeden Bezug zu Art. 5 Abs. 3 E-Privacy-Richtlinie.

Und: Ungeachtet dessen, ob die Intention des Gesetzgebers für die Europarechtskonformität einer nationalen Rechtsnorm überhaupt von Bedeutung ist, ist die Einschätzung des BGH an dieser Stelle schlicht nicht zutreffend: So hatte das für das TMG federführend zuständige Bundeswirtschaftsministerium (BMWi) noch kurz vor Wirksamwerden der DSGVO (und zuletzt auch Ende 2019) den Versuch unternommen, das Opt-Out des § 15 Abs. 3 TMG an das Opt-in des Art. 5 Abs. 3 S. 1 E-Privacy-Richtlinie anzupassen. Auch in seinem aktuellen Referentenentwurf für ein TTDSG² stellt das BMWi in der Begründung unmissverständlich klar, dass nur § 15 Abs. 1 TMG, nicht aber § 15 Abs. 3 TMG als Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie einzuordnen ist.³ Die Irrlichterei der EU-Kommission aus dem Jahr 2014, die seinerzeit auf Anfrage des BMWi hin bestätigte, Art. 5 Abs. 3 E-Privacy-Richtlinie sei in Deutschland umgesetzt, liegt lange zurück. Ein Jahr später kam der Wissenschaftliche Dienst des Europäischen Parlaments bekanntlich zu einem gegenteiligen Ergebnis. Schließlich machten Ende 2019 belastbare Gerüchte die Runde, die EU-Kommission habe mit der Einleitung eines Vertragsverletzungsverfahrens gegen Deutschland wegen der Nichtumsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie gedroht. Ein Anruf aus Karlsruhe im zuständigen Referat des BMWi hätte an dieser Stelle für Klarheit sorgen können.

Von diesen Überlegungen losgelöst stellt sich für Webseitenbetreiber freilich einmal mehr die Frage, welche Aspekte konkret zu beachten sind, um dem durch den BGH (nur) bestätigten Opt-In-Erfordernis im Zusammenhang mit dem Einsatz von Cookies auf Webseiten Rechnung zu tragen.

II. Rechtliche Anforderungen an „Cookie-Banner“

1. Erforderlichkeit eines Cookie-Banners

Der BGH hat das Einwilligungserfordernis für Cookies, soweit diese zu Marketingzwecken eingesetzt werden sollen, bejaht. Mehr gab der zu betrachtende Sachverhalt nicht her. Tatsächlich werden aber auch Cookies und Skripte, die anderen Zwecken dienen, regelmäßig erst nach der ausdrücklichen Einwilligung des Webseitenbesuchers aktiviert werden dürfen. Welche das sind, wird man bis auf Weiteres zumindest in Anlehnung an die in Art. 5 Abs. 3 S. 2 E-Privacy-Richtlinie vorgenommene Negativabgrenzung ermitteln können. Hiernach bedarf es keiner Einwilligung in die Platzierung von Cookies bzw. in das Auslesen von Informationen, die auf Endgeräten der Nutzer gespeichert sind,

wenn deren „[alleiniger] Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist [Variante 1] oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann [Variante 2].“ Mag hier vor allem Variante 2 ein wenig Argumentationsspielraum eröffnen, sollten Webseitenbetreiber gleichwohl die Position der Aufsichtsbehörden im Blick behalten, wonach stets ein „klarer Zusammenhang zwischen der unbedingten Notwendigkeit eines Cookies und dem vom Nutzer ausdrücklich angeforderten Dienst bestehen [muss]“.⁴

Technisch erforderliche „Vorgänge“ sind also einwilligungsfrei. Dieser gerätespezifischen Betrachtung muss auch die datenschutzrechtliche folgen: Kommt es im Zusammenhang mit dem Einsatz von technisch-erforderlichen Cookies oder dem Auslesen von Informationen, die das anfragende Endgerät aussendet, zu einer Verarbeitung von personenbezogenen Daten (z.B. Cookie-IDs, IP-Adressen), ist die datenschutzrechtliche Rechtsgrundlage Art. 6 Abs. 1 Buchst. f DSGVO. Zur Vorbeugung von Missverständnissen sollten Webseitenbetreiber hier gar nicht erst den Anschein erwecken, dass technisch erforderliche Cookies einer Einwilligung zugänglich sind. Über den Einsatz dieser Skripte ist ausschließlich zu informieren (vgl. aber unten 10). Insofern ist auch der weithin genutzte Begriff „Consent Management“ unglücklich. Tatsächlich geht es um „Cookie-“ oder „Script-Management“.

Alle technisch nicht erforderlichen Cookies bedürfen also bei Pageview 1 einer Einwilligung des Webseitenbesuchers. Eine Rückausnahme besteht nur in Fällen, in denen Cookies nicht bereits zum Zeitpunkt des ersten Aufrufs einer Webseite geladen werden, sondern erst im Zusammenhang mit der Aktivierung einer bestimmten Anwendung, eines iFrames o.ä., etwa auf einer Unterseite. Beispiele hierfür sind eingebundene Videoportale, Kartendienste, Payment-Dienstleister oder Gutscheineangebote nach Durchlaufen des Checkout-Prozesses in einem Online-Shop. Soweit solche Skripte nicht bereits als technisch erforderlich und damit als einwilligungsfrei eingeordnet werden können (s.o.), genügt es hier, die Einwilligung erst im Zusammenhang mit der Aktivierung des jeweiligen Skriptes einzuholen. A/B-Tests haben gezeigt, dass die Opt-In-Rate dort höher ist, wo der Webseitenbesucher einen mit der Abgabe einer Einwilligung verbundenen unmittelbaren Nutzen erkennen kann.

Ob mit Blick auf solche Cookies, die im Zusammenhang mit dem Einsatz von Trackingtools platziert werden, dann kein Einwilligungserfordernis besteht, wenn diese Tools lokal auf den Servern der Webseitenbetreiber gehostet sind, ist offen und auch unter den Aufsichtsbehörden umstritten. Mit dem BGH wird man diese Sicht klar ablehnen müssen. In Internet findet man dennoch auf Anhieb Webseiten promi-

² Referentenentwurf eines Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze, Stand: 14.07.2020.

³ Rn. 3, dort S. 37.

⁴ Art. 29-Datenschutzgruppe, WP 196 v. 07.06.2012, S. 4.

nenter Betreiber, darunter die Webseiten des EuGH sowie einer nationalen Datenschutzaufsichtsbehörde, bei deren Aufruf technisch nicht erforderliche (Tracking-)Cookies auf Endgeräten platziert werden, ohne dass zuvor die Einwilligung der Webseitenbesucher eingeholt wird. Die französische CNIL geht sogar einen Schritt weiter und gestattet den einwilligungsfreien Einsatz von Tracking-Cookies, vorausgesetzt die Cookies dienen allein der Erstellung von Statistiken unter Verwendung anonymisierter Informationen.⁵

Soweit ein „Tag Manager“ zum Zwecke der erleichterten Implementierung von Cookies und vergleichbaren Skripten zum Einsatz kommt, ist dieser grundsätzlich weder unter dem Gesichtspunkt des Endgeräteschutzes noch unter datenschutzrechtlichen Aspekten von Relevanz. Etwas anderes gilt nur dann, wenn der eingesetzte Tag Manager schon vor Eintritt der definieren Ereignisse (sog. Trigger) selbst Informationen des abrufenden Endgerätes verarbeitet oder, in der Praxis wohl selten, selbst Cookies auf Endgeräten platziert.

2. Technische Konfiguration

Im Zeitpunkt des Aufrufens einer Webseite dürfen nur solche Skripte geladen werden, die als technisch erforderlich und damit als einwilligungsfrei eingeordnet werden können. So einfach diese Erkenntnis auch ist, so oft werden in der Praxis bereits an dieser Stelle – bewusst oder unbewusst – Fehler gemacht. Fehler können mit einfachsten Mitteln am Frontend nachvollzogen und von interessierter Seite dokumentiert werden.

Kommt es aber zu einer derart fehlerhaften technischen Umsetzung, geht damit typischerweise nicht nur ein rechtswidriger Zugriff auf das Endgerät des Nutzers und eine datenschutzwidrige Verarbeitung der Cookie-ID sowie von über das Cookie erhobenen personenbezogenen Daten einher. Vielmehr setzen sich Webseitenbetreiber zusätzlich dem Vorwurf der Täuschung aus, wenn ausweislich der Ausführungen im Cookie Banner, der „Cookie Declaration“, technisch nicht erforderliche Cookies allein auf Grundlage der Einwilligung eingesetzt werden, solche Cookies jedoch im Hintergrund bereits bei Pageview 1 aktiv sind. Zumindest bei der Bemessung der Höhe eines etwaigen Bußgeldes und eines nach Art. 82 Abs. 1 DS-GVO grundsätzlich denkbaren Schadensersatzes wird man diesen Aspekt berücksichtigen müssen.

3. Verbot der Voreinstellung und Auswahlmöglichkeit

Ob eine Einwilligung in das Platzieren von Cookies auch im Wege einer voreingestellten Checkbox eingeholt werden kann, war eine der zentralen Fragen in der Rechtssache Planet 49. Die Antwort des BGH lautet bekanntlich: nein. Entlang des Sachverhalts, den der BGH zu betrachten hatte, ist dieser Befund auch richtig. Allein, der BGH hatte gerade nicht über die Konfiguration eines Cookie Managements zu entscheiden. Entscheidungserheblich war, dass mit dem Anklicken einer Schaltfläche zur Teilnahme an einem Gewinnspiel zugleich im Wege einer voreingestellten Checkbox eine Einwilligung in die Verwendung von Cookies „erteilt“ wurde. Schön herausgearbeitet wurde dieser Punkt durch den Generalanwalt am EuGH in dessen Schlussanträgen.⁶

Das Cookie Management dreht sich hingegen ausschließlich um die Frage, ob mit dem Klick auf eine Schaltfläche eine datenschutzrechtliche Einwilligung erteilt wird. Die Einwilligung ist nicht bloßes Beiwerk, sondern die einzige Willenserklärung.

Hiervon ausgehend wird dem Verbot der Voreinstellung, rechtlich verankert in Erwägungsgrund 32 S. 3 DS-GVO, jedenfalls dann Rechnung getragen, wenn dem Webseitenbesucher bei Pageview 1 unterschiedliche Auswahlmöglichkeiten angeboten werden. Kann der Webseitenbesucher zwischen unterschiedlichen Varianten wählen, von der eine das Weitersurfen auch ohne weitere Cookies ermöglicht, ist dies zweifellos hinreichend. Dass mit einem Klick auf eine der anderen Auswahlmöglichkeiten alternativ eine Einwilligung nach Maßgabe der durch den Webseitenbetreiber definierten Reichweite abgegeben werden kann, stellt insbesondere keinen Verstoß gegen das Verbot von „Opt-Out“-Einwilligungen dar. Die oft reflexartige Behauptung, infolge einer „preticked checkbox“ sei das gesamte Cookie Management fehlerhaft, springen damit regelmäßig zu kurz. Entscheidend ist die Gesamtkonfiguration. Erst wenn ein Weitersurfen ohne Cookies eine aktive Handlung im Sinne eines Abwählens, d.h. mindestens zwei Klicks (1. Abwählen, 2. Auswahl bestätigen) erfordert, begibt sich der Webseitenbetreiber in ein erhöhtes Risiko.

Die Möglichkeit des Weitersurfens, ohne dass zusätzliche Cookies platziert werden, kann auch über das Vorsehen eines „X“ am rechten oberen Rand des Cookie Banners eröffnet werden. Die dahinterstehende Logik ist dem durchschnittlichen Nutzer von Computer und Internet ohne Weiteres geläufig. Ein Hinweis im Cookie Banner, dass auch im konkreten Fall dem „X“ diese ablehnende Bedeutung zukommt, dürfte sich risikoreduzierend auswirken.

Mit etwas erhöhter Risikobereitschaft und bei Einhaltung hinreichender Transparenz, dürfte es andererseits auch ausreichend sein, die Möglichkeit der Ablehnung erst auf dem second layer, d.h. erst nach einem Klick auf „Individuelle Einstellungen“, „Mehr“ o.ä. anzubieten. Grundvoraussetzung für ein solches Vorgehen ist jedoch, dass der Webseitenbesucher auf dem first layer, im Cookie Banner, über die konkret vorzunehmenden Schritte informiert wird. Auch sollte die Möglichkeit der Verweigerung der Abgabe einer Einwilligung tatsächlich auf dem second layer vorhanden sein. Webseitenbetreiber setzen sich sonst schnell dem Vorwurf aus, die konkrete Gestaltung verletze den (ungeschriebenen) Grundsatz, nach dem die Möglichkeit des Ablehnens so einfach wie die des Akzeptierens sein muss.⁷

Zu der Frage, wie weitreichend die durch den Webseitenbetreiber definierte Auswahlmöglichkeit gehen darf, verhält sich die DS-GVO ungewohnt eindeutig. Art. 6 Abs. 1 lit a DS-GVO ordnet lediglich an, dass eine Einwilligung für „einen oder mehrere bestimmte Zwecke“ eingeholt werden

5 Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, Ziff. 51.

6 Rechtssache C-673/17, Schlussanträge des Generalanwalts vom 21.03.2019, Rz. 89.

7 Normiert ist dieser Grundsatz allein für den Widerruf einer Einwilligung, vgl. Art. 7 Abs. 3 S. 4 DS-GVO.

darf. Verarbeitungen zu mehreren Zwecken über eine Einwilligung zu legitimieren ist also möglich, stets vorausgesetzt, dass die Einwilligungserklärung zweifelsfrei alle Zwecke umfasst. Gegen die in der Praxis oft anzutreffenden Fälle, in denen durch mehrere Schaltflächen die Auswahl eröffnet wird, (1.) eine durch den Webseitenbetreiber definierte Vorauswahl, die entweder einige oder „alle“ Skripte erfasst, zu akzeptieren, (2.) weiterzusurfen ohne Abgabe einer Einwilligung in technisch nicht erforderliche Cookies und (3.) individuelle Einstellungen aktiv vornehmen zu können, ist damit nichts einzuwenden. Hier ist nichts „voreingestellt“, was erst „abgewählt“ werden müsste, um weitersurfen zu können. Diese Sichtweise steht auch im Einklang mit der Position der DSK, wonach „die Auswahlmöglichkeiten nicht „aktiviert“ voreingestellt sein dürfen.“⁸

4. Kategorisierung und Granularität der Auswahlmöglichkeiten

Schon in Anbetracht der Vielzahl der denkbaren Zwecke, zu deren Erreichung Cookies und andere Skripte eingesetzt werden, ist eine Kategorisierung bzw. Clusterung innerhalb des Cookie Managements angezeigt. Diese Vorgehensweise wird durch die DS-GVO ausdrücklich gestützt. So heißt es in Erwägungsgrund 32 S. 4 DS-GVO, dass sich eine Einwilligung „auf alle zu demselben Zweck oder denselben Zwecken vorgenommene Verarbeitungsvorgänge beziehen [sollte]“.

Die schon heute auf dem first bzw. second layer anzutreffenden Kategorien technisch nicht erforderlicher Skripte, bspw. „Statistik“, „Performance“, „Marketing“ o.ä. sind hiernach ohne weiteres möglich. Auf nachgelagerter Ebene kann der Webseitenbetreiber eine weitere Aufgliederung der von diesen Kategorien jeweils erfassten Skripte zum Zwecke einer feingranularen Auswahlmöglichkeit vornehmen. Eine Pflicht hierzu besteht hingegen nicht, kategoriebezogene Auswahlmöglichkeiten genügen. Ein Anspruch des Webseitenbesuchers, nur in ausgewählte Verarbeitungen, d.h. bezogen auf ein einzelnes Tool oder ein einzelnes Cookie, einwilligen zu können, ist von Rechts wegen nicht vorgesehen. Ohnehin fehlte es oftmals bereits an der technischen Realisierbarkeit, etwa dann, wenn durch einzelne Tools mehrere Cookies eingesetzt werden.

Losgelöst von der durch den Webseitenbetreiber gewählten Granularität bleibt freilich die Verpflichtung zur Erfüllung der Transparenzvorschriften des Art. 13 Abs. 1 und 2 DS-GVO in jedem Fall bestehen.

Von der nicht selten anzutreffenden Kategorie „Externe Dienste“, „Dienste Dritter“, „Third-Party Cookies“ o.ä. ist hingegen aus Rechtsgründen abzuraten. Hintergrund ist, dass sich Kategorien von Cookies an dem jeweils verfolgten Verarbeitungszweck orientieren. Datenschutzrechtlich schlicht falsch wäre es also von der Kategorie „Externe Dienste“ zu sprechen, wenn darin auch Auftragsverarbeiter des Webseitenbetreibers aufgelistet würden. Der Umstand, dass zur Erreichung des Zwecks auch Dritte Cookies platzieren oder dass die über Cookies erhobenen Daten an externe Empfänger weitergegeben werden, ist innerhalb der jeweiligen Kategorie und bereits auf dem first layer im Cookie Banner zu thematisieren.

5. Nudging

Will ein Webseitenbetreiber seine Webseitenbesucher zu einer bestimmten Handlung animieren, kommt der Gestaltung der entsprechenden Schaltfläche („Call-to-action“) eine besondere Bedeutung zu. Entsprechend setzen sich Schaltflächen, die nach dem Willen des Webseitenbetreibers möglichst oft angeklickt werden sollen, typischerweise in Form- und Farbgebung von anderen ab. Ob ein solches Vorgehen auch mit Blick auf die Gestaltung von Cookie-Bannern zulässig ist, ist umstritten.

Ginge es nach der Irischen Aufsichtsbehörde, müsste die Gestaltung von Cookie Bannern strengen Vorgaben genügen. In ihrer im April 2020 veröffentlichten Guidance Note⁹ heißt es hierzu auf Seite 9 wörtlich: „If you use a cookie banner or pop-up, you must not use an interface that ‘nudges’ a user into accepting cookies over rejecting them. Therefore, if you use a button on the banner with an ‘accept’ option, you must give equal prominence to an option which allows the user to ‘reject’ cookies, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them to do that, by cookie type and purpose.“

Diese paternalistische Auffassung behandelt Internetnutzer wie hilfsbedürftige Kleinkinder und beschneidet Webseitenbetreiber unverhältnismäßig in ihren Rechten. Richtig ist, dass auch bei Gestaltung von Cookie Bannern ein maßvolles Nudging zulässig ist.¹⁰ Auch eine gestalterisch hervorgehobene Schaltfläche bleibt eine „Einladung“, die Webseitenbesucher annehmen können, oder eben nicht. Grenzen werden hier allein durch das Verbot der Täuschung gezogen.

6. Kopplung von Einwilligung und Webseitennutzung

Mit der Frage der Zulässigkeit einer Kopplung von Gewinnspielteilnahme und Einwilligung hat sich der BGH in der Rechtsache Planet 49 nicht beschäftigt. Auch der EuGH¹¹ hatte sich im Rahmen des Vorlageverfahrens nicht dazu geäußert. Der BGH hatte nicht danach gefragt. Umso bemerkenswerter ist es, dass sich der Generalanwalt in seinen Schlussanträgen¹² zumindest am Rande mit Art. 7 Abs. 4 DS-GVO befasste – und zu einem eindeutigen Befund kam: Erstens könne Art. 7 Abs. 4 DS-GVO ein absolutes Kopplungsverbot nicht entnommen werden. Zweitens könne der Zweck einer Datenverarbeitung, hier: die Teilnahme an einem Gewinnspiel, von der (einwilligungsbasierten) Preisgabe personenbezogener Daten abhängig gemacht werden. Die Verarbeitung der Kontaktdaten sei dann vertraglich erforderlich, ein Fall des Art. 7 Abs. 4 DS-GVO liege gar nicht vor.¹³ Be-

8 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, S. 9.

9 Guidance Note: Cookies and other tracking technologies, April 2020, abrufbar unter www.dataprotection.ie.

10 Vgl. auch Kollmar/Schirnbacher, WRP 8/2020, 1015 (1017).

11 EuGH, Urt. v. 01.10.2019, C-673/17.

12 Rechtssache C-673/17, Schlussanträge des Generalanwalts vom 21.03.2019, Rz. 98.

13 In diese Richtung tendiert auch die DSK, vgl. Kurzpapier Nr. 3, Stand: 29.06.2017, S. 2; In Deutschland kann dieser Logik das strikte wettbewerbsrechtliche Einwilligungserfordernis des § 7 Abs. 2 UWG entgegenstehen.

reits im Jahr 2018 vertrat auch das höchste italienische Gericht¹⁴ diese Rechtsauffassung.

Bezogen auf die Einwilligung in das Aktivieren von Cookies und anderen Skripten leben ausländische Verlagsseiten in Teilen schon seit Jahren das vor, was seit einigen Monaten auch auf den Webseiten deutscher Verlage zu beobachten ist: Als sog. Freemium-Modell ausgestaltet ist die Nutzung der Webseite entweder kostenpflichtig oder wird alternativ von der Einwilligung in das Platzieren von Cookies abhängig gemacht („Cookiewall“). Die Aufsichtsbehörde in Österreich¹⁵ hat für dieses Vorgehen bereits ihren Segen erteilt. Auch der letzte Satz in Erwägungsgrund 25 E-Privacy-Richtlinie streitet für diese – zutreffende – Rechtsauffassung. Darin heißt es wörtlich: „Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt.“

Der Europäische Datenschutzausschuss („EDSA“) befasst sich in seinen im Mai 2020 veröffentlichten Guidelines zur Einwilligung explizit mit dem Thema „Cookiewalls“ und erklärt diese, abweichend von der zuvor dargestellten Position, pauschal für einen Fall unzulässiger „Conditionality“,¹⁶ allerdings ohne das Szenario einer alternativen Bezahloption zu beleuchten. Gleiches gilt für die DSK¹⁷ und die belgische Aufsichtsbehörde.¹⁸ Aufgeschlossener zeigt sich hingegen die französische CNIL, die die Zulässigkeit von Cookie-Walls einer Einzelfallbetrachtung unterzieht und bei hinreichender Transparenz als möglich erachtet.¹⁹

Tatsächlich kann ein Kopplungsverbot im Sinne von Art. 7 Abs. 4 DS-GVO bereits seinem Wortlaut nach nicht einschlägig sein. Die Norm ist nur dann anzuwenden, wenn „die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung“ von der Einwilligung in die Verarbeitung von personenbezogenen Daten abhängig gemacht wird. Das bloße „Surfen“ auf einer Webseite ist aber kein Vertrag, auch nicht das Anbieter-Nutzer-Verhältnis im Sinne von § 11 TMG. Insoweit könnte sich eine unzulässige Kopplung – wenn überhaupt – allein unter Zugrundelegung allgemeiner Erwägungen zur Wirksamkeitsvoraussetzung der Freiwilligkeit begründen lassen. Eine solche Annahme ist jedoch fernliegend. Auf die Möglichkeit der Nutzung einer bestimmten Webseite ist niemand angewiesen. Dies gilt selbst in Fällen, in denen die Webseite von Anbietern der Daseinsfürsorge betrieben wird. Die Möglichkeit, alternativ mit nämlichen Anbietern in Kontakt zu treten, wird stets bestehen. Mag das Abhängigmachen der Nutzungsmöglichkeit einer Webseite von der Abgabe einer Einwilligung ab und an als Unannehmlichkeit empfunden werden, führt dies jedenfalls nicht zu einer „Zwangssituation“, in der die Abgabe einer Einwilligung als nur noch alternativlos erscheint.

7. Weitersurfen als Einwilligung

Dass eine datenschutzrechtliche Einwilligung allein im Wege des Anklickens von Schaltflächen oder dem Aktivieren von Checkboxes erteilt werden kann, steht nirgends geschrieben. Im Gegenteil können Einwilligungen zwanglos auch

mündlich und sogar konkludent eingeholt werden, von den damit verbundenen Nachweisschwierigkeiten einmal abgesehen. Die DS-GVO ist an dieser Stelle ungewohnt progressiv: Gemäß Erwägungsgrund 32 S. 5 DS-GVO kann eine Einwilligung durch jede „Erklärung oder Verhaltensweise“ erteilt werden, „mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert.“

Diesen Erwägungsgrund hatte mutmaßlich auch die spanische Aufsichtsbehörde („aepd“) bei Erarbeitung ihrer Hinweise zur Nutzung von Cookies²⁰ im Hinterkopf. Darin heißt es auf den Seiten 29/30:

„The following actions shall also be understood as granting consent when users perform it after being informed on cookie use and being warned that to keep browsing would equal to accept cookies:

- Using the scrolling bar, provided that any information regarding cookies may be accessed without using it.
- Clicking on any link included on the webpage, other than the link to the second layer of information regarding cookies and the link to the applicable privacy policy.“

Weitersurfen kann hiernach eine eindeutige Handlung im Rechtssinne darstellen, mit der der Webseitenbesucher seine Einwilligung in das Platzieren von Cookies und darauf aufbauenden Datenverarbeitungen verdeutlicht. Bei Smartphones, Tablets usw. sollen nach zutreffender Einschätzung der aepd auch Wischgesten dem Erfordernis einer aktiven Handlung genügen. Grundvoraussetzung für die Wirksamkeit einer so erteilten Einwilligung, und darauf macht auch die aepd aufmerksam, ist freilich, dass dem Webseitenbesucher bei Pageview 1 unmissverständlich und ohne weitere Zwischenschritte die Wirkung des Weitersurfens klar gemacht wird. Eine entsprechende Information muss „ins Auge springen“.

Wird diese Wirkweise unmissverständlich verdeutlicht, liegt auch in einem schlichten Weitersurfen ohne Zweifel der erforderliche, gesonderte Erklärungswert. Die Position der DSK²¹ bzw. der irischen²² Aufsichtsbehörde, wonach das bloße Nutzen einer Webseite nicht als Ausdruck einer aktiven Willensbekundung gewertet werden könne, ist insoweit zu pauschal.

8. Informationspflichten

Ein Höchstmaß an Transparenz ist für ein Cookie Management essentiell. Zu Art und Umfang der bereitzustellenden Informa-

14 Corte di Cassazione, Entscheidung vom 02.07.2018, Az. 17278/2018.

15 DSB-D122.931/0003-DSB/2018 vom 30.11.2018.

16 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Rz. 40.

17 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, S. 10.

18 Cookies et autres traceurs, abrufbar unter <https://www.autoriteprotectiondonnees.be/cookies>.

19 Délibération n° 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération n° 2019-093 du 4 juillet 2019, Ziffer 17 und 18.

20 Guidelines on the use of cookies, Stand: November 2019, abrufbar unter www.aepd.es.

21 Vgl. DSK, Beschluss vom 12.05.2020, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 4.

22 Guidance Note: Cookies and other tracking technologies, April 2020, S. 9.

tionen hat sich auch der EuGH geäußert. Der BGH hatte in seiner Vorlageentscheidung²³ ausdrücklich danach gefragt: „Welche Informationen hat der Diensteanbieter im Rahmen der nach Art. 5 Abs. 3 der Richtlinie 2002/58/EG vorzunehmenden klaren und umfassenden Information dem Nutzer zu erteilen? Zählen hierzu auch die Funktionsdauer der Cookies und die Frage, ob Dritte auf die Cookies Zugriff erhalten?“

Der EuGH hat die Frage bejaht.²⁴ Die Darstellung, welche Dritten u.U. Zugriff auf einzelne Cookies haben, ist in der Praxis insbesondere bei Einsatz von Affiliate-Netzwerken und sog. Data Marketing Plattformen eine Herausforderung. Die DSK weist an dieser Stelle darauf hin, dass „in Fällen, in denen sich mehrere (gemeinsame) Verantwortliche auf die ersuchte Einwilligung stützen wollen, oder in denen die Daten an andere Verantwortliche übermittelt oder von anderen Verantwortlichen verarbeitet werden sollen, diese Organisationen sämtlich genannt und die Verarbeitungsaktivitäten der einzelnen Organisationen hinreichend beschrieben werden [müssen].“²⁵

Zudem ist der Rahmen der zur Verfügung zu stellenden Informationen mit den Vorgaben des EuGH längst nicht abgesteckt. Neben der Laufzeit des Cookies und möglicher Zugriffsrechte Dritter müssen selbstverständlich auch alle weiteren Pflichtinformationen aus Art. 13 Abs. 1 und 2 DS-GVO zur Verfügung gestellt werden.

Dass die Aufnahme aller dort normierten Informationen noch jede Einwilligungserklärung jäh sprengen würde, ist auch den deutschen Aufsichtsbehörden bewusst. Nach anfänglich teilweise strikter Weigerung stehen mittlerweile praktisch alle Behörden der Möglichkeit einer gestuften Informationsübermittlung (Layered Privacy Notice²⁶) offen gegenüber. Die wesentlichen Informationen gehören in die Cookie Declaration (first layer), hinsichtlich aller weiteren kann auf die Datenschutzerklärung verwiesen werden. Schon deshalb ist darauf zu achten, dass die Datenschutzerklärung (und das Impressum) bei Pageview 1 gut erreichbar sind. Pop-Ups ohne Verlinkung sind rechtswidrig, ein „Dark Pattern Design“ grenzwertig.

9. Umgang mit Widerruf

Die legitimierende Wirkung von Einwilligungen unterliegt keiner zeitlichen Verwirkung.²⁷ Wenn gleichwohl etwa die irische Aufsichtsbehörde eine „Erneuerung“ der Einwilligung nach sechs Monaten fordert,²⁸ findet dies insoweit keinen Niederschlag im Gesetz. Einwilligungen gelten bis auf Widerruf. Kommt es zu einem Widerruf, muss dieser ordnungsgemäß administriert werden. Dabei muss gemäß Art. 7 Abs. 3 S. 4 DS-GVO der Widerruf „so einfach wie die Erteilung der Einwilligung sein.“ Die Details überlässt das Gesetz den Webseitenbetreibern. Je nach technischer Ausgestaltung sind unterschiedliche Maßnahmen zur Umsetzung von Widerruf denkbar, z.B. das Löschen von Matching-Cookies oder das Setzen von Opt-Out-Cookies. Bei Letzteren sollte immer bedacht werden, dass diese auch durch den Browser des betroffenen Endgerätes akzeptiert werden. Bezogen auf Google Analytics haben die Aufsichtsbehörden deutlich gemacht, dass allein das Anbieten des Browser-Add-On keine hinreichende Widerrufsmöglichkeit darstellt.²⁹

Vorsicht ist geboten bei einer allzu überhasteten endgültigen Löschung. Zwar zieht gemäß Art. 17 Abs. 2 Buchst. b) DS-GVO ein Widerruf regelmäßig eine Löschverpflichtung nach sich. Um Nach- und Beweisproblemen aus dem Weg zu gehen, können und sollten Zeitpunkte und Umstände von Einwilligung und Widerruf für einen begrenzten Zeitraum weiterhin dokumentiert bleiben. Als Rechtsgrundlage für die weitere Speicherung kommt Art. 6 Abs. 1 Buchst. f) DS-GVO in Betracht.

Eine Mindestlaufzeit für das Opt-Out-Cookie ist durch das Gesetz nicht vorgeschrieben. Webseitenbetreiber sind hier nach ohne Weiteres berechtigt, dem (widerrufenden) Webseitenbesucher unmittelbar im Zeitpunkt des nächsten Aufsuchens der Webseite erneut mit dem Cookie Management zu konfrontieren.

10. Widerspruchsrecht gegen technisch erforderliche Cookies

Soweit im Zusammenhang mit den zum Einsatz kommenden technisch erforderlichen Skripten personenbezogene Daten verarbeitet werden, sind im Grundsatz alle Betroffenenrechte der DS-GVO zu beachten. Dies gilt insbesondere auch für das Widerspruchsrecht gemäß Art. 21 DS-GVO, wobei bezogen auf technisch erforderliche Skripte allein Abs. 1 der Norm einschlägig ist. Dass die Pflicht zur Umsetzung eines solchen allgemeinen Widerspruchs in der Regel an der Schwelle der „besonderen Situation“ des Betroffenen scheitern wird, ändert nichts an der Verpflichtung zum Hinweis auf das Widerspruchsrecht, einschließlich der Hervorhebungspflicht gemäß Art. 21 Abs. 4 Halbsatz 2 DS-GVO.

11. Erfüllung der Nachweispflicht

Wie Webseitenbetreiber im Zusammenhang mit der Implementierung eines Cookie Managements ihrer aus Art. 5 Abs. 2 DS-GVO folgenden Nachweispflicht entsprechen sollen, ist nur auf den ersten Blick unklar. Aufgrund des fehlenden direkten Kontakts mit den hinter den Endgeräten stehenden natürlichen Personen ist die Erbringung eindeutiger Nachweise ersichtlich ausgeschlossen. Auch die Grundverordnung kennt solche Situationen und hält hierfür Art. 11 DS-GVO parat.

Nicht zuletzt deshalb eröffnen auch die Aufsichtsbehörden eine pragmatische Lösung. Zur Erfüllung der Nachweispflichten genügt es hiernach, dass die Entscheidung eines Nutzers auf dem Endgerät „ohne Verwendung einer User-ID o.ä. vom Verantwortlichen gespeichert [wird].“³⁰ Nur der Vollständigkeit halber: Eine solche Information wird man freilich als technisch erforderlich und damit als einwilligungsfrei einzuordnen haben. Wird dieser Prozess dokumentiert und durch

23 BGH, Beschluss v. 05.10.2017 – I ZR 7/16.

24 EuGH, Ur. v. 01.10.2019, C-673/17, Rz. 72f.

25 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, S. 8.

26 Art. 29-Datenschutzgruppe, WP 260 v. 11.04.2018, S. 19.

27 Details bei Schulz in Gola, Datenschutz-Grundverordnung, 2. Aufl., Art. 7 Rn. 58.

28 Guidance Note: Cookies and other tracking technologies, April 2020, S. 8.

29 Vgl. DSK, Beschluss vom 12.05.2020, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 5.

30 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, S. 9.

eine nachvollziehbare Versionsverwaltung flankiert, sollte den Anforderungen der Behörden Genüge getan sein.

12. Drittstaatentransfers im Zusammenhang mit Cookies

Welche Herausforderungen das Urteil des EuGH in der Rechtssache Schrems II³¹ für den Drittstaatentransfer insgesamt mit sich bringt, wird weiterhin intensiv diskutiert. Mit Blick auf das hier betrachtete Cookie Management sei insoweit nur ein Aspekt gesondert hervorgehoben. Der EuGH,³² der Europäische Datenschutzausschuss³³ und auch die DSK³⁴ verweisen nach dem Wegfall von Privacy Shield ausdrücklich darauf, dass Drittstaatentransfers weiterhin auf Grundlage der Einwilligung der Betroffenen gemäß Art. 49 Abs. 1 Buchst. a DS-GVO möglich sind. Kommt es bei Einsatz von Cookies und den nachgelagerten Datenverarbeitungen zu einem Datentransfer in nicht-sichere Drittstaaten und stehen für diesen Drittstaatentransfer keine Garantien zur Verfügung, die den rechtlichen Vorgaben der Art. 46 und 47 DS-GVO genügen, ist damit bis auf Weiteres ein einwilligungsbasiertes Modell praktisch alternativlos.

Um der in Art. 49 Abs. 1 Buchst. a DS-GVO normierten Vorgabe der Ausdrücklichkeit der Einwilligung Rechnung zu tragen, muss der Hinweis auf die Datenübermittlung in einen nicht-sicheren Drittstaat bereits aus der Cookie Declaration hervorgehen. Den Hinweis erst auf dem second layer zu geben, genügt nicht.

In der Datenschutzerklärung müsste dann die weitere durch Art. 49 Abs. 1 Buchst. a DS-GVO geforderte Belehrung über die „bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien“ erfolgen.

Ein Verstoß gegen Kopplungsvorschriften bestünde auch im Fall der Aufnahme einer solchen Einwilligung in die Cookie Declaration nicht. Als Folgeanpassung wäre jedoch die Schaltfläche, über die der Einsatz von Cookies legitimiert werden soll, sprachlich anzupassen. Ein schlichtes „Alle akzeptieren“ wird dann nicht mehr genügen.

III. Schlussbemerkungen

Aus den Entscheidungen in der Rechtssache Planet 49 folgt für die Praxis nicht viel Neues. Kommen technisch nicht erforderliche Cookies und Skripte zum Einsatz, ist ein Opt-In-Mechanismus das Mittel der Wahl. Lässt man einmal die – nur in Teilen berechtigten – dogmatischen Erwägungen außer Acht, galt dieser Befund allerdings schon vorher. Neu ist lediglich, dass Webseitenbetreiber wegen unzulässiger Opt-Out-Lösungen nunmehr auch durch Verbraucherschutzorganisationen auf Grundlage von § 1 UKlaG in Verbindung mit § 307 BGB auf Unterlassung in Anspruch genommen werden können. Hiervon zu trennen ist die Frage, ob ein mutmaßlicher Datenschutzverstoß wettbewerbsrechtliche Unterlassungsansprüche begründet und von Verbraucherschutzorganisationen aus eigenem Recht vor den Zivilgerichten verfolgt werden kann. Zu dieser Frage hat der BGH taggleich mit der Urteilsverkündung in der Rechtssache Planet 49 er-

neut den EuGH angerufen.³⁵ Zwar ist aktuell weiterhin nicht zu beobachten, dass Verbraucherschutzorganisationen oder andere sogenannte qualifizierte Einrichtungen Webseitenbetreiber mit Verfahren überziehen. Bereits angelaufene Projekte sollten dennoch weiter flott vorangetrieben werden. Und wer bislang beständig auf Opt-Out gesetzt hat, tut gut daran, seine interne Risikoabwägung noch einmal gründlich zu durchdenken.

Spannend wird nun sein, welche konkreten Umsetzungsvarianten die Behörden und letztlich die Gerichte akzeptieren werden. Einzelne Verfahren laufen bereits. Hier wird dann auch zu klären sein, welcher Bußgeldrahmen bei Annahme eines Verstoßes Anwendung findet. Orientiert an dem Urteil des BGH ist auch in diesem Zusammenhang § 15 Abs. 3 TMG als Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie weiterhin anzuwenden. Als Folge dessen dürfte für Verstöße gegen die Norm im Anwendungsbereich der E-Privacy-Richtlinie, d.h. bezogen auf das Platzieren von Cookies oder das Auslesen von Informationen aus Endgeräten, auch nur der Sanktionsrahmen des TMG eröffnet sein. Nur für die nachgelagerte, auf Cookies aufbauende Datenverarbeitung gilt die DS-GVO.

Ob der Abschluss der Rechtssache Planet 49 tatsächlich die Zukunft des Onlinemarketings besiegelt hat, bleibt abzuwarten. Eines scheint aber gewiss: Solange Browserherstellern weiterhin freie Hand bei der Entscheidung gelassen wird, welche Informationen an das Endgerät des Nutzers durchgereicht werden, bleiben auch die hier angestellten Überlegungen zur Ausgestaltung von Cookie Bannern von nachrangiger Bedeutung.



RA Sebastian Schulz

ist als Rechtsanwalt bei HÄRTING Rechtsanwälte in Berlin tätig. Von 2012 bis 2019 leitete er den Bereich Rechtspolitik & Datenschutz beim Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bev). Zuvor war er als Referent für Datenschutz im Deutschen Bundestag

sowie für eine internationale agierende Unternehmensberatung mit dem Schwerpunkt Datensicherheit und Datenschutzmanagement tätig. Als zertifizierter Datenschutzbeauftragter und -auditor betreut der Autor schwerpunktmäßig datenschutzrechtliche Mandate. Er leitet Seminare zum Kundendatenschutz, ist Autor und Kommentator des BDSG sowie der DS-GVO und Mitglied der Schriftleitung der Datenschutz-Fachzeitschrift Privacy in Germany (PinG).

31 EuGH, Urte. v. 16.07.2020 – C-311/18.

32 EuGH, Urte. v. 16.07.2020 – C-311/18, Rz. 202.

33 EDSA, Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 v. 23.07.2020, Ziff. 8.

34 DSK, Pressemitteilung v. 28.07.2020, S. 2, Ziff. 4.

35 BGH, Beschl. v. 01.10.2019 – I ZR 186/17.

36 A.A. Kollmar/Schirnbacher, WRP 8/2020, 1015 (1016).

Dr. Wolfgang Ziebarth

Gesetzliche Strukturänderungen bei Datenschutz-Aufsichtsbehörden in EU, Bund und Ländern

Ein Beitrag auch zur aktuellen Zentralisierungs-Debatte

Der vorliegende Beitrag geht der Frage nach, inwieweit die Gesetzgeber auf Ebene der Europäischen Union und in den Mitgliedstaaten berechtigt sind, Zahl, Sitz, Ausstattung, Zuständigkeiten, Aufgaben und Befugnisse ihrer Datenschutz-Aufsichtsbehörden zu verändern. Besonderes Augenmerk soll der Situation in Deutschland gelten, wo föderal wie sektoral unterschiedliche Aufsichtsbehörden bestehen. Es soll herausgearbeitet werden, dass sich hier zwei Pole gegenüberstehen: einerseits die grundsätzlich weite Berechtigung des Gesetzgebers, Behördenstrukturen zu verändern, und andererseits die

völlige Unabhängigkeit der Datenschutzaufsicht, die aufgedrängten Änderungen entgegensteht. Daraus wird zu folgen sein, dass Strukturänderungen zwar möglich bleiben müssen, aber nur in der Weise gegen die Aufsichtsbehörde durchgesetzt werden können, dass die Unabhängigkeit der betroffenen Behörden bzw. ihrer „Mitglieder“ (Leiter) maximal geschont wird und auch kein gegenteiliger böser Schein entsteht. Änderungen werden daher in der Regel nur mit Wirkung für die jeweils nächste Amtsperiode erzwungen werden können.

I. Ausgangslage: Errichtung durch Übernahme bestehender Behördenstrukturen

1. Die Pflicht zur Errichtung von Datenschutz-Aufsichtsbehörden

Die Gesetzgeber auf Ebene der Europäischen Union und ihrer Mitgliedstaaten sind aufgrund Primär- und Sekundärrechts verpflichtet, unabhängige Datenschutz-Aufsichtsbehörden zu errichten.¹

Primärrechtlich ist eine unabhängige Datenschutzaufsicht in Art. 16 Abs. 2 S. 2 AEUV² und in Art. 8 Abs. 3 GRCh³ vorgesehen.⁴

Sekundärrechtlich wird diese Pflicht durch Art. 52 VO (EU) 2018/1725⁵ für die Ebene der Europäischen Union konkretisiert.

Für die Ebene der Mitgliedstaaten gibt Art. 51 Abs. 1 DS-GVO vor, dass für den sachlichen Anwendungsbereich der DS-GVO eine oder mehrere Datenschutz-Aufsichtsbehörden errichtet werden muss bzw. müssen.

Welche und wie viele Behörden das sind und wie die Zuständigkeiten zwischen verschiedenen Behörden verteilt sind, ist durch mitgliedstaatliches Recht zu regeln.

Dasselbe gilt gem. Art. 41 ff. JI-RL⁶ in deren Anwendungsbereich,⁷ jedoch enthält sie weniger detaillierte Vorgaben als die DS-GVO.

2. Erfüllung der Pflicht zur Errichtung von Datenschutz-Aufsichtsbehörden

Die Pflicht zur Errichtung von Datenschutz-Aufsichtsbehörden darf als erfüllt angesehen werden.

Die Europäische Union verfügt mit dem Europäischen Datenschutzbeauftragten über eine unabhängige Aufsichtsbehörde, die die Datenverarbeitungen der EU-Institutionen beaufsichtigt, Art. 52 ff. VO (EU) 2018/1725.

In Deutschland wurden die bereits vor Wirksamwerden der DS-GVO bestehenden „Datenschutz-Kontrollstellen“ i.S.d. Art. 28 DS-RL⁸ im Wesentlichen übernommen. Im

Bund ist dies aufgrund der §§ 8-16 BDSG der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).

In fast allen deutschen Ländern gibt es je eine Aufsichtsbehörde, die im jeweiligen Landesdatenschutzgesetz vorgesehen und hinsichtlich ihrer Strukturen konkretisiert ist.⁹ Der Freistaat Bayern hat sich zulässigerweise¹⁰ entschieden, an zwei Behörden festzuhalten, nämlich dem Landesbeauftragten für den Datenschutz (zuständig für öffentliche Stellen) und dem Landesamt für Datenschutzaufsicht (zuständig für nichtöffentliche Stellen).¹¹

Auch wenn das gesetzlich nicht zwingend ist, werden die Aufgaben der Aufsicht nach der DS-GVO und der JI-RL

1 Roßnagel, ZD 2015, 106, 107.

2 Vertrag über die Arbeitsweise der Europäischen Union.

3 Charta der Grundrechte der Europäischen Union.

4 Von Lewinski, DuD 2012, 564, 567.

5 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

6 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

7 Bresich/Riedl/Sourhada-Kirchmayer, ZFRV 2014, 52, 60.

8 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

9 Wilhelm, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 32. Edition, Stand: 01.11.2019, § 40 Rn. 12.

10 Ziebarth, CR 2013, 60, 67.

11 Art. 15, 18 des bayerischen Datenschutzgesetzes. Erstaunlicherweise scheint das Bayerische Landesamt für Datenschutzaufsicht, soweit es selbst Verantwortlicher ist, als öffentliche Stelle der Aufsicht des Landesbeauftragten zu unterstehen. Jedenfalls sind gegenteilige Regelungen nicht ersichtlich. Eine solche Aufsicht, die ja z.B. auch die Bewertung der Erforderlichkeit von Datenverarbeitungen zur Aufgabenerfüllung umfassen würde, wäre ein Einbruch in die völlige Unabhängigkeit des Landesamts und damit unionsrechtswidrig. Über entsprechende Aktivitäten ist dem Verfasser allerdings nichts bekannt.

grundsätzlich¹² jeweils von denselben Behörden wahrgenommen.

Besondere Zuständigkeiten bestehen in Deutschland mit Rücksicht auf die Religions- und die Medienfreiheit im Bereich der Kirchen¹³ und der Rundfunkanstalten.¹⁴ Hierauf soll im Folgenden nicht weiter eingegangen werden.

II. Denkbare Strukturänderungen

Was der Gesetzgeber einmal festgelegt hat, muss nicht ewig gleich bleiben. Aus seiner Befugnis, etwas zu regeln, folgt gewöhnlich die Befugnis, die Regelung auch wieder zu ändern. Es wäre mit dem Demokratieprinzip (Art. 20 Abs. 2 GG) nicht vereinbar, wenn einmal erfolgte Regelungen durch nachfolgende Parlamente nie wieder geändert werden könnten.¹⁵ Auch der EuGH erkennt an, dass Strukturen durch den Gesetzgeber geändert werden können.¹⁶

Änderungen sind in verschiedener Hinsicht denkbar. So könnten organisatorische Festlegungen wie der Sitz der Behörde, ihre finanzielle, sächliche und personelle Ausstattung (im Folgenden: „Organisationsänderungen“) ebenso verändert werden wie ihre sachliche und örtliche Zuständigkeit, ihre zu erfüllenden Aufgaben und die hierfür zur Verfügung stehenden Befugnisse (im Folgenden: „Tätigkeitsänderungen“).

„Organisationsänderungen“ und „Tätigkeitsänderungen“ sollen für die Zwecke dieses Beitrags unter dem gemeinsamen Oberbegriff der „Strukturänderung“ zusammengefasst werden.

1. Tätigkeitsänderungen

Neben einer Neuverteilung von Zuständigkeiten, Aufgaben und Befugnissen zwischen bestehenden Behörden ist auch die Gründung neuer und die Auflösung bisheriger Behörden theoretisch denkbar.

a) Zuständigkeiten

Behörden können neue Zuständigkeiten übertragen oder bestehende Aufgaben entzogen werden.

Derartiges ist in der Vergangenheit bereits geschehen. So wurde dem BfDI die Zuständigkeit übertragen für die Aufsicht über Finanzbehörden der Länder und über Steuerämter der Kommunen, soweit diese Daten in Bezug auf Realsteuern verarbeiten (§ 1 Abs. 2 Nr. 1 Var. 5 i.V.m. § 32 h Abs. 1 AO).¹⁷ Die Landesgesetzgeber können die Zuständigkeit des BfDI insoweit noch erweitern, soweit es um bestimmte andere Steuerarten geht (§ 32h Abs. 3 AO).

Bei solchen Gelegenheiten wird dem BfDI die Last neuer Zuständigkeiten auferlegt, den Landesbehörden werden Zuständigkeiten genommen. Nehmen Landesgesetzgeber die o.g. Regelungen zurück, erfolgt eine Änderung mit umgekehrten Vorzeichen.

Auch andere Sachmaterien könnten zwischen Bundes- und Landesbehörden wechseln. Die „Datenethikkommission“ etwa schlägt vor, die Aufsicht über nichtöffentliche Stellen weitgehend auf den BfDI zu verlagern.¹⁸

Ebenso scheint der Referentenentwurf eines TT-DSG in § 27 Abs. 1 d S. 1 i.V.m. § 9 TTDSG-RefE eine jedenfalls teilweise Aufsicht des BfDI im Bereich Telemedien vorzusehen.¹⁹

Zudem sind nicht nur die Zuständigkeiten nach der DSGVO zu verteilen. Weitere Sachmaterien, wie die Aufsichtstätigkeit im Bereich der JI-RL, im Bereich Informationsfreiheit und dergleichen können einer Behörde auferlegt, aber auch wieder entzogen werden.²⁰

Ebenso könnte die örtliche Zuständigkeit neu verteilt werden.

b) Aufgaben

Innerhalb der örtlichen und sachlichen Zuständigkeit ist die Neuordnung der zu erfüllenden Aufgaben denkbar, soweit diese nicht unionsrechtlich zwingend vorgegeben sind und daher einer Änderung durch mitgliedstaatliche Gesetzgeber entzogen sind. Freilich ist eine Änderung des Sekundärrechts denkbar; so könnte etwa die Aufgabe, an Zertifizierung und Akkreditierung (Art. 42, 43 DS-GVO) mitzuwirken, auf eine andere als die bisherige Behörde verlagert werden.

c) Befugnisse

Schließlich sind auch Befugnisse Änderungen zugänglich (s. zur unionsrechtlichen Bindung soeben unter 2.). Da die Datenschutzaufsicht in der Auswahl von Befugnissen unabhängig ist, kann die Unabhängigkeit durch Verleihung neuer Befugnisse nicht beeinträchtigt werden. Eine Beeinträchtigung ist aber durch Abschaffung von Befugnissen ebenso denkbar wie durch die Neuerrichtung materiell- oder verfahrensrechtlicher Hürden für die Ausübung von Befugnissen (vgl. z.B. § 16 Abs. 1 S. 2 BDSG).

2. Organisationsänderungen

Neben Änderungen hinsichtlich der Tätigkeit (Zuständigkeit, Aufgaben, Befugnisse) einer Behörde könnte auch organisatorisch die Behördenstruktur verändert werden.

So könnte auf Bundes- oder Landesebene eine Behörde durch eine andere (schon bestehende oder neu zu schaf-

12 Eine Ausnahme dürfte das Bayerische Landesamt für Datenschutzaufsicht darstellen, weil es keine Behörden beaufsichtigt. Ähnliches gilt für Aufsichtsbehörden der Rundfunkanstalten und Kirchen.

13 Dazu von Lewinski (o. Fn. 4), 566.

14 Smolle, in: Zilkens/Gollan, Datenschutz in der Kommunalverwaltung, 5. Aufl. 2019, Rn. 1071; König, DuD 2013, 101 ff.; Herb, ZUM 2004, 530, 531 f.

15 Vgl. EuGH, Urteil vom 09.03.2010 – C-518/07 (Kommission/Deutschland), Rn. 43, 44.

16 EuGH, Urteil vom 08.04.2014, C-288/12 (Kommission/Ungarn), Rn. 60.

17 Will, DuD 2020, 369, 371.

18 Gutachten der Datenethikkommission, <https://datenethikkommission.de/gutachten/>, S. 18, 28, 103, 101; vgl. auch Schulzki-Haddouti, Landesdatenschützer sollen Kontrolle über Firmen verlieren, 03.06.2020, <https://glm.io/148872>; zu diesbezüglichen verfassungsrechtlichen Fragen ausführlich Will (o. Fn. 17), 372.

19 <https://k1p.de/y4cb>.

20 Vgl. Art. 52 Abs. 3 DS-GVO und dazu Ziebarth, in: Sydow, DS-GVO, 2. Aufl. 2018, Art. 52 Rn. 34.

fende) Behörde ersetzt werden. Es könnten die beiden bayerischen Behörden fusionieren oder in anderen Ländern (oder im Bund) die Zuständigkeit gesplittet werden.

Zu den Organisationsänderungen sind auch erzwungene Umzüge der Behörde zu zählen.²¹ Sie etwa von der Hauptstadt in die Provinz zu verlegen oder auch innerhalb derselben Stadt (womöglich wiederholt) umziehen zu lassen, bindet Kräfte, hält sie von ihrer Aufgabenerfüllung ab und kann auch als Repressalie für unliebsame Entscheidungen der Behörde verstanden werden.²²

Eine Verkürzung der Amtszeit, Verringerung der Besoldung, Verschlechterung der Wiederwahlmöglichkeiten usw. sind ebenfalls als mögliche Organisationsänderungen zu nennen, ebenso wie Verschärfungen hinsichtlich Qualifikationsanforderungen, Höchst- oder Mindestalter oder bei Inkompatibilitäten.

III. Die völlige Unabhängigkeit der Datenschutz-Aufsichtsbehörden

Schon Art. 28 DS-RL sah vor, dass die „Datenschutz-Kontrollstellen“ völlig unabhängig zu sein hatten. In Art. 16 Abs. 2 AEUV wurde dies primärrechtlich übernommen, wobei trotz des Fehlens des Wortes „völlig“ im AEUV das Maß an Unabhängigkeit nicht etwa gesunken ist.²³

Auch Art. 51 Abs. 1 und insbesondere Art. 52 DS-GVO betonen die Unabhängigkeit, indem sie strikte Vorgaben machen zum Verbot direkter wie indirekter Beeinflussung und der Weisungsfreiheit der „Mitglieder“, also obersten Leiter der Behörden. Art. 53 Abs. 4 DS-GVO schränkt die Möglichkeit, ein „Mitglied“ vorzeitig abuberufen, ein. Denn eine Aufsichtsbehörde, deren Leiter jederzeit entlassen werden könnte, wäre weit von Unabhängigkeit entfernt.²⁴

Ähnliches hat aufgrund der JI-RL in deren Anwendungsbereich in den Mitgliedstaaten zu gelten und gilt übrigens auch für den EDSB aufgrund der VO (EU) 2018/1725.

Die völlige Unabhängigkeit wurde durch Rechtsprechung des EuGH näher konkretisiert; diese Konkretisierung hat die neuen primär- und sekundärrechtlichen Regelungen (z.B. Art. 52 DS-GVO) geprägt, die daher ebenfalls im Sinne „völliger“ Unabhängigkeit zu lesen sind.²⁵

Gerade die gegen Deutschland²⁶ und Österreich²⁷ ergangenen Urteile des EuGH betonen die völlige Unabhängigkeit der Datenschutzaufsicht.²⁸

Danach haben die Datenschutz-Aufsichtsbehörden selbstverständlich unabhängig von den zu beaufsichtigenden Institutionen zu sein,²⁹ aber auch unabhängig von Weisungen oder direkten oder indirekten Beeinflussungen von außen, wozu auch die Politik, einschließlich Regierung,³⁰ Gesetzgeber und politischen Parteien, gehört.³¹ Sie müssen „bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein“.³²

IV. Bedrohung der Unabhängigkeit der Aufsichtsbehörden durch Strukturänderungen

Strukturänderungen, die gegen den Willen einer Aufsichtsbehörde erfolgen sollen, greifen offensichtlich in deren Unabhängigkeit ein.

Nach der Rechtsprechung des EuGH ist etwa die Auflösung einer Datenschutz-Aufsichtsbehörde ein Einbruch in deren Unabhängigkeit.³³ Nichts anderes würde es bedeuten, etwa die Aufsicht über den nichtöffentlichen Bereich von den Aufsichtsbehörden der Länder auf den BfDI zu übertragen: Das Bayerische Landesamt für Datenschutzaufsicht wäre dann ohne Tätigkeitsbereich, den übrigen Aufsichtsbehörden der übrigen Länder ginge ein wichtiger Teil ihrer Tätigkeitsbereiche verloren.

Die „Wegnahme“ von Zuständigkeiten, Aufgaben oder Befugnissen geht zwar nicht so weit wie die Auflösung einer Behörde, aber in dieselbe Richtung. Es würde sich um Maßnahmen handeln, die eine indirekte Beeinflussung der Behörde durch die Politik darstellen.

Zu berücksichtigen ist, dass nicht erst eine einzelne, konkrete Änderung in die Unabhängigkeit eingreift, sondern bereits die Möglichkeit der Änderung als Damoklesschwert einer Repressalie über der Aufsichtsbehörde schwebt. Wer weiß, dass ihm eine Zuständigkeit jederzeit entzogen, er jederzeit mit ungewollten Zuständigkeiten überladen, seine Behörde in die Provinz verlegt oder gar aufgelöst werden kann, wird möglicherweise Konflikte scheuen, die auszuhalten im Interesse des effektiven Grundrechtsschutzes³⁴ zu seinen Amtspflichten gehören. Jedenfalls entsteht ein entsprechender böser Schein.

Der EuGH hat in gefestigter Rspr. entschieden, „dass Art. 28 Abs. 1 Unterabs. 2 der RL 95/46 dahin auszulegen ist, dass die für die Überwachung der Verarbeitung personenbezogener Daten zuständigen Kontrollstellen mit einer Unab-

21 Vgl. zum sächsischen Rechnungshof und dessen Umzug nach Döbeln VerfGH Sachsen, Urteil vom 25.02.2014 – Vf. 71-I-12, NJOZ 2014, 705; kritisch dazu Ziebarth (o. Fn. 19), Art. 54 Rn. 12.

22 Ziebarth (o. Fn. 19), Art. 54 Rn. 12.

23 Selmayr, in: Selmayr/Ehmann, DS-GVO, 2. Aufl. 2018, Art. 52 Rn. 13.

24 Ziebarth (o. Fn. 10), 64

25 Kühling/Martini et al., Die DS-GVO und das nationale Recht, 2016, S. 160 ff.

26 EuGH (o. Fn. 15).

27 EuGH, Urteil vom 16.12.2012, C-614/10 (Kommission/Österreich); dazu Bresich/Riedl/Sourhada-Kirchmayer (o. Fn. 7), 55 ff.

28 Vgl. im Detail Thomé, Reform der Datenschutzaufsicht – Effektiver Datenschutz durch verselbstständigte Aufsichtsbehörden, 2015, S. 66 ff.

29 Kühling/Martini et al (o. Fn. 24), S. 20 f.

30 EuGH (o. Fn. 26), Rn. 45 ff, 56 ff., 62 ff.; Schwartmann/Theodorou, RDV 2014, 61, 64 ff.

31 Wilhelm (o. Fn. 9), § 40 Rn. 12; Roßnagel (o. Fn. 1), 107 ff; Ziebarth (o. Fn. 10), 64; vgl. auch Giesen, RDV 1998, 15, 16; Wippermann, DÖV 1994, 929.

32 EuGH (o. Fn. 15), Rn. 25; ähnlich Groß, DuD 2002, 684, 685; vgl. auch Hellermann/Wieland, DuD 2000, 284, 285.

33 EuGH (o. Fn. 16).

34 Vgl. schon BVerfG, Urteil vom 15.12.1983, 1 BvR 209 u.a. = BVerfGE 65, 1, 46; EuGH (o. Fn. 16), Rn. 48.

hängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt u.a. jede Anordnung und jede sonstige wie auch immer geartete äußere Einflussnahme aus, sei sie unmittelbar oder mittelbar, an denen ihre Entscheidungen ausgerichtet werden könnten und durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe erfüllen, zwischen dem Schutz des Rechts auf Privatsphäre und dem freien Verkehr personenbezogener Daten ein ausgewogenes Verhältnis herzustellen (vgl. in diesem Sinne Urteile Kommission/Deutschland, Rn. 30, und Kommission/Österreich, Rn. 41 und 43).³⁵

Der EuGH führt im Urteil Kommission/Ungarn weiter aus, „dass schon die bloße Gefahr einer politischen Einflussnahme auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte daraus nämlich ein "voraussehlender Gehorsam" dieser Stellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstelle folgen. Zum anderen erfordert Art. 28 Abs. 1 UnterAbs. 2 der RL 95/46 angesichts der Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben sind (Urteile Kommission/Deutschland, Rn. 36, und Kommission/Österreich, Rn. 52).

Dürfte aber ein Mitgliedstaat das Mandat einer Kontrollstelle vor seinem ursprünglich vorgesehenen Ablauf beenden, ohne die von den anwendbaren Rechtsvorschriften zu diesem Zweck im Voraus festgelegten Grundsätze und Garantien zu beachten, könnte die Drohung einer solchen vorzeitigen Beendigung, die dann während der gesamten Ausübung des Mandats über dieser Stelle schwebte, zu einer Form des Gehorsams dieser Stelle ggü. den politisch Verantwortlichen führen, die mit dem Unabhängigkeitsgebot nicht vereinbar wäre (vgl. in diesem Sinne Urteil Kommission/Österreich, Rn. 51). Dies gilt auch dann, wenn das vorzeitige Ende des Mandats auf einer Umstrukturierung oder einer Änderung des Modells beruht; diese sind in einer Weise zu gestalten, dass sie die Anforderungen der geltenden Rechtsvorschriften an die Unabhängigkeit erfüllen.

Zudem könnte in einer solchen Situation nicht davon ausgegangen werden, dass die Kontrollstelle bei ihrer Tätigkeit in jedem Fall über jeden Verdacht der Parteilichkeit erhaben ist. Das Unabhängigkeitsgebot in Art. 28 Abs. 1 UnterAbs. 2 der RL 95/46 ist daher notwendigerweise dahin auszulegen, dass es die Verpflichtung umfasst, die Dauer des Mandats der Kontrollstellen bis zu seinem Ablauf zu beachten und sie nur unter Einhaltung der Grundsätze und Garantien der anwendbaren Rechtsvorschriften vorzeitig zu beenden.³⁶

Die vorzeitige Abberufung des Mitglieds oder die vorzeitige Auflösung seiner Behörde dürften abseits persönlicher Verfolgung die schwerwiegendsten Beeinträchtigungen der Unabhängigkeit darstellen. Die nachteilige Änderung der Tätigkeit (Zuständigkeit, Aufgaben, Befugnisse) oder der Organisation der Behörde beeinträchtigt die Unabhängigkeit zwar graduell weniger, strukturell aber eben auch.

Denn es handelt sich auch bei solchen Änderungen um „sonstige wie auch immer geartete äußere Einflussnahme [...], sei sie unmittelbar oder mittelbar, an denen ihre Entscheidungen ausgerichtet werden könnten und durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe erfüllen“.³⁷ Sie sind daher grundsätzlich unzulässig.

V. Lösungsansatz

1. Grundsatz

Will man die völlige Unabhängigkeit der Datenschutz-Aufsichtsbehörde ernstnehmen und dennoch die Rechte des Gesetzgebers nicht unnötig beschneiden, so muss zwischen den beiden Positionen „praktische Konkordanz“ hergestellt werden. Beide Positionen müssen möglichst ohne Verletzung der Gegenposition berücksichtigt werden.

Spätere Parlamente dürfen nicht auf ewig auf Entscheidungen früherer Parlamente festgelegt werden,³⁸ Strukturänderungen müssen also prinzipiell möglich sein. Gleichzeitig ist die Unabhängigkeit zu wahren, vor allem, indem Willkür und der Eindruck der „Bestrafung“ der Behörde vermieden werden.

Dazu sollten Strukturänderungen nur bei wirklich bestehender „Not-Wendigkeit“ im Wortsinn überhaupt angedacht werden. Kommission und Europäischer Datenschutzbeauftragter haben im Verfahren Kommission/Ungarn vertreten, Änderungen (dort: Verkürzungen der Amtszeit vor ihrem Ablauf) seien nur, aber immerhin, „aus schwerwiegenden und objektiv nachprüfbaren Gründen“ möglich.³⁹ Dem ist der EuGH indes nicht gefolgt, sondern er hat politisch gewillkürte vorzeitige Beendigungen der Amtszeit schlechthin für unzulässig erklärt.⁴⁰

Hält der Gesetzgeber Änderungen für nötig, ist das Einvernehmen mit der Aufsichtsbehörde zu suchen. Kann kein Einvernehmen hergestellt werden, sollte der Änderungswunsch noch einmal überdacht werden.

Wird er weiterhin für unumgänglich gehalten, so scheint ein die Unabhängigkeit respektierender Weg nur wie folgt gegeben zu sein: Es ist eine so lange Übergangsfrist bis zum Inkrafttreten der Änderung vorzusehen, dass bis dahin die Amtszeit des Mitglieds der Aufsichtsbehörde (also aller Mitglieder aller betroffener Aufsichtsbehörden ohne Einvernehmen) abgelaufen und entweder nach Wiederwahl die neue Amtszeit des bisherigen Mitglieds begonnen hat oder ein neues Mitglied im Amt ist.⁴¹

Denn in diesen beiden Fällen besteht kein böser Schein unzulässiger Einflussnahme.

35 EuGH (o. Fn. 16), Rn. 51.

36 EuGH (o. Fn. 16), Rn. 53-55.

37 Dazu EuGH (o. Fn. 16), Rn. 51.

38 Vgl. Ziebarth (o. Fn. 10), 64.

39 Dazu EuGH (o. Fn. 16), Rn. 38.

40 Dazu EuGH (o. Fn. 16), Rn. 53 ff.

41 So zu erzwungenen Umzügen auch schon Ziebarth (o. Fn. 19), Art. 54 Rn. 12 und Ziebarth, in: Sydow (Hrsg.), BDSG, 1. Aufl. 2020, § 8 Rn. 6.

Ein neues Mitglied wird kaum für Handlungen des Vorgängers „abgestraft“ werden. Auch ein wiedergewähltes Mitglied dürfte nicht „abgestraft“ worden sein: es hätte ja gar nicht wiedergewählt werden müssen.

Nach cursorischer Prüfung zeigt sich, dass Änderungen, die alle Aufsichtsbehörden in Bund und Ländern betreffen, bei fehlendem Einvernehmen eine lange Vorlaufzeit benötigen. So endet die im Sommer begonnene Amtszeit in Schleswig-Holstein 2026.⁴² Allerdings können Unschärfen nicht ausgeschlossen werden. Vorzeitige Beendigungen von Amtszeiten (wie in Hessen wegen der früheren Koppelung an die Legislaturperiode), unterjährige Beginn- und Enddaten, Weiterbeschäftigung bis zur Ernennung eines Nachfolgers sowie Übergangsvorschriften anlässlich des Wirksamwerdens der DS-GVO machen es nicht immer leicht, das korrekte Datum des Endes einer Amtszeit zu prognostizieren.

In Sachsen-Anhalt etwa scheint die Amtsdauer im März 2017 abgelaufen, ein Nachfolger nicht gewählt und der Amtsinhaber bis heute nur übergangsweise im Amt zu sein.⁴³ Auch diese Konstellation ist ob ihrer jederzeitigen Beendbarkeit keine, die völliger Unabhängigkeit gerecht wird – auch wenn das Funktionieren in der Praxis für eine für alle Beteiligten annehmbare Situation zu sprechen scheint und ein in einer „Bonusamtszeit“ befindlicher, keine Nachteile im persönlichen Fortkommen mehr befürchten müßender Amtsinhaber sicherlich besonders immun gegen unsachliche Beeinflussungsversuche ist.

2. Ausnahmen

Es ist denkbar, dass es zu der unter I. aufgestellten Regel Ausnahmen gibt.

a) Objektiv unabweisbare Notwendigkeit

Denkbar sind etwa objektiv unabweisbare Notwendigkeiten. Ist etwa das Amtsgebäude durch Bombendrohung oder wegen schwerer baulicher Mängel gefährdet, mag die Polizei die Evakuierung oder die Baubehörde eine Nutzungsuntersagung verfügen und die Aufsichtsbehörde so zu Arbeitsunterbrechungen oder zum Umzug „zwingen“. Auch infektionsschutzrechtliche Anordnungen können sich auf die Tätigkeit der Aufsichtsbehörde auswirken.

Hier ist freilich höchste Rücksichtnahme auf die völlige Unabhängigkeit geboten.

b) Bagatelländerungen

Eine Ausnahme können auch solche Strukturänderungen darstellen, die so geringfügig wirken, dass sie als Bagatelle keinen unzulässigen Einfluss auf die Tätigkeit haben und auch keinen derartigen bösen Schein erzeugen können. Sollten sie sich allerdings auffällig häufen, so wäre dem mit Misstrauen zu begegnen.

VI. Fazit

Die Gesetzgeber in Bund und Ländern, aber auch auf europäischer Ebene, behalten zwar das Recht, Strukturänderungen, also Tätigkeits- und Organisationsänderungen, hinsichtlich der Datenschutz-Aufsichtsbehörden vorzunehmen.

Diese stellen jedoch erhebliche Eingriffe in deren primär- und sekundärrechtlich angeordnete völlige Unabhängigkeit dar. Sie haben daher grundsätzlich im Einvernehmen mit der Aufsichtsbehörde zu erfolgen.

Wenn dieses nicht erreichbar ist, kann die Änderung frühestens nach Ablauf der Amtszeit des Mitglieds der Aufsichtsbehörde erfolgen, also entweder wenn nach Wiederwahl die neue Amtszeit des bisherigen Mitglieds begonnen hat oder wenn ein neues Mitglied im Amt ist. Sind mehrere Aufsichtsbehörden betroffen, so ist das Ende der Amtszeiten aller das Einvernehmen nicht herstellender „Mitglieder“ abzuwarten.



Dr. Wolfgang Ziebarth

ist Referent in Abt. 4 (Datenschutz im nichtöffentlichen Bereich) beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Er gibt in diesem nicht dienstlich veranlassten Beitrag ausschließlich seine persönliche Auffassung wieder.

⁴² § 1 Abs. 1 S. 1 Errichtungsgesetz ULD SH; VG Schleswig, Beschluss vom 19.08.2020, 12 B 36/20, Beck RS 2020, 21000.

⁴³ Vgl. das Vorwort zum 16. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Veroeffentlichungen/Taetigkeitsberichte/TB_16/16._Taetigkeitsbericht_Datenschutz.pdf).

Kurzbeiträge

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (50): Verarbeitungen zur Vertragserfüllung; Datenschutzbeauftragte im Gesundheitsbereich (u.a. im 25. Tätigkeitsbericht der LfDI Niedersachsen (2019) vom 03.09.2020)

Zusammengestellt und erläutert von Prof. Peter Gola*

I. Betroffene nutzen ihre Rechte

Der Jahresbericht der LfDI Niedersachsen statuiert immer wieder eingehende Beschwerden über die Nichtbeachtung des Auskunftsrechts nach Art. 15 DS-GVO als im nicht-öffentlichen Bereich mit 1882 Fällen häufigsten Beschwerdegrund. Laut den Beschwerdeführern werden Auskunftsbegehren von den Verantwortlichen oft nicht oder nicht vollständig beantwortet (25. TB, S. 88 ff). Probleme bereite auch das Recht auf Erhalt von Kopien und auf Löschung.

1. Der Anspruch auf Auskunft

Die LfDI zeigt zunächst die wesentlichen bei einer Auskunft mitzuteilenden Informationen auf und räumt ein, dass angesichts des Umfangs der zu erteilenden Auskunft die Beantwortung eines Auskunftsersuchens fehleranfällig sei. Schon die Anzahl von Beschwerden auf diesem Gebiet zeige, dass vielen Bürgern der Schutz ihrer persönlichen Daten wichtig sei. Bedauerlicherweise sei jedoch noch nicht allen Verantwortlichen das Recht auf Auskunft bzw. dessen Umfang bekannt, weshalb hier weiterhin Aufklärungsbedarf bestehe.

Nach Art. 15 Abs. 1 DS-GVO könne jede Person vom Verantwortlichen zunächst eine Bestätigung verlangen, dass dieser personenbezogene Daten verarbeitet, die sie betreffen. Trifft das zu, hat der Betroffene Anspruch auf Auskunft über dies in § 15 Abs. 1 DS-GVO genannten Verarbeitungszwecke und seine insoweit bestehenden Datenschutzrechte. Im Einzelnen ergab sich hinsichtlich der Befolgung des Art. 15 Abs. 1 DS-GVO sodann folgendes Bild: Viele Beschwerden waren deshalb begründet, da tatsächlich keine Auskunft erteilt wurde. Unvollständige Auskünfte wurden dagegen nur in wenigen Fällen gegeben. Übersehen wurde, dass die Auskunft nicht auf Stammdaten beschränkt ist, sondern sich etwa auch auf Telefonvermerke oder Gesprächsnotizen, die zu dem Betroffenen angelegt wurden, erstrecken. Für die Erteilung der Auskunft gelten das Genauigkeits- und das Verständlichkeitsgebot aus Art. 12 Abs. 1 Satz 1 DS-GVO, was eine gewisse Aufbereitung oder Erläuterung erforderlich machen kann.

Es gab allerdings auch einige unbegründete Beschwerden, u.a. weil der Verantwortliche die Auskunft hinreichend erteilt hatte oder die Antwortfrist von einem bzw. von bis zu drei Monaten nach Art. 12 Abs. 3 DS-GVO noch nicht verstrichen war. Mit Blick auf die Auskunftsfrist hatten Beschwerdeführer mitunter unrealistische Vorstellungen. Sie waren der Auffassung, der Verantwortliche habe binnen einer selbstgesetzten Frist von beispielsweise drei Tagen die gewünschte Auskunft zu erteilen.

2. Das Recht auf Kopie

Geltend gemacht wurde zudem das Recht auf Kopie gemäß Art. 15 Abs. 3 DS-GVO, wobei jedoch zu der Frage, in welcher Form eine Kopie zur Verfügung zu stellen ist, noch keine einheitliche Auslegung besteht. Die LfDI weist drauf hin, dass nach einer von ihr nicht geteilten Auffassung der Anspruch auf Kopie auch durch Überlassung einer strukturierten Zusammenfassung der verarbeiteten Daten erfüllt werden könne. Dies sei nicht überzeugend, da nach allgemeinem Verständnis mit einer Kopie eine originalgetreue Reproduktion gemeint sei. Es werde also die Herausgabe der Informationen in der Form gefordert, in der sie dem Verantwortlichen vorliegen.

In der Praxis sei dennoch grundsätzlich ein gestuftes Verfahren denkbar: Das heißt, der Verantwortliche könnte zunächst Auskünfte in Form aufbereiteter Daten erteilen. Bei einer großen Datenmenge könne der Verantwortliche zudem eine Präzisierung der erbetenen Auskunft verlangen (Erwägungsgrund 63). Fordert der Betroffene jedoch ausdrücklich eine Kopie seiner gesamten personenbezogenen Daten, muss der Verantwortliche dieser Forderung grundsätzlich nachkommen. Eine Begrenzung des Anspruchs erfolge allerdings durch Rechte anderer Personen sowie aufgrund etwaiger Geheimhaltungspflichten. Daher sei eine Abstimmung mit dem Betroffenen darüber sinnvoll, wie und in welchem Umfang die Auskunft und die Erstellung der Kopie erfolgen sollen.

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

3. Das Recht auf Löschung

Jede betroffene Person hat gemäß Art. 17 Abs. 1 DS-GVO einen Anspruch auf Löschung ihrer personenbezogenen Daten, wenn die Daten nicht mehr notwendig sind (Zweckentfall), bei Widerruf der zugrundeliegenden Einwilligung, bei Fehlen einer Rechtsgrundlage für die Verarbeitung oder bei Bestehen einer gesetzlichen Löschpflicht.

Sodann zeigt die LfDI die Pflicht zur Löschung und die insoweit nach Art. 17 Abs. 3 DS-GVO bzw. § 35 BDSG bestehenden Ausnahmen auf, wobei sie die bisweilen vertretene Auffassung, dass die Verschlüsselung von Daten mit deren Löschung gleichzusetzen sei, zutreffend nicht teilt. Durch eine Verschlüsselung wird nur die Vertraulichkeit der Daten geschützt. Dies ändert aber nichts an der Bewertung als personenbezogene Daten, zumal der Verantwortliche und ggf. auch Dritte eine Entschlüsselung vornehmen können. Weitgehend kamen die Verantwortlichen den Löschungsbegehren nach, konnten dieses aber oft nicht sofort erfüllen, sondern brauchten zeitlichen Vorlauf.

4. Die Informationspflichten

Jeder Verantwortliche unterliegt der Informationspflicht; entweder nach Art. 13 DS-GVO, wenn die Daten bei der betroffenen Person erhoben werden oder gemäß Art. 14 DS-GVO, wenn die Daten anderweitig erhoben werden. Die LfDI weist dabei darauf hin, dass anders als in digitalen Umgebungen das Erfordernis der Information zum Erhebungszeitpunkt in bestimmten, nicht-digitalen (Alltags-)Situationen zu Fragen der praktischen Anwendung führen kann. Im Regelfall reicht es hier daher nach Auffassung der LfDI aus, wenn beim ersten Kontakt Basisinformationen zu den Betroffenenrechten gegeben werden. Zu den weiteren Informationen kann der Verantwortliche auf seine Webseite verweisen oder ein entsprechendes Informationsblatt anbieten. Meist wurde bei Beschwerden in diesem Bereich eine unzureichende Information gerügt, nur in wenigen Fällen unterblieb die Information ganz. Insgesamt waren Beschwerden zur Informationspflicht im Laufe des Jahres 2019 stark rückläufig. Das zeigt, dass die Verantwortlichen sich offenbar ihrer Pflicht zunehmend bewusst sind.

II. Datenverarbeitung zur Vertragserfüllung

Der Europäische Datenschutzausschuss (EDSA) hat in den Leitlinien 2/2019 „on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects“ (Version 2.0) eine umfassende Bewertung der Datenverarbeitung im Zusammenhang mit Online-Dienstleistungen vorgenommen. Die LfDI Niedersachsen (25. TB, S. 24 ff) nimmt dies zum Anlass, diesbezüglich Zulässigkeit der Datenverarbeitung zusammengefasst darzustellen:

„Was Gegenstand eines Vertrags ist, obliegt grundsätzlich der Entscheidung der Vertragsparteien. Dies bedeutet jedoch nicht, dass Datenverarbeitungen allein deshalb gemäß

Art. 6 Abs. 1 lit b DS-GVO erlaubt sind, weil sie im Vertragstext genannt werden. Art. 6 Abs. 1 lit b DS-GVO erlaubt Datenverarbeitungen, die der Erfüllung oder dem Abschluss eines Vertrags dienen. Doch welche Verarbeitungen personenbezogener Daten können auf diese Norm gestützt werden? Voraussetzungen: Wirksamer Vertrag und Erforderlichkeit. Wer eine Ware bei einem Versandhändler bestellt, gibt seine Anschrift zum Versand und seine Zahlungsdaten preis, um den offenen Betrag zu begleichen. Der Händler kann sich bei der Nutzung dieser Daten zur Abwicklung des Kaufs auf die Rechtsgrundlage des Art. 6 Abs. 1 lit b DS-GVO berufen.

Damit Unternehmen und Behörden Datenverarbeitungen zur Vertragserfüllung auf Art. 6 Abs. 1 lit b DS-GVO stützen können, müssen zwei Voraussetzungen erfüllt sein. Der Vertrag muss nach nationalem Recht wirksam zustande gekommen und die Datenverarbeitung muss objektiv zur Vertragserfüllung erforderlich sein. Es ist also nicht ausreichend, wenn die Datenverarbeitung zur Vertragserfüllung lediglich nützlich ist. Darüber hinaus reicht es nicht aus, dass die Datenverarbeitung von den Allgemeinen Geschäftsbedingungen (AGB) eines Website-Betreibers gedeckt ist. Die Datenverarbeitung muss mit der vertragstypischen Leistung so eng verknüpft sein, dass die Leistung ohne sie nicht erbracht werden kann.

Die Beurteilung dessen, was vertragstypisch ist, hängt von den wesentlichen Merkmalen des jeweiligen Vertrags und den Erwartungen der Vertragsparteien ab. Bei Verträgen, die verschiedene unterschiedliche Vertragstypen vereinen (sog. typengemischter Vertrag), muss jede vertragstypische Leistung isoliert betrachtet werden. Dient die Datenverarbeitung der Umsetzung eines nicht vertragstypischen Inhalts, müssen die Voraussetzungen einer anderen Rechtsgrundlage des Art. 6 Abs. 1 DS-GVO erfüllt sein.

Art. 6 Abs. 1 lit b DS-GVO legitimiert nicht nur die Datenverarbeitungen, die mit dem Austausch der vertraglichen Leistungen einhergehen. Die Rechtsgrundlage greift auch für Datenverarbeitungen, die im Fall unterbliebener oder verspäteter Leistungen (z.B. Mahnung wegen unterlassener Zahlung, Produktreklamationen), im Widerrufs-, Rücktritts- oder Kündigungsfall erfolgen. Auch die weitere Aufbewahrung von Daten für den Garantie- oder Gewährleistungsfall lässt sich noch auf diese Rechtsgrundlage stützen.

Art. 6 Abs. 1 lit b DS-GVO ist dagegen keine geeignete Rechtsgrundlage, wenn die Datenverarbeitung der Optimierung der Website, der Betrugsprävention oder personalisierten Werbeanzeigen dient. Werden die Daten allerdings zur Personalisierung von Inhalten verarbeitet, die nicht der Werbung dienen, kann die Rechtsgrundlage wiederum greifen. Dies ist der Fall, wenn die Personalisierung des Inhalts Wesensmerkmal der Dienstleistung ist. Denkbar ist dies z.B. bei Foto-Apps, die auf Grundlage eines hochgeladenen Fotos das Alter des Nutzers schätzen".

III. Zu wenig Zeit für Datenschutzbeauftragte

Unter Ziff.7.2 des 25. TB berichtet die LfDI über den Arbeits- und Zeitaufwand von Datenschutzbeauftragten in Krankenhäusern: „Die datenschutzrechtlichen Handlungsfelder in den Krankenhäusern sind vielfältig. Die betrieblichen DSB vor Ort müssen die Einhaltung des Datenschutzes gegenüber den Beschäftigten genauso kontrollieren wie den Schutz der Patientendaten. Dies setzt nicht nur umfangreiche Kenntnisse im Datenschutzrecht voraus, sondern auch ausreichende Zeitannteile bzw. eine ausreichende Anzahl an Beschäftigten, welche den DSB, nicht nur während des Urlaubs oder bei Abwesenheit, vertreten und unterstützen. Die verspätete Meldung einer Datenpanne, nur weil der DSB nicht erreichbar gewesen ist, wird von mir nicht toleriert. Zwar sehen die Datenschutzgesetze keine gesetzliche Pflicht zur Freistellung von DSB vor. Dennoch sollte jedem Verantwortlichen bewusst sein, dass in einem Krankenhaus mittlerer Größe mit mehreren Dutzend Beschäftigten und Tausenden von Patienten pro Jahr mindestens eine Vollzeitstelle für den Datenschutz eingeplant werden muss“.

IV. Bestellung von Datenschutzbeauftragten im Gesundheitsbereich

Zur Bestellpflicht von Datenschutzbeauftragten im Gesundheitsbereich allgemein fasst der HDSI wie folgt zusammen (<https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/bestellung-von-datenschutzbeauftragten-im-Gesundheitsbereich>). „Mit Wirksamwerden der DS-GVO am 25. Mai 2018 gelten für die Bestellpflicht von Datenschutzbeauftragten Art. 37 DS-GVO und § 38 BDSG-neu i.V.m. Art. 35 DS-GVO. Ergänzend zu den Bestellpflichten des Art. 37 Abs. 1 DS-GVO hat der deutsche Gesetzgeber für die Benennung betrieblicher Datenschutzbeauftragter nationale Sonderregelungen geschaffen und sich dafür entschieden, das bereits aus dem deutschen Recht bekannte Kriterium der quantitativen Bestellpflicht beizubehalten (vgl. § 38 BDSG). Mit Beschluss vom 27.06.2019 hat der Bundestag entschieden, dass ein Datenschutzbeauftragter zu benennen ist, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind“.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten im Gesundheitsbereich ergibt sich damit aus einem der folgenden Umstände:

1. Regelmäßig sind mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 Satz 1 BDSG). Hinsichtlich der 20-Personengrenze stellt § 38 BDSG nicht nur auf Mitarbeiter ab. Dies entspricht der bisherigen Praxis der Aufsichtsbehörden. Weil wir bisher bei der Beschäftigten-Grenze auch den Arzt, Apotheker usw. als Chef der Praxis mitgezählt haben, ist ein Datenschutzbeauftragter ab 19 Mitarbeitern zu bestellen. Mitzuzählen sind zudem Auszubildende und die sich in Mutterschutz und Elternzeit befindenden Mitarbeiter. Nicht mitgezählt wird hingegen das Reinigungspersonal.
2. Verantwortlicher ist eine öffentliche Stelle oder Behörde (Art. 37 Abs. 1 lit a DS-GVO).
3. Die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten, Daten zu religiösen oder weltanschaulichen Überzeugungen, Daten zum Sexualleben) (Art. 37 Abs. 1 lit c DS-GVO; Größere Einheiten, wie private Krankenhäuser, führen in jedem Fall eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten durch und sind daher sowohl zur Durchführung einer Datenschutz-Folgenabschätzung als auch zur Bestellung eines Datenschutzbeauftragten verpflichtet)
4. Es ist eine Datenschutz-Folgenabschätzung durchzuführen (§ 38 Abs. 1 Satz 2 BDSG). Grundsätzlich ist es von der DS-GVO nicht gewollt, dass jede Arztpraxis oder Apotheke einen Datenschutzbeauftragten bestellen oder eine Datenschutz-Folgenabschätzung durchführen muss, nur weil Gesundheitsdaten verarbeitet werden (siehe auch die vergleichbare Bewertung zur Datenschutz-Folgenabschätzung in ErwGr. 91 Satz 4 zu Art. 35 Abs. 3 lit b DS-GVO sowie Nr. 2.1.3 des WP 243 der Art. 29-Gruppe unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 bzw. http://ec.europa.eu/newsroom/document.cfm?doc_id=44100), so dass derzeit beim Hessischen Datenschutzbeauftragten davon ausgegangen wird, dass eine Datenschutzfolgenabschätzung in der Arztpraxis tatsächlich nur bei besonderen Verfahren in Betracht zu ziehen ist, die nicht im herkömmlichen Praxisalltag eingesetzt werden (z.B. besondere Analysen von Genmaterial, Einsatz neuer Technologien etc.). In Zweifelsfällen sollte hierzu mit der Aufsichtsbehörde Rücksprache genommen werden.

Sperrt Art. 79 Abs. 1 DS-GVO Unterlassungsklagen gegen Verantwortliche?

Zugleich Besprechung von VG Regensburg, Gerichtsbescheid v. 06.08.2020 – RN 9 K 19.1061

Steffen Sundermann*

Das Zusammenspiel zwischen gerichtlichen Rechtsbehelfen und der DS-GVO beschäftigt, zunehmend die Praxis. Ob und unter welchen Voraussetzungen Verbraucherschutzvereinen eine Klagebefugnis aus Art. 80 DS-GVO zusteht¹ und welche Rechte gegenüber den Aufsichtsbehörden nach den Art. 77 und 78 DS-GVO durchgesetzt werden können,² wird bereits intensiv diskutiert. Art. 79 DS-GVO, der gerichtliche Rechtsbehelfe gegen Verantwortliche zum Gegenstand hat, stand bislang hingegen nicht im Fokus des Interesses. Das dürfte sich mit der Entscheidung des VG Regensburg vom 06.08.2020 ändern. Dieses hat entschieden, dass Art. 79 Abs. 1 DS-GVO bestimmte gerichtliche Rechtsbehelfe gegen Verantwortliche und Auftragsverarbeiter sperre und daher eine allgemeine Leistungsklage in Form der Unterlassungsklage nach §§ 1004 Abs. 1, 823 Abs. 2 BGB im Anwendungsbereich der DS-GVO nicht statthaft sei.

I. Sachverhalt der Entscheidung des VG Regensburg vom 06.08.2020

Der Kläger begehrt die Verurteilung der Beklagten, einer Kleinstadt in Niederbayern („Stadt P.“), dazu, den Betrieb eine Videoüberwachungsanlage und die Aufzeichnung der dadurch entstehenden Bilder zu unterlassen. Die Anlage überwacht mittels mehrerer Kameras einen Platz („K.-Garten“) im Zentrum der Stadt P., an welchen der zentrale Omnibusbahnhof, ein Einkaufszentrum und die Universität angrenzen. Auf dem Platz finden Wochenmärkte und Veranstaltungen statt. Die Polizei der Stadt P. hat den Platz als „Brennpunkt“ ausgemacht, da es dort zu Straftaten, insbesondere zu Drogendelikten komme, weshalb die Videoüberwachung notwendig sei. Der Platz ist kleiner als ein Fußballfeld und wird von den Kameras nahezu vollständig erfasst. Der Kläger durchquert den Platz regelmäßig und wird wiederholt von den Kameras erfasst. Der Kläger sieht sich hierdurch in seinen Rechten verletzt, insbesondere da die polizeiliche Kriminalitätsstatistik keinen Anlass zu einer Videoüberwachung des K.-Gartens gebe.

II. Problemaufriss

Die DS-GVO räumt einer von einer Datenverarbeitung betroffenen Person sowohl ein Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DS-GVO) als auch das Recht, ihre Rechte gerichtlich durchzusetzen (Art. 78 und 79 DS-GVO) ein. Die Entscheidung des VG Regensburg vom 06.08.2020 beleuchtet einen bisher weniger beachteten Aspekt der DS-GVO: Die Befugnis betroffener Personen, gegen Verantwortliche oder Auftragsverarbeiter auf Unterlassung rechtswidriger Verar-

beitungen ihrer personenbezogenen Daten zu klagen und das damit zusammenhängende Verhältnis zwischen aufsichtsbehördlichem Verfahren und den gerichtlichen Rechtsbehelfen gegen den Verantwortlichen oder den Auftragsverarbeiter. Die Entscheidung des VG Regensburg trifft diesbezüglich drei Aussagen mit grundsätzlicher Bedeutung: Erstens, Art. 79 Abs. 1 DS-GVO begrenze die Klagebefugnis auf Verletzungen der Betroffenenrechte.³ Zweitens, Art. 79 Abs. 1 DS-GVO setze eine Rechtsverletzung voraus, die über die bloße rechtswidrige Verarbeitung personenbezogener Daten hinausgehe.⁴ Drittens, Art. 79 Abs. 1 DS-GVO sperre Klagen, die auf andere Rechtsverletzungen gestützt seien; Rechtsschutz sei nur über eine Beschwerde bei der Aufsichtsbehörde zu erlangen.⁵

Würde sich diese Auffassung durchsetzen, hätte dies erhebliche praktische Konsequenzen: Betroffene Personen könnten keine allgemeinen Leistungsklagen nach den §§ 1004 Abs. 1, 823 Abs. 2 BGB – weder zivilrechtlich noch öffentlich-rechtlich – erheben, soweit der Anwendungsbereich des Art. 79 DS-GVO eröffnet ist. Das VG Regensburg stellt sich damit gegen die bisherige Rechtsprechung zu Art. 79 DS-GVO.⁶ Wissenschaft und Praxis gingen bisher außerdem weitestgehend einheitlich davon aus, dass Art. 77 und 79 DS-GVO das Konzept der Datenschutz-Richtlinie fortführen und der betroffenen Person das uneingeschränkte Wahlrecht lassen, sich an die Aufsichtsbehörde zu wenden oder ihre Rechte auf dem Klageweg zu verfolgen,⁷ ohne dass eine Sperrwirkung zulasten einer

* Der Autor ist Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit und Doktorand an der Universität Kasel. Der Beitrag gibt ausschließlich die private Meinung des Autors wieder und wurde nicht in dienstlicher Eigenschaft erstellt.

1 Siehe dazu Spittka, GRUR-Prax2019, 272 ff.; EuGH, Urt. v. 29.7.2019 – C-40/17 und BGH, Beschl. v. 28.05.2020 – IZR 186/17.

2 Vgl. Will, ZD 2020, 219 f.; OVG Hamburg, Urt. v. 07.10.2019 – 5 Bf 279/17 -, juris Rn. 63 ff.

3 VG Regensburg, Gerichtsbescheid v. 06.08.2020 – RN 9 K 19.1061, Rn. 16-18.

4 VG Regensburg, Gerichtsbescheid v. 06.08.2020 – RN 9 K 19.1061, Rn. 18 und 24.

5 VG Regensburg, Gerichtsbescheid v. 06.08.2020 – RN 9 K 19.1061, Rn. 18, 20 und 21.

6 OLG Frankfurt, Beschl. v. 19.02.2020 – 6 W 19/20 – WRP 2020, 628 ff.; Herbrich, jurisPR-ITR 19/2020 Anm. 5 m.w.N.; LG Frankfurt, Beschl. v. 15.10.20 – 2-03 O 356/20.

7 Nemitz, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 79 DS-GVO Rn. 1.

8 Die Frage wird soweit ersichtlich einzig von Kreße, in: Sydow, Europäische Datenschutzgrundverordnung, Art. 79 DS-GVO Rn. 29 aufgegriffen. Dieser vertritt dabei die Ansicht, die sich das Gericht, einschließlich der Argumentation, weitestgehend zu eigen macht; Herbrich, jurisPR-ITR 19/2020 Anm. 5 weist zutreffend darauf hin, dass das Gericht die Kommentarstelle, die nur von „vorbeugende Unterlassungsklagen“ spricht, sehr weit auslegt.

Variante vorliegt.⁸ Ist sie in eigenen Rechten betroffen, kann die betroffene Person ihre Rechte also selbst durchsetzen oder sich an die zuständige Aufsichtsbehörde wenden, die dann nach objektiven Maßstäben prüft. Unter bestimmten Voraussetzungen kann sie auch gerichtlich gegen die Aufsichtsbehörde vorgehen und hat einen Anspruch darauf, dass diese tätig wird. Die Entscheidung des VG Regensburg stellt auch dieses Verständnis nun in Frage, indem sie bei Ansprüchen, die auf die Unterlassung von Verarbeitungen gerichtet sind, gerichtlichen Rechtsschutz direkt gegen den Verantwortlichen oder Auftragsverarbeiter ausschließt und somit den Weg über die Aufsichtsbehörden forciert.

Die Argumentation des Gerichts fußt dabei zu großen Teilen auf einer eng am Wortlaut des Art. 79 Abs. 1 DS-GVO orientierten Auslegung. Dabei fokussiert sich das Gericht darauf, dass nach dem Wortlaut des Art. 79 Abs. 1 DS-GVO eine Verletzung der betroffenen Personen in ihren „*aufgrund dieser Verordnung zustehenden Rechte[n]*“ vorliegen muss. Das Gericht leitet daraus ab, dass nur Verletzungen von Rechten, die betroffenen Personen durch die DS-GVO ausdrücklich eingeräumt werden, gerichtlich gerügt werden könnten. Andere Ansprüche, die sich auf Normen stützen, die nicht ausdrücklich als Betroffenenrechte formuliert sind, würden durch Art. 79 Abs. 1 DS-GVO gesperrt; also auch Klagen, die auf Unterlassung einer rechtswidrigen Verarbeitung gerichtet seien, da es kein entsprechendes Betroffenenrecht gebe. Solche Rechtsverletzungen könnten nur über eine Beschwerde bei der Aufsichtsbehörde gem. Art. 77 Abs. 1 DS-GVO unterbunden werden.

Damit diese Argumentation durchgreift, müssen zwei Voraussetzungen erfüllt sein: Zum einen muss Art. 79 Abs. 1 DS-GVO so zu verstehen sein, dass nur ausdrücklich als Betroffenenrechte formulierte Normen der DS-GVO subjektive Rechte vermitteln (dazu unter III.) und zum anderen, dass Art. 79 Abs. 1 DS-GVO abschließend ist, also weitergehenden Rechtsbehelfen entgegensteht (dazu unter IV.). Keine der Voraussetzungen kann bei genauerer Betrachtung als gegeben angesehen werden. Wortlaut, Gesetzessystematik und die Intention des Ordnungsgebers sprechen – entgegen der Annahme des Gerichts – gegen ein solches Verständnis des Art. 79 Abs. 1 DS-GVO. Die Entscheidung vermag daher in ihren Ausführungen zu Art. 79 Abs. 1 DS-GVO im Ergebnis nicht zu überzeugen.

III. Verletzung subjektiver Rechtspositionen der DS-GVO

Die Betrachtungsweise, die das Gericht seiner Entscheidung zugrunde legt, weicht erheblich von derjenigen ab, die Verwaltungsgerichte in ständiger Praxis zugrunde legen, wenn es um die Frage geht, ob ein Kläger seine Klage auf eine bestimmte Norm stützen kann: Eine Untersuchung der konkreten Norm im Wege der Auslegung daraufhin, ob diese dem Kläger subjektive Rechte vermittelt.⁹ Nach der üblicherweise im Verwaltungsrecht herangezogenen Schutz-

normtheorie ist zu fragen, ob die entsprechende Norm zumindest auch den Schutz der Interessen des Klägers bezweckt oder ob es sich um einen reinen Rechtsreflex handelt.¹⁰ Nach dieser Sichtweise vermitteln nicht nur Normen subjektive Rechte, die ein Recht ausdrücklich als ein solches subjektives Recht benennen, sondern auch Normen, bei denen eine Auslegung ergibt, dass sie gerade auch dem Interessenschutz des Einzelnen dienen.¹¹

Für die Frage, ob eine rechtswidrige Datenverarbeitung Gegenstand einer Unterlassungsklage sein kann, ist also durch Auslegung zu ermitteln, ob die Art. 5 ff. DS-GVO, die die Rechtmäßigkeit der Verarbeitung maßgeblich regeln, zumindest auch dem Interessenschutz des Einzelnen dienen. Dass die Art. 5 ff. DS-GVO subjektive Rechte vermitteln, dürfte nicht ohne erheblichen Argumentationsaufwand in Frage zu stellen sein.¹² Immerhin benennt Art. 5 Abs. 1 lit a DS-GVO explizit die Interessen der betroffenen Person an einer rechtmäßigen, für sie transparenten, nach Treu und Glauben erfolgenden Verarbeitung als Schutzzweck der Art. 5 ff. DS-GVO. Die betroffene Person wird in den Art. 5 ff. DS-GVO, insbesondere in Art. 6 Abs. 1 DS-GVO auch mehrfach explizit genannt, so knüpft Art. 6 Abs. 1 lit a DS-GVO an das Einverständnis der betroffenen Person an und Art. 6 Abs. 1 lit f DS-GVO an die berechtigten Interessen dieser. Die Charakteristika einer Norm, die nach der Lehre der Schutznorm subjektive Rechte vermittelt, liegen in Bezug auf die Art. 6 Abs. 1 DS-GVO somit vor.

Soweit Art. 79 Abs. 1 DS-GVO also von den Rechten der betroffenen Person spricht, die dieser „*aufgrund dieser Verordnung*“ zustehen, dürften nicht nur die Betroffenenrechte der Art. 12 ff DS-GVO erfasst sein, sondern auch alle weiteren Normen, die subjektive Rechte vermitteln, insbesondere die Art. 5 ff. DS-GVO.¹³ Damit unterfallen auch rechtswidrige Verarbeitungen personenbezogener Daten dem Wortlaut des Art. 79 Abs. 1 DS-GVO, selbst wenn diese nicht die Betroffenenrechte der Art. 12 ff. DS-GVO betreffen.

Art. 79 Abs. 1 DS-GVO setzt weiter voraus, dass eine subjektive Rechtsposition verletzt wurde, wobei das Gericht die Frage aufwirft, welche Voraussetzungen für eine Verletzung i.S.d. Art. 79 Abs. 1 DS-GVO vorliegen müssen. Das Gericht unterscheidet in diesem Zusammenhang zwischen der „*bloßen*“ Rechtswidrigkeit der Datenverarbeitung, worauf sich ein Widerspruchsrecht nach Art. 21 DS-GVO und ein Beschwerderecht nach Art. 77 DS-GVO stützen lässt und der zusätzlichen, nach Ansicht der betroffenen Person ge-

9 Schmidt-Kötters, in: BeckOK VwGO, 54. Edition 2019, § 42 VwGO Rn. 155.

10 Wahl, in: Schoch/Schneider/Bier, VwGO, vor § 42 Abs. 2 Rn. 95.

11 Wysk, VwGO, 3. Aufl. 2020, § 42 VwGO Rn. 114.

12 Herbrich, jurisPR-ITR 19/2020 Anm. 5; Mundil, in: BeckOK Datenschutzrecht, 32. Edition 2020, Art. 79 DS-GVO Rn. 7; Gola/Piltz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 26, die sogar so weit gehen, allen Normen der DS-GVO aufgrund des Art. 1 Abs. 1 DS-GVO Schutznormcharakter zuzusprechen; Vgl auch ErwGr. 2 Satz 1 DS-GVO.

13 Boehm, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 79 DS-GVO Rn. 10; Moos/Schefzig, in: Taeger/Gabel, DS-GVO – BDSG, 3. Aufl. 2019, Art. 79 DS-GVO Rn. 7 u. 9; Mundil, in: BeckOK Datenschutzrecht, 32. Edition 2020, Art. 79 DS-GVO Rn. 7.

14 VG Regensburg, Gerichtsbescheid v. 06.08.2020 – RN 9 K 19.1061 Rn. 24.

gebenen Rechtsverletzung.“¹⁴ Das Gericht verweist darauf, dass der Wortlaut des Art. 77 Abs. 1 und des Art. 79 Abs. 1 DS-GVO dafür spreche, dass der Verordnungsgeber bewusst zwischen einem Verstoß gegen die DS-GVO (Art. 77 Abs. 1 DS-GVO) und einer Verletzung der eigenen Rechte (Art. 79 Abs. 1 DS-GVO) unterschieden habe. Nach Ansicht des Gerichts verletzt daher eine bloße rechtswidrige Verarbeitung personenbezogener Daten alleine noch nicht die Rechte der betroffenen Person und erfordere eine zusätzliche, darüberhinausgehende subjektive Rechtsverletzung durch die rechtswidrige Verarbeitung.

Dieser Ansatz ist weder mit dem gesetzgeberischen Konzept, das der DS-GVO zugrunde liegt noch mit Art. 8 Abs. 2 GRCh zu vereinbaren, vor deren Hintergrund auch der Wortlaut der Art. 77 Abs. 1 und 79 Abs. 1 DS-GVO auszulegen ist. Nach Art. 1 Abs. 2 DS-GVO soll die Verordnung „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“ schützen. Die DS-GVO versteht sich also als einfachgesetzliche Umsetzung der Grundrechte, insbesondere des Art. 8 GRCh.¹⁵ Nach Art. 8 Abs. 2 GRCh dürfen personenbezogene Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.“ Es handelt sich um die grundrechtlichen Vorgaben, die wiederum durch die Art. 5 ff. DS-GVO konkretisiert werden. Art. 8 Abs. 2 GRCh ist dabei ausweislich seines Wortlauts schon verletzt, wenn eine Verarbeitung ohne Rechtsgrundlage vorliegt, spricht durch eine bloße rechtswidrige Verarbeitung. Art. 8 GRCh sieht dabei gerade keine „Bagatelgrenze“ vor.¹⁶ Daher betrachtet der EuGH beispielweise auch schon die Veröffentlichung von Namen von Empfängern von Agrarsubventionen im Internet als einen Eingriff in das Grundrecht auf Datenschutz und fordert nicht, dass weitere Rechtsverletzungen durch die Veröffentlichung entstanden sein müssen.¹⁷ Das VG Regensburg verwischt somit die bereits auf Grundrechtsebene bestehende Grenze zwischen Verletzung des Rechts auf Schutz personenbezogener Daten und einem dadurch entstandenen Schaden. Lediglich ersteres wird von Art. 79 Abs. 1 DS-GVO vorausgesetzt. Eines Schadens bedarf es vielmehr erst für die Geltendmachung von Schadenersatzansprüchen, weshalb deren Voraussetzungen auch separat von den Art. 77 und 79 DS-GVO in Art. 82 DS-GVO geregelt sind.¹⁸

Ein Kläger ist durch eine rechtswidrige Verarbeitung in eigenen Rechten verletzt, wenn seine eigenen personenbezogenen Daten betroffen sind, da dadurch (bei einem nicht-öffentlichen Verantwortlichen zumindest mittelbar) in den persönlichen Schutzbereich des Art. 8 Abs. 1 GRCh eingegriffen wird.¹⁹ Dieser Schutzbereich liegt ausweislich des Art. 1 Abs. 2 DS-GVO auch der DS-GVO zugrunde. Die Entscheidung über die Klagebefugnis hat – entgegen der Auffassung des Gerichts – anhand dieses Kriteriums zu erfolgen und bedarf keiner darüber hinausgehenden Verletzung der Rechte des Klägers.

IV. Sperrwirkung des Art. 79 Abs. 1 DS-GVO für Klagen gegen den Verantwortlichen

Auch die zweite Voraussetzung dafür, dass die Auslegung des Gerichts zu Art. 79 DS-GVO zutrifft, liegt nicht vor: Art. 79 Abs. 1 DS-GVO ist nicht abschließend und entfaltet keine Sperrwirkung. Aus der Norm ergibt sich nicht, dass der Verordnungsgeber die Intention hatte, das Recht der betroffenen Person auf weitere gerichtliche Rechtsbehelfe einzuschränken. Die Formulierung „jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf“ dürfte vielmehr von der Intention getragen gewesen sein, eine europaweit geltende Garantie für betroffene Personen zu schaffen, ihre Rechte gerichtlich durchsetzen können.²⁰ Art. 77 Abs. 1 und Art. 79 Abs. 1 DS-GVO garantieren der betroffenen Person auf diese Weise auch ein Wahlrecht zwischen einer Beschwerde bei bzw. einer Klage gegen die Aufsichtsbehörde und einer Klage gegen den Verantwortlichen.²¹ Dass der Verordnungsgeber darüber hinaus bezweckte, bei bestimmten Rechtsverstößen den Weg ausschließlich über die Aufsichtsbehörden zu forcieren, ist nicht ersichtlich und hätte einer ausdrücklicheren Regelung bedurft. Dies spiegelt sich auch systematisch wieder: Die Existenz des Art. 82 Abs. 6 DS-GVO, der einen über Art. 79 Abs. 1 DS-GVO hinausgehenden gerichtlichen Rechtsbehelf enthält, zeigt bereits, dass Art. 79 Abs. 1 DS-GVO die Frage, welche Rechtsbehelfe für betroffene Personen statthaft sind, gerade nicht abschließend regelt und diese nicht auf die Betroffenenrechte beschränkt. Nach Art. 82 Abs. 1 DS-GVO können betroffene Personen Schadenersatz „wegen eines Verstoßes gegen diese Verordnung“ verlangen. In Art. 82 Abs. 6 DS-GVO wird ausdrücklich normiert, dass Schadenersatzansprüche gerichtlich, ohne Umweg über die Aufsichtsbehörde durchgesetzt werden können und zwar bei den Gerichten, die „nach den in Art. 79 Abs. 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind“. Demnach können betroffene Personen also Schadenersatzansprüche, die auf rechtswidrige Verarbeitungen zurückgehen, direkt vor den Gerichten einklagen. Es erscheint wenig überzeugend anzunehmen, dass der Verordnungsgeber nur für Schadenersatzklagen den Weg zu den Gerichten ermöglichen wollte, nicht aber für allgemeine Leistungsklagen, die

15 Boehm, in: Simitis/Hornung/Spiecker, Datenschutzrecht, Art. 79 DS-GVO Rn. 10.

16 Augsberg, in: Groeben, von der/Schwarze, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 8 GRCh, Rn. 6.

17 EuGH, Urt. v. 09.11.2010 – C-92/09 und C-93/09, Slg. 2010, I-11 063 Rn. 29; Johlen, in: Stern/Sachs, GRCh, 1. Aufl. 2016, Art. 8 GRCh, Rn. 35.

18 LG Hamburg, Urt. v. 04.09.2020 – 324 S 9/19, Rn. 32.

19 Jarass, EU-Grundrechte-Charta, 3. Aufl. 2016, Art. 8 GRCh Rn. 5 und 6.

20 Herbrich, jurisPR-ITR 19/2020 Anm. 5 m.w.N.

21 In diesem Sinne auch Nemitz, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 79 DS-GVO Rn. 1; Werkmeister, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 79 DS-GVO Rn. 3.

auf Unterlassung gerade dieser rechtswidrigen Verarbeitungen gerichtet sind. Die Konsequenz, dass betroffene Personen rechtswidrige Verarbeitungen ihrer Daten nicht auf dem Klageweg unterbinden könnten, sondern nachfolgend nur Schadenersatz für diese fordern könnten (i.S.e. „dulde und liquidiere“), wäre wohl nur zu akzeptieren, wenn der Verordnungsgeber sich bewusst für diese entschieden hätte. Für eine solche Zielsetzung des Verordnungsgebers fehlt allerdings jeglicher Anhaltspunkt. Es erscheint demgegenüber überzeugender anzunehmen, dass der Verordnungsgeber Unklarheit darüber ausräumen wollte, ob die DS-GVO die Geltendmachung von Schadenersatzansprüchen einer betroffenen Person ermöglicht und dies daher ausdrücklich normierte, ebenso wie er mit den Art. 77 Abs. 1 und 79 Abs. 1 DS-GVO Zweifel darüber ausräumen wollte, dass betroffene Personen gegen Verletzungen ihrer Rechte gerichtlich und aufsichtsbehördlich vorgehen können.

Gegen die Annahme, Art. 79 Abs. 1 DS-GVO stehe der gerichtlichen Durchsetzung von Unterlassungsansprüchen gegen rechtswidrige Verarbeitung entgegen, spricht weiterhin, dass sich ansonsten Rechtsschutzlücken auftun, die der Verordnungsgeber nicht beabsichtigt haben kann. Blicke betroffenen Personen lediglich der Weg über die Aufsichtsbehörden, um rechtswidrige Datenverarbeitungen unterbinden zu lassen, so würde dies bedeuten, dass Betroffene nur einen Anspruch auf eine angemessene Untersuchung ihrer Beschwerde (Art. 57 Abs. 1 lit f DS-GVO) durch die Aufsichtsbehörde hätten. Was genau dies umfasst, ist umstritten, teilweise wird Art. 57 Abs. 1 lit f DS-GVO im Sinne von Ermessen ausgelegt,²² teilweise im Sinne eines reinen Petitionsrechts.²³ Nach allen Ansichten hat die betroffene Person aber jedenfalls kein Recht darauf, dass die Aufsichtsbehörde eine bestimmte Maßnahme gegenüber dem Verantwortlichen oder Auftragsverarbeiter ergreift.²⁴ Entsprechend hat auch noch kein Verwaltungsgericht eine Aufsichtsbehörde zum Ergreifen bestimmter Maßnahmen gegenüber dem Verantwortlichen verpflichtet, obwohl entsprechende Anträge die Verwaltungsgerichte bereits seit längerem beschäftigen.²⁵ Die betroffene Person kann also nicht darauf klagen, dass die Aufsichtsbehörde den Verantwortlichen dazu verpflichtet, eine bestimmte Verarbeitung zu unterlassen. Der betroffenen Person stünde daher, folgte man der Auffassung des Gerichts, kein wirksamer gerichtlicher Rechtsbehelf zur Verfügung, um einen Verantwortlichen zur Unterlassung einer rechtswidrigen Verarbeitung

ihrer Daten zu verpflichten. Dieses Ergebnis stünde im Widerspruch zum Wortlaut des Art. 79 Abs. 1 DS-GVO²⁶ sowie zur erklärten Zielsetzung der DS-GVO, die (Grund-)Rechte der Betroffenen zu stärken,²⁷ indem sie diesen die entsprechenden Rechtsbehelfe zur Durchsetzung ihrer Rechte an die Hand gibt.

V. Fazit

Die eingangs dargestellten Kernaussagen des VG Regensburg erweisen sich als unzutreffend: Art. 79 Abs. 1 DS-GVO begrenzt die Klagebefugnis nicht auf Verletzungen der Betroffenenrechte, da auch andere Normen der DS-GVO subjektive Rechte vermitteln. Eine Verletzung der eigenen Rechte i.S.d. Art. 79 Abs. 1 DS-GVO liegt bereits vor, wenn die eigenen personenbezogenen Daten entgegen der Art. 5 ff. DS-GVO verarbeitet werden, und setzt keine darüber hinausgehende Verletzung durch die rechtswidrige Verarbeitung voraus.²⁸ Eine „bloße“ rechtswidrige Verarbeitung der eigenen personenbezogenen Daten befugt somit zu einer Klage gegen den Verantwortlichen nach Art. 79 Abs. 1 DS-GVO. Art. 79 Abs. 1 DS-GVO kommt weiter keine Sperrwirkung gegenüber anderen Rechtsbehelfen zu, da er nicht abschließend ist. Die betroffene Person hat also bei einer rechtswidrigen Verarbeitung ihrer personenbezogenen Daten sowohl die Möglichkeit, sich nach Art. 77 Abs. 1 DS-GVO an die Aufsichtsbehörde zu wenden, als auch, direkt gerichtlich gegen den Verantwortlichen nach Art. 79 Abs. 1 DS-GVO, auch in Form einer allgemeinen Leistungsklage, vorzugehen.

22 So Nemitz, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 77 DS-GVO Rn. 17; VG Ansbach, Urt. v. 08.08.2019 – AN 14 K 19.00272 m krit. Anm. Will, ZD 2020, 219 f.; VG Ansbach, Urt. v. 16.03.2020 – AN 14 K 19.00464; in diese Richtung auch OVG Hamburg, Urt. v. 7.10.2019 – 5 Bf 279/17 –, juris Rn. 63 ff.

23 VG Berlin, Beschl. v. 28.01.2019 – 1 L 1.19 (n.v.); Körfner, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 77 DS-GVO Rn. 5; Koreng, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar DS-GVO, 2018, Art. 77 DS-GVO Rn. 20.

24 Ausnahmsweise kann eine solche Verpflichtung bei einer Ermessensreduktion auf Null möglich sein.

25 OVG Hamburg, Urt. v. 07.10.2019 – 5 Bf 279/17 –, juris Rn. 63 ff; VG Ansbach, Urt. v. 16.03.2020 – AN 14 K 19.00464.

26 „betroffene Person hat [...] das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte [...] verletzt wurden“.

27 Vgl. ErwGr. 2 Satz 1 DS-GVO.

28 Eine solche Verletzung mag man für das Vorliegen eines Schadens fordern, vgl. LG Hamburg, Urt. v. 04.09.2020 – 324 S 9/19, auf einen Schaden nimmt Art. 79 Abs. 1 DS-GVO jedoch nicht Bezug.

Praxisfälle zum Datenschutzrecht VII: Musterfalllösung zur Heimarbeit

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

I. Sachverhalt

Die Personalsachbearbeiterin P des Unternehmens U ist stark ausgelastet. Häufig nimmt sie daher Arbeit mit nach Hause und bearbeitet dort Personalvorgänge. Da U nicht für jeden Mitarbeiter firmeneigene Laptops zur Verfügung stellt, benutzt sie dafür ihren eigenen PC, mit dem sie auch Zugriff auf die Personaldateien von U hat. Regelungen zur Arbeit von Zuhause existieren bei U nicht. Die Vorgehensweise wurde P aber vom Personalleiter L ausdrücklich gestattet. Wie beurteilen Sie den Fall?

II. Musterfalllösung

1. Telearbeit/Homeoffice, Mobiles Arbeiten und BYOD

Bei der Arbeit abseits des Arbeitsplatzes im Unternehmen unterscheidet man zwischen verschiedenen Erscheinungsformen.

Bei der *Telearbeit* erbringen Beschäftigte ihre Arbeitsleistung wechselnd zwischen dem Arbeitsplatz im Büro und im häuslichen Umfeld, wobei die IT-Ausstattung (Laptop, PC etc.) mit dem Unternehmen bzw. der Dienststelle verbunden ist.¹ In den letzten Jahren ist der Begriff der Telearbeit mehr und mehr dem des *Homeoffice* gewichen. Beide Begriffe beschreiben jedoch die Einrichtung eines festen Arbeitsplatzes im häuslichen Umfeld der Beschäftigten.

Mobiles Arbeiten ist im Gegensatz zur Telearbeit ortsunabhängig möglich, da es den Fokus auf den Einsatz mobiler Endgeräte setzt, die einen Fernzugriff auf die IT-Systeme des Arbeitsgebers ermöglichen.² Diese Form der Arbeit ermöglicht maximale Flexibilität bei der Erbringung der täglichen Arbeitsleistung und erfreut sich wachsender Beliebtheit. Häufig werden Arbeitsplätze in den Unternehmen bzw. Dienststellen nicht mehr mit sperrigen PCs versehen, sondern mit Laptops und entsprechenden Dockingstations, die die Mitnahme des mobilen Geräts in Meetings, auf Dienstreisen, nach Hause etc. ermöglichen. Mittels *Mobile Device Management* (MDM) können Mobilgeräte wie Laptops, Tablets oder Smartphones dabei zentral durch die IT-Abteilung der ausgebenden Organisation verwaltet werden. So kann die IT-Abteilung z.B. die Verwendung sicherer Passwörter erzwingen, bestimmen, welche Apps eine Anwendergruppe installieren darf, oder bei Verlust oder Diebstahl ein Endgerät aus der Ferne sperren und gespeicherte Inhalte löschen. Fortschrittliche *Enterprise Mobility Management* (EMM)-Lösungen ermöglichen es, die zentrale Verwaltung auf einen abgeschotteten geschäftlichen Bereich (Containerisierung) oder Unternehmensanwendungen samt der damit verbunde-

nen Daten (Mobile Application Management – MAM) zu beschränken.³ Dies erlangt insbesondere dann Bedeutung, wenn die private Nutzung der mobilen Endgeräte des Arbeitgebers gestattet ist.

Die Arbeit abseits des Arbeitsplatzes kann über vom Arbeitgeber bereitgestellte stationäre oder mobile IT-Infrastruktur erfolgen. Teilweise erlauben Arbeitgeber aber auch die Verwendung privater Geräte des Mitarbeiters für dienstliche Zwecke bzw. präferieren aus Kostenersparnisgründen die Verwendung privater Geräte sogar. In diesen Fällen spricht man von *BYOD* (Bring Your Own Device). *BYOD*-Lösungen sind mit größeren rechtlichen und organisatorischen Hürden verbunden als die Arbeit mit vom Arbeitgeber bereitgestellter Infrastruktur. Insbesondere sind Regelungen bzw. Vorkehrungen bzgl. der Kontrolle und Löschung beruflicher Daten sowie der deutlichen Trennung von beruflichen und privaten Inhalten zu treffen.⁴ Der Einsatz von *BYOD* ist prinzipiell rechtskonform gestaltbar. Die praktischen Hürden sind aber nicht unerheblich,⁵ weshalb der Weg über unternehmens-/behördeneigene Geräte häufig vorzugswürdig ist.

Die verschiedenen Erscheinungsformen der Arbeit abseits des Arbeitsplatzes im Unternehmen bringen unterschiedliche datenschutzrechtliche Risiken mit sich, denen durch entsprechende technische und organisatorische Maßnahmen Rechnung getragen werden muss.

Im Normalfall kann Homeoffice ebenso wenig wie die Nutzung eigener privater IT-Infrastruktur für berufliche Zwecke einseitig vom Arbeitgeber angeordnet werden. Auch dass Arbeitnehmer z.B. zur besseren Vereinbarung von Familie und Beruf an Telearbeit/Homeoffice interessiert sein können, führt nicht zu einer diesbezüglichen Erweiterung des Weisungsrechts (§ 106 GewO) des Arbeitgebers.⁶ Arbeitgeber können ihre Arbeitnehmer grundsätzlich nur dann anweisen, im Homeoffice ihre Arbeit zu erledigen, wenn dies in einer individualvertraglichen Vereinbarung geregelt ist. Ob ein entsprechendes Weisungsrecht auch durch Kollektiv-

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

1 BfDI, „Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser“, Stand: Juli 2020, S. 5, abrufbar unter <https://t1p.de/38et> (zuletzt abgerufen am 24.10.2020).

2 BfDI, a.o.O., S. 6.

3 Vgl. Computerwoche.de, *BYOD, Security, App-Management: Die besten Lösungen fürs Mobile Device Management*, 21.09.2018, abrufbar unter <https://t1p.de/fhkd> (zuletzt abgerufen am 24.10.2020).

4 BfDI, a.o.O., S. 16 f.

5 Vgl. dazu auch nachstehend unter 2.c).

6 LAG Berlin-Brandenburg, U. v. 14.11.2018 – 17 Sa 562/18.

vereinbarung eingeführt werden kann,⁷ erscheint fraglich, da die Regelungsbefugnis des Betriebs-/Personalrats auf die betriebliche bzw. dienstliche Sphäre beschränkt ist. Durch Kollektivvereinbarung kann nicht über den privaten Bereich und das Eigentum der Mitarbeiter bestimmt werden. Durch Kollektivvereinbarung können also die Voraussetzungen und Rahmenbedingungen für die Tätigkeit im Homeoffice geregelt werden. Die Entscheidung über das „Ob“ verbleibt aber grundsätzlich beim Mitarbeiter.

Etwas anderes kann nur in Ausnahmefällen gelten, wie etwa durch die veränderte Gefährdungslage an den betrieblichen Arbeitsplätzen bedingt durch die Corona-Pandemie.⁸ So hatte eine 60-jährige Beamtin nach Beschluss des VG Berlin⁹ eine befristete Anordnung zur coronabedingten Homeofficetätigkeit gegen ihren Willen hinzunehmen, auch wenn ihr Heimarbeitsplatz (noch) nicht entsprechend ausgerüstet war und sie daher vorübergehend für drei Wochen faktisch keinen Dienst leisten konnte.

Vorliegend kann festgehalten werden, dass P ihre Arbeitsleistung auch mittels Telearbeit/Homeoffice erbringt und zwar über ihre private IT-Infrastruktur (BYOD). Diese Vorgehensweise wurde ihr auch ausdrücklich gestattet.

2. Zulässigkeit von Telearbeit/Homeoffice mit eigenen Endgeräten im konkreten Fall

a) Fragestellung

Es stellt sich die Frage, ob die Gestattung des Personalleiters L, dass P dienstliche Personalvorgänge zu Hause mittels ihrer privaten IT bearbeiten darf, mit dem Datenschutzrecht vereinbar ist.

b) Verbot mit Erlaubnisvorbehalt einschlägig?

Fraglich ist, ob die mit der Arbeit im Homeoffice verbundene Verlegung der Datenverarbeitung in die Wohnung der Mitarbeiterin unter das Grundprinzip des Verbots mit Erlaubnisvorbehalt (ErwG 40 DS-GVO) fällt und die Auslagerung der Tätigkeit damit einer speziellen datenschutzrechtlichen Rechtsgrundlage bedarf. Dies ist nicht der Fall, weil es sich bei der Auslagerung nicht um eine eigenständige Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO handelt. Die Mitarbeiterin nimmt weiterhin arbeitsvertragliche Tätigkeiten wahr und ist eine dem Verantwortlichen unterstellte Person gem. Art. 29 DS-GVO.

c) Technisch-organisatorischer Datenschutz

Als Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO hat Unternehmen U die Anforderungen an die Datensicherheit gem. Art. 32 DS-GVO zu erfüllen. Gem. Art. 32 Abs. 1 DS-GVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten.

Ob Telearbeit/Homeoffice datenschutzrechtlich zulässig ist, hängt von der Art der ausgelagerten Tätigkeit, der Einigung der häuslichen Arbeitsstätte sowie der Vertrauensbasis¹⁰ mit dem jeweiligen Beschäftigten ab.

Besondere Bedeutung kommt bei der Entscheidung über das Ob der Tätigkeit im Homeoffice zu, welche konkreten Arten personenbezogener Informationen verarbeitet werden sollen. Kann angesichts der besonderen Gefährdungen beim Homeoffice – z.B. Möglichkeit der Kenntnisnahme durch andere Familienmitglieder oder Gäste, erhöhte Verlustgefahr von Datenträgern/Geräten insbes. auf dem Transportweg, eingeschränkte Kontrollierbarkeit von Datenverarbeitungsvorgaben – und der Vertraulichkeit der konkret in Rede stehenden Daten kein angemessenes Schutzniveau geschaffen werden, darf die Arbeit im Homeoffice grundsätzlich nicht gestattet werden.¹¹ Eine kritische Prüfung ist insbes. geboten bei den besonders geschützten Daten nach Art. 9 f. DSGVO, wozu etwa Gesundheitsinformationen zählen, oder Informationen, die einem Berufs- oder Amtsgeheimnis unterliegen.

Auch Personaldaten unterliegen einem besonderen Schutz. Dies gilt nicht nur für Informationen, die Teil der formellen Personalakte sind. Geschützt sind grundsätzlich sämtliche Informationen über den/die Arbeitnehmer/in, die mit dem Arbeitsverhältnis in einem unmittelbaren inneren Zusammenhang stehen, also auch in elektronischen Datenbanken – z.B. Personalverwaltungssystemen – gespeicherte Daten (materiellrechtlicher Personalaktenbegriff).¹² Personalakten(daten) dürfen nicht allgemein zugänglich sein; sie müssen sorgfältig verwahrt und vor unbefugter Einsichtnahme durch Dritte geschützt werden. Der Kreis der mit derartigen Informationen befassten Beschäftigten muss eng gehalten werden.¹³

Ob bestimmte Datenarten, etwa Gesundheits- oder Beurteilungsdaten von Beschäftigten, dabei per se von einer Verarbeitung im Homeoffice auszuschließen sind, erscheint fraglich.¹⁴ Entscheidend sind stets die Umstände des Einzelfalls, also die konkrete Gefährdungslage und die konkret ergriffenen Maßnahmen zum Schutz der Informationen.¹⁵ Zu berücksichtigen ist, dass regelmäßig auch bei einer Tätigkeit vor Ort im Firmen- bzw. Dienststellenbüro nicht alle datenschutzrechtlichen Risiken ausgeschaltet werden können. Dies gilt insbesondere für den Fall, dass Mitarbeiter mit krimineller Energie oder Schädigungsabsicht handeln.

7 So ohne nähere Auseinandersetzung Dury/Leibold, Home-Office und Datenschutz, ZD-Aktuell 2020, 04405; kritisch insofern Suwelack, ZD 2020, 561 (566).

8 Vgl. Gola/Klug, Die Entwicklung des Datenschutzrechts, NJW 2020, 2774 (2776); Suwelack, ZD 2020, 561 (562) m.w.N.

9 VG Berlin, Beschluss vom 14.04.2020 – VG 28 L 119/20.

10 Vgl. Koreng/Lachenmann/Bergt, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, Anm. 1.

11 Koreng/Lachenmann/Bergt, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, D. III. 2. a.a.O.

12 Simitis/Hornung/Spiecker gen. Döhmman/Seifert, Datenschutzrecht, 1. Aufl. 2019, Art. 88 Rn. 167.

13 Vgl. BAG, Urteil vom 17.05.1983 – 1 AZR 1249/79.

14 So noch BfDI, 22. TB (2007/2008), 11.4; ähnlich BlnBDI, Jahresbericht 2012, 10.2.

Erforderlich ist ein Sicherheitskonzept, das die tatsächlichen örtlichen und personellen Gegebenheiten berücksichtigt. Es muss ein geeigneter Ort für die Arbeit in der Wohnung gefunden werden, zumindest ein nicht einsehbarer Computerarbeitsplatz. Eine abschließbare Aufbewahrungsmöglichkeit für Dokumente/Akten muss gewährleistet sein, wobei allerdings ein Transport von Unterlagen wegen der damit einhergehenden Gefahren (Verlust bzw. Bruch der Vertraulichkeit) nach Möglichkeit zu vermeiden ist. Auch der Ausdruck von Dokumenten sollte möglichst unterbleiben, vor allem über private Hardware. Zugriffe auf das Firmennetzwerk sollten nur verschlüsselt per VPN (Virtual Private Network) erfolgen und Dateien grundsätzlich im Firmennetzwerk abgelegt werden und nicht lokal. Berufliche und private Daten dürfen nicht vermischt werden. Schwierigkeiten entstehen insoweit vielfach dann, wenn Mitarbeiter private mobile Endgeräte, insbesondere Smartphones, für ihre berufliche Tätigkeit einsetzen (BYOD). Zwar könnte mittels der angesprochenen EMM-Lösungen auf technischer Ebene eine Trennung zwischen privaten und beruflichen Inhalten erreicht werden. Praktisch dürfen aber die wenigsten Beschäftigten bereit sein, ihre privaten Geräte vom Arbeitgeber verwalten und kontrollieren zu lassen. U.a. dies spricht gegen den Einsatz von BYOD-Lösungen.

Ein wichtiger Aspekt ist auch die Wahrnehmung der Kontrollrechte durch den Arbeitgeber. Für die Arbeit der Beschäftigten im Homeoffice ist festzulegen, dass der Arbeitgeber seinen gesetzlichen Kontrollpflichten auch in der häuslichen Umgebung der Beschäftigten nachkommen darf und hierfür Zugang zur Wohnung erhält. Gleiches muss für den Datenschutzbeauftragten, Betriebsrat sowie für die Aufsichtsbehörde gelten.

Die der neuen Arbeitssituation entsprechenden besonderen Verhaltenspflichten des Mitarbeiters sind in einem Ergänzungsvertrag zum Arbeitsvertrag oder einer Unternehmensrichtlinie festzulegen, der/die die in Art. 32 Abs. 1 DS-GVO geforderten Maßnahmen für den Anwendungsfall konkretisiert. Sofern die Rahmenbedingungen von Telearbeit/Homeoffice über eine Richtlinie geregelt werden, sollte

der/die Beschäftigte diese Regelungen explizit durch Unterschrift bestätigen, bevor ihm/ihr eine Genehmigung erteilt wird, von zu Hause zu arbeiten.

d) Ergebnis

Schon aufgrund fehlender Rahmenbedingungen, insbesondere eines dem Arbeitgeber etc. eingeräumten Kontrollrechts in der Wohnung, hätte Personalleiter L die Tätigkeit von P vom heimischen Arbeitsplatz aus nicht genehmigen dürfen. Angesichts des erhöhten Schutzbedarfs von Personaldaten ist auch der Einsatz privater IT-Infrastruktur durch P bedenklich. Die Genehmigung ist daher zurückzuziehen. Eine Tätigkeit von Zuhause kann erst dann erfolgen, wenn die vorbeschriebenen Bedingungen eingehalten werden.

e) Praxishinweis

Wie schon unter Ziff. 1 erwähnt, stellt die aktuell andauernde Corona-Pandemie Unternehmen und Behörden vor besondere Herausforderungen, die u.U. einen kurzfristigen Umzug von Beschäftigten ins Homeoffice mit sich bringen. Trotzdem haben Arbeitgeber als Verantwortliche i.S.d. DS-GVO die datenschutzrechtlichen Vorgaben zu beachten und einen geordneten Umzug zu veranlassen. Die Aufsichtsbehörden haben hierzu Praxishinweise und Checklisten veröffentlicht, die sich Verantwortliche zur Hilfe nehmen können und sollten.¹⁶

15 Ähnlich inzwischen auch der BfDI, „Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser“, Stand: Juli 2020, S. 9, abrufbar unter <https://t1p.de/38et> (zuletzt abgerufen am 24.10.2020).

16 U.a. ULD Schleswig-Holstein, Datenschutz: Plötzlich im Homeoffice – und nun?, <https://t1p.de/aa68> (zuletzt abgerufen am 24.10.2020); BSI, Tipps für sicheres mobiles Arbeiten, <https://t1p.de/5avt> (zuletzt abgerufen am 24.10.2020); LDA Bayern, Datenschutzrechtliche Regelungen bei Homeoffice, Best-Practice-Prüfkriterien, <https://t1p.de/vwo0> (zuletzt abgerufen am 24.10.2020); LfD Niedersachsen, Hilfestellung zum Datenschutz im Homeoffice, <https://t1p.de/1lq7> (zuletzt abgerufen am 24.10.2020); zum Einsatz von konferenz-Software vgl. die Orientierungshilfe der DSK vom 23.10.2020, <https://t1p.de/ot0y/zuletzt> abgerufen am 24.10.2020) sowie Gerling/Gerling/Hessel/Petereic, DuD 2020, 740.

Rechtsprechung

Persönlichkeitsgutachten auf einer Partnervermittlungs-Website ist keine Lieferung „digitaler Inhalte“

(Europäischer Gerichtshof, Urteil vom 8. Oktober 2020 – C-641/19 –)

1. Art. 14 Abs. 3 der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates ist dahin auszulegen, dass zur Bestimmung des anteiligen Betrags, den der Verbraucher an den Unternehmer zu zahlen hat, wenn er ausdrücklich verlangt hat, dass die Ausführung des geschlossenen Vertrags während der Widerrufsfrist beginnt, und dann den Vertrag widerruft, grundsätzlich auf den im Vertrag vereinbarten Preis für die Gesamtheit der vertragsgegenständlichen Leistungen abzustellen und der geschuldete Betrag zeitanteilig zu berechnen ist. Nur wenn der geschlossene Vertrag ausdrücklich vorsieht, dass eine oder mehrere der Leistungen gleich zu Beginn der Vertragsausführung vollständig und gesondert zu einem getrennt zu zahlenden Preis erbracht werden, ist bei der Berechnung des dem Unternehmer nach Art. 14 Abs. 3 dieser Richtlinie zustehenden Betrags der volle für eine solche Leistung vorgesehene Preis zu berücksichtigen.
2. Art. 14 Abs. 3 der Richtlinie 2011/83 im Licht deren 50. Erwägungsgrundes ist dahin auszulegen, dass für die Beurteilung, ob der Gesamtpreis im Sinne dieser Bestimmung überhöht ist, der Preis für die Dienstleistung, den der betreffende Unternehmer anderen Verbrauchern unter den gleichen Bedingungen anbietet, sowie der Preis einer zum Zeitpunkt des Vertragsabschlusses von anderen Unternehmern erbrachten gleichwertigen Dienstleistung zu berücksichtigen sind.
3. Art. 16 Buchst. m in Verbindung mit Art. 2 Nr. 11 der Richtlinie 2011/83 ist dahin auszulegen, dass die Erstellung eines Persönlichkeitsgutachtens auf einer Partnervermittlungs-Website auf der Grundlage eines auf dieser Website durchgeführten Persönlichkeits-tests keine Lieferung „digitaler Inhalte“ im Sinne dieser Bestimmung darstellt.

Sachverhalt:

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 2 Nr. 11, Art. 14 Abs. 3 und Art. 16 Buchst. m der Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25.

Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates (ABL 2011, L 304, S. 64).

Es ergeht im Rahmen eines Rechtsstreits zwischen EU als Verbraucherin und der PE Digital GmbH über den Betrag, der Letzterer zusteht, nachdem EU das Recht auf Widerruf des zwischen ihnen geschlossenen Vertrags ausgeübt hat.

PE Digital, eine Gesellschaft mit Sitz in Deutschland, betreibt die Partnervermittlungs-Website „Parship“ (www.parship.de). Sie bietet ihren Nutzern zwei Formen der Mitgliedschaft an, nämlich die kostenlose Basis-Mitgliedschaft mit sehr eingeschränkter Kontaktmöglichkeit zu anderen Nutzern und die zahlungspflichtige sogenannte Premium-Mitgliedschaft für eine Dauer von 6, 12 oder 24 Monaten. Die Premium-Mitgliedschaft ermöglicht den Nutzern, während der Dauer ihrer Mitgliedschaft mit allen anderen Premium-Mitgliedern – d.h. deutschlandweit über 186 000 Nutzern – Kontakt aufzunehmen und mit ihnen Nachrichten und Bilder auszutauschen.

Zur Premium-Mitgliedschaft gehört insbesondere die sogenannte Kontaktgarantie, mit der das Zustandekommen einer bestimmten Anzahl von Kontakten zu anderen Nutzern garantiert wird. Als Kontakt zählt dabei jede von dem betreffenden Nutzer gelesene Textantwort auf eine von ihm verschickte Nachricht sowie eine vom Nutzer erhaltene Nachricht, auf die hin er mindestens zwei Textnachrichten mit dem anderen Nutzer ausgetauscht und gelesen hat.

Durchschnittlich werden in der ersten Woche der Premium-Mitgliedschaft 31,3 Nachrichten, in der zweiten Woche 8,9 Nachrichten, in der dritten Woche 6,1 Nachrichten, in der vierten Woche 5,1 Nachrichten und ab der fünften Woche weniger als fünf Nachrichten versendet und empfangen.

Für jedes Mitglied wird unmittelbar nach der Anmeldung ausgehend von einem etwa dreißigminütigen Persönlichkeitstest zu partnerschaftsrelevanten Eigenschaften, Gewohnheiten und Interessen automatisiert eine Auswahl von Partnervorschlägen aus demselben Bundesland erstellt. Bei einer 12-monatigen Premiummitgliedschaft macht diese Auswahl bereits nahezu die Hälfte aller Partnervorschläge aus, die das Mitglied während der Vertragslaufzeit erhält. Der Algorithmus für den Persönlichkeitstest wurde unter der Leitung eines Diplompsychologen erstellt und entwickelt.

Premium-Mitglieder erhalten das computergenerierte Testergebnis in Form eines 50-seitigen „Persönlichkeitsgutachtens“; von Basis-Mitgliedern kann es gegen Entgelt als Teilleistung erworben werden.

Am 4. November 2018 schloss EU als Verbraucherin mit PE Digital einen Vertrag über eine Premium-Mitgliedschaft für zwölf Monate zu einem Preis von 523,95 Euro (im Folgenden: in Rede stehender Vertrag). Dieser Preis lag mehr als doppelt so hoch wie der, den PE Digital manchen anderen ihrer Nutzer für dieselbe Vertragsdauer im selben Jahr berechnete. PE Digital belehrte EU entsprechend den Anforderungen des Art. 246a § 1 Abs. 2 Satz 1 Nrn. 1 und 3 EGBGB über ihr Widerrufsrecht, und diese bestätigte PE Digital, dass Letztere mit der vertraglichen Leistung vor Ablauf der Widerrufsfrist beginnen solle.

Nachdem EU den in Rede stehenden Vertrag am 8. November 2018 widerrufen hatte, stellte ihr PE Digital einen Betrag von insgesamt 392,96 Euro als Wertersatz in Rechnung.

EU erhob beim Amtsgericht Hamburg (Deutschland) Klage auf Rückzahlung sämtlicher an PE Digital geleisteter Zahlungen.

Gestützt auf den vom Juni 2014 datierenden Leitfaden der Europäischen Kommission zur Richtlinie 2011/83, insbesondere auf des-

sen Abschnitt 6.5.1 betreffend Art. 14 Abs. 3 dieser Richtlinie, ist das vorliegende Gericht der Ansicht, dass dann, wenn die Gesamtleistung unterscheidbare Teilleistungen enthalte, die vereinbarungsgemäß nicht alle gleichzeitig erbracht würden, für die Berechnung des dem Unternehmer zustehenden Abgeltungsbetrages deren jeweiliger Laufzeit Rechnung zu tragen sei.

Hinsichtlich der Berechnung des „Betrag[s], der verhältnismäßig dem entspricht, was bis zu dem Zeitpunkt, zu dem der Verbraucher den Unternehmer von der Ausübung des Widerrufsrechts unterrichtet, im Vergleich zum Gesamtumfang der vertraglich vereinbarten Leistungen geleistet worden ist“ im Sinne von Art. 14 Abs. 3 der Richtlinie 2011/83 zieht das vorliegende Gericht die Berücksichtigung nicht nur der vom Unternehmer erbrachten Leistung, sondern auch des Wertes der Leistung, der sich realisiert habe und dem Verbraucher zugutegekommen sei, in Betracht.

Nach Ansicht des vorlegenden Gerichts ist die Abgeltung, die der Verbraucher dem Unternehmer im Fall des Widerrufs des geschlossenen Vertrags nach Art. 14 Abs. 3 der Richtlinie 2011/83 und § 357 Abs. 8 BGB zu zahlen hat, zu berechnen, indem als Erstes die einzelnen vertraglich vorgesehenen Teilleistungen voneinander abgegrenzt würden. Als Zweites sei der Preis der einzelnen Teilleistungen unter Berücksichtigung ihres Wertes für den Durchschnittsverbraucher in Anbetracht des Vertragszwecks zu bestimmen, wofür Statistiken über das Verhalten der Verbraucher heranzuziehen seien. Als Drittes seien die Teile des zu zahlenden Betrags für die einzelnen Teilleistungen einerseits anhand des Umfangs, in dem die Teilleistungen bereits erbracht worden seien, und andererseits im Hinblick auf den Wert der erbrachten Leistungen zu errechnen. Als Viertes ergebe die Addition der so berechneten Beträge die vom Verbraucher geschuldete Gesamtsumme.

Insoweit könne allerdings in der Übermittlung des Persönlichkeitsgutachtens zu Beginn der Erfüllung des in Rede stehenden Vertrags – als abgrenzbare Teilleistung – eine Bereitstellung von nicht auf einem körperlichen Datenträger gelieferten digitalen Inhalten gesehen werden, was zur Anwendung der Ausnahmebestimmungen des Art. 14 Abs. 4 Buchst. b Ziff. ii und des Art. 16 Buchst. m der Richtlinie 2011/83 sowie von § 356 Abs. 5 und § 357 Abs. 9 BGB führen würde.

Diese Auslegung führte jedoch dazu, dass dem Verbraucher das Widerrufsrecht versagt würde, und griffe damit in seine Rechte ein.

Unter Bezugnahme auf Art. 14 Abs. 3 der Richtlinie 2011/83 im Licht ihres 50. Erwägungsgrundes vertritt das vorliegende Gericht im Übrigen die Auffassung, dass ein Gesamtpreis, der doppelt so hoch sei wie der Preis, der anderen Nutzern für dieselbe Leistung in Rechnung gestellt werde, nicht „überhöht“ im Sinne dieser Bestimmung sei, solange er den Marktwert der erbrachten Dienstleistung nicht erreiche oder nur unwesentlich überschreite.

Unter diesen Umständen hat das Amtsgericht Hamburg beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

Ist Art. 14 Abs. 3 der Richtlinie 2011/83 mit Hinblick auf deren 50. Erwägungsgrund dahin gehend auszulegen, dass der vom Verbraucher zu leistende „Betrag, der verhältnismäßig dem entspricht, was bis zu dem Zeitpunkt, zu dem der Verbraucher den Unternehmer von der Ausübung des Widerrufsrechts unterrichtet, im Vergleich zum Gesamtumfang der vertraglich vereinbarten Leistungen geleistet worden ist“, bei einem Vertrag, nach dessen Inhalt keine einheitliche Leistung geschuldet ist, sondern eine sich aus mehreren Teilleistungen zusammensetzende Gesamtleistung, rein zeitanteilig zu berechnen ist, wenn zwar der Verbraucher für die Gesamtleistung zeitanteilig bezahlt, aber die Teilleistungen unterschiedlich schnell erbracht werden?

Ist Art. 14 Abs. 3 der Richtlinie 2011/83 dahin gehend auszulegen, dass der vom Verbraucher zu leistende „Betrag, der verhältnismäßig dem entspricht, was bis zu dem Zeitpunkt, zu dem der Verbraucher den Unternehmer von der Ausübung des Widerrufsrechts unterrichtet, im Vergleich zum Gesamtumfang der vertraglich vereinbarten Leistungen geleistet worden ist“, auch dann rein zeitan-

teilig zu berechnen ist, wenn eine (Teil-)Leistung zwar kontinuierlich erbracht wird, aber zu Beginn der Vertragslaufzeit einen höheren oder niedrigeren Wert für den Verbraucher hat?

Sind Art. 2 Nr. 11 der Richtlinie 2011/83 und Art. 2 Nr. 1 der Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (ABL 2019, L 136, S. 1) dahin gehend auszulegen, dass auch solche Dateien „digitale Inhalte“ im Sinne von Art. 2 Nr. 11 der Richtlinie 2011/83 und Art. 2 Nr. 1 der Richtlinie 2019/770 darstellen können, die als Teilleistung im Rahmen einer vornehmlich als „digitale Dienstleistung“ im Sinne des Art. 2 Nr. 2 der Richtlinie 2019/770 erbrachten Gesamtleistung bereitgestellt werden, mit der Folge, dass der Unternehmer das Widerrufsrecht nach Art. 16 Buchst. m der Richtlinie 2011/83 hinsichtlich der Teilleistung zum Erlöschen bringen könnte, der Verbraucher aber, falls dem Unternehmer dies nicht gelänge, den Vertrag insgesamt widerrufen könnte und wegen Art. 14 Abs. 4 Buchst. b Ziff. ii der Richtlinie 2011/83 für diese Teilleistung keinen Abgeltungsbetrag zu leisten hätte?

Ist Art. 14 Abs. 3 der Richtlinie 2011/83 mit Hinblick auf deren 50. Erwägungsgrund dahin gehend auszulegen, dass der für eine Dienstleistung vertraglich vereinbarte Gesamtpreis im Sinne des Art. 14 Abs. 3 Satz 3 der Richtlinie 2011/83 „überhöht“ ist, wenn er erheblich höher liegt, als der für eine inhaltlich identische Dienstleistung von demselben Unternehmer für dieselbe Vertragslaufzeit und auch im Übrigen unter denselben Rahmenbedingungen mit einem anderen Verbraucher vereinbarte Gesamtpreis?

Zu den Vorlagefragen

Zur ersten und zur zweiten Frage

Mit seiner ersten und seiner zweiten Frage, die zusammen zu prüfen sind, möchte das vorliegende Gericht im Wesentlichen wissen, ob Art. 14 Abs. 3 der Richtlinie 2011/83 dahin auszulegen ist, dass zur Bestimmung des anteiligen Betrags, den der Verbraucher an den Unternehmer zu zahlen hat, wenn er ausdrücklich verlangt hat, dass die Ausführung des geschlossenen Vertrags während der Widerrufsfrist beginnt, und dann den Vertrag widerruft, auf den im Vertrag vereinbarten Preis für die Gesamtheit der vertraglich vorgesehenen Leistungen abzustellen und der geschuldete Betrag zeitanteilig zu berechnen ist oder ob dem Umstand Rechnung zu tragen ist, dass eine der vertragsgegenständlichen Leistungen dem Verbraucher vor dessen Widerruf in vollem Umfang erbracht wurde.

Nach Art. 14 Abs. 3 der Richtlinie 2011/83 hat der Verbraucher, der vom Unternehmer den Beginn der Vertragsausführung vor Ablauf der Widerrufsfrist verlangt hat, wenn er in diesem Zusammenhang sein Widerrufsrecht ausübt, dem Unternehmer „einen Betrag [zu zahlen], der verhältnismäßig dem entspricht, was bis zu dem Zeitpunkt, zu dem der Verbraucher den Unternehmer von der Ausübung des Widerrufsrechts unterrichtet, im Vergleich zum Gesamtumfang der vertraglich vereinbarten Leistungen geleistet worden ist“. Weiter wird in dieser Bestimmung klargestellt, dass „[d]er anteilige Betrag, den der Verbraucher ... zu zahlen hat, auf der Grundlage des vertraglich vereinbarten Gesamtpreises berechnet [wird]“.

Der anteilige Betrag, den der Verbraucher gemäß Art. 14 Abs. 3 der Richtlinie 2011/83 zu zahlen hat, ist grundsätzlich unter Berücksichtigung aller Leistungen zu berechnen, die Gegenstand des Vertrags sind, d.h. der Hauptleistung und der Nebenleistungen, die für die Erbringung dieser Hauptleistung erforderlich sind. Wenn nämlich die Vertragsparteien einen Preis für die erbrachten Leistungen vorsehen, entspricht dieser Preis grundsätzlich allen diesen Leistungen, Hauptleistungen wie Nebenleistungen.

Nur wenn der Vertrag ausdrücklich vorsieht, dass eine oder mehrere der Leistungen gleich zu Beginn der Vertragsausführung vollständig und gesondert zu einem getrennt zu zahlenden Preis erbracht werden, kann der Verbraucher sachgerecht entscheiden, ob er gemäß Art. 7 Abs. 3 der Richtlinie 2011/83 ausdrücklich verlangen soll, dass der Unternehmer mit der Ausführung der Dienstleistung während der Frist für die Ausübung des Widerrufsrechts beginnt. Nur in einem solchen Fall ist daher bei der Berechnung des dem Unternehmer nach Art. 14 Abs. 3 dieser Richtlinie zustehenden Betrags der volle für eine solche Leistung vorgesehene Preis zu berücksichtigen.

Die vorstehend in den Rn. 28 und 29 vorgenommene Auslegung entspricht dem im vierten Erwägungsgrund der Richtlinie 2011/83 genannten Ziel, für ein möglichst ausgewogenes Verhältnis zwischen einem hohen Verbraucherschutzniveau und der Wettbewerbsfähigkeit der Unternehmen zu sorgen (vgl. entsprechend Urteile vom 23. Januar 2019, Walbusch/Walter Busch, C 430/17, EU:C:2019:47, Rn. 41, vom 27. März 2019, Slewco, C 681/17, EU:C:2019:255, Rn. 39, und vom 10. Juli 2019, Amazon EU, C 649/17, EU:C:2019:576, Rn. 44).

Im vorliegenden Fall sah der in Rede stehende Vertrag aber keinen gesonderten Preis für irgendeine Leistung vor, die als von der in diesem Vertrag vorgesehene Hauptleistung abtrennbar angesehen werden kann.

In Anbetracht der vorstehenden Erwägungen ist auf die erste und die zweite Frage zu antworten, dass Art. 14 Abs. 3 der Richtlinie 2011/83 dahin auszulegen ist, dass zur Bestimmung des anteiligen Betrags, den der Verbraucher an den Unternehmer zu zahlen hat, wenn er ausdrücklich verlangt hat, dass die Ausführung des geschlossenen Vertrags während der Widerrufsfrist beginnt, und dann den Vertrag widerruft, grundsätzlich auf den im Vertrag vereinbarten Preis für die Gesamtheit der vertragsgegenständlichen Leistungen abzustellen und der geschuldete Betrag zeitanteilig zu berechnen ist. Nur wenn der geschlossene Vertrag ausdrücklich vorsieht, dass eine oder mehrere der Leistungen gleich zu Beginn der Vertragsausführung vollständig und gesondert zu einem getrennt zu zahlenden Preis erbracht werden, ist bei der Berechnung des dem Unternehmer nach Art. 14 Abs. 3 dieser Richtlinie zustehenden Betrags der volle für eine solche Leistung vorgesehene Preis zu berücksichtigen.

Zur vierten Frage

Mit seiner vierten Frage, die an zweiter Stelle zu prüfen ist, möchte das vorliegende Gericht im Wesentlichen wissen, nach welchen Kriterien zu beurteilen ist, ob der Gesamtpreis im Sinne von Art. 14 Abs. 3 der Richtlinie 2011/83 überhöht ist.

Nach Art. 14 Abs. 3 der Richtlinie 2011/83 „[wird, i]st der Gesamtpreis überhöht, ... der anteilige Betrag auf der Grundlage des Marktwerts der erbrachten Leistung berechnet“.

Diese Bestimmung ist im Licht des 50. Erwägungsgrundes der Richtlinie 2011/83 auszulegen, wonach der Marktwert festzulegen ist, indem der Preis einer zum Zeitpunkt des Vertragsabschlusses von anderen Unternehmern erbrachten gleichwertigen Dienstleistung zum Vergleich herangezogen wird.

Somit sind für die Beurteilung, ob der Gesamtpreis etwa überhöht ist, alle Umstände in Bezug auf den Marktwert der erbrachten Dienstleistung relevant, d.h. sowohl der Vergleich mit dem Preis, den der betreffende Unternehmer von anderen Verbrauchern unter den gleichen Bedingungen verlangt, als auch der Vergleich mit dem Preis einer von anderen Unternehmern erbrachten gleichwertigen Dienstleistung.

In Anbetracht der vorstehenden Erwägungen ist auf die vierte Frage zu antworten, dass Art. 14 Abs. 3 der Richtlinie 2011/83

im Licht deren 50. Erwägungsgrundes dahin auszulegen ist, dass für die Beurteilung, ob der Gesamtpreis im Sinne dieser Bestimmung überhöht ist, der Preis für die Dienstleistung, den der betreffende Unternehmer anderen Verbrauchern unter den gleichen Bedingungen anbietet, sowie der Preis einer zum Zeitpunkt des Vertragsabschlusses von anderen Unternehmern erbrachten gleichwertigen Dienstleistung zu berücksichtigen sind.

Zur dritten Frage

Mit seiner zuletzt zu prüfenden dritten Frage möchte das vorliegende Gericht im Wesentlichen wissen, welche Konsequenz für die Bestimmung des vom Verbraucher gemäß Art. 14 Abs. 3 der Richtlinie 2011/83 an den Unternehmer zu zahlenden Betrags daraus zu ziehen ist, dass eine der Leistungen, die Gegenstand des geschlossenen Vertrags sind, die Lieferung von nicht auf einem körperlichen Datenträger gelieferten digitalen Inhalten betrifft, die vom Verbraucher nach Art. 16 Buchst. m dieser Richtlinie nicht widerrufen werden kann.

Wie sich aus der Vorlageentscheidung ergibt, besteht die Leistung, die Gegenstand der dritten Frage ist, darin, dass dem Verbraucher das oben in Rn. 15 genannte Persönlichkeitsgutachten bereitgestellt wird.

In diesem Zusammenhang fragt sich das vorliegende Gericht nach der Relevanz von Art. 16 Buchst. m der Richtlinie 2011/83 im Ausgangsverfahren, nach dem die Mitgliedstaaten bei Fernabsatzverträgen über die Lieferung von nicht auf einem körperlichen Datenträger gelieferten digitalen Inhalten kein Widerrufsrecht vorsehen, wenn die Ausführung mit vorheriger ausdrücklicher Zustimmung des Verbrauchers und seiner Kenntnisnahme, dass er hierdurch sein Widerrufsrecht verliert, begonnen hat.

Zu den „digitalen Inhalten“ ist darauf hinzuweisen, dass sie in Art. 2 Nr. 11 der Richtlinie 2011/83 als „Daten, die in digitaler Form hergestellt und bereitgestellt werden“ definiert werden.

Wie es im 19. Erwägungsgrund dieser Richtlinie heißt, werden als „digitale Inhalte“ ... Daten [bezeichnet], die in digitaler Form hergestellt und bereitgestellt werden, wie etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte, unabhängig davon, ob auf sie durch Herunterladen oder Herunterladen in Echtzeit (Streaming), von einem körperlichen Datenträger oder in sonstiger Weise zugegriffen wird“.

Art. 16 Buchst. m der Richtlinie 2011/83, der eine Ausnahme vom Widerrufsrecht darstellt, ist als unionsrechtliche Vorschrift, welche die zum Schutz der Verbraucher gewährten Rechte beschränkt, eng auszulegen (vgl. entsprechendes Urteil vom 14. Mai 2020, NK [Planung eines Einfamilienhauses], C 208/19, EU:C:2020:382, Rn. 40 und 56 sowie die dort angeführte Rechtsprechung).

Unter diesen Umständen ist festzustellen, dass Dienstleistungen wie die auf der im Ausgangsverfahren in Rede stehenden Partnervermittlungs-Website bereitgestellten, die dem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten und die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen, als solche nicht als Lieferung „digitaler Inhalte“ im Sinne von Art. 16 Buchst. m der Richtlinie 2011/83 in Verbindung mit Art. 2 Nr. 11 und im Licht des 19. Erwägungsgrundes dieser Richtlinie angesehen werden können.

Ebenso wenig kann angenommen werden, dass die Erstellung eines Persönlichkeitsgutachtens wie des oben in Rn. 15 genannten im Rahmen einer Partnervermittlungs-Website unter

die in Art. 16 Buchst. m in Verbindung mit Art. 2 Nr. 11 der Richtlinie 2011/83 vorgesehene Ausnahme fällt.

Nach alledem ist auf die dritte Frage zu antworten, dass Art. 16 Buchst. m in Verbindung mit Art. 2 Nr. 11 der Richtlinie 2011/83 dahin auszulegen ist, dass die Erstellung eines Persönlichkeitsgutachtens auf einer Partnervermittlungs-Website auf der Grundlage eines auf dieser Website durchgeführten Persönlichkeitstests keine Lieferung „digitaler Inhalte“ im Sinne dieser Bestimmung darstellt.

Rechtsbehelf gegen ein Auskunftsersuchen in Steuersachen (Ls)

(Europäischer Gerichtshof, Urteil vom 6. Oktober 2020 – C-245/19 und C-246/19 –)

1. Art. 47 der Charta der Grundrechte der Europäischen Union in Verbindung mit deren Art. 7, 8 und 52 Abs. 1 ist dahin auszulegen,
 - dass er es verbietet, dass Rechtsvorschriften eines Mitgliedstaats, mit denen das von der Richtlinie 2011/16/EU des Rates vom 15. Februar 2011 über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung und zur Aufhebung der Richtlinie 77/799/EWG in der durch die Richtlinie 2014/107/EU des Rates vom 9. Dezember 2014 geänderten Fassung eingeführte Verfahren zum Informationsaustausch auf Ersuchen durchgeführt wird, es ausschließen, dass eine Person, die Inhaberin von Informationen ist, gegen eine Entscheidung, mit der die zuständige Behörde dieses Mitgliedstaats sie dazu verpflichtet, ihr diese Informationen zu erteilen, um einem Ersuchen um Informationsaustausch der zuständigen Behörde eines anderen Mitgliedstaats nachzukommen, einen Rechtsbehelf einlegen kann, und
 - dass er es nicht verbietet, dass solche Rechtsvorschriften es ausschließen, dass der Steuerpflichtige, gegen den in diesem anderen Mitgliedstaat die dem Ersuchen zugrunde liegende Untersuchung gerichtet ist, sowie Dritte, die von den fraglichen Informationen betroffen sind, einen Rechtsbehelf gegen eine solche Entscheidung einlegen können.
2. Art. 1 Abs. 1 und Art. 5 der Richtlinie 2011/16 in der durch die Richtlinie 2014/107 geänderten Fassung sind dahin auszulegen, dass eine Entscheidung, mit der die zuständige Behörde eines Mitgliedstaats einen Informationsinhaber verpflichtet, ihr diese Informationen zu übermitteln, um einem von der zuständigen Behörde eines anderen Mitgliedstaats gestellten Ersuchen um Informationsaustausch nachzukommen, zusammen mit diesem Ersuchen als auf Informationen bezogen anzusehen ist, denen die voraussichtliche Erheblichkeit nicht offensichtlich völlig zu fehlen scheint, sofern darin die Identität des Inhabers der fraglichen Informationen, die des Steuerpflichtigen, der von den dem Ersuchen um Infor-

mationsaustausch zugrunde liegenden Ermittlungen betroffen ist, und der von diesen Ermittlungen erfasste Zeitraum angegeben wird und sie Verträge, Rechnungen und Zahlungen betreffen, die nicht näher bestimmt, aber durch Kriterien eingegrenzt sind, die darauf bezogen sind, dass sie erstens durch den Informationsinhaber geschlossen, erstellt oder getätigt wurden, zweitens in die von den fraglichen Ermittlungen erfassten Steuerjahre fielen und drittens einen Zusammenhang mit dem betreffenden Steuerpflichtigen aufweisen.

Zu den Voraussetzungen eines Auslistungsanspruchs gegen den Verantwortlichen eines Internet-Suchdienstes nach Art. 17 DS-GVO

(Bundesgerichtshof, Urteil vom 27. Juli 2020 – VI ZR 405/18 –)

1. Die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte und dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, fällt, sofern die Informationen – wie hier – personenbezogene Daten enthalten, in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung (Art. 2 Abs. 1 DS-GVO).
2. Das in Art. 17 Abs. 1 DS-GVO niedergelegte "Recht auf Löschung" ist insoweit schon aufgrund der für den Betroffenen letztlich unwägbar und zudem stetem Entwicklungsfortschritt unterworfenen technischen Voraussetzungen der beanstandeten Datenverarbeitung nicht auf das schlichte Löschen von Daten zu verengen, sondern – entsprechend der zielorientierten weiteren Artikelüberschrift – als „Recht auf Vergessenwerden“ normativ zu verstehen, so dass ihm unabhängig von der technischen Umsetzung auch das Auslistungsrecht der von einer Suchmaschine betroffenen Person unterfällt (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-507/17).
3. Ein Anspruch auf Auslistung aus Art. 17 Abs. 1 DS-GVO entfällt, wenn die vorgenommene Datenverarbeitung auf der Grundlage aller relevanten Umstände zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist (Art. 17 Abs. 3 Buchst. a i.V.m. Art. 6 Abs. 1 Buchst. f, Art. 9 Abs. 2 Buchst. g, Art. 21 Abs. 1 Satz 2 DS-GVO).

Sachverhalt:

Der Kläger verlangt von der Beklagten, es als verantwortliche Stelle für die Verarbeitung von Daten in dem Index des Internet-Suchdienstes „Google“ zu unterlassen, bei einer Suche nach seinem Namen bestimmte Ergebnislinks anzuzeigen, die auf ihn identifizierende Presseveröffentlichungen hinführen.

Der Kläger war bis April 2012 Geschäftsführer des Regionalverbands des Arbeiter-Samariter-Bundes in Mittelhessen (ASB-Mittelhessen). Der ASB-Mittelhessen hat über 500 Beschäftigte und mehr als 35.000 Mitglieder, er organisiert und finanziert Bauprojekte, Einrichtungen und Pflegedienste. Im Jahr 2011 wies der ASB-Mittelhessen ein finanzielles Defizit von knapp einer Million Euro auf. Der Kläger meldete sich kurz zuvor auf Grund gesundheitlicher Probleme krank. Die regionale Presse berichtete wiederholt über die finanzielle Schieflage des ASB-Mittelhessen.

Am 17. Mai 2015 forderte der Kläger die Beklagte auf, verschiedene Ergebnislinks aus ihren Suchergebnislisten zu entfernen, die bei Eingabe seines Vor- und Familiennamens – sowohl isoliert als auch in Verbindung mit bestimmten Ortsangaben – in die Suchmaschine angezeigt würden. Dieser Aufforderung kam die Beklagte teilweise nach, nicht aber in Bezug auf die noch im Streit befindlichen Ergebnislinks zu den o.g. Veröffentlichungen.

Das Landgericht hat die auf die Auslistung auch dieser fünf Suchergebnisse gerichtete Klage abgewiesen. Die Berufung des Klägers blieb vor dem Oberlandesgericht ohne Erfolg. Mit der vom Berufungsgericht zugelassenen Revision verfolgt der Kläger sein Auslistungsbegehren weiter.

Aus den Gründen:

Nach Auffassung des Berufungsgerichts, dessen Entscheidung unter anderem in AfP 2019, 446 veröffentlicht ist, ergibt sich der vom Kläger geltend gemachte Anspruch nicht aus Art. 17 DS-GVO. Zwar sei der Anwendungsbereich der DS-GVO eröffnet und werde das Rechtsschutzbegehren des Klägers grundsätzlich von Art. 17 DS-GVO erfasst. Doch lägen die Voraussetzungen des Art. 17 DS-GVO nicht vor. Zwar sei zu berücksichtigen, dass die verlinkten Art. insoweit Gesundheitsdaten des Klägers i.S.d. Art. 9 Abs. 1 DS-GVO enthielten, als darüber berichtet werde, dass sich der Kläger krank gemeldet habe, er sich in einer Reha-Maßnahme bzw. einer seit langer Zeit terminierten medizinischen Behandlung befunden habe und aus gesundheitlichen Gründen nicht im Dienst gewesen sei. Doch sei die Verarbeitung der Daten zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich (Art. 17 Abs. 3 Buchst. a DS-GVO). Die insoweit notwendige Abwägung des Rechts des Klägers auf informationelle Selbstbestimmung auf der einen Seite und des Rechts der Beklagten und der Nutzer ihrer Suchmaschine auf Kommunikationsfreiheit auf der anderen Seite führe im Ergebnis dazu, dass die Datenverarbeitung insgesamt rechtmäßig sei.

Insoweit sei zunächst zu berücksichtigen, dass den Betreiber einer Suchmaschine nach der Rechtsprechung des erkennenden Senats (Urteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350) erst dann spezifische Verhaltenspflichten träfen, wenn er durch einen konkreten Hinweis Kenntnis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Verletzung des allgemeinen Persönlichkeitsrechts des Betroffenen durch den Inhalt einer in der Ergebnisliste der Suchmaschine nachgewiesenen Internetseite erlangt habe. Lege man diesen Maßstab an, gehe die Abwägung zu Lasten des Klägers, da es zumindest an einer für die Beklagte offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung fehle.

Im Zeitpunkt ihrer Veröffentlichung sei die Berichterstattung rechtmäßig gewesen. Sie habe wahre Tatsachenbehauptungen enthalten. Die berichteten Umstände entstammten der Sozial-sphäre des Klägers und seien zu unkonkret, um ein genaues Ausmaß der gesundheitlichen Auswirkungen des Klägers zu offenbaren. Zudem habe die Berichterstattung zur Begründung gedient, warum der Kläger in der aktuellen Schieflage des ASB-Mittelhessen nicht zur Mitarbeit zur Verfügung gestanden habe.

Hinsichtlich der Verlinkung durch die Beklagte sei zu berücksichtigen, dass das Internet ohne Suchmaschinen nicht mehr sinnvoll nutzbar wäre. Zu beachten sei zudem das Interesse der Autoren der verlinkten Presseartikel aus Art. 5 Abs. 1 GG. Schließlich habe die Beklagte auch nicht ein dem Kläger zustehendes Recht auf Vergessenwerden missachtet. Der im Streitfall vorliegende Zeitablauf von sechs bis sieben Jahren seit Veröffentlichung der Artikel lasse nicht eindeutig auf die Erledigung jeglichen Informationsinteresses schließen, auch wenn sich die finanzielle Situation des ASB-Mittelhessen mittlerweile gebessert habe und der – offenbar gesunde – Kläger dort auch nicht mehr tätig sei. Vielmehr sei zu berücksichtigen, dass die Vorkommnisse, um die es gehe und die aufgrund von Stellenstreichungen, Streichungen bei Leistungen etc. auf viele Menschen Auswirkungen gehabt hätten, erst wenige Jahre zurücklägen, die Rechtsprechung das berechnete Interesse der Öffentlichkeit nicht nur an der Information über das aktuelle Zeitgeschehen, sondern auch an der Möglichkeit anerkenne, vergangene zeitgeschichtliche Ergebnisse zu recherchieren, und die Vorkommnisse letztlich auch zu dem beruflichen Werdegang des Klägers gehörten, die nicht ohne Weiteres aus seinem Leben gestrichen werden könnten.

Diese Erwägungen halten revisionsrechtlicher Überprüfung im Ergebnis stand. Der Kläger hat derzeit keinen Anspruch gegen die Beklagte auf Auslistung der streitgegenständlichen Ergebnislinks.

Der geltend gemachte Anspruch ergibt sich nicht aus Art. 17 Abs. 1 DS-GVO.

1. Allerdings ist die Datenschutz-Grundverordnung zeitlich (a), sachlich (b) und räumlich (c) anwendbar.

a) Die Datenschutz-Grundverordnung gilt seit dem 25. Mai 2018 (Art. 99 Abs. 2 DS-GVO) unmittelbar in jedem Mitgliedstaat der Europäischen Union.

b) Die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte und dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, fällt, sofern die Informationen – wie hier – personenbezogene Daten enthalten, in den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung (Art. 2 Abs. 1 DS-GVO). Sie ist als automatisierte „Verarbeitung personenbezogener Daten“ im Sinne von Art. 4 Nr. 1 und 2 DS-GVO einzustufen. Als verantwortliche Stelle für die Verarbeitung von Daten in dem Index des Internet-Suchdienstes ist die Beklagte "Verantwortlicher" im Sinne von Art. 4 Nr. 7 DS-GVO (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3504 Rn. 35 i.V.m. 33; vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2259 Rn. 41).

Die streitgegenständliche Tätigkeit der Beklagten unterfällt auch nicht der Öffnungsklausel nach Art. 85 DS-GVO i.V.m. der Bereichsausnahme des § 57 Abs. 1 Satz 4 RStV. Die automatisierte bloße Auflistung von redaktionellen Beiträgen stellt keine eigene journalistisch-redaktionelle Gestaltung dar (vgl. BVerfG, NJW 2020, 314, 316 ff. Rn. 36, 41, 105, 138 – Recht auf Vergessen II; Buchner/Tinnefeld, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., Art. 85 DS-GVO Rn. 12, 26; zu den Vorgängervorschriften vgl. EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2263 Rn. 85; Senatsurteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350, 368 Rn. 44; zur umstrittenen Bedeutung von Art. 85 Abs. 1 DS-GVO in diesem Zusammenhang weitergehend etwa Lauber-Rönsberg, AfP 2019, 373, 377 mwN). Dies nimmt die Beklagte auch nicht für sich in Anspruch.

c) Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung auf die in den Vereinigten Staaten von Amerika ansässige Beklagte folgt bereits aus Art. 3 Abs. 1 DS-GVO. Nach

den tatrichterlichen Feststellungen betreibt die Beklagte eine deutsche Niederlassung und bietet in deutscher Sprache Nutzern in Deutschland die Möglichkeit an, über ihren Suchdienst gezielt nach im Internet vorhandenen Informationen zu suchen und auf sie zuzugreifen, wobei die Nutzer letztlich als „Bezahlung“ ihre Daten zur Verfügung stellen, um das Leistungsangebot nutzen zu können. Daher kann der Umstand, dass die Suchmaschine von einem Unternehmen eines Drittstaates betrieben wird, nicht dazu führen, dass die Verarbeitung personenbezogener Daten, die zum Betrieb der Suchmaschine im Rahmen der gewerblichen und Werbetätigkeit einer Niederlassung des für die Verarbeitung Verantwortlichen im Hoheitsgebiet eines Mitgliedstaates ausgeführt wird, den in der Datenschutz-Grundverordnung vorgesehenen Garantien und Verpflichtungen entzogen wird (EuGH, Urteil vom 24. September 2019 – Rs. C-507/17, NJW 2019, 3499, 3500 Rn. 48 ff. i.V.m. 41; vgl. bereits EuGH, Urteil vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2260 Rn. 45 ff.). Auf das zusätzliche Vorliegen der Voraussetzungen des Art. 3 Abs. 2 DS-GVO kommt es danach nicht mehr an.

2. Die internationale Zuständigkeit der deutschen Gerichte folgt insoweit aus Art. 79 Abs. 2 DS-GVO. Die Beklagte hat in Deutschland eine Niederlassung (Art. 79 Abs. 2 Satz 1 i.V.m. Erwägungsgrund 22 DS-GVO); zudem hat der Kläger als betroffene Person seinen gewöhnlichen Aufenthalt in Deutschland (Art. 79 Abs. 2 Satz 2 DS-GVO; vgl. jeweils im Überblick Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., Art. 79 DS-GVO Rn. 15 ff.; Boehm, in: Simitis/Hornung/Spiecker gen. Döhm, Datenschutzrecht, 2019, Art. 79 DS-GVO Rn. 17 ff.).

3. Das auf dauerhafte Auslistung der von ihm beanstandeten Suchergebnisse gerichtete Rechtsschutzbegehren des Klägers ist grundsätzlich von Art. 17 Abs. 1 DS-GVO erfasst. Dies gilt unbeschadet des Umstandes, dass die technische Umsetzung dieses Begehrens sich nicht in dem einmaligen Löschen von Daten durch die Beklagte erschöpfte, sondern weitere Maßnahmen, etwa die Aufnahme der beanstandeten Information in eine Datenbank erforderte, um die erneute Indexierung dieser Information unter dem fraglichen Suchbegriff zu verhindern (vgl. Veil, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2018, Art. 17 Rn. 89; Spindler, in: Spindler/Schmitz, TMG, 2. Aufl., Vorb. vor § 7 Rn. 83). Der Begriff der Löschung i.S.d. Art. 17 DS-GVO ist autonom auszulegen. Das in Art. 17 Abs. 1 DS-GVO niedergelegte „Recht auf Löschung“ ist insoweit schon aufgrund der für den Betroffenen letztlich unwägbar und zudem stetem Entwicklungsfortschritt unterworfenen technischen Voraussetzungen der beanstandeten Datenverarbeitung nicht auf das schlichte Löschen von Daten zu verengen, sondern – entsprechend der zielorientierten weiteren Art.überschrift – als „Recht auf Vergessenwerden“ normativ zu verstehen, so dass ihm unabhängig von der technischen Umsetzung auch das Auslistungsrecht der von einer Suchmaschine betroffenen Person unterfällt (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-507/17, NJW 2019, 3499, 3500 Rn. 45 f.; Rs. C-136/17, NJW 2019, 3503, 3506 Rn. 53 ff.).

4. Der Kläger muss sich auch nicht darauf verweisen lassen, vorrangig die für die von der Beklagten verlinkten Artikel verantwortlichen Presseorgane in Anspruch zu nehmen. Die Haftung des Suchmaschinenbetreibers bzw. Verantwortlichen eines Internet-Suchdienstes ist nicht subsidiär, da ein wirksamer und umfassender Schutz der betroffenen Person nicht erreicht werden kann, wenn diese grundsätzlich vorher oder parallel bei den Inhabern der Inhalte die Löschung der sie betreffenden Informationen erwirken müsste. Die Tätigkeit eines Suchmaschinenbetreibers ist ein für sich stehender Akt der Datenverarbeitung, der

folglich auch hinsichtlich der damit einhergehenden Grundrechtsbeschränkungen eigenständig zu beurteilen ist. Daher kann die Abwägung im Rahmen des Anspruchs aus Art. 17 Abs. 1 DS-GVO gegen den Suchmaschinenbetreiber zu einem anderen Ergebnis führen als im Rahmen des Anspruchs gegen den Betreiber der verlinkten Webseite, da sowohl die berechtigten Interessen, die die Datenverarbeitung rechtfertigen, unterschiedlich sein können als auch die Folgen, die die Verarbeitungen für die betroffene Person, insbesondere für ihr Privatleben, haben (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-507/17, NJW 2019, 3499, 3500 Rn. 44 i.V.m. 41; Rs. C-136/17, NJW 2019, 3503, 3506 Rn. 52 i.V.m. 33; vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2263 Rn. 82 ff.; BVerfG, NJW 2020, 314, 324 Rn. 112 – Recht auf Vergessen II; Senatsurteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350, 368 f. Rn. 45).

5. Schließlich hat der Kläger die – ohne vorherige Beanstandung durch einen Betroffenen zu einer proaktiven, also von ihr aus vorzunehmenden Prüfung des Inhalts der von ihrer Suchmaschine generierten Nachweise nicht verpflichtete (vgl. Senatsurteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350, 361 f. Rn. 34; BVerfG, NJW 2020, 314, 324 Rn. 113 – Recht auf Vergessen II) – Beklagte bereits vor Klageerhebung durch Benennung der konkret beanstandeten Ergebnislinks und eine im Zusammenhang erfolgte Darstellung des zugrunde liegenden Sachverhalts und seiner rechtlichen Erwägungen in formeller Hinsicht hinreichend deutlich auf die aus seiner Sicht vorliegende Rechtswidrigkeit der Datenverarbeitung hingewiesen und die Beklagte insoweit zur Auslistung aufgefordert (vgl. zum Antragserfordernis auch EuGH, Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3504 ff. Rn. 48, 66, 68, 77 i.V.m. 33; vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2264 Rn. 94 ff.).

6. Indes liegen die materiellen Voraussetzungen für das klägerische Auslistungsbegehren nicht vor. Der Kläger hat keinen Anspruch gegen die Beklagte auf Auslistung der streitgegenständlichen Ergebnislinks aus Art. 17 Abs. 1 DS-GVO, weil die von der Beklagten vorgenommene Datenverarbeitung auf der Grundlage aller relevanten Umstände des Streitfalls zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist (Art. 17 Abs. 3 Buchst. a i.V.m. Art. 6 Abs. 1 Buchst. f, Art. 9 Abs. 2 Buchst. g, Art. 21 Abs. 1 Satz 2 DS-GVO).

a) Einschlägige Grundlage des klägerischen Auslistungsbegehrens ist Art. 17 Abs. 1 DS-GVO. Danach steht – soweit im Streitfall relevant – der betroffenen Person der Anspruch zu, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 Buchst. a DS-GVO) oder die betroffene Person Widerspruch gegen die Verarbeitung ihrer Daten eingelegt hat und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen (Art. 17 Abs. 1 Buchst. c DS-GVO) oder die personenbezogenen Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 Buchst. d DS-GVO).

Der Kläger nimmt der Sache nach das Vorliegen der Voraussetzungen für alle drei genannten Varianten für sich in Anspruch. Die erste Variante betrifft den Zeitablauf zwischen dem erstmaligen Erscheinen der in der Ergebnisliste der Beklagten nachgewiesenen Artikel in den Jahren 2011 bis 2013 und dem Schluss der letzten Tatsachenverhandlung im August 2018. Die zweite Variante beruht auf dem schon im Auslistungsbegehren selbst liegenden Widerspruch des Klägers gegen die Datenverarbeitung durch die Beklagte. Mit der dritten Variante nimmt der Kläger die besondere Sensibilität seiner in den verlinkten Artikeln enthaltenen, von der Beklagten vorübergehend gespeicherten und über den Nachweis in ihren Ergebnislisten zugänglich

gemachten Gesundheitsdaten in den Blick, deren Verarbeitung nach Art. 9 Abs. 1 DS-GVO grundsätzlich untersagt ist.

b) Eine binnendifferenzierte Prüfung der genannten Anspruchsvarianten ist hier gleichwohl nicht geboten. Art. 17 Abs. 1 DS-GVO gilt insgesamt nicht, soweit die Datenverarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist (Art. 17 Abs. 3 Buchst. a DS-GVO). Dieser Umstand ist Ausdruck der Tatsache, dass das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht ist, sondern, wie im vierten Erwägungsgrund der Datenschutz-Grundverordnung ausgeführt, im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss (EuGH, Urteil vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3506 Rn. 57). Diese Grundrechtsabwägung ist auf der Grundlage aller relevanten Umstände des Einzelfalles und unter Berücksichtigung der Schwere des Eingriffs in die Grundrechte der betroffenen Person einerseits, der Grundrechte der Beklagten, der Interessen ihrer Nutzer und der Öffentlichkeit sowie der Grundrechte der Anbieter der in den beanstandeten Ergebnislinks nachgewiesenen Inhalte andererseits umfassend vorzunehmen (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3506 ff. Rn. 59, 68 f., 77; vom 29. Juli 2019 – Rs. C-516/17, AfP 2019, 424, 430 ff. Rn. 57 f., 72, 81; vom 14. Februar 2019 – Rs. C-345/17, NJW 2019, 2451, 2455 Rn. 65 f.; EGMR, NJW 2020, 295, 296 f. Rn. 89 ff., NJW 2017, 2091, 2093 Rn. 56 f.; BVerfG, NJW 2020, 314, 322 Rn. 96 ff., 120 – Recht auf Vergessen II).

Im Hinblick auf diese in rechtlicher wie tatsächlicher Hinsicht gebotene umfassende Prüfung muss die Abwägung jeweils zu demselben Ergebnis führen unabhängig davon, ob der Abwägungsvorgang seinen Ausgangspunkt in der Frage nimmt, ob die Verarbeitung der Daten allgemein zur Wahrung der berechtigten Interessen der Beklagten oder eines Dritten erforderlich war (Art. 6 Abs. 1 Buchst. f DS-GVO), ob die Verarbeitung speziell der Gesundheitsdaten des Klägers aus Gründen eines erheblichen öffentlichen Interesses erforderlich war (Art. 9 Abs. 2 Buchst. g DS-GVO), oder ob die Beklagte zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten des Klägers als der betroffenen Person überwiegen (Art. 21 Abs. 1 Satz 2 DS-GVO). Geboten ist daher eine einheitliche Gesamtabwägung der widerstreitenden Grundrechte, die alle nach den Umständen des Streitfalles aufgeworfenen Einzelaspekte berücksichtigt (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3506 f. Rn. 59, 66; vom 13. Mai 2014 – Rs. C-131/12, NJW 2014, 2257, 2262 Rn. 76).

c) Nach der Rechtsprechung des Bundesverfassungsgerichts sind in dem Bereich der unionsrechtlich vollständig vereinheitlichten Regelungen nicht die Grundrechte des Grundgesetzes, sondern allein die Unionsgrundrechte maßgeblich. Der Streitgegenständliche Auslistungsanspruch ist nach dem unionsweit abschließend vereinheitlichten Datenschutzrecht zu beurteilen (BVerfG, NJW 2020, 314, 316 Rn. 34 – Recht auf Vergessen II; im Unterschied dazu für Regelungsbereiche, in denen die Datenschutz-Grundverordnung den Mitgliedstaaten einen Beurteilungsspielraum einräumt: BVerfG, NJW 2020, 300, 302 ff. Rn. 51, 74 – Recht auf Vergessen I). Maßstab der konkretisierenden Anwendung von Art. 17 Abs. 3 Buchst. a DS-GVO durch den Senat ist daher die Charta der Grundrechte der Europäischen Union (vgl. BVerfG, NJW 2020, 314, 316 Rn. 42, 46 – Recht auf Vergessen II). Wie die Grundrechte des Grundgesetzes gewährleisten auch die Grundrechte der Charta Schutz nicht nur im Staat-Bürger-Verhältnis, sondern auch in privatrechtlichen

Streitigkeiten. Eine Lehre der „mittelbaren Drittwirkung“, wie sie das deutsche Recht kennt, wird der Auslegung des Unionsrechts dabei zwar nicht zugrunde gelegt. Im Ergebnis kommt den Unionsgrundrechten für das Verhältnis zwischen Privaten jedoch eine ähnliche Wirkung zu. Die Grundrechte der Charta können einzelfallbezogen in das Privatrecht hineinwirken (BVerfG, NJW 2020, 314, 322 Rn. 96 f. – Recht auf Vergessen II).

d) Auf Seiten des Klägers sind die Grundrechte auf Achtung des Privat- und Familienlebens aus Art. 7 GRCh und auf Schutz personenbezogener Daten aus Art. 8 GRCh einzustellen.

Art. 7 GRCh begründet das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation, Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Eine Entsprechung haben diese Garantien in Art. 8 EMRK, der seinerseits das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz – und dabei insbesondere auch vor der Verarbeitung personenbezogener Daten – schützt (vgl. Art. 52 Abs. 3 GRCh). Die Gewährleistungen der Art. 7 und Art. 8 GRCh sind dabei eng aufeinander bezogen. Jedenfalls soweit es um die Verarbeitung personenbezogener Daten geht, bilden diese beiden Grundrechte eine einheitliche Schutzverbürgung. Das gilt insbesondere für den Schutz Betroffener vor Nachweisen einer Suchmaschine (BVerfG, aaO, Rn. 98 f. mwN).

Art. 7, Art. 8 GRCh schützen vor der Verarbeitung personenbezogener Daten und verlangen die „Achtung des Privatlebens“. Unter personenbezogenen Daten werden dabei alle Informationen verstanden, die eine bestimmte oder bestimmbare natürliche Person betreffen. Demnach ist das Recht auf Achtung des Privatlebens nicht eng zu verstehen und beschränkt sich insbesondere nicht auf höchstpersönliche oder besonders sensible Sachverhalte. Insbesondere wird die geschäftliche und berufliche Tätigkeit hiervon nicht ausgeschlossen (BVerfG, aaO, Rn. 100 mwN).

e) Auf Seiten der beklagten Suchmaschinenverantwortlichen ist ihr Recht auf unternehmerische Freiheit aus Art. 16 GRCh einzustellen (aa). Demgegenüber kann sie sich für die Verbreitung von Suchnachweisen nicht auf Art. 11 GRCh berufen (bb). Einzustellen sind jedoch die von einem solchen Rechtsstreit möglicherweise unmittelbar betroffenen Grundrechte Dritter und damit vorliegend die Meinungsfreiheit der Inhalteanbieter (cc). Zu berücksichtigen sind darüber hinaus die Informationsinteressen der Nutzer (dd) (BVerfG, aaO, Rn. 102).

aa) Die unternehmerische Freiheit gewährleistet die Verfolgung wirtschaftlicher Interessen durch das Angebot von Waren und Dienstleistungen. Der durch Art. 16 GRCh gewährte Schutz umfasst die Freiheit, eine Wirtschafts- oder Geschäftstätigkeit auszuüben, die Vertragsfreiheit und den freien Wettbewerb. Hierzu gehört auch das Angebot von Suchdiensten. Die beklagte Suchmaschinenverantwortliche fällt auch in den persönlichen Schutzbereich des Art. 16 GRCh. Die Unionsgrundrechte schützen grundsätzlich nicht nur natürliche, sondern auch juristische Personen. Für die unternehmerische Freiheit folgt das bereits aus dem Wortlaut, der auf „Unternehmen“ abstellt, die typischerweise als juristische Personen organisiert sind. Dem Schutz des Art. 16 GRCh steht auch nicht entgegen, dass die Beklagte eine juristische Person mit Sitz außerhalb der Europäischen Union ist. Die Grundrechte der Grundrechtecharta gelten grundsätzlich für Inländer und Ausländer gleichermaßen und machen insoweit auch für juristische Personen keinen Unterschied (BVerfG, aaO, Rn. 103 f. mwN).

bb) Hingegen kann sich die beklagte Suchmaschinenverantwortliche für ihre Tätigkeit nicht auf die Freiheit der Meinungsäußerung aus Art. 11 GRCh berufen. Zwar sind die von ihr angebotenen Suchdienste und die von ihr hierfür verwendeten Mittel

zur Aufbereitung der Suchergebnisse nicht inhaltsneutral, sondern können auf die Meinungsbildung der Nutzer erheblichen Einfluss ausüben. Jedoch bezwecken diese Dienste nicht die Verbreitung bestimmter Meinungen (BVerfG, aaO, Rn. 105). Darauf beruft sich auch die Beklagte selbst nicht.

cc) In die Abwägung zwischen Betroffenen und Suchmaschinenverantwortlichen sind allerdings auch die Grundrechte der Inhalteanbieter einzustellen, um deren Veröffentlichung es geht.

(1) Soweit in einem Rechtsstreit zwischen einem Betroffenen und dem Suchmaschinenverantwortlichen über eine Auslistung notwendig zugleich über eine in der Auslistung liegende Einschränkung von Grundrechten Dritter mitentschieden wird, sind auch diese in die Prüfung einzubeziehen. Die Rechtmäßigkeit der Entscheidung gegenüber Dritten gehört dann zu den objektiven Rechtmäßigkeitsvoraussetzungen von Einschränkungen der Unternehmensfreiheit, die unter Berufung auf das eigene Grundrecht des Art. 16 GRCh geltend gemacht werden können. Hierin liegt nicht eine Geltendmachung unmittelbar der Grundrechte Dritter. Einem Suchmaschinenverantwortlichen darf danach nichts aufgegeben werden, was die Grundrechte Dritter verletzt (BVerfG, aaO, Rn. 107).

(2) In dem Rechtsstreit, ob einem Suchmaschinenverantwortlichen die Bereitstellung bestimmter Suchnachweise zu untersagen ist, wird die Frage einer möglichen Grundrechtsverletzung des Art. 11 GRCh gegenüber dem Inhalteanbieter als Äußerndem oftmals mit berührt. Dabei kommt es nicht auf die hier nicht zu entscheidende Frage an, ob oder wie weit ein Inhalteanbieter gegenüber einem Suchmaschinenbetreiber Anspruch auf Verbreitung seiner Inhalte haben kann. Denn es geht in dieser Konstellation nicht darum, ob der Suchmaschinenverantwortliche zu einem Nachweis verpflichtet werden kann, sondern ob ihm gegen seinen Willen verboten werden kann, die von einem Inhalteanbieter bereitgestellten Beiträge zu verbreiten. In einem solchen Verbot kann zugleich eine eigenständige Einschränkung der Freiheit des Inhalteanbieters als Äußerndem aus Art. 11 GRCh liegen. Denn diesem wird dadurch ein bereitstehender Dienstleister genommen und so in Teilen zugleich ein wichtiges Medium für die Verbreitung seiner Berichte (BVerfG, aaO, Rn. 108).

Soweit über das Verbot gegenüber dem Suchmaschinenverantwortlichen in Ansehung des von dem Inhalteanbieter verantworteten konkreten Inhalts der streitigen Seiten zu entscheiden ist, ist die Einwirkung auf diesen auch nicht etwa ein bloßer Reflex einer Anordnung gegenüber dem Suchmaschinenverantwortlichen. Vielmehr knüpft die Entscheidung unmittelbar an die Äußerung und an den Gebrauch der Meinungsfreiheit an. Es geht in der Entscheidung gezielt darum, die Verbreitung des Beitrags wegen seines Inhalts zu beschränken. In dieser Konstellation kann über den Antrag eines Betroffenen auf Unterlassung des Bereitstellens von Suchnachweisen gegenüber einem Suchmaschinenverantwortlichen nicht ohne Berücksichtigung der Frage entschieden werden, ob und wie weit der Inhalteanbieter gegenüber den Betroffenen nach Art. 11 GRCh zur Verbreitung der Information berechtigt ist (BVerfG, aaO, Rn. 109 mwN).

dd) In die Abwägung sind ebenfalls die Zugangsinteressen der Internetnutzer einzustellen. Zu berücksichtigen ist das Interesse einer breiten Öffentlichkeit am Zugang zu Information als Ausdruck des in Art. 11 GRCh verbürgten Rechts auf freie Information. Rechnung zu tragen ist dabei auch der Rolle, die der Presse in einer demokratischen Gesellschaft hierbei zukommt. Insoweit stehen allerdings nicht individuelle Rechte der Nutzerinnen und Nutzer aus Art. 11 GRCh auf Informationszugang zu der konkret betroffenen Internetseite in Frage, sondern

die Informationsfreiheit als im Wege der Abwägung zu berücksichtigendes Prinzip, dem bei der Einschränkung des Art. 16 GRCh Rechnung zu tragen ist (vgl. EuGH, Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3506 ff. Rn. 59, 68 f., 77; vom 29. Juli 2019 – Rs. C-516/17, AfP 2019, 424, 430 ff. Rn. 57 f., 72, 81; EGMR, NJW 2020, 295, 296 f. Rn. 89 ff., NJW 2017, 2091, 2093 Rn. 56; BVerfG, aaO, Rn. 110 mwN).

f) Grundlage der Abwägung ist die Würdigung des Vorgehens des Suchdienstes der Beklagten als für sich stehender Akt der Datenverarbeitung, der folglich auch hinsichtlich der damit verbundenen Grundrechtseinschränkungen eigenständig zu beurteilen ist. Insbesondere geht die Frage seiner Rechtmäßigkeit nicht in der Frage der Rechtmäßigkeit der Veröffentlichung des Beitrags seitens der Inhalteanbieter auf. Da die betroffenen Rechte, Interessen und Belastungen bei einem Vorgehen des Betroffenen gegen den Suchmaschinenverantwortlichen andere sein können als bei einem Vorgehen gegenüber dem Inhalteanbieter (vgl. oben B I 4), bedarf es einer eigenen Abwägung (BVerfG, aaO, Rn. 112).

Die für die Grundrechtsabwägung erforderliche Unterscheidung zwischen den verschiedenen Datenverarbeitern stellt indes nicht in Frage, dass es hierbei Wechselwirkungen geben kann und für ein Unterlassungsbegehren gegenüber einem Suchmaschinenverantwortlichen unter Umständen auch die Situation des Betroffenen gegenüber dem Inhalteanbieter mit in den Blick genommen werden muss (BVerfG, aaO, Rn. 114). Soweit daher wie in der Regel im deutschen Recht (§§ 823, 1004 BGB analog) bei der Beurteilung der Rechtmäßigkeit der Verbreitung eines Berichts seitens des dem Medienprivileg unterfallenden Inhalteanbieters dessen Wirkung für den Betroffenen im Internet in der Abwägung mitzuberocksichtigen ist (vgl. Senatsurteil vom 18. Dezember 2018 – VI ZR 439/17, NJW 2019, 1881, 1883 f. Rn. 16 f., 20; BVerfG, NJW 2020, 300, 310 Rn. 101 ff., 114 ff. – Recht auf Vergessen I), muss regelmäßig die Entscheidung über die Rechtmäßigkeit solcher Verbreitung auch die Entscheidung gegenüber den Suchmaschinenverantwortlichen anleiten. Soweit ein Inhalteanbieter sowohl unter Berücksichtigung der Verbreitungsbedingungen im Internet (und damit zugleich der namensbezogenen Auffindbarkeit durch Suchmaschinen) als auch unter Berücksichtigung des Zeitfaktors im Verhältnis zu den Betroffenen zur Verbreitung eines Berichts berechtigt ist, kann für den Nachweis einer solchen Seite durch einen Suchmaschinenverantwortlichen diesbezüglich nichts anderes gelten (BVerfG, NJW 2020, 314, 325 Rn. 118 – Recht auf Vergessen II).

Unberührt bleibt hiervon, dass die Abwägung zwischen Betroffenen und Suchmaschinenverantwortlichen stets im Spannungsfeld der Zumutbarkeit möglicher Schutzmaßnahmen seitens des Suchmaschinenverantwortlichen und der Zumutbarkeit anderweitig zu erlangender Schutzmöglichkeiten seitens der jeweils Betroffenen steht und auch unter diesem Gesichtspunkt der Ausgang der Abwägung gegenüber verschiedenen Datenverarbeitern unterschiedlich ausfallen kann und gegebenenfalls muss. Dabei können auch Unterschiede zu beachten sein, die sich etwa aus der verschiedenen leichten Erreichbarkeit von Schutz ergeben oder die die Wirksamkeit von Schutzmaßnahmen betreffen (BVerfG, aaO, Rn. 119).

g) Im Rahmen der Abwägung ist zu berücksichtigen, dass das Internet ohne die Hilfestellung einer Suchmaschine aufgrund der nicht mehr überschaubaren Flut von Daten für den Einzelnen nicht sinnvoll nutzbar wäre. Letztlich ist damit die Nutzung des Internets insgesamt auf die Existenz und Verfügbarkeit von Suchmaschinen angewiesen, deren Geschäftsmodell daher von der Rechtsordnung gebilligt worden und gesellschaftlich er-

wünscht ist (vgl. Senatsurteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350, 361 f. Rn. 34). Auf der Kehrseite hat die Tätigkeit von Suchmaschinen maßgeblichen Anteil an der weltweiten Verbreitung personenbezogener Daten, da sie diese jedem Internetnutzer zugänglich macht, der eine Suche anhand des Namens der betroffenen Person durchführt, und zwar auch denjenigen, die die Webseite, auf der diese Daten veröffentlicht sind, sonst nicht gefunden hätten. Dies kann dazu führen, dass die Nutzer der Suchmaschine mit der Ergebnisliste einen strukturierten Überblick über die zur betreffenden Person im Internet zu findenden Informationen erhalten, anhand dessen sie ein mehr oder weniger detailliertes Profil der Person erstellen können (EuGH, Urteil vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3504 Rn. 36). Vor diesem Hintergrund ist das Gewicht allein der wirtschaftlichen Interessen des Suchmaschinenverantwortlichen grundsätzlich nicht hinreichend schwer, um den Schutzanspruch Betroffener zu beschränken. Demgegenüber haben das Informationsinteresse der Öffentlichkeit sowie vor allem die hier einzubeziehenden Grundrechte Dritter größeres Gewicht (BVerfG, aaO, Rn. 120).

Vorliegend ist die Meinungsfreiheit der durch die Entscheidung belasteten Inhalteanbieter als unmittelbar mitbetroffenes Grundrecht – und nicht nur als zu berücksichtigendes Interesse – in die Abwägung einzubeziehen. Daher gilt hier keine Vermutung eines Vorrangs des Schutzes des Persönlichkeitsrechts, sondern sind die sich gegenüberstehenden Grundrechte gleichberechtigt miteinander abzuwägen. Ebenso wenig wie Einzelne gegenüber den Medien einseitig darüber bestimmen können, welche Informationen im Rahmen der öffentlichen Kommunikation über sie verbreitet werden, haben sie eine solche Bestimmungsmacht gegenüber den Suchmaschinenbetreibern (BVerfG, aaO, Rn. 121). Auf der anderen Seite folgt aus dem Gebot einer gleichberechtigten Abwägung der sich gegenüberstehenden Grundrechte aber auch, dass der Verantwortliche einer Suchmaschine nicht erst dann tätig werden muss, wenn er von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung des Betroffenen Kenntnis erlangt. An seiner noch zur Rechtslage vor Inkrafttreten der Datenschutz-Grundverordnung entwickelten gegenteiligen Rechtsprechung (Senatsurteil vom 27. Februar 2018 – VI ZR 489/16, BGHZ 217, 350, 363 Rn. 36 i.V.m. 370 f. Rn. 52) hält der Senat insoweit nicht fest.

Wenn sich Betroffene – wie hier – nicht schon gegen die Ermöglichung namensbezogener Suchabfragen überhaupt, sondern gegen deren Wirkung hinsichtlich einzelner sie nachteilig betreffender Beiträge wenden, kommt es für die Gewichtung ihrer Grundrechtseinschränkung maßgeblich auf die Wirkung ihrer Verbreitung an. Bezugspunkte sind dabei die Wirkungen der Verbreitung des streitbefangenen Beitrags für die Persönlichkeitsentfaltung, wie sie sich spezifisch aus den Suchnachweisen ergeben, insbesondere auch unter Berücksichtigung der Möglichkeit namensbezogener Suchabfragen. Hierfür reicht nicht eine Würdigung der Berichterstattung in ihrem ursprünglichen Kontext, sondern ist auch die leichte und fortdauernde Zugänglichkeit der Informationen durch die Suchmaschine in Rechnung zu stellen. Insbesondere ist auch der Bedeutung der Zeit zwischen der ursprünglichen Veröffentlichung und deren späterem Nachweis Rechnung zu tragen (BVerfG, aaO, Rn. 122 mwN).

h) Nach diesen Grundsätzen haben die Grundrechte des Klägers hinter den Grundrechten der Beklagten und den in deren Waagschale zu legenden Interessen ihrer Nutzer, der Öffentlichkeit und der für die verlinkten Zeitungsartikel verantwortlichen Presseorgane zurückzutreten.

aa) Die Revision stellt die Wahrheitsgemäßheit der in den verlinkten Presseartikeln geschilderten Tatsachen sowie die ursprüngliche Rechtmäßigkeit dieser Berichterstattung insgesamt nicht in Frage. Anhaltspunkte für deren Rechtswidrigkeit sind auch im Übrigen nicht ersichtlich. Es bedarf daher im Streitfall keiner Entscheidung, wie einer etwaigen Unaufklärbarkeit oder zumindest Ungewissheit über den Wahrheitsgehalt von Drittäußerungen, die in der Suchergebnisliste ausgewiesen werden, im Rahmen der Abwägung Rechnung zu tragen wäre (vgl. hierzu den Vorlagebeschluss des Senats nach Art. 267 AEUV vom 27. Juli 2020 – VI ZR 476/18).

(1) Bei den von der Beklagten nachgewiesenen PresseArt.n handelt es sich um journalistisch gestaltete Berichte der Tagespresse über die wirtschaftlichen Schwierigkeiten des bundesweit zweitgrößten Regionalverbandes des Arbeiter-Samariter-Bundes. Der Arbeiter-Samariter-Bund ist eine der größten und bekanntesten Hilfs- und Wohlfahrtsorganisationen in Deutschland, er finanziert und betreibt Dienste und Einrichtungen insbesondere der Altenpflege, der Kinderbetreuung, der Notfallrettung sowie des Krankentransports. Allein der betroffene Regionalverband beschäftigt über 500 Mitarbeiter und hat über 35.000 Vereinsmitglieder. Die in den Art.n berichteten erheblichen finanziellen Schwierigkeiten des Regionalverbandes waren mit ihren möglichen Auswirkungen auf die Beschäftigten, aber vor allem auch auf die Kunden und Nutznießer der angebotenen Pflege-, Betreuungs- und Krankendienste von erheblichem öffentlichen Interesse; die Berechtigung des Berichterstattungsinteresses der Tagespresse steht daher im Ausgangspunkt außer Frage.

(2) Das berechtigte Berichterstattungsinteresse erstreckte sich unter den Umständen des Streitfalls ohne weiteres auch auf die Nennung der verantwortlichen Mitglieder der Geschäftsführung des Regionalverbandes und damit auch auf die namentliche Nennung des Klägers. Der Kläger war als damaliger Geschäftsführer des Regionalverbandes in herausgehobener Funktion für den Regionalverband tätig und in dieser zumindest auch für die finanzielle Lage dieses Verbandes (gesamt-)verantwortlich. Gegenstand der Berichterstattung war daher die berufliche Sphäre des Klägers, wobei der Senat nicht verkennt, dass die Kommunikationsbedingungen im Internet, insbesondere die Auffindbarkeit und Zusammenführung von Informationen mittels namensbezogener Suchabfragen, dazu führen, dass für deren Auswirkungen zwischen Privat- und Sozialsphäre kaum mehr zu unterscheiden ist (vgl. BVerfG, NJW 2020, 314, 326 Rn. 128 – Recht auf Vergessen II).

An der Berechtigung des Berichterstattungsinteresses ändert sich im Ausgangspunkt auch nichts durch den Umstand, dass über die Krankmeldung des Klägers sowie seine laufende Reha-Maßnahme und krankheitsbedingte Unerreichbarkeit berichtet wurde. Die Abwesenheit des Geschäftsführers eines regional bedeutenden Arbeitgebers und Anbieters von Pflege- und Krankendiensten in einer Krise und deren Gründe sind von hohem öffentlichen Interesse, die berichteten bloßen Umstände der – nicht näher ausgeführten – Krankschreibung und laufenden Reha-Maßnahme des Klägers dagegen von geringem Gewicht (vgl. zur Abwägungszugänglichkeit einer Presseberichterstattung über die gesundheitliche Situation einer im Fokus des öffentlichen Interesses stehenden Person Senatsurteil vom 29. November 2016 – VI ZR 382/15, NJW 2017, 1550, 1552 Rn. 20 ff.). Im Ergebnis ist die Berichterstattung als solche daher vom Kläger hinzunehmen. Dies gilt, zumal die Mitteilung der Umstände auch entlastende Wirkung haben kann, weil sie Spekulationen entgegentritt, die Abwesenheit des Geschäftsführers sei auf ar-

beitsrechtliche Konsequenzen wegen eines etwaigen Fehlverhaltens zurückzuführen (vgl. insbesondere PresseArt. URL Nr. 3).

bb) Die von der Beklagten nachgewiesenen Presseartikel dürfen von den hierfür verantwortlichen Presseorganen auch unter Berücksichtigung des Zeitfaktors noch im Internet zum Abruf bereitgestellt – und damit zugleich durch namensbezogene Abfragen über Suchmaschinen auffindbar gehalten – werden.

(1) Der Zeitablauf kann sowohl das Gewicht des öffentlichen Interesses als auch das der Grundrechtsbeeinträchtigung modifizieren. Welche Bedeutung dem Verstreichen von Zeit für die spätere Geltendmachung eines Schutzanspruchs gegenüber einer ursprünglich rechtmäßigen Veröffentlichung zukommt, lässt sich nur unter Erfassung des konkreten Schutzbedarfs des Betroffenen in Abwägung mit den entgegenstehenden Grundrechten und dabei zugleich der öffentlichen Bedeutung der fraglichen Informationen beurteilen (BVerfG, NJW 2020, 300, 311 Rn. 120 – Recht auf Vergessen I).

(a) Ein maßgeblicher Gesichtspunkt liegt hierfür zunächst in Wirkung und Gegenstand der Berichterstattung. Je stärker die Verbreitung zurückliegender Berichte das Privatleben und die Entfaltungsmöglichkeiten der Person als ganze beeinträchtigen, desto größeres Gewicht kann einem Schutzanspruch zukommen. Dies steht zugleich in einer Wechselwirkung mit Gegenstand und Anlass der Berichterstattung: Soweit Berichte sich mit dem Verhalten einer Person in der Sozialsphäre befassen, kann ihrer Zugänglichkeit auch langfristig eher Gewicht zukommen, als wenn sie allein von privatem, bewusst nicht vor anderen gezeigtem Verhalten oder Fehlverhalten handeln. Maßgeblich ist insoweit nicht zuletzt auch das öffentliche Interesse an der fortwährenden Erreichbarkeit der Informationen (BVerfG, aaO, Rn. 121).

(b) Bedeutung kommt auch der Frage zu, wieweit die berichteten Ereignisse in einer Folge weiterer hiermit einen Zusammenhang bildender Vorkommnisse stehen. Zurückliegende Ereignisse können eher fortdauernde Bedeutung behalten, wenn sie eingebunden sind in eine Abfolge etwa gesellschaftspolitischer oder kommerzieller Aktivitäten oder durch nachfolgende Begebenheiten neue Relevanz erhalten, als wenn sie für sich allein stehen.

Entsprechend kann zu berücksichtigen sein, ob und wieweit Betroffene in der Zwischenzeit dazu beigetragen haben, das Interesse an den Ereignissen oder ihrer Person wachzuhalten. Hat eine Person die Öffentlichkeit gesucht und ohne Not Aufmerksamkeit erzeugt, die das Interesse an den ursprünglichen Berichten reaktualisiert, kann ihr Interesse, von einer Konfrontation mit der Ausgangsberichterstattung verschont zu bleiben, entsprechend geringer zu gewichten sein. Insoweit gehört zu der Chance auf ein Vergessen auch ein Verhalten, das von einem „Vergessenwerdenwollen“ getragen ist (BVerfG, aaO, Rn. 122 f.).

(c) Dagegen ist das Kriterium der "Zweckerreichung" in Bezug auf die Verbreitung von Beiträgen, die der öffentlichen Meinungsbildung dienen, in der Regel kein geeignetes Kriterium, um die Dauer ihrer rechtmäßigen Verbreitung zu bestimmen. Denn bei solchen Beiträgen stützt sich die Verbreitung nicht auf eine spezifische Erlaubnis für einen bestimmten Zweck, sondern wurzelt in den Kommunikationsfreiheiten und dem sich hieraus ergebenden Recht, Zwecke der Kommunikation selbst setzen, ändern oder in Bezug auf das weitere Kommunikationsgeschehen auch offenlassen zu können (BVerfG, NJW 2020, 314, 327 Rn. 132 – Recht auf Vergessen II).

(d) Für das Gewicht der Beeinträchtigung kommt es auch darauf an, in welcher Einbindung die Informationen unter den konkreten Umständen im Netz kommuniziert werden. So macht es einen Unterschied, ob über ein lang zurückliegendes Ereignis

etwa in Form eines auf Skandalisierung hin angelegten personenbezogenen Blogs berichtet wird oder im Rahmen eines Bewertungsportals, bei dem sich die Aussagekraft älterer Informationen durch neuere Eintragungen relativiert und damit unter Umständen auch lange zurückliegende Informationen noch vorgehalten werden dürfen. Es kommt insoweit auf die tatsächliche Belastung für die Betroffenen an.

Die Belastung der Betroffenen bestimmt sich dabei nicht abstrakt aus der Tatsache, dass eine Information im Netz irgendwie zugänglich ist, sondern hängt auch daran, wie weit sie hierdurch tatsächlich breitenwirksam gestreut wird. Von Bedeutung kann dabei auch sein, wieweit sie von Suchmaschinen prioritär kommuniziert wird. Da Kommunikation und Kommunikationsbedingungen des Internets freilich individuell verschieden und volatil sind, gibt es insoweit kein objektives Maß. Jedoch stellt sich auch im Netz die Bedeutung von Informationen erst aus Kommunikationszusammenhängen her und erhalten diese unterschiedliche Verbreitung und Sichtbarkeit. Maßgeblich ist insoweit eine Beurteilung der gesamten Belastungswirkung aus Sicht des Betroffenen zum Zeitpunkt der Entscheidung über sein Schutzbegehren – die dann in die Abwägung mit den Kommunikationsfreiheiten einzustellen ist (BVerfG, NJW 2020, 300, 311 Rn. 124 f. – Recht auf Vergessen I).

(2) Nach diesen Grundsätzen überwiegt auch unter Berücksichtigung der Kommunikationsbedingungen des Internets jedenfalls zum gegenwärtigen Zeitpunkt das fortdauernde öffentliche Interesse an der Berichterstattung das Persönlichkeitsrecht des Klägers noch.

(a) Bei den geschilderten wirtschaftlichen Schwierigkeiten des Regionalverbandes des Arbeiter-Samariter-Bundes handelte es sich nicht um ein singuläres, für sich allein stehendes Ereignis, sondern um eine Fehlentwicklung, die mehrjährige Sanierungsbemühungen nach sich zog und langfristige Einsparungen bis hin zu Entlassungen einzelner Mitarbeiter und der deutlichen Erhöhung des Betreuungsschlüssels in den Kindertagesstätten erforderlich machte. Entsprechend ist auch die Rolle der insoweit Verantwortlichen wie dem Kläger als damaligem Geschäftsführer nicht nur von vorübergehendem Interesse, sondern zeitgeschichtlich bedeutsam und fortwirkend relevant. Die seit den berichteten Ereignissen vergangene Zeitspanne von zuletzt gut sieben Jahren ist demgegenüber noch nicht derart groß, als dass sie das Interesse an der niedrighen Erreichbarkeit der Informationen – auch über die namensbezogene Suche mittels einer Suchmaschine – in den Hintergrund treten ließe. Die der Berichterstattung inmitten stehenden Ereignisse haben das Potential der fortwirkenden Relevanz; darüber hinaus besteht ein zeitgeschichtlich anerkanntes Interesse an ihrer Recherche. Im Übrigen ist zu beachten, dass der Kläger keinen Anspruch darauf hat, öffentlich so wahrgenommen zu werden, wie es den eigenen Wünschen entspricht (vgl. BVerfG, aaO, Rn. 107; BVerfG [Kammer], NJW 2020, 1793, 1794 Rn. 9).

(b) Dies gilt auch angesichts des Umstands der über den Kläger berichteten krankheitsbedingten Abwesenheit. Die unspezifische Information, der Kläger sei krank und unterziehe sich derzeit einer Reha-Maßnahme, diene in erster Linie der Erläuterung, warum der Kläger als Geschäftsführer für seinen Arbeitgeber in der Krise nicht greifbar war. Sie erlaubt keinerlei Rückschlüsse auf die Art der Krankheit des Klägers und entfaltet daher auch unter Berücksichtigung des Zeitfaktors keine entscheidende Mehrbelastung für den Kläger, sondern kann im Gegenteil als krankheitsbedingte Entschuldigung für seine Abwesenheit zur Unzeit sogar auch entlastend verstanden werden.

cc) Die Grundrechtsbeeinträchtigung des Klägers erhält auch im Streitverhältnis zur Beklagten kein entscheidend anderes Gewicht.

(1) Die Beklagte weist die fraglichen Presseartikel auf eine entsprechende Suchanfrage unkommentiert in ihren Ergebnislisten nach (vgl. BVerfG, NJW 2020, 300, 311 Rn. 124 – Recht auf Vergessen I). Die streitgegenständlichen Nachweise sind ausweislich der vom Berufungsgericht in Bezug genommenen Suchanfragen nicht auf die isolierte Namenssuche, sondern jeweils auf eine mit einer Ortsangabe kombinierte Namenssuche erfolgt, die die Kenntnis der bestehenden Name-Ort-Verbindung durch den Nutzer bereits voraussetzt. Schließlich werden die angegriffenen Ergebnislinks durch den Nachweis zahlreicher weiterer, teilweise vorrangig platzierter, im Netz befindlicher Informationen relativiert (vgl. BVerfG, aaO, Rn. 125; BVerfG [Kammer], NJW 2020, 1793, 1795 Rn. 16).

(2) Entgegen der Auffassung der Revision führen weder der Umstand, dass es sich bei den von der Beklagten verarbeiteten personenbezogenen Daten des Klägers teilweise um Gesundheitsdaten (Art. 9 Abs. 1, Art. 4 Nr. 15 DS-GVO) handelt, noch der Zeitablauf seit dem erstmaligen Erscheinen der verlinkten Presseartikel zu einem grundsätzlichen Vorrang der Auslistungsinteressen des Klägers im Sinne eines Regel-Ausnahme-Mechanismus. Beiden Aspekten kommt zwar im Rahmen der Gesamtabwägung der widerstreitenden Rechte und Interessen auf Seiten des Klägers Bedeutung zu. Ein schematisches Vorrang- oder Regel-Ausnahme-Verhältnis des Persönlichkeitsrechts des Klägers im Verhältnis zu den Rechten der Beklagten und den auf deren Seite zu berücksichtigenden Rechten und Interessen der Inhabanten, der Öffentlichkeit und der Nutzer der Suchmaschinen lässt sich aus ihnen jedoch nicht ableiten, zu-mal die enthaltenen Gesundheitsdaten völlig unspezifischer Natur sind. Aufgrund der entscheidungsanleitenden Bedeutung der wie oben ausgeführt nach den Umständen des Streitfalles im Verhältnis zu den Inhabanten vorliegenden Rechtmäßigkeit der Berichterstattung und ihres Vorhaltens kann auch im Verhältnis zur Beklagten als verantwortlicher Stelle für die Verarbeitung von Daten in dem Index des Internetsuchdienstes kein grundsätzliches Vorrangverhältnis angenommen werden; die widerstreitenden Grundrechte stehen sich vielmehr auch insoweit im Ausgangspunkt gleichberechtigt gegenüber (s. oben B I 6 f und g; BVerfG, NJW 2020, 314, 325 f. Rn. 118, 121 – Recht auf Vergessen II).

Im Hinblick auf das Kriterium des Zeitablaufs ist ergänzend darauf hinzuweisen, dass sich auch dieses selbst einer schematischen Betrachtung verschließt (vgl. BVerfG, NJW 2020, 300, 311 Rn. 126 – Recht auf Vergessen I), also schon nicht klar wäre, zu welchem konkreten Zeitpunkt eine zunächst offen vorzunehmende Gesamtabwägung in ein Vorrangverhältnis mit Regel-Ausnahme-Mechanismus umschlagen sollte.

7. Ein Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union (Art. 267 Abs. 3 AEUV) wegen der Auslegung des Art. 17 DS-GVO ist entgegen der Ansicht der Revision nicht veranlasst. Ein Vorabentscheidungsersuchen ist erforderlich, wenn sich eine entscheidungserhebliche und der einheitlichen Auslegung bedürftige Frage des Unionsrechts stellt. Dies ist hier nicht der Fall. Die Rechtslage ist durch die zwischenzeitliche Rechtsprechung des Europäischen Gerichtshofs (Urteile vom 24. September 2019 – Rs. C-136/17, NJW 2019, 3503, 3504 ff. Rn. 68, 77 i.V.m. 33; Rs. C-507/17, NJW 2019, 3499, 3500 ff. Rn. 44 ff., 67 i.V.m. 41) hinreichend geklärt (vgl. BVerfG, NJW 2020, 314, 327 f. Rn. 137 ff. – Recht auf Vergessen II).

Im Hinblick auf den Anwendungsvorrang des vorliegend unionsweit abschließend vereinheitlichten Datenschutzrechts (vgl. BVerfG, aaO, Rn. 34, 41) und die bei Prüfung eines Auslistungsbe-

gehrens nach Art. 17 DS-GVO vorzunehmende umfassende Grundrechtsabwägung kann der Kläger seinen Anspruch auch nicht auf Vorschriften des nationalen deutschen Rechts stützen (vgl. Nolte/Werkmeister, in: Gola, DS-GVO, 2. Aufl., Art. 17 Rn. 73; Herbst, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl., Art. 17 Rn. 89; Kamann/Braun, in: Ehmann/Selmayr, DS-GVO, 2. Aufl., Art. 17 Rn. 75).

Benachteiligung wegen der Religion bei Kopftuchverbot einer Lehrerin (Ls)

(Bundesarbeitsgericht, Urteil vom 27. August 2020 – 8 AZR 62/19 –)

1. Eine Regelung, die – wie § 2 Berliner Neutralitätsgesetz – das Tragen eines sog. islamischen Kopftuchs durch eine Lehrkraft im Dienst ohne Weiteres, d.h. schon wegen der bloß abstrakten Eignung zur Begründung einer Gefahr für den Schulfrieden oder die staatliche Neutralität in einer öffentlichen bekenntnisoffenen Gemeinschaftsschule verbietet, führt zu einem unverhältnismäßigen Eingriff in die Religionsfreiheit nach Art. 4 GG, sofern das Tragen des Kopftuchs nachvollziehbar auf ein als verpflichtend verstandenes religiöses Gebot zurückzuführen ist.
2. § 2 Berliner Neutralitätsgesetz ist daher verfassungskonform dahin auszulegen, dass das Verbot des Tragens eines sog. islamischen Kopftuchs nur im Fall einer konkreten Gefahr für den Schulfrieden oder die staatliche Neutralität gilt.
3. Da das Land eine solche konkrete Gefahr für diese Schutzgüter indes nicht dargetan hat, ist nach § 15 Abs. 2 AGG wegen eines Verstoßes gegen das Benachteiligungsverbot des AGG die Zahlung einer Entschädigung iHv. 5.159,88 Euro angemessen.

Anspruch des Betriebsrats auf Einsicht und Auswertung von Entgeltlisten nach EntgTranspG

(Bundesarbeitsgericht, Beschluss vom 28. Juli 2020 – 1 ABR 6/19 –)

Das entgeltlistenbezogene Einsichts- und Auswertungsrecht nach § 13 Abs. 2 Satz 1 EntgTranspG ist an die Zuständigkeit des Betriebsrats für die Beantwortung individueller Auskunftsverlangen nach § 10 Abs. 1 EntgTranspG gebunden. Es besteht nicht, wenn der Arbeitgeber die Erfüllung der Auskunftspflicht berechtigterweise an sich gezogen hat.

Sachverhalt:

A. Die Beteiligten streiten über die Übergabe von Bruttoentgeltlisten. Die Zentralverwaltung der Arbeitgeberin ist ein Betrieb mit mehr als 4.000 Beschäftigten. Dort ist ein 27-köpfiger Betriebsrat gewählt. Dieser hat einen Betriebsausschuss gebildet.

Nach dem Inkrafttreten des Gesetzes zur Förderung der Entgelttransparenz zwischen Frauen und Männern (Entgelttransparenzgesetz – EntgTranspG –) hat die Arbeitgeberin von der dort vorgesehenen Möglichkeit Gebrauch gemacht, die Verpflichtung zur Erfüllung individueller Auskunftsverlangen von Beschäftigten generell zu übernehmen. Sie unterrichtet den Betriebsrat regelmäßig über konkrete Auskunftsverlangen und deren Beantwortung. In diesem Zusammenhang gewährt sie Einblick in die Listen über die Bruttolöhne und -gehälter, welche nach Geschlecht aufgeschlüsselt die Entgeltbestandteile einschließlich übertariflicher Zulagen und individuell ausgehandelter Zahlungen enthalten. Die Listen können entweder auf einem zur Verfügung gestellten Rechner als PDF-Datei oder als Ausdruck eingesehen werden. Es besteht die Möglichkeit, sich Notizen zu machen und Berechnungen anzustellen.

Der Betriebsrat hat in dem von ihm eingeleiteten Verfahren die Übergabe dieser Entgeltlisten an den Betriebsausschuss geltend gemacht. § 13 Abs. 1 Satz 1 EntgTranspG weist ihm die Aufgabe zu, die Durchsetzung der Entgeltgleichheit von Frauen und Männern im Betrieb zu fördern. Dazu sei der Betriebsausschuss nach § 13 Abs. 2 Satz 1 EntgTranspG berechtigt, die Bruttoentgeltlisten einzusehen und auszuwerten. Das Auswertungsrecht umfasse auch die Herausgabe der Listen in bearbeitungsfähigen Dateiformaten, hilfsweise in einer anderen auswertbaren (Papier-)Form.

Die Arbeitgeberin hat beantragt, die Anträge abzuweisen. Sie hat die Auffassung vertreten, die Einsichts- und Auswertungsbeziehung nach § 13 Abs. 2 Satz 1 EntgTranspG erweitere nicht den allgemeinen betriebsverfassungsrechtlichen Anspruch aus § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG um ein Recht auf Überlassung der Listen über die Bruttolöhne und -gehälter.

Das Arbeitsgericht hat die Anträge abgewiesen. Das Landesarbeitsgericht hat die Beschwerde des Betriebsrats zurückgewiesen. Mit seiner Rechtsbeschwerde verfolgt der Betriebsrat sein Begehren weiter.

Aus den Gründen:

B. Die zulässige Rechtsbeschwerde ist unbegründet. Zu Recht haben die Vorinstanzen dem in der Rechtsbeschwerde noch anfallenden Begehren des Betriebsrats nicht entsprochen. Der zulässige Hauptantrag ist unbegründet. Der Hilfsantrag fällt nicht zur Entscheidung an.

I. Der hauptsächlich gestellte Antrag ist – entgegen der Ansicht der Arbeitgeberin – zulässig.

1. Er bedarf allerdings der Auslegung.

a) Der Betriebsrat bezieht die begehrte Übergabeverpflichtung nach ihrer sprachlichen Fassung auf Listen über Bruttoentgelte mit einem näher beschriebenen Inhalt. Damit sind die Listen bezeichnet, die von der Arbeitgeberin nach Maßgabe des § 13 Abs. 3 Satz 1 EntgTranspG aufbereitet werden und in die sie Einsicht gewährt. Es fehlt an jeglichem Anhaltspunkt, dass der Betriebsrat die Übergabe inhaltlich anderer – von der Arbeitgeberin noch herzustellender – Listen erstrebt.

b) Die Übergabe der bei der Arbeitgeberin bereits vorgehaltenen Listen soll in spezifischen Dokument-Dateitypen („elektronisch im Format *.xls oder *.txt“) erfolgen. Diese entsprechen nicht dem Dateiformat bei der gewährten Einsichtnahme (PDF-Datei oder Ausdruck). Damit sind sie Bestandteil der beanspruchten Verpflichtung.

c) Die – ausdrücklich erst in der Beschwerdeinstanz formulierte – Ausnahme der leitenden Angestellten bei der Listenbeschreibung hat lediglich klarstellenden Charakter. Es ist nichts dafür ersichtlich, dass der Betriebsrat ein Rechtsschutzziel verfolgt, das über seinen Zuständigkeitsbereich hinausginge.

d) Soweit im Antrag der Übergabezweck angeführt ist, handelt es sich um ein bloßes Element der Antragsbegründung. Die Beteiligten gehen übereinstimmend davon aus, dass die streit-

befangenen Entgeltlisten mit keiner anderen Intention als der ihrer Auswertung unter den Gesichtspunkten des EntgTranspG übergeben werden sollen. Streitig ist nach ihrem Vorbringen vielmehr, ob das Auswertungsrecht des § 13 Abs. 2 Satz 1 EntgTranspG eine Pflicht der Arbeitgeberin zur Listenübergabe an den Betriebsausschuss begründet. Zwar „übermittelt“ die Arbeitgeberin die Entgeltlisten bereits in dem Sinn, als sie im PDF-Format eingesehen werden können und Gelegenheit besteht, Notizen zu fertigen und Berechnungen anzustellen. Es geht dem Betriebsrat aber um die Weitergabe der die Bruttoentgeltlisten darstellenden Daten in den bezeichneten Dateiformaten an den Betriebsausschuss zu dessen Verfügung.

2. In diesem Verständnis ist der Antrag hinreichend bestimmt iSv. § 253 Abs. 2 Nr. 2 ZPO. Anders als die Arbeitgeberin eingewandt hat, ist das Übergabeverlangen nicht deshalb unzulänglich beschrieben, weil hinsichtlich der Entgeltlisten der Zeitpunkt des dort abzubildenden Personalbestands unklar wäre. Es geht dem Betriebsrat um keine anderen Listen als die, in welche die Arbeitgeberin – auch nach ihrem eigenen Vortrag – Einsicht gewährt.

II. Der Hauptantrag ist unbegründet.

1. Die Arbeitgeberin ist nicht nach § 13 Abs. 2 Satz 1 EntgTranspG zur Übergabe der Bruttoentgeltlisten verpflichtet. Dabei kann offenbleiben, ob das nach dieser Vorschrift bestehende Recht, die Listen über die Bruttolöhne und -gehälter i.S.d. § 80 Abs. 2 Satz 2 BetrVG einzusehen und auszuwerten, einen Anspruch auf deren Übergabe gewährt. Jedenfalls korrespondiert es mit der Aufgabe des Betriebsrats nach § 14 Abs. 1 Satz 1 bis Satz 3 EntgTranspG (bei tarifgebundenen und tarifenwendenden Arbeitgebern) bzw. nach § 15 Abs. 2 iVm. § 14 Abs. 1 Satz 1 bis Satz 3 EntgTranspG (bei nicht tarifgebundenen und nicht tarifenwendenden Arbeitgebern) im Zusammenhang mit der Erfüllung einer Auskunftspflicht nach § 10 Abs. 1 EntgTranspG. Es besteht daher nicht, wenn es der Arbeitgeber – wie im vorliegenden Fall – nach § 14 Abs. 2 Satz 1 bzw. § 15 Abs. 2 EntgTranspG übernommen hat, die Auskunft selbst zu erteilen.

a) Entsprechend dem im Abschnitt 2 des EntgTranspG geltenden individuellen Verfahren zur Überprüfung von Entgeltgleichheit haben Beschäftigte nach §§ 10 ff. EntgTranspG in Betrieben mit in der Regel mehr als 200 Beschäftigten bei demselben Arbeitgeber einen inhaltlich mit näheren Maßgaben versehenen individuellen Auskunftsanspruch. In dieses Verfahren ist der Betriebsrat eingebunden. An ihn wenden sich Beschäftigte tarifgebundener und tarifenwendender Arbeitgeber für ihr Auskunftsverlangen (§ 14 Abs. 1 Satz 1 EntgTranspG). Entsprechendes gilt für Beschäftigte nicht tarifgebundener und nicht tarifenwendender Arbeitgeber (§ 15 Abs. 2 EntgTranspG). Damit ist der Betriebsrat für die Erteilung der Auskunft grundsätzlich zuständig, wobei er die Verpflichtung nach § 14 Abs. 1 Satz 4 EntgTranspG auf den Arbeitgeber übertragen kann. Der Arbeitgeber seinerseits ist berechtigt, nach Maßgabe von § 14 Abs. 2, § 15 Abs. 2 EntgTranspG die Erfüllung der Auskunftspflicht generell oder im Einzelfall an sich zu ziehen.

b) § 13 Abs. 2 und Abs. 3 EntgTranspG flankiert die von § 14 Abs. 1 und § 15 Abs. 2 EntgTranspG vorgesehene Stellung des Betriebsrats als Adressat eines individuellen Auskunftsverlangens nach § 10 Abs. 1 EntgTranspG (BAG 7. Mai 2019 – 1 ABR 53/17 – Rn. 28, BAGE 166, 309). Hat der Arbeitgeber entsprechend der ihm gesetzlich eröffneten Möglichkeit die Erfüllung der Auskunftspflicht an sich gezogen, besteht das Einsichts- und Auswertungsrecht des § 13 Abs. 2 Satz 1 EntgTranspG nicht. Dieses ist an die Zuständigkeit des Betriebsrats für die Auskunftserteilung gebunden. Das geben Systematik und der Zweck der Norm vor.

aa) Allerdings lässt der Normwortlaut mehrere inhaltliche Deutungen zu.

(1) Er ist unmissverständlich dahingehend, dass das Recht nach § 13 Abs. 2 Satz 1 EntgTranspG, die Listen über die Bruttolöhne und -gehälter iSd. § 80 Abs. 2 Satz 2 BetrVG einzusehen und auszuwerten, aufgabengebunden ist. Das legt bereits die Überschrift von § 13 EntgTranspG nahe, die dessen Regelungsgegenstände mit „Aufgaben und Rechte des Betriebsrates“ zusammenfasst. Den entsprechenden Aufgabenbezug verdeutlicht vor allem die Präposition „für“ im Zusammenhang mit dem textlichen Ausdruck „die Erfüllung seiner Aufgaben“. Das Possessivpronomen „seiner“ bezieht sich zwar grammatikalisch gesehen auf den dort angeführten Betriebsausschuss bzw. den nach § 28 Abs. 1 Satz 3 BetrVG beauftragten Ausschuss; diese werden jedoch insoweit anstelle des Betriebsrats tätig.

(2) Die Aufgaben selbst sind mit der inhaltsbezogenen Verweisung „nach Abs. 1“ beschrieben. Allerdings ist der gesamte „Abs. 1“ von § 13 EntgTranspG rechtstechnisch von vornherein ein nur bedingt verweisungstauglicher Text, denn sein Satz 3 beschreibt keine Aufgaben, sondern bestimmt, dass betriebsverfassungsrechtliche, tarifrechtliche oder betrieblich geregelte Verfahren unberührt bleiben.

(3) Soweit auf Satz 1 und Satz 2 von § 13 Abs. 1 EntgTranspG Bezug genommen wird, gibt deren Normtext ein bestimmtes inhaltliches Verständnis nicht zwingend vor. Die Formulierung, wonach der Betriebsrat „[i]m Rahmen seiner Aufgabe nach § 80 Abs. 1 Nummer 2a des Betriebsverfassungsgesetzes ... die Durchsetzung der Entgeltgleichheit von Frauen und Männern im Betrieb“ fördert, wobei er „insbesondere die Aufgaben nach § 14 Abs. 1 und § 15 Abs. 2“ EntgTranspG wahrnimmt, deutet zwar darauf hin, dass das Einsichts- und Auswertungsrecht des § 13 Abs. 2 Satz 1 EntgTranspG unabhängig davon besteht, ob der Betriebsrat die Auskunft zu erteilen hat oder ob – so in Betrieben unterhalb des Schwellenwerts von in der Regel mehr als 200 Beschäftigten – ein individueller Auskunftsanspruch iSv. §§ 10 ff. EntgTranspG überhaupt geltend gemacht werden kann (so MHD ArbR/Arnold 4. Aufl. § 314 Rn. 34; Bauer/Krieger/Günther AGG/EntgTranspG 5. Aufl. § 13 EntgTranspG Rn. 18; BeckOK ArbR/Roloff Stand 1. Juni 2020 EntgTranspG § 13 Rn. 5; DKW/Buschmann 17. Aufl. § 80 Rn. 130a; ErfK/Schlachter 20. Aufl. EntgTranspG § 13 Rn. 3; Weber GK-BetrVG 11. Aufl. § 80 Rn. 130; Günther/Heup/Mayr NZA 2018, 545, 547; HWK/Thies 9. Aufl. § 13 EntgTranspG Rn. 3; Kania NZA 2017, 819, 820; Kocher AuR 2018, 8, 15; Kuhn/Schwindling DB 2018, 509, 515; Oerder/Wenckebach EntgTranspG § 13 Rn. 4). Allerdings verschließt sich diese Aufgabenbeschreibung sprachlich auch keinem Verständnis dahingehend, dass mit Satz 1 von § 13 Abs. 1 EntgTranspG der bereits in § 80 Abs. 1 Nr. 2a BetrVG enthaltene Aspekt der Förderung einer Durchsetzung von Entgeltgleichheit – aus Gründen der Klarstellung – angeführt ist. Denn § 80 Abs. 1 Nr. 2a BetrVG zählt seinerseits bei der dort festgelegten Förderaufgabe des Betriebsrats zur Durchsetzung der tatsächlichen Gleichstellung der Geschlechter die hierfür einschlägigen Bereiche (Einstellung, Beschäftigung, Aus-, Fort- und Weiterbildung und beruflicher Aufstieg) nicht abschließend auf. Mit dem Adverb „insbesondere“ in Satz 2 von § 13 Abs. 1 EntgTranspG können daher auch lediglich die in § 14 Abs. 1 und § 15 Abs. 2 EntgTranspG geregelten spezifischen Zuständigkeitsaufgaben des Betriebsrats besonders betont sein, deren Wahrnehmung das Einsichts- und Auswertungsrecht des § 13 Abs. 2 Satz 1 EntgTranspG dient.

bb) Für letzteres Verständnis spricht die Normsystematik. Nach § 13 Abs. 2 Satz 2 EntgTranspG kann der einsichts- und auswertungsrechtlich zuständige Ausschuss „mehrere Auskunftsverlangen bün-

deln und gemeinsam behandeln“. Die gliederungsmäßige Stellung dieser Berechtigung lässt darauf schließen, dass im Satz 1 der Vorschrift geregelte Einsichts- und Auswertungsrecht in Abhängigkeit von der Zuständigkeit des Betriebsrats zur Beantwortung von Auskunftsverlangen zu verstehen. Zudem kann zumindest § 13 Abs. 5 EntgTranspG ein sinnvoller Regelungsgehalt nur dann bemessen werden, wenn entweder der Arbeitgeber von der ihm möglichen Übernahme der Beantwortung von Auskunftsverlangen keinen Gebrauch gemacht oder der Betriebsrat Entsprechendes nicht verlangt hat. Auch § 13 Abs. 4 EntgTranspG knüpft an Auskunftsverlangen – hier der leitenden Angestellten – an.

cc) Gesetzessystematische Überlegungen stützen dieses Verständnis.

(1) Die Regelungen des mit „Aufgaben und Rechte des Betriebsrates“ überschriebenen § 13 EntgTranspG finden sich im Gesetzesabschnitt „Individuelle Verfahren zur Überprüfung von Entgeltgleichheit“. In diesem Abschnitt sind der Auskunftsanspruch und hierzu die Anspruchsberechtigung, Formalien, Bezugspunkt, Gegenstand und Reichweite ebenso festgelegt wie ein Verfahren zur Geltendmachung und Behandlung von Auskunftsverlangen mit regelhafter – vom Arbeitgeber sowie Betriebsrat aber auch „verzichtbarer“ – Einbindung des Betriebsrats. Sämtliche Vorschriften des § 13 EntgTranspG dürften damit eher die spezifischen Rechte und Aufgaben des Betriebsrats bei seiner regelhaften Verfahrenseinbindung betreffen. Dies zeigt auch § 10 Abs. 3 EntgTranspG, wonach ein Auskunftsverlangen mit einer Antwort „nach Maßgabe der §§ 11 bis 16“ – was die Regelungen in § 13 EntgTranspG einschließt – erfüllt ist. Ebenso nimmt § 14 Abs. 1 Satz 2 EntgTranspG – im unmittelbaren Anschluss an die in Satz 1 festgelegte Zuständigkeit des Betriebsrats für Auskunftsverlangen im Verfahren bei tarifgebundenen und tarifynwendenden Arbeitgebern – Bezug auf § 13 EntgTranspG. Die dort angesprochenen „Vorgaben ... nach § 13“ greifen also im Zusammenhang mit einem Auskunftsverlangen von Beschäftigten.

(2) Ein systematischer Normtextvergleich von § 13 Abs. 2 Satz 1 EntgTranspG mit § 15 Abs. 4 Satz 5 EntgTranspG gebietet keine bestimmte Lesart. Die besondere Informationsverpflichtung des nicht tarifgebundenen und nicht tarifynwendenden Arbeitgebers nach § 15 Abs. 4 Satz 5 EntgTranspG knüpft zwar ausdrücklich an die Zuständigkeit des Betriebsrats für die Beantwortung des Auskunftsverlangens an („[s]oweit“). Ein Gegenschluss zu § 13 Abs. 2 Satz 1 EntgTranspG ist aber nicht zwingend, weil Satz 5 von § 15 Abs. 4 EntgTranspG nicht die Entgeltlisteneinsicht und -auswertung betrifft, sondern die Bereitstellung erforderlicher Informationen regelt.

(3) Der Umstand, dass die Übergangsbestimmung des § 25 Abs. 1 EntgTranspG allein den Auskunftsanspruch nach § 10 EntgTranspG – und nicht auch § 13 EntgTranspG – in Bezug nimmt, ist nicht aussagekräftig. Versteht man die Einsichts- und Auswertungsrecht als ein mit der Zuständigkeit des Betriebsrats für die Beantwortung von Auskunftsverlangen korrespondierendes Recht, wäre eine gesonderte Übergangsbestimmung überflüssig. Aus ihrem Fehlen vermag daher nichts abgeleitet zu werden.

(4) Die auf Abs. 2 Satz 1 und Abs. 3 Satz 3 von § 13 EntgTranspG bezogene textvergleichende Regelungssystematik führt zu keinem eindeutigen Ergebnis. Die Norm des § 13 Abs. 3 Satz 3 EntgTranspG legt die inhaltlichen Anforderungen für die Verpflichtung des Arbeitgebers zur Aufbereitung der Entgeltlisten fest. Die Formulierung in § 13 Abs. 3 EntgTranspG, die nicht ausdrücklich aufgabenbezogen ist, zwingt jedoch nicht zu dem Gegenschluss, bei den von § 13 Abs. 2 Satz 1 EntgTranspG angesprochenen Aufgaben müsse es sich um weitergehende als die der Auskunftserteilung handeln.

dd) Sinn und Zweck des Einsichts- und Auswertungsrechts streiten deutlich dafür, dass es eine Zuständigkeit des Betriebsrats für die Beantwortung individueller Auskunftsverlangen voraussetzt.

(1) Damit der Betriebsrat individuelle Auskunftsansprüche der Beschäftigten nach § 10 EntgTranspG ordnungsgemäß erfüllen kann, bedarf es einer Berechtigung, die Entgeltlisten nicht nur einzusehen, sondern auch auszuwerten. Das ist durch den gesetzlichen Mindestinhalt und -umfang der Auskunft vorgegeben (§ 11 EntgTranspG). Die inhaltlichen Anforderungen an die Auskunftserteilung begründen einen spezifischen Informationsbedarf des nach der Regelkonzeption des EntgTranspG für die Beantwortung von Auskunftsverlangen zuständigen Betriebsrats. Im Hinblick darauf ist mit § 13 Abs. 2 Satz 1 EntgTranspG eine über das Einblicksrecht des § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG hinausgehende entgeltlistenbezogene Auswertungsberechtigung festgelegt (vgl. zB Erk/Schlachter 20. Aufl. EntgTranspG § 13 Rn. 3). Eine solche Notwendigkeit der Entgeltlistenauswertung ist der – genereller verfassten – Aufgabe des Betriebsrats zur Förderung der Durchsetzung der Entgeltgleichheit nicht in vergleichbarer Weise immanent. Hierzu bedarf es vielmehr der Darlegung des Betriebsrats, für welche konkreten Förderungsmaßnahmen bestimmte Auskünfte benötigt werden (vgl. dazu zB BAG 24. April 2018 – 1 ABR 6/16 – Rn. 34). Das gilt auch, wenn die – nach ihrem eindeutigen Wortlaut – auf eine „Förderung“ der Durchsetzung der Entgeltgleichheit von Frauen und Männern gerichtete Aufgabe des Betriebsrats eine solche zur Überwachung der Einhaltung des Entgeltgleichheitsgebots enthielte. Ungeachtet dessen, dass eine entsprechende Überwachungsaufgabe nicht aus § 80 Abs. 1 Nr. 2a BetrVG oder § 13 Abs. 1 Satz 1 Entg-TranspG folgte, sondern aus § 80 Abs. 1 Nr. 1 BetrVG (vgl. zB BAG 26. September 2017 – 1 ABR 27/16 – Rn. 17), stünde auch sie unter dem Vorbehalt der Erforderlichkeit einer Auswertung der Bruttoentgeltlisten. Hierfür reichten weder allgemein gehaltene Hinweise auf gesetzliche Aufgaben unter Wiederholung des Gesetzeswortlauts aus, noch wäre die Erforderlichkeit allein mit dem Bestehen einer Überwachungsaufgabe impliziert (vgl. zB BAG 9. April 2019 – 1 ABR 51/17 – Rn. 16 ff., BAGE 166, 269).

(2) Die in den Gesetzesmaterialien verlautbarte Intention des Gesetzgebers zeigt deutlich die Bindung des Einsichts- und Auswertungsrechts an die regelhaft dem Betriebsrat zugewiesene Aufgabe der Erfüllung von Auskunftsverpflichtungen. Nach der Begründung des Gesetzentwurfs der Bundesregierung bestimmt der in „sechs Absätze gegliedert[e]“ Paragraph des § 13 EntgTranspG „die Aufgaben und Rechte des Betriebsrats und speziell des Betriebsausschusses im Rahmen des Auskunftsanspruchs der Beschäftigten nach § 10“ EntgTranspG (BT-Drs. 18/11133 S. 62). Zu Abs. 2 von § 13 EntgTranspG heißt es ua.:

„Satz 1 regelt, auf welcher Datengrundlage der Betriebsausschuss die Antwort auf das Auskunftersuchen der Beschäftigten zu erstellen hat und wie er an die erforderlichen Informationen gelangt. Dazu bestimmt Satz 1, dass der Betriebsausschuss ... für die Erfüllung seiner Aufgaben nach Abs. 1 das Recht hat, die in § 80 Abs. 2 Satz 2 des Betriebsverfassungsgesetzes genannten Listen über die Bruttolöhne und -gehälter einzusehen und auszuwerten.“

Damit ist der Gesetzgeber davon ausgegangen, dass das entgeltlistenbezogene Einsichts- und Auswertungsrecht der Beantwortung individueller Auskunftsverlangen dienen soll. Nach seinen Vorstellungen ist der Regelungszweck des § 13 Abs. 2 Satz 1 EntgTranspG mit der Zuständigkeit des Betriebsrats zur Beantwortung individueller Auskunftsverlangen verknüpft.

ee) Ein solches Normverständnis verbietet sich nicht deshalb, weil § 13 Abs. 2 Satz 1 EntgTranspG dann kein anderer Regelungsgehalt zukäme als § 13 Abs. 3 EntgTranspG. Abs. 2

von § 13 EntgTranspG legt als Bezugsobjekt der Einsichts- und Auswertungsberechtigung die in § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG genannten Listen über die Bruttolöhne und -gehälter fest. Das bezieht sich – ggf. in einem für das Auskunftsverlangen relevanten Umfang – auf die vom Arbeitgeber tatsächlich geführten Listen. Demgegenüber verpflichtet Abs. 3 von § 13 EntgTranspG den Arbeitgeber nicht nur dazu, dem Betriebsausschuss Einblick „in die Listen über die Bruttolöhne und -gehälter der Beschäftigten“ zu gewähren, sondern die Listen auch nach näheren Maßgaben aufzubereiten. Das Einblicksrecht nach § 13 Abs. 3 EntgTranspG umfasst also spezifische Listen mit bestimmten Aufschlüsselungen und Angaben, was – anders als beim Einsichts- und Auswertungsrecht nach Abs. 2 Satz 1 EntgTranspG – den Arbeitgeber verpflichtet, entsprechende Listen ggf. erst herzustellen (ganz hM vgl. zB Bauer/Krieger/Günther AGG/EntgTranspG 5. Aufl. § 13 EntgTranspG Rn. 14; DKW/Buschmann § 80 Rn. 130a; Fitting BetrVG 30. Aufl. § 80 Rn. 111). Beide Vorschriften – das Recht nach § 13 Abs. 2 Satz 1 EntgTranspG und die Verpflichtung nach § 13 Abs. 3 EntgTranspG – sind mit der nach dem EntgTranspG konzeptionell-regelhaften Einbindung des Betriebsrats in das individuelle Verfahren zur Überprüfung von Entgeltgleichheit verknüpft.

c) Danach kommt dem Betriebsrat auf der Grundlage der den Senat bindenden tatsächlichen Feststellungen des Landesarbeitsgerichts das beanspruchte Einsichts- und Auswertungsrecht des § 13 Abs. 2 Satz 1 EntgTranspG schon dem Grunde nach nicht zu. Es bedarf daher keiner Entscheidung, ob das in dieser Vorschrift genannte Auswertungsrecht auch ein Recht auf Überlassung der Entgeltlisten zur Verfügung des Betriebsausschusses umfasst. Die Arbeitgeberin hat die Erfüllung der Auskunftsverpflichtung generell übernommen. Ihre Berechtigung hierzu folgt, sollte sie tarifgebunden oder tarifenwendend sein, aus § 14 Abs. 2 Satz 1 EntgTranspG oder, sollte sie nicht tarifgebunden und nicht tarifenwendend sein, aus § 15 Abs. 2 iVm. § 14 Abs. 2 Satz 1 EntgTranspG. Mangels gegenteiliger Anhaltspunkte ist davon auszugehen, dass die Übernahme § 14 Abs. 2 Satz 1 bis Satz 3 EntgTranspG entspricht, ohne dass es darauf ankäme, welche Folge eine Verletzung der entsprechenden Vorschriften zur Übernahme zeitigte. Auch der Betriebsrat hat diesbezüglich keine Beanstandungen erhoben und die streitbefangene Listenübergabe nicht auf seine Zuständigkeit für die Erfüllung der Auskunftsverpflichtung gestützt.

2. Im Übrigen folgt die mit dem Hauptantrag geltend gemachte Verpflichtung weder aus § 13 Abs. 3 EntgTranspG noch aus § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG oder aus § 80 Abs. 2 Satz 1 iVm. Satz 2 Halbs. 1 BetrVG.

a) § 13 Abs. 3 EntgTranspG und § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG tragen die streitbefangene Übergabeverpflichtung schon deshalb nicht, weil sie als Einblicksrechte in die Listen über die Bruttolöhne und -gehälter konzipiert sind. Das stellt auch der Betriebsrat nicht in Abrede. Entsprechend hat er sein Begehren im Wesentlichen mit der entgeltlistenbezogenen Auswertungsberechtigung begründet.

b) Auch die aus § 80 Abs. 2 Satz 1 iVm. Abs. 2 Satz 2 Halbs. 1 BetrVG folgende Verpflichtung des Arbeitgebers, den Betriebsrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten sowie ihm auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen, vermag die erstrebte Listenübergabe nicht zu begründen. Dabei kann zugunsten des Betriebsrats eine entgeltgleichheitsbezogene Aufgabe – welche allerdings nicht allein unter Wiederholung des Gesetzeswortlauts von § 80 Abs. 1 Nr. 1 oder Nr. 2a BetrVG aufzuzeigen wäre – unterstellt werden. Denn der Aus-

kunftsanspruch des Betriebsrats nach § 80 Abs. 2 Satz 1 BetrVG wird zwar im Bereich der Löhne und Gehälter nicht durch die Regelung des Satzes 2 Halbs. 2 der Vorschrift verdrängt. Er begründete jedoch keinen entgeltlistenbezogenen Anspruch, der über eine Einblicknahme hinausginge (ausf. zur insoweit gebotenen teleologischen Reduktion von § 80 Abs. 2 Satz 1 BetrVG BAG 30. September 2008 – 1 ABR 54/07 – Rn. 31, BAGE 128, 92).

III. Der Hilfsantrag fällt nicht zur Entscheidung an. Er steht unter der Bedingung, dass der vom Betriebsrat hauptsächlich erstrebte Anspruch allein daran scheitert, dass eine Übergabe der Listen nicht in den bezeichneten Dateiformaten verlangt werden kann. Wie im Hilfsantrag ausdrücklich formuliert, bezieht er sich auf die Übergabe der „im Hauptantrag genannten Liste“, nur in einer anderen Form (Papierform mit der Eignung zur Umwandlung in elektronisches Format). Die so verstandene Bedingung der Abweisung des Hauptantrags tritt nicht ein.

Auskunfts berechtigte nach dem Entgelttransparenzgesetz (Ls)

(Bundesarbeitsgericht, Urteil vom 25. Juni 2020 – 8 AZR 145/19 –)

1. Nach § 10 Abs. 1 Satz 1 Entgelttransparenzgesetz (EntgTranspG) haben „Beschäftigte“ zur Überprüfung der Einhaltung des Entgeltgleichheitsgebots im Sinne dieses Gesetzes einen Auskunftsanspruch nach Maßgabe der §§ 11 bis 16.
2. Nach § 5 Abs. 2 EntgeltTranspG sind ua. Arbeitnehmerinnen und Arbeitnehmer Beschäftigte im Sinne dieses Gesetzes. Die Begriffe „Arbeitnehmerin“ und „Arbeitnehmer“ in § 5 Abs. 2 Nr. 1 EntgTranspG sind nicht eng iSd. Arbeitnehmerbegriffs des innerstaatlichen Rechts, sondern unionsrechtskonform in Übereinstimmung mit dem Arbeitnehmerbegriff der Richtlinie 2006/54/EG weit auszulegen.
3. Danach können im Einzelfall auch arbeitnehmerähnliche Personen iSd. innerstaatlichen Rechts Arbeitnehmer iSv. § 5 Abs. 2 Nr. 1 EntgeltTranspG sein.

Entschädigung bei Benachteiligung wegen Schwerbehinderung (Ls)

(Bundesarbeitsgericht, Urteil vom 28. Mai 2020 – 8 AZR 170/19 –)

1. Die Entschädigung nach § 15 Abs. 2 AGG hat eine Doppelfunktion. Sie dient einerseits der vollen Schadenskompensation und andererseits der Prävention, wobei jeweils der Grundsatz der Verhältnismäßigkeit zu wahren ist.
2. Bei der Bestimmung der angemessenen Entschädigung für den erlittenen immateriellen Schaden nach § 15 Abs. 2 AGG steht den Tatsachengerichten nach § 287 Abs. 1 ZPO ein weiter Ermessensspielraum zu. Die Festsetzung der angemessenen Entschädigung durch das

Tatsachengericht unterliegt infolgedessen nur einer eingeschränkten revisionsgerichtlichen Kontrolle. Das Revisionsgericht kann lediglich überprüfen, ob das Berufungsgericht die Rechtsnorm zutreffend ausgelegt, ein Ermessen ausgeübt, die Ermessensgrenze nicht überschritten hat und ob es von seinem Ermessen einen fehlerfreien Gebrauch gemacht hat.

3. Hiernach war eine Entschädigung iHv. 5.100,00 Euro angemessen. Dieser Betrag entspricht ca. 1,5 auf der ausgeschriebenen Stelle erzielbaren Bruttomonatsentgelten. Mit diesem Betrag wird der Kläger angemessen für den durch die unzulässige Diskriminierung – ausschließlich – wegen der (Schwer)Behinderung erlittenen immateriellen Schaden entschädigt; dieser Betrag ist zugleich auch erforderlich, aber auch ausreichend, um die notwendige abschreckende Wirkung zu erzielen.

(Nicht amtliche Leitsätze)

Auskunft hinsichtlich anderweitigen Erwerbs (Ls)

(Bundesarbeitsgericht, Urteil vom 27. Mai 2020 – 5 AZR 387/19 –)

Der Arbeitgeber hat gegen den Arbeitnehmer, der Vergütung wegen Annahmeverzugs fordert, einen Auskunftsanspruch über die von der Agentur für Arbeit und dem Jobcenter unterbreiteten Vermittlungsvorschläge. Grundlage des Auskunftsbegehrens ist eine Nebenpflicht aus dem Arbeitsverhältnis nach § 242 BGB.

Zum Umfang der Unterrichtung des Betriebsrats bei außerordentlicher Kündigung

(Bundesarbeitsgericht, Urteil vom 7. Mai 2020 – 2 AZR 678/19 –)

1. Nach § 102 Abs. 1 Satz 1 BetrVG ist der Betriebsrat vor jeder Kündigung unter Mitteilung der Gründe für die Kündigung zu hören (§ 102 Abs. 1 Satz 2 BetrVG).
2. Der Betriebsrat soll die Stichhaltigkeit und Gewichtigkeit der Kündigungsgründe beurteilen und sich über sie eine eigene Meinung bilden können. Die Anhörung soll dem Betriebsrat dagegen nicht die selbständige – objektive – Überprüfung der rechtlichen Wirksamkeit der beabsichtigten Kündigung ermöglichen (vgl. BAG 22. September 2016 – 2 AZR 700/15 – Rn. 25).
3. Danach musste die Beklagte den Betriebsrat im Hinblick auf die hier vorrangig beabsichtigte außerordentliche fristlose Kündigung weder über einen möglichen besonderen Kündigungsschutz noch über die (Nicht-)Wahrung der Ausschlussfrist des § 626 Abs. 2 BGB unterrichten.

Diese Informationen „gehört nicht zu den „Gründen für die Kündigung“ i.S.v. § 102 Abs. 1 Satz 2 BetrVG.

(Nicht amtliche Leitsätze)

Aus den Gründen:

I. Die vom Berufungsgericht für die Unwirksamkeit der außerordentlichen fristlosen Kündigung gegebene Begründung hält einer revisionsrechtlichen Überprüfung nicht stand. Die Kündigung ist nach den vom Berufungsgericht getroffenen Feststellungen nicht gemäß § 102 Abs. 1 Satz 3 BetrVG unwirksam. Die Beklagte musste den Betriebsrat weder über einen Sonderkündigungsschutz unterrichten noch weitere Ausführungen zur Wahrung der Kündigungserklärungsfrist des § 626 Abs. 2 BGB machen.

1. Nach § 102 Abs. 1 Satz 1 BetrVG ist der Betriebsrat vor jeder Kündigung zu hören. Der Arbeitgeber hat ihm die Gründe für die Kündigung mitzuteilen (§ 102 Abs. 1 Satz 2 BetrVG). Eine ohne Anhörung des Betriebsrats ausgesprochene Kündigung ist gemäß § 102 Abs. 1 Satz 3 BetrVG unwirksam.

2. Die Mitteilungspflicht des Arbeitgebers im Rahmen von § 102 Abs. 1 Satz 2 BetrVG reicht nicht so weit wie seine Darlegungslast im Prozess (BAG 26. März 2015 – 2 AZR 417/14 – Rn. 46, BAGE 151, 199). Der notwendige Inhalt der Unterrichtung gemäß § 102 Abs. 1 Satz 2 BetrVG richtet sich vielmehr nach Sinn und Zweck des Beteiligungsrechts. Dieser besteht darin, den Betriebsrat durch die Unterrichtung in die Lage zu versetzen, sachgerecht, dh. ggf. zugunsten des Arbeitnehmers auf den Arbeitgeber einzuwirken. Der Betriebsrat soll die Stichhaltigkeit und Gewichtigkeit der Kündigungsgründe beurteilen und sich über sie eine eigene Meinung bilden können. Die Anhörung soll dem Betriebsrat nicht die selbständige – objektive – Überprüfung der rechtlichen Wirksamkeit der beabsichtigten Kündigung ermöglichen (vgl. BAG 22. September 2016 – 2 AZR 700/15 – Rn. 25).

3. Danach musste die Beklagte den Betriebsrat im Hinblick auf die vorrangig beabsichtigte außerordentliche fristlose Kündigung nicht darüber unterrichten, dass der Kläger – möglicherweise – einen besonderen Kündigungsschutz genoss. Ungeachtet der Frage, ob ein solcher überhaupt zu den „Gründen für die Kündigung“ i.S.v. § 102 Abs. 1 Satz 2 BetrVG gehören kann, muss ein Arbeitgeber, der außerordentlich fristlos kündigen möchte, dem Betriebsrat jedenfalls nicht mitteilen, dass dem Arbeitnehmer ein Sonderkündigungsschutz zukommt, der – wie § 20 Nr. 4 und Nr. 5 des Einheitlichen Manteltarifvertrags für die Metall- und Elektroindustrie in Nordrhein-Westfalen vom 18. Dezember 2003 (EMTV) – zwar eine ordentliche Kündigung weitgehend ausschließt, die Möglichkeit einer „fristlosen“ Kündigung aber ausdrücklich „unberührt“ lässt. Dem Betriebsrat werden insoweit keine Einwände abgeschnitten. Er kann der Absicht einer außerordentlichen fristlosen Kündigung in beiden Fällen (ordentliche Kündbarkeit und ordentliche Unkündbarkeit) gleichermaßen entgegensetzen, dem Arbeitgeber sei es zuzumuten, die ordentliche Kündigungsfrist einzuhalten (zutreffend LAG Düsseldorf 24. August 2001 – 18 Sa 366/01 – zu I 2 b der Gründe). Dabei spielt es keine Rolle, ob die Kündigungsfrist „real“ (ordentliche Kündbarkeit) oder „fiktiv“ (ordentliche Unkündbarkeit) ist. Neben der Sache liegt der Einwand des Klägers, der Betriebsrat müsse von einem tariflichen Sonderkündigungsschutz wissen, um beurteilen zu können, ob ein förmlicher Widerspruch nach § 102 Abs. 3 BetrVG in Betracht komme. Diese Möglichkeit ist ihm in Bezug auf eine beabsichtigte außerordentliche fristlose Kündigung – nicht eine solche mit notwendiger Auslaufzeit – in jedem Fall verschlossen.

4. Die Anhörung des Betriebsrats war auch nicht im Hinblick auf die Kündigungserklärungsfrist des § 626 Abs. 2 BGB fehlerhaft. Die Wahrung der Ausschlussfrist gehört nicht zu den „Gründen für die Kündigung“ i.S.v. § 102 Abs. 1 Satz 2 BetrVG. Deshalb muss der Arbeitgeber hierzu keine gesonderten Ausführungen machen. Ein solches Erfordernis überdehnte die Zwecke des Anhörungsverfahrens. Es liefe darauf hinaus, dem Gremium die – objektive – Überprüfung der Wirksamkeit der beabsichtigten Kündigung zu ermöglichen (ebenso Hertzfeld FA 2013, 107, 109; Raab GK-BetrVG 11. Aufl. § 102 Rn. 98; siehe auch HaKo-BetrVG/Braasch 5. Aufl. § 102 Rn. 69; Humberg/Kemper JR 2017, 191, 196). Das bedeutet allerdings zum einen nicht, dass der Arbeitgeber nicht angeben müsste, wann der Kündigungssachverhalt sich zugetragen hat. Nur so wird es dem Betriebsrat ermöglicht, die Stichhaltigkeit und Gewichtigkeit der Kündigungsgründe zu beurteilen und sich über sie eine eigene Meinung zu bilden. Zum anderen dürfen dem Betriebsrat mögliche – durch das Gesetz nicht inhaltlich begrenzte – Einwände gegen die beabsichtigte Kündigung nicht – gezielt – abgeschnitten werden. Das gilt auch für den möglichen Einwand, eine außerordentliche Kündigung sei aus Sicht des Gremiums verfristet. Soweit der Arbeitgeber gegenüber dem Betriebsrat (freiwillig) Angaben macht, die für die Einhaltung der Frist des § 626 Abs. 2 BGB von Bedeutung sind, müssen diese wahrheitsgemäß erfolgen (vgl. BAG 23. Oktober 2014 – 2 AZR 736/13 – Rn. 14). Diesen Anforderungen werden die Anhörungsschreiben vorliegend gerecht. Sie enthalten die erforderlichen Angaben darüber, zu welchem Zeitpunkt sich der Kündigungssachverhalt ereignet haben soll.

II. Die angefochtene Entscheidung hinsichtlich der außerordentlichen fristlosen Kündigung stellt sich nicht aus anderen Gründen als richtig dar (§ 561 ZPO).

III. Danach ist das Berufungsurteil aufzuheben. Der Senat kann aufgrund der fehlenden Feststellungen über den teilweise streitig gebliebenen Sachverhalt nicht selbst über die Wirksamkeit der außerordentlichen fristlosen Kündigung vom 7. März 2018 entscheiden (§ 563 Abs. 3 ZPO).

Kündigungsschutz einer Schwangeren vor Arbeitsantritt

(Bundesarbeitsgericht, Urteil vom 27. Februar 2020 – 2 AZR 498/19 –)

Das Kündigungsverbot gegenüber einer schwangeren Arbeitnehmerin gemäß § 17 Abs. 1 Satz 1 Nr. 1 MuSchG gilt auch für eine Kündigung vor der vereinbarten Tätigkeitsaufnahme.

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer ordentlichen Kündigung.

Der Beklagte, der in der Regel nicht mehr als zehn Arbeitnehmer beschäftigt, schloss mit der Klägerin am 9./14. Dezember 2017 einen Arbeitsvertrag über eine Tätigkeit als Rechtsanwaltsfachangestellte. Nach dessen § 1 Nr. 1 sollte „das Arbeitsverhältnis“ am 1. Februar 2018 beginnen. § 1 Nr. 2 bestimmte, dass der Vertrag unbefristet geschlossen sei bei einer Probezeit von sechs Monaten. Während dieser sollte das Arbeitsverhältnis beiderseits mit einer Frist von zwei Wochen gekündigt werden können. Gemäß § 13 sollte die

Klägerin im Falle einer schuldhaften Nichtaufnahme oder vertragswidrigen Beendigung der Tätigkeit eine Vertragsstrafe zahlen. Nach § 18 Nr. 2 des Vertrags war sie verpflichtet, bereits in der Zeit vom 27. bis zum 29. Dezember 2017 für eine tägliche Arbeitszeit von mindestens fünf Stunden auf Abruf zur Verfügung zu stehen.

Mit Schreiben vom 18. Januar 2018 informierte die Klägerin den Beklagten darüber, dass bei ihr eine Schwangerschaft festgestellt und aufgrund einer chronischen Vorerkrankung „mit sofortiger Wirkung ein komplettes Beschäftigungsverbot“ attestiert worden sei. Der Beklagte kündigte „das zwischen uns bestehende Arbeitsverhältnis“ mit Schreiben vom 30. Januar 2018 zum 14. Februar 2018.

Aus den Gründen:

Die Revision des Beklagten ist unbegründet. Das Landesarbeitsgericht hat zu Recht entschieden, dass die Kündigung vom 30. Januar 2018 gem. § 17 Abs. 1 Satz 1 Nr. 1 MuSchG iVm. § 134 BGB nichtig ist.

I. Nach § 17 Abs. 1 Satz 1 Nr. 1 MuSchG ist die Kündigung gegenüber einer Frau während ihrer Schwangerschaft unzulässig, wenn dem Arbeitgeber zum Zeitpunkt der Kündigung die Schwangerschaft bekannt oder sie ihm innerhalb von zwei Wochen nach Zugang der Kündigung mitgeteilt worden ist. § 17 Abs. 2 Satz 1 MuSchG bestimmt, dass die für den Arbeitsschutz zuständige oberste Landesbehörde oder die von ihr bestellte Stelle in besonderen Fällen, die nicht mit dem Zustand der Frau in der Schwangerschaft im Zusammenhang stehen, ausnahmsweise die Kündigung für zulässig erklären kann. § 17 Abs. 1 MuSchG enthält ein gesetzliches Verbot iSd. § 134 BGB. Eine Kündigung unter Verstoß gegen dieses Verbot ist gem. § 134 BGB nichtig (zu § 9 MuSchG aF zuletzt BAG 26. März 2015 – 2 AZR 237/14 – Rn. 10, BAGE 151, 189).

II. Das Landesarbeitsgericht hat zu Recht angenommen, das Kündigungsverbot gem. § 17 Abs. 1 Satz 1 Nr. 1 MuSchG gelte auch für eine Kündigung vor der vereinbarten Tätigkeitsaufnahme (ebenso BeckOK ArbR/Dahm Stand 1. Dezember 2019 MuSchG § 17 Rn. 6; Roos/Bieresborn/Betz MuSchG/BEEG 2. Aufl. § 17 MuSchG Rn. 13; Just, in: Tillmanns/Mutschler MuSchG/BEEG 2. Aufl. § 17 MuSchG Rn. 9; Hk-MuSchG/BEEG/Schöllmann 5. Aufl. MuSchG § 17 Rn. 14; Küttner/Poeche Personalarbuch 2019 Mutterschutz Rn. 41; zu § 9 Abs. 1 MuSchG aF: Buchner/Becker MuSchG/BEEG 8. Aufl. § 9 MuSchG Rn. 2; LAG Düsseldorf 30. September 1992 – 11 Sa 1049/92 –; zum Anwendungsbereich gem. § 1 Nr. 1 MuSchG aF vgl. auch LAG Berlin-Brandenburg 30. September 2016 – 9 Sa 917/16 – zu B I 1 der Gründe; aA APS/Linck 5. Aufl. BGB § 622 Rn. 55; KR/Spilger 12. Aufl. § 622 BGB Rn. 151). Dies ergibt die Auslegung von § 17 Abs. 1 Satz 1 iVm. § 1 Abs. 2 Satz 1 MuSchG.

1. Der Gesetzeswortlaut ist nicht eindeutig. § 17 Abs. 1 Satz 1 MuSchG normiert ein Kündigungsverbot ua. gegenüber (werdenden) Müttern ohne nähere Bestimmung, welche Rechtsverhältnisse oder diesen zugrunde liegenden Verträge davon erfasst sind. Dafür ist auf den persönlichen Anwendungsbereich des Mutterschutzgesetzes abzustellen. Dieser ist in § 1 Abs. 2 Satz 1 MuSchG mit Wirkung ab dem 1. Januar 2018 neu gefasst worden. Danach gilt das Gesetz für Frauen „in einer Beschäftigung iSv. § 7 Abs. 1 SGB IV“ sowie ferner gem. § 1 Abs. 2 Satz 2 MuSchG, „unabhängig davon, ob ein solches Beschäftigungsverhältnis vorliegt“, für Frauen in weiteren, im Streitfall nicht einschlägigen Tätigkeitsformen. Nach § 7 Abs. 1 Satz 1 SGB IV ist Beschäftigung die nicht selbständige Arbeit, insbesondere in einem Arbeitsverhältnis. Satz 2 der Vorschrift nennt als Anhaltspunkte für eine Beschäftigung eine Tätigkeit nach Weisungen und eine Eingliederung in die Arbeitsorganisation des Weisungs-

gebers. Dies lässt auch eine Lesart zu, wonach die Geltung des Mutterschutzgesetzes und damit des Kündigungsverbots in § 17 Abs. 1 MuSchG voraussetzt, dass eine Beschäftigung bereits in Vollzug gesetzt, die Tätigkeit also bereits aufgenommen ist.

2. Schon die Gesetzessystematik legt dagegen ein Verständnis nahe, wonach es nur auf das Bestehen eines auf eine Beschäftigung i.S.v. § 7 Abs. 1 SGB IV gerichteten Rechtsverhältnisses ankommt. Dies zeigt die synonyme Verwendung der Begriffe „Beschäftigung“ in § 1 Abs. 2 Satz 1 MuSchG und „ein solches Beschäftigungsverhältnis“ in Satz 2 der Bestimmung. Erfasst ist damit insbesondere ein Arbeitsverhältnis (§ 7 Abs. 1 Satz 1 SGB IV). Ein solches entsteht bereits mit Abschluss des Arbeitsvertrags (Schaub ArbR-HdB/Linck 18. Aufl. § 29 Rn. 8). Dies gilt selbst dann, wenn die Tätigkeit erst zu einem späteren Zeitpunkt aufgenommen werden soll. Auch in diesem Fall werden bereits mit dem Vertragsabschluss wechselseitige Verpflichtungen begründet. Der Arbeitnehmer verpflichtet sich, die vereinbarte Tätigkeit ab dem vereinbarten Zeitpunkt zu erbringen, der Arbeitgeber, ihn ab diesem Zeitpunkt zu beschäftigen und vertragsgemäß zu vergüten. Auch Nebenpflichten wie die Pflicht zur Rücksichtnahme auf die Interessen der Gegenpartei gem. § 241 Abs. 2 BGB entstehen bereits mit Vertragsabschluss. Dem steht nicht entgegen, dass im arbeitsrechtlichen Sprachgebrauch für den Beginn des Arbeitsverhältnisses ggf. auch erst auf den vereinbarten Einstellungszeitpunkt bzw. den vereinbarten Zeitpunkt der Arbeitsaufnahme abgestellt wird (für den Beginn der Wartezeit nach § 1 Abs. 1 KSchG vgl. BAG 24. Oktober 2013 – 2 AZR 1057/12 – Rn. 30 f., BAGE 146, 257). Das zutreffende Verständnis des Merkmals „Arbeitsverhältnis“ ist vom jeweiligen Regelungszweck abhängig. Das ändert jedoch nichts daran, dass zwischen dem Abschluss des Arbeitsvertrags als grundsätzlich maßgeblichem Zeitpunkt für den Beginn eines Arbeitsverhältnisses und dem möglicherweise davon abweichenden Zeitpunkt der tatsächlichen Arbeitsaufnahme zu unterscheiden ist. Auch die zwischen einem Dienstverhältnis und einem „angetretenen Dienstverhältnis“ differenzierenden Ausführungen in der Entscheidung des Sechsten Senats des Bundesarbeitsgerichts vom 23. Februar 2017 (– 6 AZR 665/15 – Rn. 30, BAGE 158, 214) bestätigen entgegen der Auffassung der Revision, dass ein Dienstverhältnis bereits dann bestehen kann, wenn es noch nicht angetreten ist.

3. Jedenfalls nach dem Normzweck des Kündigungsverbots in § 17 Abs. 1 Satz 1 MuSchG ist für dessen Eingreifen die Bekanntgabe einer bestehenden Schwangerschaft nach Abschluss des Arbeitsvertrags ausreichend. Die Aufnahme der vereinbarten Tätigkeit ist hierfür nicht erforderlich.

a) Das Kündigungsverbot soll die (werdende) Mutter temporär vor dem Verlust des Arbeitsplatzes schützen. Hierdurch werden der Bestand des Arbeitsverhältnisses während der Schwangerschaft und nach der Entbindung gewährleistet (Hk-MuSchG/BEEG/Schöllmann 5. Aufl. MuSchG § 17 Rn. 1a). Die Regelung in § 17 Abs. 1 Satz 1 MuSchG setzt Art. 10 der Richtlinie 92/85/EWG (Mutterschutzrichtlinie 92/85/EWG, ABL L 348 vom 28. November 1992 S. 1) um (vgl. BT-Drs. 18/8963 S. 87; BeckOK ArbR/Dahm Stand 1. Dezember 2019 § 17 MuSchG Rn. 1; ErfK/Schlachter 20. Aufl. MuSchG § 17 Rn. 1). Danach sind die Mitgliedstaaten verpflichtet, die erforderlichen Maßnahmen zu treffen, um Kündigungen von Beginn der Schwangerschaft bis zum Ende des Mutterschaftsurlaubs zu verbieten. Eine Kündigung kann sich schädlich auf die physische und psychische Verfassung von Schwangeren, Wöchnerinnen oder stillenden Arbeitnehmerinnen auswirken, eine Schwangere kann durch den sonst drohenden Arbeitsplatzverlust sogar zum baldigen Abbruch ihrer Schwanger-

schaft veranlasst werden (EuGH 22. Februar 2018 – C-103/16 – [Porras Guisado] Rn. 45 f. und 61 f.). Die Arbeitnehmerin und mittelbar das Kind sollen nicht durch wirtschaftliche Existenzängste belastet (vgl. auch §§ 18 ff. MuSchG), seelische Zusatzbelastungen durch einen Kündigungsschutzprozess vermieden werden (vgl. BAG 26. April 1956 – GS 1/56 – zu I 4 der Gründe, BAGE 3, 66; BeckOK ArbR/Dahm aaO; ErfK/Schlachter aaO).

b) Der demnach mit dem Kündigungsverbot bezweckte Gesundheits- und Existenzsicherungsschutz ist nur dann gewährleistet, wenn die Kündigung eines Arbeitsvertrags unabhängig davon unzulässig ist, ob die Tätigkeit erst zu einem späteren Zeitpunkt aufgenommen werden soll. Ein rechtlich geschütztes Bedürfnis, das die wirtschaftliche Existenz sichernde Arbeitsverhältnis zu erhalten, besteht auch bei einer vor der vereinbarten Tätigkeitsaufnahme bekannt gegebenen Schwangerschaft. Dies gilt jedenfalls dann, wenn die beabsichtigte Tätigkeitsaufnahme innerhalb der Schutzzeiten liegt. Auch die psychischen Belastungen der schwangeren Arbeitnehmerin sind keine anderen, wenn das Arbeitsverhältnis, das anderenfalls während ihrer Schwangerschaft fortbestünde, bereits vor der in Aussicht genommenen Tätigkeitsaufnahme gekündigt werden könnte.

c) Dieses Verständnis des Normzwecks von § 17 Abs. 1 Satz 1 MuSchG liegt auch nicht außerhalb der in § 1 Abs. 1 MuSchG generell formulierten Zwecke des Mutterschutzgesetzes. Das Gesetz schützt nicht nur die Gesundheit der (werdenden) Mutter und ihres Kindes „am Arbeitsplatz“ (§ 1 Abs. 1 Satz 1 MuSchG), sondern soll es der Frau gem. Satz 2 der Bestimmung auch ermöglichen, ihre Beschäftigung während der Schwangerschaft und nach der Entbindung fortzusetzen, sowie Benachteiligungen während dieser Zeit entgegenwirken. Dazu dient insbesondere auch das Kündigungsverbot (BT-Drs. 18/8963, S. 48). Damit eine Beschäftigung während der Schwangerschaft fortgesetzt werden kann, ist es erforderlich, dass eine Kündigung des Arbeitsverhältnisses auch bereits vor der vereinbarten Tätigkeitsaufnahme ausgeschlossen ist. Dass mit „Beschäftigung“ auch insoweit nicht lediglich eine tatsächliche Ausübung der Tätigkeit, sondern das zugrunde liegende Beschäftigungsverhältnis gemeint ist, ergibt sich schon daraus, dass das Mutterschutzgesetz mit den Leistungen nach §§ 18 ff. MuSchG gerade auch für Zeiten eines Beschäftigungsverbots eine wirtschaftliche Absicherung der Frau sicherstellen soll.

d) Ob das Kündigungsverbot des § 17 Abs. 1 MuSchG selbst dann Anwendung findet, wenn die Kündigung einen Arbeitsvertrag betrifft, nach welchem der Dienstantritt zu einem Zeitpunkt erfolgen soll, zu dem die Schutzzeiten schon wieder abgelaufen sein werden, bedarf hier keiner Entscheidung. Dafür dürfte sprechen, dass eine psychische Belastung auch daraus erwachsen kann, dass keine wirtschaftliche Absicherung für die Zeit nach Ablauf der Schutzfristen besteht. Der Arbeitgeber wiederum könnte nach Ablauf der Schutzfristen ohnehin ohne die Beschränkung des § 17 Abs. 1 MuSchG kündigen.

4. Die Entstehungsgeschichte von § 1 Abs. 2 Satz 1 MuSchG stützt das Verständnis, das Kündigungsverbot des § 17 Abs. 1 MuSchG greife grundsätzlich bereits mit Abschluss des Arbeitsvertrags. (wird ausgeführt)

III. Die vorstehende Auslegung des Kündigungsverbots gem. § 17 Abs. 1 MuSchG steht im Einklang mit dem Unionsrecht. Das kann der Senat ohne ein darauf gerichtetes Vorabentscheidungsersuchen an den Gerichtshof der Europäischen Union nach Art. 267 Abs. 3 AEUV beurteilen. Die dafür relevanten Fragen zur Auslegung des Unionsrechts sind durch den Gerichtshof bereits geklärt. Ob die Auslegung des deutschen Rechts darüber hinaus sogar unionsrechtlich geboten ist, bedarf keiner Entscheidung.

IV. Entgegen der Auffassung der Revision bestehen gegen die vorstehende Auslegung des Kündigungsverbots gem. § 17 Abs. 1 MuSchG keine verfassungsrechtlichen Bedenken. (wird ausgeführt)

a) Soweit sie aufgrund des Kündigungsverbots an das Arbeitsverhältnis mit der (werdenden) Mutter gebunden bleiben, gilt dies zum einen nur zeitlich begrenzt, zum anderen besteht bei außergewöhnlichen Umständen die Möglichkeit einer Zulässigkeitsklärung der Kündigung nach § 17 Abs. 2 Satz 1 MuSchG. (wird ausgeführt)

b) Die Kosten für Zeiten von Beschäftigungsverboten gem. §§ 18, 20 MuSchG müssen die Arbeitgeber nicht allein tragen. Es gilt vielmehr das Umlageverfahren gem. § 1 Abs. 2, § 7 AAG (Umlage U2). Nach § 1 Abs. 2 AAG werden Leistungen gem. §§ 18, 20 MuSchG vollständig von den Krankenkassen erstattet. Die Arbeitgeber müssen nach § 7 AAG lediglich ihren Anteil zur Umlage erbringen.

Keine Abhängigkeit des Inkrafttretens einer Betriebsvereinbarung von einem Belegschaftsquorum (Ls)

(Bundesarbeitsgericht, Beschluss vom 28. Juli 2019 – 1 ABR 4/19 –)

- 1. Die normative Wirkung einer Betriebsvereinbarung kann nicht von einem Zustimmungsquorum der Belegschaft abhängig gemacht werden. Eine solche Regelung widerspricht den Strukturprinzipien der Betriebsverfassung.**
- 2. Der Betriebsrat wird als Organ der Betriebsverfassung im eigenen Namen kraft Amtes tätig und ist weder an Weisungen der Arbeitnehmer gebunden, noch bedarf sein Handeln deren Zustimmung.**
- 3. Eine von ihm abgeschlossene Betriebsvereinbarung gilt kraft Gesetzes unmittelbar und zwingend. Damit gestaltet sie unabhängig vom Willen oder der Kenntnis der Parteien eines Arbeitsvertrags das Arbeitsverhältnis und erfasst auch später eintretende Arbeitnehmer. Das schließt es aus, die Geltung einer Betriebsvereinbarung an das Erreichen eines Zustimmungsquorums verbunden mit dem Abschluss einer einzelvertraglichen Vereinbarung mit dem Arbeitgeber zu knüpfen.**

Tätowierungsverbot für Bayerische Polizeivollzugsbeamte (Ls)

(Bundesverwaltungsgericht, Urteil vom 14. Mai 2020 – 2 C 13.19 –)

- 1. Mit der Neufassung des Art. 75 Abs. 2 Satz 2 BayBG im Jahr 2018 hat der bayerische Gesetzgeber unmittelbar die parlamentarische Leitentscheidung getroffen, dass sich Polizeivollzugsbeamte in dem beim Tragen der (Sommer-)Uniform sichtbaren Körperbereich nicht tätowieren lassen dürfen.**

2. Das in Art. 75 Abs. 2 Satz 2 BayBG normierte Verbot für Polizeivollzugsbeamte, sich an Kopf, Hals, Händen und Unterarmen im sichtbaren Bereich tätowieren oder vergleichbar behandeln zu lassen, verletzt weder das allgemeine Persönlichkeitsrecht dieser Beamten noch verstößt es gegen den Grundsatz der Verhältnismäßigkeit. Denn dieses Verbot ist geeignet und erforderlich, das vom Gesetzgeber vorgegebene Ziel eines einheitlichen und neutralen Erscheinungsbildes der Polizei zu fördern.

Rechtsweg zu den Arbeitsgerichten bei einem Rechtsstreit um Datenschutz eines Angestellten der Erzdiözese

(Landesarbeitsgericht Nürnberg, Beschluss vom 29. Mai 2020 – 8 Ta 36/20 –)

Bei einem Rechtsstreit eines bei der Erzdiözese im Rahmen eines privatrechtlichen Arbeitsvertrages angestellten Arbeitnehmers auf Schadensersatz wegen Verstößen gegen das kirchliche Datenschutzgesetz (KDG) ist der Rechtsweg zu den Arbeitsgerichten gegeben und nicht zu den nach KDSGO errichteten interdiözesanen Datenschutzgerichten.

Aus den Gründen:

Für eine Klage auf Schadensersatz aufgrund eines Datenschutzrechtsverstoßes sind im Rahmen eines privatrechtlichen Arbeitsverhältnisses auch mit der Kirche die Arbeitsgerichte ausschließlich und nicht das kirchliche Interdiözesane Datenschutzgericht zuständig. Die ausschließliche Zuständigkeit der staatlichen Arbeitsgerichte und damit der Rechtsweg zu den Arbeitsgerichten kann nicht durch kirchliches Recht abgeändert werden.

a) Nach § 2 Abs. 1 Nr. 3 a ArbGG sind die Gerichte für Arbeitssachen ausschließlich zuständig für bürgerliche Rechtsstreitigkeiten zwischen Arbeitnehmern und Arbeitgebern aus dem Arbeitsverhältnis aa) Soweit die Kirchen die Dienstverhältnisse ihrer Beschäftigten weder im Rahmen öffentlich-rechtlicher Grundsätze ordnet noch die geistigen Amtsträger entsprechend ihres Amtes beschäftigt noch eine Tätigkeit von Ordensangehörigen in kirchlichen Einrichtungen vorliegt, kommt das jeweilige Arbeitsverhältnis durch einen privatrechtlichen Arbeitsvertrag zustande. Die Kirche ist somit Arbeitgeber im Sinne des § 2 ArbGG.

bb) Diese ausschließliche Zuständigkeit der Arbeitsgerichte für bürgerliche Rechtsstreitigkeiten aus einem Arbeitsverhältnis kann nach § 4 ArbGG nur nach Maßgabe der §§ 101 – 110 ArbGG ausgeschlossen werden.

Die Verfassung garantiert die Schiedsgerichtsbarkeit in gleichem Umfang wie die Privatautonomie. Grundsätzlich gestattet das Grundgesetz neben der staatlichen Rechtsprechung auch eine gleichwertige private Rechtsprechung. Dieser Grundsatz wird durch § 4 eingeschränkt. Nur noch für das in den §§ 101 – 110 ArbGG geregelte Schiedsverfahren findet in engen Grenzen der Ausschluss der Arbeitsgerichtsbarkeit statt. Ein außergerichtliches oder schiedsgerichtliches Vorverfahren wird von der Regel des § 4 ArbGG nicht umfasst. Regelungen im kirchlichen Bereich, nach denen im Streitfall zunächst eine innerkirchliche Schlichtungsstelle anzurufen ist, sind im Regelfall so auszulegen, dass

auch ohne Anrufung der Schlichtung Klage beim Arbeitsgericht erhoben werden kann. Die Interdiözesanen Datenschutzgerichte sind keine Schiedsgerichte im Sinne der §§ 101 ff.

b) Das verfassungsrechtlich gewährte Selbstbestimmungsrecht der Kirchen steht der ausschließlichen Zuständigkeit der staatlichen Arbeitsgerichte im Rahmen von Streitigkeiten aus einem Arbeitsverhältnis mit der Kirche nicht entgegen.

Zwar ordnet und verwaltet nach Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV jede Religionsgemeinschaft ihre Angelegenheiten selbständig, dies aber nur innerhalb der Schranken der für alle geltenden Gesetze. Das Selbstordnungs- und Selbstverwaltungsrecht der Religionsgemeinschaften umfasst grundsätzlich auch die Befugnis zur selbständigen Kontrolle des selbst gesetzten Rechts durch kircheneigene Gerichte. Die Normen des ArbGG sind jedoch Teil der für alle geltenden im Sinne des Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV. Nur bei Streitigkeiten, bei denen es ausschließlich um die Anwendung kirchlichen Mitarbeitervertretungsrechts geht, ist die Zuständigkeit staatlicher Gerichte ausgeschlossen. Dies folgt aus Art. 140 GG i.V.m. Art. 137 Abs. 3 WRV und findet in § 118 Abs. 2 BetrVG, § 112 BPersVG seinen einfach gesetzlichen Ausdruck. Insoweit hat § 3 Abs. 3 KAGO deklaratorische Bedeutung und stellt insoweit lediglich klar, dass für Streitigkeiten aus dem Arbeitsverhältnis die Zuständigkeit der kirchlichen Gerichte für Arbeitssachen nicht gegeben ist, da die Zuständigkeit der Arbeitsgerichte für diese Streitigkeiten aus einem privatrechtlichen Arbeitsverhältnis durch Kirchenrecht gerade nicht ausgeschlossen werden kann. Bei Rechtsstreitigkeiten aus einem privatrechtlichen Arbeitsverhältnis sind die Normen des ArbGG auch für die Kirchen verbindlich. Die staatlichen Gerichte müssen jedoch kirchliches Recht anwenden, wenn von diesem die Entscheidung des Rechtsstreits abhängt (BAG, Urteil v. 11.11.2008, Az. 1 AZR 646/07, in juris recherchiert).

c) Der Rechtsweg zu den Arbeitsgerichten ist für den vorliegenden Rechtsstreit auch nicht durch höherrangiges Europarecht ausgeschlossen. (wird ausgeführt)

(2) Die DS-GVO verweist somit bezüglich der sachlichen Zuständigkeit bzw. bezüglich des Rechtswegs auf die Zuständigkeit der Gerichte des Mitgliedsstaates. Das in der DS-GVO den Kirchen gewährte Recht, ihren Datenschutz umfassend innerhalb kirchenrechtlicher Vorschriften zu regeln, d.h. von ihrer Rechtssetzungsbefugnis zum Erlass von materiell-rechtlichen Spezialvorschriften im Rahmen des Datenschutzes Gebrauch zu machen, umfasst nicht die Befugnis, eine nach staatlichem Recht vorgeschriebene ausschließliche Zuständigkeit einer Gerichtsbarkeit zugunsten einer eigenen kirchlichen Gerichtsbarkeit auszuschließen.

Die in § 2 KDSGO geregelte sachliche Zuständigkeit der kirchlichen Gerichte für Datenschutzangelegenheiten für gerichtliche Rechtsbehelfe des betroffenen Arbeitnehmers gegen den Verantwortlichen kann somit nur Rechtsstreitigkeiten betreffen, für die nach nationalem Recht keine anderweitige ausschließliche Gerichtsbarkeit gegeben ist. Für Streitigkeiten aus einem Arbeitsverhältnis, hier mögliche Schadensersatzansprüche aufgrund Datenschutzverstößen im Rahmen eines BEM, bleibt die ausschließliche Zuständigkeit der staatlichen Gerichtsbarkeit, nämlich der Arbeitsgerichtsbarkeit unberührt.

(3) Die Zuständigkeit der staatlichen Arbeitsgerichte für Klagen eines Arbeitnehmers auf Schadensersatz nach § 50 KDG ergibt sich nach Ansicht des Beschwerdegerichtes jedoch insbesondere aus den Regelungen der KDSGO.

So kann nach § 14 Abs. 2 KDSGO das Interdiözesane Datenschutzgericht lediglich erkennen auf Verwerfung des Antrages als unzulässig, Zurückweisung des Antrages als unbegründet oder Feststellung des Vorliegens und Umfangs einer Daten-

schutzverletzung. Das Interdiözesane Datenschutzgericht kann bei Begründetheit des Antrages somit nicht über einen beziffernten Schadensersatzanspruch im Rahmen einer Leistungsklage entscheiden. Darüber hinaus unterliegen kirchengerichtliche Entscheidung im Gegensatz zu staatlichen Entscheidungen nicht der Zwangsvollstreckung. Sie stellen keine Vollstreckungstitel im Sinne der §§ 704, 794 ZPO dar.

Aus alledem ergibt sich nach Ansicht des Beschwerdegerichts, dass für den vorliegenden Rechtsstreit der Rechtsweg zu den Arbeitsgerichten eröffnet ist.

d) Zu beachten ist dabei jedoch, dass im arbeitsgerichtlichen Verfahren Bescheide der kirchlichen Datenschutzaufsicht mit Tatbestandswirkung zu berücksichtigen sind und Urteile der kirchlichen Datenschutzgerichtsbarkeit betreffend die Feststellung von Datenschutzverstößen im arbeitsgerichtlichen Verfahren Rechtskraftwirkung zukommt. In einem individualarbeitsrechtlichen Verfahren, bei dem es um eine Verletzung kirchlicher datenschutzrechtlicher Vorschriften geht, z.B. in einem Kündigungsschutzverfahren oder einer Klage gegen eine Abmahnung oder – wie hier – einer Klage auf Schadensersatz, könnte sich die Frage stellen, ob wegen Vorentscheidung auszusetzen wäre. Gemäß § 148 ZPO kann das Gericht, wenn die Entscheidung des Rechtsstreits ganz oder zum Teil von dem Bestehen oder Nichtbestehen eines Rechtsverhältnisses abhängt, das den Gegenstand eines anderen anhängigen Prozesses bildet, anordnen, dass die Verhandlung bis zur Erledigung des anderen Rechtsstreits auszusetzen ist. Hier sind entscheidend die Umstände des Einzelfalls. Dies, da im Rahmen der Ermessensentscheidung nach § 148 ZPO gegenüber dem vorrangigen Zweck einer Aussetzung – einander widersprechender Entscheidung zu verhindern – insbesondere die Nachteile einer langen Verfahrensdauer und die dabei entstehenden Folgen für die Parteien abzuwägen sind. Dabei ist der Beschleunigungsgrundsatz des § 9 ArbGG ebenso zu berücksichtigen wie die Voraussetzungen zum Schutz vor überlanger Verfahrensdauer (Dr. T. R. in „Die kirchliche Datenschutzgerichtsbarkeit im arbeitsgerichtlichen Verfahren“, NZA 2020, 616 ff.). Wird im Falle eines bei staatlichen Arbeitsgerichten eingeleiteten Verfahrens, in dem die Verletzung kirchlicher datenschutzrechtlicher Vorschriften eine Rolle spielen, ein paralleles Verfahren bei der kirchlichen Datenschutzgerichtsbarkeit nicht eingeleitet, dann kann und muss das staatliche Arbeitsgericht die Frage einer datenschutzrechtlichen Pflichtverletzung am Maßstab des kirchlichen Rechts und unter Beachtung des verfassungsrechtlich limitierten Einklanggebots des Art. 91 DS-GVO prüfen (Dr. T. R. in „Die kirchliche Datenschutzgerichtsbarkeit im arbeitsgerichtlichen Verfahren“, VI. Zusammenfassung, NZA 2020, 616 ff.).

Bestattungsgesetz hat Vorrang vor Informationsfreiheitsgesetz (Ls)

(Verwaltungsgerichtshof Mannheim, Beschluss vom 6. August 2020 – VG 10 S 1856/20 –)

Es besteht kein Informationsfreiheitsanspruch nach § 1 Abs. 2 LIFG auf Erteilung einer anonymisierten Auskunft zu Gesundheitsangaben und Todesursachen, die sich aus den bei einem Landratsamt eingegangenen Todesbescheinigungen ergeben, die Verstorbene betreffen, bei denen ein Zusammenhang mit einer Covid-19-Infektion angenommen wird. § 22 Abs. 4 und 5 BestattG BW ist im Sinne des § 1

Abs. 3 LIFG eine Rechtsvorschrift, die den Zugang zu amtlichen Informationen vorrangig und abschließend regelt.

Zum Auskunftsanspruch gegenüber einer Bank (Ls)

(Amtsgericht Bonn, Urteil vom 30. Juli 2020 – 118 C 315/19 –)

1. Ein Bankkunde hat gem. Art. 15 DS-GVO gegen die Bank einen Anspruch auf Datenauskunft, der sich auch auf die Bankbewegungen zu seinem Girokonto erstreckt.
2. Der Begriff der „personenbezogenen Daten“ nach Art. 4 DS-GVO ist weit gefasst und umfasst nach der Legaldefinition in Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierbare natürliche Person beziehen.
3. Unter die Vorschrift fallen damit sowohl im Kontext verwendete persönliche Informationen wie Identifikationsmerkmale (z.B. Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht, Augenfarbe, Größe und Gewicht) oder innere Zustände (z.B. Meinungen, Motive, Wünsche, Überzeugungen und Werturteile) als auch sachliche Informationen, wie etwa Vermögens- und Eigentumsverhältnisse, Kommunikations- und Vertragsbeziehungen und alle sonstigen Beziehungen der betroffenen Person zu Dritten und ihrer Umwelt.
4. Auch solche Aussagen, die eine subjektive und/oder objektive Einschätzung zu einer identifizierten oder identifizierbaren Person liefern, weisen einen Personenbezug auf.
5. Der Auskunftsanspruch erfasst in Ansehung dieser Grundsätze mehr als nur die „Stammdaten“.
6. Dieser extensiven Ansicht zufolge sind daher z.B. einem Arbeitnehmer alle elektronisch verarbeiteten Arbeitszeitchecklisten, Entgeltunterlagen, Lohnkonten sowie den Arbeitnehmer betreffende E-Mails zu übermitteln, sofern und soweit keine Rechte Dritter betroffen sind.
7. Unter Ansehung dieser extensiven Auslegung des Begriffs der personenbezogenen Daten erscheint es gerechtfertigt, auch Kontobewegungen auf einem Bankkonto als vom Auskunftsanspruch erfasst anzusehen.
8. Soweit die Bank einwendet, dass der Kunde diese Daten bereits durch die Kontoauszüge erlangt hätte, die er über das Online-Banking abrufen konnte, führt dieser Einwand nicht zum Erlöschen der Datenauskunftsanspruchs i.S.v. § 362 Abs. 1 BGB. Denn das Zurverfügungstellen über das Online-Portal erfolgte nicht in Ansehung eines datenschutzrechtlichen Auskunftsanspruchs, sondern zur Erfüllung der Verpflichtung der Bank aus dem Zahlungsdienstleistungsvertrag, laufend Auszüge und periodische Rechnungsabschlüsse zu erteilen.
9. Zwar besteht Sinn und Zweck des Datenauskunftsanspruchs gem. dem Erwägungsgrund 63 zur DS-GVO zu-

Datenschutz und Informationsfreiheit auf Länderebene



Roßnagel [Hrsg.]
**Hessisches
 Datenschutz- und
 Informationsfreiheitsgesetz**
 HDSIG
 Handkommentar
 2021, ca. 750 S.,
 geb., ca. 98,- €
 ISBN 978-3-8487-6808-0
 Erscheint ca. Februar 2021

Der neue Handkommentar ermöglicht eine rechtssichere Handhabung der datenschutzrechtlichen Vorschriften. Die Autoren erläutern zudem im Detail, unter welchen Voraussetzungen und in welchen Verfahren den Bürgern ein Anspruch auf Zugang zu amtlichen Informationen zusteht.



Krügel | Schmieder [Hrsg.]
**Niedersächsisches
 Datenschutzgesetz**
 Handkommentar
 2021, ca. 500 S.,
 geb., ca. 98,- €
 ISBN 978-3-8487-5692-6
 Erscheint ca. Februar 2021

Der Handkommentar erläutert das Landesrecht im Rahmen des übergeordneten EU-Rechts und stellt Bezüge zu den bundesrechtlichen Vorschriften des BDSG her. Durch die einheitliche Struktur der Kommentierungen ermöglicht er einen schnellen Zugang zum Gesamtwerk.

Portofreie Buch-Bestellungen
 unter www.nomos-shop.de
 Alle Preise inkl. Mehrwertsteuer



nächst darin, die Rechtmäßigkeitskontrolle im Hinblick auf die Verarbeitung der personenbezogenen Daten zu ermöglichen. Gleichwohl begründet die Verfolgung eines darüber hinausgehenden bzw. anders gelagerten Zwecks (z.B. die Vorbereitung eines Gerichtsverfahrens) noch nicht den Einwand des Rechtsmissbrauchs. Nichts anderes kann daher gelten, wenn der Betroffene die Datenauskunft benötigen, um seine Position gegenüber Dritten zu stärken.

10. Der Streitwert einer Datenauskunft ist mit 5.000,00 EUR zu bemessen.

(Mitgeteilt von RA Konstantin Mertsiotakis, Brühl)

Personalratswahl mit Corona-Einschränkungen (Ls)

(Verwaltungsgericht Köln, Beschluss vom 7. Oktober 2020 – 33 K 1757/20.PVB –)

1. Eine Berechtigung zur Anfechtung einer Personalratswahl liegt nicht vor, wenn zahlreiche Beschäftigte wegen der Anordnung von Telearbeit zwar vor der Wahl im Betrieb nicht erreichbar, jedoch nicht gehindert waren, ihre Stimme per Briefwahl oder persönlich am Wahltag abzugeben.
2. Das Betretungsverbot für bestimmte Beschäftigte wäre nur dann eine Wahlbehinderung, wenn es nach den Umständen des Einzelfalls bei objektiver Betrachtung auf eine Erschwerung der Wahl gerichtet gewesen wäre. Daran fehle es, da die Maßnahme offenkundig dem Infektionsschutz diene und die die Beschäftigten hinreichend informiert gewesen seien.

(Nicht amtliche Leitsätze)

Anforderungen an eine Beschwerde bei der Aufsichtsbehörde (Ls)

(Verwaltungsgericht Mainz, Urteil vom 22. Juli 2020 – 1 K 473/19 –)

1. Eine datenschutzrechtliche Beschwerde muss alle Informationen enthalten, die erforderlich sind, damit die Aufsichtsbehörde den Sachverhalt erfassen und ggf. weiter aufklären, ihre Zuständigkeit überprüfen und etwaige Datenschutzverstöße feststellen kann. Die Beschwerde muss daher zumindest Angaben über die betroffene Person und den Verantwortlichen enthalten und zumindest ansatzweise zum Ausdruck bringen, welcher Verstoß gegen datenschutzrechtliche Vorschriften gerügt wird.
2. Der Beschwerdeführer kann von der Aufsichtsbehörde keine Ermittlungen ins Blaue hinein verlangen.

(Nicht amtliche Leitsätze)

Berichte, Informationen, Sonstiges

BayLDA: Typische Fehler bei Auskunftersuchen

Wie dem Tätigkeitsbericht für das Jahr 2019 der Bayerischen Datenschutz-Aufsichtsbehörde (BayLDA, 9. TB Zif. 5.1 zu entnehmen ist, gibt es einige typische Fehler bei Auskunftersuchen, sowohl bei den Unternehmen als auch den Betroffenen.

No-Go 1: Ignorieren von Auskunftsbegehren bei Identitätszweifeln

Bestehen Zweifel an der Identität des Betroffenen, können gemäß Art. 12 Abs. 6 DS-GVO Informationen als Nachweis der Identität angefordert werden. Die pauschale Behauptung von Zweifeln an der Identität genügt nicht, um Auskunftsbegehren per se unbeantwortet zu lassen. Beispiel Telefax: Auch Anfragen per Telefax ohne Absenderkennung müssen vom Verantwortlichen bearbeitet werden. Von einer Identifikationssicherheit kann grundsätzlich auch im Falle eines Telefaxes mit Absenderkennung nicht zweifelsfrei ausgegangen werden, da die Möglichkeit der Fälschung besteht.

No-Go 2: Auskunft über ausschließlich Stammdaten als personenbezogene Daten

Die bloße Beauskunftung von Stammdaten der betroffenen Person genügt nicht, um den Anforderungen des Art. 15 DS-GVO gerecht zu werden. Zu den personenbezogenen Daten gehören neben den Stammdaten unter anderem auch die Folgenden:

- Daten, welche Rückschlüsse auf das Konsumverhalten des Betroffenen geben (Einkäufe, Bestellungen, etc.)
- Kontodaten
- Körperliche Merkmale
- Interne Vermerke und Bewertungen
- Gesprächs- und Telefonvermerke

Bei einer großen Menge von personenbezogenen Daten kann der Verantwortliche eine Präzisierung der Anfrage anfordern.

No-Go 3: Einreichen der Beschwerde vor Verstreichen der Frist

Nicht zu vernachlässigen ist, dass nach Art. 12 Abs. 3 DS-GVO der Verantwortliche dazu verpflichtet ist, der betroffenen Person die sie betreffenden Informationen „unverzüglich, in jedem Fall aber innerhalb eines Monats“ zur Verfügung zu stellen. Ist aufgrund der Komplexität und Anzahl der Anträge eine Auskunft nicht innerhalb eines Monats möglich, kann eine Fristverlängerung von zwei Monaten unter Angabe der Gründe geltend gemacht werden. „Unverzüglich“ bedeutet nicht, dass eine Reaktion auf die Anfrage sofort zu erfolgen hat, sondern dass die Anfrage „ohne schuldhaftes Zögern“ zu bearbeiten ist. Die Aufsichtsbehörde kann nur tätig werden, wenn die Reaktion innerhalb der Monatsfrist ausbleibt oder die Auskunft unvollständig oder nicht rechtmäßig erfolgt ist.

No-Go 4: Zweck des Rechts auf Auskunft außer Acht lassen

Durch das Recht auf Auskunft haben betroffene Personen die Möglichkeit, die Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten zu überprüfen. Auf Basis dieses Wissens können weitere Betroffenenrechte, wie beispielsweise das Recht auf Berichtigung gemäß Art. 16 DS-GVO, ausgeübt werden. Mit dem Recht auf Auskunft sollen ausschließlich Datenschutzziele verfolgt werden. Dieses Recht soll nicht zur Sammlung von Beweisen für andere bestehende Konflikte dienen.

No-Go 5: Geltendmachung des Rechts auf Auskunft gegenüber dem Anwalt der Gegenseite

Ein Auskunftsrecht aus Art. 15 DS-GVO gegenüber Rechtsanwälten, die nicht für den/die Auskunft-Begehrende(n) tätig wurden (sondern z.B. für die gegnerische Partei) besteht gemäß § 29 Abs. 1 Satz 2 BDSG i.V.m. § 43a Abs. 2 BRAO nicht, weil die erwünschten Informationen einer gesetzlichen

Verschwiegenheitspflicht unterfallen. Das datenschutzrechtliche Auskunftsrecht liefert somit keine Möglichkeit, um vom Anwalt der Gegenseite die Offenlegung von Informationen zu erzwingen (siehe auch das anschließende Kapitel 5.2 des Tätigkeitsberichts).

No-Go 6: Beschwerde ohne beweiskräftige Nachweise

Die Datenschutzaufsichtsbehörde weiß zunächst nicht, welche Daten der Verantwortliche konkret speichert und verarbeitet. Sind betroffene Personen der Auffassung, die Auskunft ist nicht richtig oder nicht vollständig, benötigen wir beweiskräftige Nachweise, welche die Aussage des Verantwortlichen widerlegen, um ihm gegenüber darauf Bezug nehmen zu können.

No-Go 7: Berufung auf unverhältnismäßigen Aufwand ohne Darlegung der Umstände

Bei Berufung auf einen unverhältnismäßigen Aufwand i.S.d. § 34 Abs. 1 Nr. 2 BDSG ist der Verantwortliche dazu verpflichtet, der betroffenen Person die konkreten Umstände darzulegen.

Datenverarbeitungen des Betriebsarztes

Das Netzwerk Datenschutzexpertise (Autoren Karin Schuler und Thilo Weichert) beschäftigt sich in seiner aktuellen Veröffentlichung „Die Datenverarbeitung des Betriebsarztes – Hinweise zum datenschutzgerechten Umgang mit Patientendaten durch Betriebsärzte und betriebsärztliche Dienste“ mit einem Thema, welches sich in der Schnittmenge des Medizinrechts und des Datenschutzrechts abspielt, wobei ebenso so viele spannende Fragen des Arbeitsrechts und des Mitbestimmungsrechts, sowie die dort bestehenden spezifischen Regelungen, zur Anwendung kommen. (abrufbar. www.netzwerk-datenschutz-expertise.de)

Literaturhinweise

Alexander Roßnagel, Christian Geminn, **Datenschutz-Grundverordnung verbessern** – Änderungsvorschläge aus Verbrauchersicht, Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, 198 S., 54,00 €

Das Buch kann unter: <https://www.nomos-shop.de/titel/datenschutzgrundverordnung-verbessern-id-97389/> als Open Access erschienenes E-Book kostenlos heruntergeladen werden.

Es analysiert die Regelungen der DSGVO vor dem Hintergrund der inzwischen mehr als zwei Jahre Erfahrung, bewertet sie – vor allem aus dem Blickwinkel der Verbraucherinnen und Verbraucher – und leitet daraus 33 konkrete Verbesserungsvorschläge des Verordnungstextes ab. Die in dem Buch präsentierten Analysen, Bewertungen und Vorschläge sollen ermöglichen, die Ziele der Verordnung besser zu erreichen und ihre Akzeptanz zu stärken. Sie sollen dazu beitragen, Argumente für die notwendige Diskussion zur Fortentwicklung des Datenschutzrechts in der Europäischen Union zu liefern und Möglichkeiten aufzuzeigen, wie Grundrechte und Freiheiten in der Entwicklung zu einer digitalen Welt besser gefördert und geschützt werden können.

(Redaktion)

Sebastian Buten, **Die Betroffenenrechte nach der DS-GVO und ihre Umsetzung in der kommunalen Praxis**, Kommunal- u. Schul-Verlag, Wiesbaden, 1. Aufl. 2020, 189 S., xx,x €

Der Verfasser des Buches arbeitet im Fachbereich Steuerungsberatung der Stadt Meppen und hat und hat die Text als Masterarbeit eines berufs begleitenden Studiums an der Hochschule Osnabrück gefertigt.

Dass das Thema Datenschutz bei den Datenverarbeitungen einer Kom-

mune ein besonderes Gewicht hat, steht außer Frage. Der Autor widmet sich einem Teil der sich insoweit stellenden Probleme, nämlich den Betroffenenrechten nach der DSGVO. Dabei geht es um die Daten der Bürger, weil auf die bereichsspezifischen Regelungen für Beschäftigte nicht explizit eingegangen wird. Der Autor erwähnt, dass, wie sich am Beispiel von Cambridge Analytica zeige, bereits in der Vergangenheit personenbezogene Daten immer wieder unzulässigerweise verarbeitet wurden und dass Daten auch bei einer zulässigen Verarbeitung kompromittierend wirken können. Ein effektiver Schutz ist insbesondere bei der Datenverarbeitung durch Kommunen wichtig, da hier nicht nur einfache Kundendaten, sondern auch sensible Daten (z.B. Sozialdaten gem. § 35 SGB I, § 67 SGB X) verarbeitet werden. Die Arbeit soll darüber hinaus Kommunen die Erfüllung der Betroffenenrechte erleichtern und als Arbeitshilfe dienen, damit die datenschutzrechtlichen Vorgaben praxisgerecht umgesetzt werden können. Dieser Zielrichtung wird das Buch durchaus gerecht.

(Schriftleitung)

Tassilo-Rouven König, **Beschäftigten-datenschutz in der Beratungspraxis**, Nomos, Baden-Baden, 2020, 221 S., 39,00 €

Das Buch ist eine praxisbezogene, fundierte Auseinandersetzung mit dem Beschäftigtendatenschutz mit durchaus hinreichenden Fußnoten und weiteren Hinweisen. Es liefert anhand der Judikatur entwickelte und sofort umsetzbare Erläuterungen und Muster zum Zusammenspiel von Arbeitsrecht und Datenschutzrecht im Betrieb, u.a. zu folgenden typischen Problemkreisen:

- Fragerecht und Umgang mit Bewerberdaten beim Recruiting

- Datenschutzrechtliche Einwilligung und Betriebsvereinbarung
- Zugriff auf und Privatnutzung von dienstlichen „mobile devices“, E-Mail-Account und Internet
- Mitarbeiterfotografien
- Auskunftsrecht und Datenkopie nach Art. 15 DS-GVO
- Gesundheitsdaten und Betriebliches Eingliederungsmanagement (BEM)
- Datenschutz bei HR-IT-Systemen (Personalentwicklung, Zielerreichungsprozesse, Leistungskontrolle)
- Digitale Personalakte, bei denen alle relevanten Aspekte, zumindest im Ergebnis zusammengefasst, abgehandelt wurden.

Es schließt ab mit einigen Mustern für Checklisten und „Routineschreiben“.

(Schriftleitung)

Thomas Götz, **Big Data im Personalmanagement: Datenschutzrecht und betriebliche Mitbestimmung Theorie und Praxis des Arbeitsrechts**, Band 17, 1. Aufl. 2020, Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden, 233 S., 62,00 €

Das Werk, das die Doktorarbeit des Autors darstellt, erarbeitet ein transparentes Regelungskonzept zur Umsetzung von Big-Data-Analysen (auch „People-Analytics“) im Personalwesen. Ausgehend vom abstrakten Datenschutzrecht werden anhand konkreter Anwendungsbeispiele Lösungen entwickelt, die den Interessenausgleich zwischen Arbeitgeber, Arbeitnehmern und Betriebsrat praxisnah ermöglichen. Daneben untersucht das Werk Besonderheiten der betrieblichen Mitbestimmung bei der algorithmischen Verarbeitung von Beschäftigtendaten.

(Schriftleitung)

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.

Buchholz, Stefan/Kirsch, Marcus, IT-forensische Analyse von Telekommunikationsdaten im Beschäftigungsverhältnis aus dem Blickwinkel des TKG, der DSGVO und des BDSG, Ping 2020, S. 249

Der Artikel befasst sich mit der Frage, ob Arbeitgeber im Falle einer gestatteten Privatnutzung des betrieblichen Internetanschlusses bzw. des betrieblichen E-Mail-Accounts gegenüber ihren Mitarbeitern zu einem TK-Diensteanbieter gemäß § 3 Nr. 6 TKG werden und somit auch das Fernmeldegeheimnis zu wahren haben.

Gerling, Rainer W., Bring your own Device revisited, Datenschutz Praxis, 11/2020, S. 6

Die Corona-Pandemie hat zu vielfach unvorbereiteten und unregulierten Arbeiten im Homeoffice geführt. Der Beitrag legt den Entwurf einer Betriebsvereinbarung vor, mit der im Unternehmen für klare und sichere Verhältnisse gesorgt werden kann.

Grages Jan-Michael, Recht auf Vergessenwerden: Der BGH schärft die Konturen, K&R 2020, S. 726

Beim „Recht auf Vergessenwerden“ ergänzt und überlagert das europäische Datenschutzrecht die nationalen Gewährleistungen des allgemeinen Persönlichkeitsrechts. Betroffene gewinnen neue Möglichkeiten, um gegen Verweise auf missliebige Berichterstattung im Internet vorzugehen. Seit dem wegweisenden EuGH-Urteil „Google Spain“ ergehen hierzu regelmäßig Entscheidungen, die die im Beitrag dargestellten Vorgaben weiterentwickeln.

Krocker, Maximilian, Art. 22 DSGVO – ein Schuss in den Ofen?, Ping 2020, S. 255

Art. 22 DSGVO hat mit seinem Verbot automatisierter Entscheidungen einen weiten Anwendungsbereich und gewährt Betroffenen signifikante Rechte. In der Praxis spielt die Norm zwar kaum eine Rolle, jedoch birgt sie Risiken, deren Eindämmung nur schwer oder sogar unmöglich ist. Dieser Beitrag setzt sich mit den (verfassungsrechtlichen) Problemen und Potenzialen von Art. 22 DSGVO auseinander und zeigt auf, in welche Richtung sich die Regulierung von automatischen Einzelfallentscheidungen entwickeln könnte.

Nägele, Peter/Petric, Ronald/Schemmel, Frank, Die Datenschutzfolgeabschätzung in der Praxis, DuD 2020, S. 719

Nach Auffassung der Autoren fristet die DSFA trotz ihres Datenschutzpotenzials zur Erkennung und Abmilderung von Risiken ein Schattendasein. Der Beitrag erörtert u.a. diesbezüglich Aspekte, die in der Praxis und im Zusammenspiel mit den Aufsichtsbehörden bedeutsam sind, und den Bedarf an europaweit verbindlichen, einheitlichen Regelungen.

Quiel, Philipp/Piltz, Carlo, Die Relevanz von "Übereinkommen Nr. 108" bei der Prüfung des Datenschutzniveaus in Drittländern durch Unternehmen, K&R 2020, S. 731

Nach dem EuGH-Urteil in der Rechtssache Schrems II wird vermehrt deutlich, dass diese Entscheidung bei weitem nicht nur Auswirkungen auf Datenübermittlungen in die USA hat. Selbst einige Länder auf dem europäischen Kontinent sind im Sinne der Datenschutz-Grundverordnung (DS-GVO) Drittländer und für Übermittlungen in diese Staaten gelten ebenfalls die Vorgaben aus Kapitel V der Verordnung.

Roßnagel, Alexander, Die Evaluierung der Datenschutz-Grundverordnung, MMR 2020, S. 657

Der Autor zeigt an Hand der zwischenzeitlich gemachten Erfahrungen mit dem Regelungspotenzial der DS-GVO erkennbaren Novellierungsbedarf auf.

Suwelack, Felix, Datenschutzrechtliche Vorgaben für Homeoffice und Remote Work, ZD 2020, S. 561

Der Beitrag will u.a. ein Leitfaden für Arbeitgeber sein, um die u.a. durch die Corona-Pandemie erzwungene Umstellung auf „Heimarbeit“ nachhaltig und rechtssicher zu gestalten, um in Krisenfällen kurzfristig entsprechende Maßnahmen treffen zu können.

Wybitul, Tim/Brams, Isabelle, Neues zum immateriellen Schadensersatz wegen Datenschutzverstößen, CR 2020, S. 571

Der Beitrag geht an Hand einer Entscheidung des ArbG Düsseldorf (Urt. v. 05.03.2020 – 9 Ca 6557/18 –) der Reichweite eines sich aus Art. 82 DS-GVO ergebenden Schmerzensgeldanspruchs nach, d.h. der Frage ob dieser auch bei einer nicht vollständigen Auskunftserteilung nach Art. 15 DS-GVO fällig werden kann.



Vorbilder der Arbeitswelt in Corona-Zeiten: Der Hacker

Die Dunkle Seite des Datenschutzes

Darknet klingt dunkel, böse und gefährlich. Aber ist es das auch? Der Begriff beschreibt eine virtuelle Umgebung, in der Teilnehmer ihre Verbindungen untereinander manuell herstellen. Im Unterschied zu konventionellen Netzwerken werden Verbindungen hier nicht automatisch und willkürlich veranlasst. Das Darknet bietet ein höheres Maß an Sicherheit, weil Dritte nicht ohne Weiteres auf Verbindungen zugreifen können. Oft ist die Existenz des Netzwerks gar nicht bekannt. Damit ist das Darknet genauso so wenig ein verbotener Ort, wie ein dunkler, tiefer Wald das ist. Dass man sich dort verstecken kann, bedeutet weder, dass das Verstecken verboten ist, noch dass es ein Raum ohne Regeln wäre. Man darf im Darknet sowie im Verstecken der körperlichen Welt nur Erlaubtes tun. Das Recht gilt dort für alle, die es nutzen. Es gilt auch für alle, die das Recht dort durchsetzen müssen. Weil Polizei- und Strafverfolgungsbehörden rechtstreu sein müssen, und nur le-

gale Mittel einsetzen dürfen, geraten sie gegenüber Kriminellen, die ihr Unwesen dort mittels Technik verschleiern, ins Hintertreffen. Auch durch aus Datenschutzgründen gepriesene und für jedermann leicht bedienbare soziale Netzwerke wie Telegram, die hohen Schutz der Privatsphäre gewährleisten, bekommt der Datenschutz eine dunkle Kehrseite. Bei Telegram, so wurde nun berichtet, können Drogen, Waffen und Hackerprogramme wie im Darknet leicht und unentdeckt gehandelt werden. Längst nicht jeder, der das Darknet nutzt, ist ein Krimineller. Staat und Datenschützer stehen vor dem Dilemma, die Bürger im Darknet nicht unter Generalverdacht stellen zu dürfen und zugleich ein Auge auf diese virtuelle Umgebung haben zu müssen, um deren redliche Nutzer und das Recht zu schützen. Das ist eine Herkulesaufgabe für einen Staat, der der Organisation von Schwere Kriminalität nicht tatenlos zusehen darf. Man kann Kampfdrohnen nicht

mit Taschenmessern stoppen. Ebenso kann man die von Kriminellen eingesetzten Mittel von Verschlüsselungstechnik bis hin zu künstlicher Intelligenz nicht bekämpfen, wenn man ihnen nicht auf Augenhöhe begegnet. Es gilt, die Strafverfolgungsbehörden technisch und mit Fachwissen auszustatten. In diesen Kraftakt investiert die Justizpolitik etwa in NRW viel Energie und Geld. Auch im Netz muss es im Rechtsstaat gelingen, Freiheit und Sicherheit gleichzeitig zu gewährleisten. Dazu gehört es, den Schutz der Privatsphäre da zu wahren, wo er rechtmäßig in Anspruch genommen wird. Da wo das Recht es verlangt und gebietet, muss man mit den Mitteln des Rechts eingreifen.



die neue
Aufgabe
des DSB



**Organisieren Sie mit dem
Leitfaden interne Kontrollen,
Datenschutz-Audits und
Überwachung effektiv,
nachweisbar, risikoorientiert!**

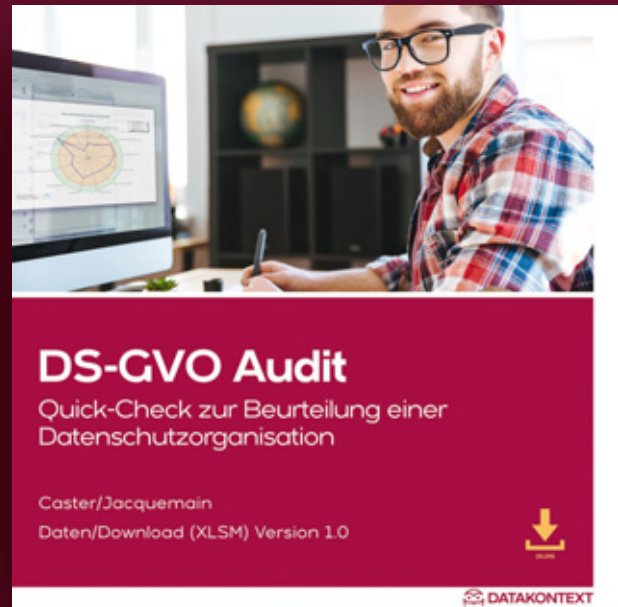
Die Überwachungsaufgabe des
Datenschutzbeauftragten nach DS-GVO

Autoren: Ralf Herweg / Thomas Müthlein
1. Auflage 2020 / 88 Seiten / DIN A4
ISBN 78-3-89577-853-7
69,99 € inkl. E-Book (PDF)

Bestellen Sie direkt unter:
datakontext.com/ueberwachungsaufgabe

Ihr ständiger
Begleiter im
Datenschutz-
Management.

Datenschutz-
organisationen
prüfen und
beurteilen mit
begrenztem
Zeitaufwand.



Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Ihre DS-GVO Umsetzung smart auditiert und visualisiert.

Bestellen Sie direkt unter: datakontext.com