

# RDV

Zeitschrift für Datenschutz  
und Digitalisierung

Recht der Datenverarbeitung

## Herausgeber

Prof. Dr. Rolf Schwartmann  
Andreas Jaspers  
Prof. Dr. Gregor Thüsing

## Ehrenherausgeber

Prof. Peter Gola

## in Kooperation mit

Gesellschaft für Datenschutz  
und Datensicherheit (GDD) e.V.

## Praxisbeirat

Dr. Peter Allgayer  
Kristin Benedikt  
Dr. Stefan Brink  
Paula Cipierre  
Monish Darda  
Dr. Jens Eckhardt  
Thomas Fuchs  
Prof. Dr. Bernd Grzeszick  
Dr. h.c. Marit Hansen  
Markus Hartmann  
Prof. Dr. Christian-Henner Hentsch  
Prof. Dr. Herwig Hofmann  
Dr. Marek Jansen  
Prof. Dr. Tobias Keber  
Prof. Ulrich Kelber  
Dr. Martin Kessen  
Kevin Leibold  
Thomas Muthlein  
Prof. Dr. Boris P. Paal  
Prof. Dr. Heinz-Joachim Pabst  
Yvette Reif  
Frederick Richter  
Steve Ritter  
Maria Christina Rost  
Prof. Dr. Frauke Rostalski  
Prof. Dr. Prof. h.c. Jürgen Taeger  
Rebekka Weiß  
Steffen Weiß  
Prof. Dr. Christiane Wendehorst  
Kai Zenner

## Redaktion

Lucia Burkhardt  
Moritz Köhler  
Eva-Maria Pottkämper

## AUFSÄTZE

**GOLA:** Hinweisgeberschutz nach dem HinSchG, dem LkSG und weiteren bereichsspezifischen Melderegungen – ein Überblick

**FRANCK:** Zertifizierungsstellen nach der DS-GVO als Beliehene?

**WYBITUL:** Wie geht es weiter mit DS-GVO-Bußgeldern?

## KURZBEITRÄGE

**REIF:** Praxisfälle zum Datenschutzrecht XXIII: Fotografien und Anzeige von Falschparkern durch Privatpersonen

**GMEINER:** Erstattung von Rechtsanwaltskosten im kirchengerichtlichen Datenschutzverfahren

**MANNAH:** Die Anonymisierung im Kontext von Krisenresilienzplattformen

## RECHTSPRECHUNG

**EuGH:** Voraussetzungen eines immateriellen Schadenersatzanspruchs nach Art. 82 DS-GVO

**EuGH:** Reichweite des Rechts auf Kopie aus Art. 15 Abs. 3 S. 1 DS-GVO

**EuGH:** Kein Recht auf Löschung bei Verstößen gegen Artt. 26 und 30 DS-GVO

**EuG:** Kein Personenbezug bei fehlenden Mitteln des Datenempfängers zur Re-Identifizierung mit Anm. von Paul C. Johannes, LL.M.

**OLG Hamm:** Ein Schmerzensgeldanspruch setzt keine objektiv nachvollziehbare Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht voraus

**LG Heidelberg:** (Mit-)Verantwortlichkeit von Google Ireland neben Google LLC aus den USA bei Lösungsansprüchen nach Art. 17 Abs. 1 DS-GVO

**AG München:** Erlöschen von ungenutzten Einwilligungserklärungen

**VG Gelsenkirchen:** Einwand unzulässiger Rechtsausübung kann Auskunftersuchen entgegenstehen





**Hybrid:  
Online &  
in Köln**

# 47. DAFTA

15.-17. November 2023

# 42. RDV-Forum

14. November 2023

KI, Gesetzgeber und EuGH – Neue Herausforderungen für den betrieblichen Datenschutz

Jetzt anmelden: [datakontext.com/dafta-2023](https://datakontext.com/dafta-2023)

<b>EDITORIAL</b>	<b>211</b>	<b>Kein Personenbezug bei fehlenden Mitteln des Datenempfängers zur Re-Identifizierung</b> (EuG, Urt. v. 26.04.2023) mit Anm. von Paul C. Johannes, LL.M.	<b>254</b>
<b>VERANSTALTUNGEN</b>	<b>212</b>		
<b>REDAKTION</b>	<b>213</b>		
<b>AUFSÄTZE</b>			
Prof. Peter GOLA <b>Hinweisgeberschutz nach dem HinSchG, dem LkSG und weiteren bereichsspezifischen Melderegeln – ein Überblick</b>	<b>213</b>	<b>Ein Schmerzensgeldanspruch setzt keine objektiv nachvollziehbare Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht voraus</b> (OLG Hamm, Urt. v. 20.01.2023)	<b>257</b>
Prof. Dr. Lorenz FRANCK <b>Zertifizierungsstellen nach der DS-GVO als Beliehene?</b>	<b>223</b>	<b>(Mit-)Verantwortlichkeit von Google Ireland neben Google LLC aus den USA bei Lösungsansprüchen nach Art. 17 Abs. 1 DS-GVO</b> (LG Heidelberg, Urt. v. 31.03.2023)	<b>259</b>
Tim WYBITUL <b>Wie geht es weiter mit DS-GVO-Bußgeldern?</b>	<b>229</b>	<b>Einwand unzulässiger Rechtsausübung kann Auskunftersuchen entgegenstehen</b> (VG Gelsenkirchen, Beschl. v. 08.02.2023)	<b>260</b>
<b>KURZBEITRÄGE</b>			
RAin Yvette REIF, LL.M. <b>Praxisfälle zum Datenschutzrecht XXIII: Fotografien und Anzeige von Falschparkern durch Privatpersonen</b>	<b>235</b>	<b>Kein Anspruch auf Löschung der Daten eines Geschäftsführers aus dem Handelsregister</b> (OLG Celle, Beschl. v. 24.02.2023)	<b>262</b>
Robert GMEINER <b>Erstattung von Rechtsanwaltskosten im kirchengerichtlichen Datenschutzverfahren</b>	<b>239</b>	<b>Voraussetzungen einer freiwilligen Einwilligung und Anforderungen an eine Übermittlung von IP-Adressen in die USA</b> (LG Köln, Urt. v. 12.01.2023)	<b>263</b>
Sakyi MANNAH <b>Die Anonymisierung im Kontext von Krisenresilienzplattformen</b>	<b>241</b>	<b>PRESSEVERÖFFENTLICHUNGEN: Verwaltungsgericht Köln verpflichtet Bundesgesundheitsministerium zur Herausgabe von Unterlagen zur Maskenbeschaffung</b> (VG Köln, Urt. v. 19.01.2023)	<b>264</b>
<b>RECHTSPRECHUNG</b>			
<b>HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ:</b>			
<b>Voraussetzungen eines immateriellen Schadenersatzanspruchs nach Art. 82 DS-GVO</b> (EuGH, Urt. v. 04.05.2023)	<b>246</b>	<b>BERICHTE, INFORMATIONEN, SONSTIGES</b>	
<b>Reichweite des Rechts auf Kopie aus Art. 15 Abs. 3 S. 1 DS-GVO</b> (EuGH, Urt. v. 04.05.2023)	<b>249</b>	<b>Das Forschungsdatengesetz</b>	<b>265</b>
<b>Erlöschen von ungenutzten Einwilligungserklärungen</b> (AG München, Urt. v. 14.02.2023)	<b>251</b>	<b>Prof. Dr. Tobias Keber neuer Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg</b>	<b>266</b>
<b>WICHTIGES AUS DER RECHTSPRECHUNG:</b>			
<b>Kein Recht auf Löschung bei Verstößen gegen Artt. 26 und 30 DS-GVO</b> (EuGH, Urt. v. 04.05.2023)	<b>252</b>	<b>BERICHT AUS BRÜSSEL</b>	
		<b>Endspurt in der EU-Digitalpolitik</b>	<b>266</b>
		<b>BUCHBESPRECHUNG</b>	<b>267</b>
		<b>NETZBLICK</b>	<b>268</b>

**HERAUSGEGEBEN VON**

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

Andreas Jaspers, Rechtsanwalt, Bonn

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

*Gemeinsam verantw. für den Textteil – Anschrift der Herausgeber GDD e.V., Heinrich-Böll-Ring 10, 53119 Bonn*

**EHRENHERAUSGEBER**

Prof. Peter Gola

**IN KOOPERATION MIT**

Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn

**PRAXISBEIRAT**

Dr. Peter Allgayer, Richter am Bundesgerichtshof

Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg

Dr. Stefan Brink, Institut für Digitalisierung der Arbeitswelt, Berlin

Paula Cipierre, Palantir Technologies, Berlin

Monish Darda, Chief Technology Officer (CTO) von Icertis, Bellevue, Washington (USA)

Dr. Jens Eckhardt, Rechtsanwalt, Düsseldorf

Thomas Fuchs, LL.M. Eur., Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Prof. Dr. Bernd Grzeszick, Richter am Verfassungsgericht Nordrhein-Westfalen

Dr. h.c. Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein

Markus Hartmann, Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Köln

Prof. Dr. Christian-Henner Hentsch, M.A., LL.M., Kölner Forschungsstelle für Medienrecht, Technische Hochschule, Köln

Prof. Dr. Herwig Hofmann, Universität Luxemburg

Dr. Marek Jansen, Google Deutschland, Köln

Prof. Dr. Tobias Keber, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Prof. Ulrich Kelber, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn

Dr. Martin Kessen, Richter am Bundesgerichtshof, Karlsruhe

Kevin Leibold, LL.M., Rechtsanwalt, Düsseldorf

Thomas Muthlein, DMC Datenschutz Management & Consulting, Frechen

Prof. Dr. Boris P. Paal, M.Jur. (Oxford), Universität Leipzig

Prof. Dr. Heinz-Joachim Pabst, Hochschule des Bundes für öffentl. Verwaltung, Köln

Yvette Reif, LL.M., stellv. Geschäftsführerin der GDD e.V., Bonn

Frederick Richter, LL.M., Vorstand Stiftung Datenschutz, Leipzig

Steve Ritter, BSI, Bonn

Maria Christina Rost, Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Wiesbaden

Prof. Dr. Frauke Rostalski, Universität zu Köln

Prof. Dr. Prof. h.c. Jürgen Taeger, Rechtsanwalt, Köln

Rebekka Weiß, LL.M., Bitkom, Berlin

Steffen Weiß, LL.M., Rechtsanwalt, Hamburg

Prof. Dr. Christiane Wendehorst, Universität Wien

Kai Zenner, Digitalreferent im Europäischen Parlament

**Redaktion**

Lucia Burkhardt

Moritz Köhler

Eva-Maria Pottkämper

(Verantwortlich für den Rechtsprechungsteil)

**Redaktionsbüro**

Serena Roller | Christina Wengenroth

Anschrift Redaktion/-Büro

DATAKONTEXT GmbH

Augustinusstr. 11a | 50226 Frechen-Königsdorf

Telefon: +49 228 969675-00

RDV-Redaktion@datakontext.com

**Erscheinungsweise**

6 x jährlich

**Bezugspreis**

Jahresabonnement € 174,-

Einzelheft € 25,-

MwSt. im Preis enthalten, jeweils zzgl. Versandkosten

**Vertrieb**

Dieter Schulz

Tel.: +49 2234 98949-99

dieter.schulz@datakontext.com

**Abo-Service**

Telefon: +49 89 2183-7110

Telefax: +49 89 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

Augustinusstr. 11a | 50226 Frechen-Königsdorf

Telefon: +49 2234 98949-0

Telefax: +49 2234 98949-32

www.datakontext.com

Geschäftsführung: Dr. Karl Ulrich

HRB 337678

**Satz**

alka mediengestaltung gmbh

Rücksgasse 3 | 53332 Bornheim

**Druck**

Grafisches Centrum Cuno GmbH & Co. KG

Gewerbering West 27 | 39240 Calbe (Saale)

**Anzeigenverwaltung**

DATAKONTEXT GmbH, Frechen

Wolfgang Scharf (verantwortlich)

Telefon: +49 2234 98949-60

wolfgang.scharf@datakontext.com

www.datakontext.com

**Manuskripte**

Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an das Redaktionsbüro 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.

**Hinweis**

Weil in der RDV bereits bestehende und veröffentlichte Texte integriert sind, wird teilweise, auch zur besseren Lesbarkeit, nur die männliche Sprachform verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

# Der Datenschutzbeauftragte als interne Meldestelle nach dem HinSchG?

Gemäß § 15 Abs. 1 S. 1 Hinweisgeberschutzgesetz (HinSchG) müssen die mit einer internen Meldestelle betrauten Personen bei der Ausübung ihrer Tätigkeit unabhängig sein. Allerdings dürfen diese Personen neben ihrer Tätigkeit als interne Meldestelle auch andere Aufgaben und Pflichten übernehmen, vgl. § 15 Abs. 1 S. 2 HinSchG. Dabei ist sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu Interessenkonflikten mit der Tätigkeit als interne Meldestelle führen, (§ 15 Abs. 1 S. 3 HinSchG). Gleiches gilt für die Tätigkeit des Datenschutzbeauftragten, (Art. 38 Abs. 6 DS-GVO).

Dies führt zu der Fragestellung, ob sich die beiden Ämter des Datenschutzbeauftragten und der internen Meldestelle nebeneinander vereinbaren lassen. Erwägungsgrund 56 der EU-Hinweisgeberschutzrichtlinie führt exemplarisch einige Personen eines Unternehmens auf, die die Rolle der internen Meldestelle wahrnehmen könnten. Dort wird unter anderem auch der Datenschutzbeauftragte als zulässige Person genannt, der zugleich die Rolle der internen Meldestelle bekleiden kann. Auf diesen Erwägungsgrund nimmt auch die Gesetzesbegründung zum HinSchG Bezug. Die Ausübung beider Ämter ist somit rechtlich möglich.

Jedoch stellt sich die Frage, ob eine gleichzeitige Ausübung der Ämter auch sinnvoll ist. Gerade bei mittleren und großen Unternehmen besteht die Gefahr von Interessenkonflikten, die der gleichzeitigen Ausübung widersprechen:

Zunächst könnte der zeitliche Umfang der beiden Tätigkeiten zu einem Interessenkonflikt führen. Je größer ein Unternehmen ist, desto mehr Zeit muss dem Datenschutzbeauftragten zur Aufgabenerfüllung eingeräumt werden. Gleiches gilt für die Erfüllung der Aufgaben der internen Meldestelle. Es ist also zu befürchten, dass die gleichzeitige Wahrnehmung beider Ämter zu einer Vernachlässigung eines Amtes führt. Zudem besteht bei einer zeitlichen Überlastung des internen Meldekanals die Gefahr, dass die hinweisgebenden Personen ihre Meldung an die externe Meldestelle weitergeben. Dies hat zur Folge, dass die jeweiligen Missstände im Unternehmen nicht intern gelöst werden können, sondern direkt ein behördliches (Bußgeld-)Verfahren droht.

Sowohl der Datenschutzbeauftragte als auch die Person der internen Meldestelle unterliegen besonderen Verschwiegenheits- und Geheimhaltungspflichten. Jedoch besteht mit § 9 HinSchG eine Ausnahme von diesen Pflichten, sodass im Vergleich zur DS-GVO ein anderes Geheimhaltungsniveau besteht. Dieses unterschiedliche Schutzniveau könnte ebenfalls zu einem Interessenkonflikt führen. Darüber hinaus besteht die Gefahr der faktischen Selbstkontrolle. Die interne Meldestelle legt das jeweilige Meldeverfahren im Unternehmen (§ 17 HinSchG) sowie angemessene Folgemaßnahmen (§ 18 HinSchG) fest und ist somit als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO einzustufen. Da es gemäß Art. 37 Abs. 1 lit. b DS-GVO die primäre Aufgabe des Datenschutzbeauftragten ist, den Verantwortlichen zu überwachen, würde die gleichzeitige Ausübung beider Stellen zu einer faktischen Selbstkontrolle führen. Diese Selbstkontrolle stellt einen Interessenkonflikt dar, so dass die Ausübung beider Rollen unzulässig ist.

Die aufgezeigten Interessenkonflikte und Risiken verdeutlichen, dass durch die Einbindung einer weiteren Person und die klare Benennung der einzelnen Pflichten, diese Risiken umgangen bzw. verringert werden können. Insbesondere wegen der faktischen Selbstkontrolle ist die klare personelle Trennung von Datenschutzbeauftragtem und interner Meldestelle zu empfehlen.



**RA Andreas Jaspers**

ist Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Termine	Thema	Ort	Kontakt
04.-08.09.2023	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V./DATAKONTEXT
07.09.2023	DS beim Einsatz von Apps & Smartphones im UN	Online	GDD e.V./DATAKONTEXT
12.-13.09.2023	Datenschutz kompakt	Online	GDD e.V./DATAKONTEXT
12.09.2023	Unbeabsichtigte Datenschutz-Verstöße – Kompaktkurs	Online	GDD e.V./DATAKONTEXT
13.09.2023	Microsoft 365/Office 365 – Kompaktkurs	Online	GDD e.V./DATAKONTEXT
14.09.2023	Die Aufgaben und der Tätigkeitsbericht des betrieblichen DSB praxisnah im Unternehmen	Köln	GDD e.V./DATAKONTEXT
14.09.2023	TTDSG: Onlinedatenschutz auf dem Weg zur ePrivacy-Verordnung	Online	GDD e.V./DATAKONTEXT
18.09.2023	Planung und Umsetzung der Überwachungsaufgaben des DSB	Frankfurt/Main	GDD e.V./DATAKONTEXT
19.09.2023	Datenschutz Aktuell	Köln	GDD e.V./DATAKONTEXT
19.09.2023	Whistleblowing und Datenschutz	Online	GDD e.V./DATAKONTEXT
20.-21-09.2023	Datenschutz-Management – Teil 3	Online	GDD e.V./DATAKONTEXT
20.09.2023	Mobile- und Homeoffice	Köln	GDD e.V./DATAKONTEXT
20.09.2023	Einführung gesetzlicher Wirksamkeitstest im UN – Kompaktkurs	Online	GDD e.V./DATAKONTEXT
25.-27.09.2023	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V./DATAKONTEXT
26.-27.09.2023	Ausbildung zum/zur Datenschutzkoordinator/in	Köln	GDD e.V./DATAKONTEXT
26.09.2023	DS-Prozess Austritt – Kompaktkurs	Online	GDD e.V./DATAKONTEXT
27.09.2023	Strategischer Umgang mit Bußgeldbescheiden	Online	GDD e.V./DATAKONTEXT
28.09.2023	Datenschutz International	Online	GDD e.V./DATAKONTEXT
09.10.2023	Datenschutz und Betriebsrat unter der DS-GVO	Köln	GDD e.V./DATAKONTEXT
10.10.2023	Datenschutz und IT-Sicherheit bei der Nutzung von Cloud Services	Online	GDD e.V./DATAKONTEXT
10.10.2023	Datenschutz-Fehler bei Bewerbungen – Kompaktkurs	Online	GDD e.V./DATAKONTEXT
10.10.2023	Prüfung zum/zur Datenschutzkoordinator/in	Online	GDD e.V./DATAKONTEXT
24.-25.10.2023	Arbeitsgemeinschaft (ARGE) betrieblicher Datenschutz	Köln/ Düsseldorf	GDD e.V./DATAKONTEXT



**DATAKONTEXT GmbH, [www.datakontext.com](http://www.datakontext.com), Tel. +49 2234 98949-40**

## REDAKTION

Moritz Köhler ist Doktorand bei Prof. Dr. Rolf Schwartmann und wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln. Er hat Anfang 2023 in Freiburg sein erstes Staatsexamen abgeschlossen. Seine Forschungsschwerpunkte liegen in den Bereichen Künstliche Intelligenz, Datenschutz und Medienrecht. So ist er aktuell an Kommentierungen zu DS-GVO/BDSG sowie zur KI-Verordnung beteiligt. Als Mitglied der RDV-Redaktion wird er an der Auswahl und Aufbereitung praxisrelevanter Entscheidungen im Recht der Datenverarbeitung mitwirken.



Moritz Köhler

## AUFSÄTZE

Prof. Peter Gola

## Hinweisgeberschutz nach dem HinSchG, dem LkSG und weiteren bereichsspezifischen Melderegulungen – ein Überblick

Mit einigen Verzögerungen wurde nunmehr die EU-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. L 305 v. 26.11.2019, S. 1789), in nationales Recht umgesetzt. Neben dem sog. Whistleblowing als „Stammgesetz“ regelnden Hinweisgeberschutzgesetz – HinSchG (BGBl. I v. 02.06.2023), bestehen weitere bereichsspezifische Melderegulungen. Ebenfalls aktuell ist das seit dem 01.01.2023 geltende Lieferkettensorgfaltspflichtengesetz – LkSG- (BGBl. I v. 22.07.2022), das größere Unternehmen zur Installation eines angemessenen unternehmensinternen Beschwerdeverfahrens verpflichtet. Es bietet sich an, die neuen Hinweisverfahren und bereits – ggf. im Rahmen der Compliance freiwillig oder kraft gesetzlicher Verpflichtung – etablierte Meldeverfahren zu koordinieren.

### I. Einführung

#### 1. Ein neues „einheitliches“ Schutzsystem

Mit dem neuen HinSchG<sup>1</sup> soll der Schutz natürlicher Personen gewährleistet werden, die im Rahmen ihrer beruflichen Tätigkeit beobachtete Verstöße gegen in einem umfangreichen Katalog aufgelistete (Schutz)-Regelungen anzeigen.<sup>2</sup> Betroffenen sind Meldungen über rechtswidrige oder missbräuchliche

<sup>1</sup> Bruns, Das neue Hinweisgeberschutzgesetz, NJW 2023, 1609.

<sup>2</sup> Fuhlrott/Henckel, Hinweisgeberschutzgesetz: Handlungsbedarf für Unternehmen und Personalabteilungen, ArbRAktuell 2022, 441; Schoch/Kumar, Der neue Entwurf eines Hinweisgeberschutzgesetzes, CB 2022, 181; Scholz, Hinweisgeberschutz zwischen Legalitäts- und Legalitätskontrollpflicht, AG 16/2022, 553; Thüsing/Musiol, Hinweise zum Hinweisgeberschutzgesetz, BB 2022, 2420; Zimmer/Schwung, Hilfe für Hinweisgeber – Beweislastumkehr nach § 36 II HinSchG-RegE, NZA 2022, 1167; Zimmer/Humphrey, Meldesysteme nach der Whistleblower-Richtlinie der EU, BB 2022, 372.

Handlungen (§ 3 Abs. 2 HinSchG) eines Unternehmens oder der öffentlichen Hand, d.h. von in § 3 Abs. 9 HinSchG mit dem neuen Begriff des „Beschäftigungsgebers“ erfassten Einrichtungen.<sup>3</sup>

Während bislang im deutschen Recht der Schutz hinweisgebender Personen gesetzlich nur fragmentarisch und uneinheitlich in verschiedenen Lebensbereichen ausgestaltet war, soll das HinSchG in Gestalt eines „Stammgesetzes“<sup>4</sup> ein einheitliches Schutzsystem für Hinweisgeber schaffen. Mit internen und externen „Meldekanälen“ und auch mit dem Weg an die Öffentlichkeit sollen hinweisgebenden Personen drei Meldewege eröffnet werden, wobei der interne Meldeweg ggf. für Beschäftigte Vorrang haben soll. Damit gilt weiterhin in gewissem Umfang der vor allem aus dem Rücksichtnahmegebot des § 241 Abs. 2 BGB gefolgerte Vorrang betriebsinterner Aufklärung. Wendet sich der Beschäftigte gleichwohl an die Aufsichtsbehörde, bedeutet das kein dortiges Verwendungsverbot der Information.

## 2. Die bisherigen gesetzlichen Einzelfallregelungen

### a) Beispiele

Schon bisher konnten Mitarbeiter – ohne Konsequenzen fürchten zu müssen – gemäß fallbezogenen gesetzlichen Regelungen Meldungen über Gesetzesverstöße bei der jeweils zuständigen Behörde machen. Diese Regelungen sollen neben denen des HinSchG fortbestehen.

Meldungen konnten bzw. können bei der zuständigen Behörde z.B. bei mangelhaftem Arbeitsschutz (§ 17 Abs. 2 ArbSchG), bei Korruptionsstraftaten (§ 67 Abs. 2 Nr. 3 BBG) oder in Fällen von Geldwäsche (§ 48 GWG) erfolgen.

Ferner gibt es für Kredit- und Finanzdienstleister Vorgaben für Meldesysteme und interne Kontrollverfahren (z.B. § 25a Abs. 1 S. 3 Nr. 3 KWG, §§ 47, 53a Abs. 5 des Gesetzes über das Aufspüren von Gewinnen schwerer Straftaten).

§ 4d Abs. 6 des Gesetzes über die Bundesanstalt für Finanzdienstleistungsaufsicht (FinDAG) schützt Mitarbeiter, die – ggf. nur potenzielle – Verstöße gegen Rechtsnormen melden, deren (Nicht)-Einhaltung zu überwachen oder zu sanktionieren in der Kompetenz der Bundesanstalt für Finanzaufsicht liegt. Meldende Personen dürfen wegen der Information der Behörde arbeitsrechts-, haftungs- oder strafrechtlich belangt werden, es sei denn, dass die Meldung vorsätzlich oder grob fahrlässig unberechtigt erfolgte. Die Identität legitim einmeldender Personen ist grundsätzlich vertraulich zu behandeln. Auch anonyme Meldungen unterliegen der sachgerechten Bearbeitungspflicht (§ 4d Abs. 3 FinDAG).

Eine weitgehend entsprechende Regelung enthält § 3b Abs. 5 des Börsengesetzes (BörsG). Betroffen sind Meldungen im Zuständigkeitsbereich der Börsenaufsichtsbehörde. Sie trifft geeignete Vorkehrungen, um eine vertrauliche Meldung von möglichen oder tatsächlichen Verstößen gegen das Börsenverhalten regelnde Normen, zu ermöglichen. Mitarbeiter der beaufsichtigten Unternehmen oder Personen, die bei einer Börse beschäftigt sind, dürfen vertraglich hinsichtlich der Abgabe von Meldungen nicht eingeschränkt werden. Entgegenstehende Vereinbarungen sind unwirksam (§ 3b Abs. 6 BörsG). Die Meldungen können auch anonym erfolgen.

Zum Schutz der Identität der meldenden Person sieht § 3b Abs. 3 S. 1 BörsG zudem vor, dass die Identität des Meldenden

nicht bekannt gegeben wird, es sei denn die Person hat ihre ausdrückliche Zustimmung dazu gegeben. Zudem ist nach Abs. 5 geregelt, dass Mitarbeiter von beaufsichtigten Unternehmen oder Personen für die Meldung grundsätzlich weder arbeitsrechtlich noch strafrechtlich verantwortlich gemacht werden.

Neu ist schließlich die noch darzustellende Pflicht der Betreiber globaler Lieferketten nach dem LkSG zur Einrichtung eines „angemessenen unternehmensinternen Beschwerdeverfahrens“ (§ 8 LkSG).

### b) Interne Hinweisrechte

Wohl nur zur Klarstellung weist die Gesetzesbegründung zum HinSchG<sup>5</sup> darauf hin, dass auch die Rechte der Beschäftigten auf Konsultation ihrer Vertreter unberührt bleiben, d.h. also konkret § 80 Abs. 1 Nr. 3 BetrVG/§ 62 Abs. 1 Nr. 3 BPersVG. Gleiches gilt auch ohne Hinweis hierauf für das (Hinweis-)Recht der Beschäftigten sich nach Art. 38 Abs. 4 und Art. 57 Abs. 1 lit. f DS-GVO mit Hinweisen an die interne und externe Datenschutzkontrollinstanz zu wenden. Obwohl die Mitarbeitervertretung nach § 79a BetrVG/§ 68 BPersVG<sup>6</sup> und jedenfalls auch der interne Datenschutzbeauftragte<sup>7</sup> Teil der verantwortlichen Stelle sind – müssen sie die Informanten ggf., – d.h. in jedem Falle, wenn der Meldende es wünscht – gegenüber dem Arbeitgeber vertraulich behandeln (Art. 38 Abs. 5 DS-GVO; § 80 Abs. 1 Nr. 3 BetrVG).

### c) Das GeschGehG

Das Geschäftsgeheimnisgesetz<sup>8</sup> brachte den Unternehmen neuen Handlungsbedarf zum Schutz ihrer Geschäftsgeheimnisse; gleichzeitig enthält es Regelungen, die ggf. von dem Geheimhaltungsschutz von Geschäftsgeheimnissen befreien. Nach § 5 Nr. 2 GeschGehG wird die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses nicht untersagt, wenn diese zum Schutz eines berechtigten bzw. öffentlichen Interesses an der Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens erfolgt.<sup>9</sup> Erfasst bzw. privilegiert wird hiermit der Tatbestand des internen und externen Whistleblowings.<sup>10</sup> Zudem werden „illegale“ Geschäftsgeheimnisse nicht durch den Geheimnisbegriff des § 2 Nr. 1 GeschGehG geschützt.<sup>11</sup>

3 Angekündigte Kommentierungen: Fissenwert, Erste Hilfe zum Hinweisgeberschutzgesetz, C.H. Beck; Fischer/Pellmann/Schoch (Hrsg.), HinSchG – Hinweisgeberschutzgesetz, Fachmedien Recht und Wirtschaft; Thüsing (Hrsg.), HinSchG, C.H. Beck.

4 BT-Drs. 20/3442 v. 19.09.2022, S. 34.

5 Vgl. BT-Drs. 20/3442 v. 19.09.2022, S. 34.

6 Gola, Mitarbeitervertretungen und Datenschutzbeauftragte als „Gewährleister“ des Datenschutzes der Beschäftigten, RDV 2022, 306.

7 Gola, in: Gola/Heckmann, DS-GVO/BDSG; Art. 4 DS-GVO Rn. 57.

8 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) vom 18.04.2019; BGBl. I S. 466.

9 Reinfeld, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, S 85 ff.

10 Trebeck/Schulte-Wissermann, Die Geheimnisschutzrichtlinie und deren Anwendbarkeit im Kontext mit Whistleblowing, NZA 2018, 1175.

11 Vgl. bei Brockhaus, Das Geschäftsgeheimnis – Zur Frage der Strafbarkeit von Hinweisgebern unter Berücksichtigung der Whistleblowing-Richtlinie, ZIS 3/2020, 109; Hauck, Grenzen des Geheimnisschutzes, WRP 2018, 1032; Böning/Heidfeld, Gesetzentwurf zum Schutz von Geschäftsgeheimnissen (GeschGehG) – Maulkorb zu Lasten der Beschäftigten, AuR 2018, 555; Hauck, Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) ist in Kraft, GRUR-Prax 2019, 223; Scholtyssek/Judis, Das neue Geschäftsgeheimnisgesetz – Risiken, Chancen und konkreter Handlungsbedarf für Unternehmen, CCZ 2020, 23.

Entweder sind solche Informationen schon nicht von „wirtschaftlichem Wert“, was § 2 Nr. 1 lit. a GeschGehG voraussetzt, oder es besteht kein „berechtigtes Interesse“ an ihrer Geheimhaltung, was § 2 Nr. 1 lit. c GeschGehG verlangt.<sup>12</sup>

Erlaubt wird auch die Offenlegung von Geschäftsgeheimnissen durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn diese erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann (§ 5 Nr. 3 GeschGehG).<sup>13</sup>

### 3. Freiwillig etablierte Regelungen (Codes of Conduct)

Parallel zu gesetzgeberischen Überlegungen hat das Thema „Whistleblowing“ in den vergangenen Jahren auch einen immer höheren Stellenwert im Rahmen an sich freiwilliger, aber fallbezogen aus den Geschäftsführerpflichten<sup>14</sup> fließenden Compliance- und Governance-Strukturen von Unternehmen eingenommen.<sup>15</sup> Ergeben sich Verdachtsmomente für Straftaten oder sonstige Fehlhandlungen, muss der Geschäftsführer diesen unverzüglich nachgehen. Ferner muss der Geschäftsführer geeignete organisatorische Vorkehrungen treffen, um Pflichtverletzungen von Unternehmensangehörigen zu verhindern.<sup>16</sup> Neben präventiver Intervention<sup>17</sup> und im Verdachtsfall erforderlichen Ermittlungen sind Meldeverfahren Bestandteil der betrieblichen Compliance. In sog. Codes of Conducts oder Compliance- bzw. Ethikregelungen<sup>18</sup> werden Mitarbeiter – im Rahmen des Zumutbaren (§§ 305 ff. BGB)<sup>19</sup> – verpflichtet, innerbetriebliches<sup>20</sup> Fehlverhalten von Kollegen in einem strukturierten Meldeverfahren – z.B. über einen eine Garantenfunktion<sup>21</sup> einnehmenden Compliance-Officer mitzuteilen. Rechtsverstöße sollen möglichst frühzeitig innerbetrieblich<sup>22</sup> aufgedeckt, abgestellt und geahndet werden. Die Verarbeitung der Daten der meldenden und gemeldeten Beschäftigten muss mit § 26 Abs. 1 S. 1 und ggf. S. 2 BDSG vereinbar sein.<sup>23</sup> Auch ohne entsprechende ausdrückliche Vorgabe müssen derartige Vorkehrungen von Verfolgungsbehörden und Gerichten bei gleichwohl eingetretenen Rechtsverstößen bei gegenüber dem Unternehmen zu ziehenden Konsequenzen positiv berücksichtigt werden.<sup>24</sup>

### 4. Grenzen der Hinweispflicht

Die oben angesprochenen, zur Einrichtung von Meldeverfahren verpflichtenden gesetzlichen Regelungen enthalten zwar Bestimmungen, die die Mitarbeiter zu ihrer Nutzung motivieren sollen, eine gesetzliche Verpflichtung hierzu enthalten sie nicht. Abzustellen ist insofern – ausgerichtet am Einzelfall – auf die betriebliche Treuepflicht und ggf. auf diese konkretisierenden betrieblichen Regelungen.

Der Arbeitgeber kann Beschäftigte im Rahmen eines Meldeverfahrens zu nichts verpflichten was sie ihm nicht bereits auf Grund ihrer Treuepflicht schulden. Auch bei der Pflicht Normverstöße von Beschäftigten, d.h. von Kollegen anzuzeigen, besteht eine Zumutbarkeitsgrenze.<sup>25</sup> Dabei ist auch die Position des Beschäftigten relevant.<sup>26</sup> Hier ist nach der Schwere der Pflichtverletzung des Gemeldeten und nach dem Verantwortungsbereich des Meldenden zu differenzieren.

Schon gar nicht besteht eine Pflicht zur strafrechtlichen Selbstbelastung. Das ergibt sich aus dem strafrechtlichen Grundsatz „nemo tenetur se ipsum accusare“.<sup>27</sup> Wenn eigene Verfehlungen gemeldet werden, kann das jedoch – ggf. gemäß interner Ethikregelungen – zum Verzicht auf Konsequenzen führen.

Informationen über einen von Kollegen drohenden bzw. verursachten gravierenderen Schaden sind an den Arbeitgeber weiterzuleiten.<sup>28</sup> Der Arbeitgeber überschreitet somit nicht seine Regelungsbefugnis, wenn er Beschäftigte anweist ihnen bekannt gewordene Informationen über das Unternehmen schädigende strafrechtliche Handlungen weiterzugeben.<sup>29</sup>

Einen Vorschlag für eine sachgerechte Regelung macht Schulz<sup>30</sup> mit folgender Formulierung: „Der Arbeitnehmer ist verpflichtet, ihm bekannt gewordenes Fehlverhalten von anderen Arbeitnehmern und Dritten gegenüber dem Arbeitgeber anzuzeigen, wenn ein konkreter Verdacht gegeben ist, das Fehlverhalten im sachlichen, räumlichen und personalbezogenen Zurechnungszusammenhang zum Unternehmen steht, das Fehlverhalten dazu geeignet ist, das Unternehmen zu schädigen und das Fehlverhalten mit Strafe oder Geldbuße bedroht ist.“

### 5. Betriebs-/Dienstvereinbarung als Rechtsgrundlage

Geregelt werden können bzw. müssen Meldepflichten ggf. auch in einer Betriebs-/Dienstvereinbarung. Für eine umfassende Betriebsvereinbarung ist es irrelevant, dass die Einführung des Verfahrens teils mitbestimmungsfrei – und damit freiwillig – und teils mitbestimmungspflichtig ist. Sie kann Basis der Verpflichtung des Unternehmens aus § 4 Abs. 4 LkSG sein, die Interessen seiner Beschäftigten beim Liefer-

12 A.A. Garden/Híramente, Die neue Whistleblowing-Richtlinie der EU – Handlungsbedarf für Unternehmen und Gesetzgeber, BB 2019, 963; Dann/Markgraf, Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, NJW 2019, 1774.

13 Reinhardt-Kasperek/Kaindl, Whistleblowing und die EU-Geheimnisschutzrichtlinie. Ein Spannungsverhältnis zwischen Geheimnisschutz und Schutz der Hinweisgeber?, BB 2018, 1332.

14 Vgl. OLG Nürnberg, Urt. v. 30.05.2022 – 12 U 1520/19; dazu Bartz/Bittner, Vier Augen sehen mehr als zwei – Die Pflicht der Geschäftsführung zur Schaffung von Compliance-Strukturen, CCZ 2022, 319.

15 Ströbel/Böhm/Breinig/Wybitul, Beschäftigtendatenschutz und Compliance: Compliance-Kontrollen und interne Ermittlungen nach der EU-Datenschutz-Grundverordnung und dem neuen Bundesdatenschutzgesetz; CCZ 2018, 14.

16 BGH, Urt. v. 08.10.1984 – II ZR 175/83.

17 Staristach/Hauck/Jüttner/Pohlmann, Compliance als präventive Intervention, CCZ 2022, 312.

18 Vgl. hierzu die Zusammenstellung diesbezüglicher Regelungen im Dax notierten Unternehmen bei Thüsing/Fütterer/Jäntsich, Petzen ist „doof“, RDV 2018, 133, sowie bei Gola, Handbuch Beschäftigtendatenschutz, Rn. 796 ff.

19 Gola; Handbuch Beschäftigtendatenschutz; Rn. 783 ff.

20 Der außerbetriebliche Lebensbereich ist der Regelungsbefugnis des Arbeitgebers bzw. der Betriebsparteien entzogen, vgl. Gola, Handbuch Beschäftigtendatenschutz, Rn. 785.

21 BGH, Urt. v. 17.07.2009 – 5 Str. 314/08, ebenso OLG Frankfurt; Urt. v. 22.05.1987 – 15g401/86.

22 Vgl. bei Reuling, Der innerbetriebliche Abhilfeversuch des Whistleblowers zwischen Gesetzgebung und Rechtsprechung; RdA 2022, 317.

23 Zur Transparenz gegenüber den Betroffenen vgl. Gola, Handbuch Beschäftigtendatenschutz, Rn 789 ff.

24 BGH, Urt. v. 09.05.2017 – 1StR265/16; st. Rspr. BAG, Urt. v. 01.06.1995 – 6 AZR 912/94; v. 03.07.2003 – 2 AZR 235/02; v. 07.12.2006 – 2 AZR 400/05.

25 Steffen/Stöhr, Die Umsetzung von Compliance-Maßnahmen im Arbeitsrecht, RdA 2017, 43.

26 Führungskräfte unterliegen insoweit aufgrund ihrer Treuepflicht einer besonderen Verpflichtung; BAG, Urt. v. 12.05.1958 – 2 AZR 953/07.

27 BGH, Urt. v. 23.02.1989 – IX ZR 236, 86.

28 St. Rspr. BAG, Urt. v. 01.06.1995 – 6 AZR 912/94; v. 03.07.2003 – 2 AZR 235/02; v. 07.12.2006 – 2 AZR 400/05.

29 Müller-Bonanni/Sagan, Arbeitsrechtliche Aspekte der Compliance, BB 2008, 28.

30 Schulz, Compliance – Internes Whistleblowing, BB 2012, 634.

kettenmanagement – soweit hierbei Gestaltungsfreiheit besteht – „angemessen zu berücksichtigen. Basis kann § 106 Abs. 3 BetrVG sein, nach dem die Geschäftsleitung den Wirtschaftsausschuss rechtzeitig und umfassend zu allen Fragen der unternehmerischen Sorgfaltspflicht in Lieferketten zu unterrichten hat.

In der Regel bedarf auch die detaillierte Einführung einer gesetzlichen Meldepflicht der Zustimmung der Mitarbeitervertretung. Das gilt zwar nicht für das Ob, aber für das Wie. Das gilt auch bei einer den Spielraum des HinSchG oder des LkSG nutzenden Gesetzesumsetzung. Geregelt werden notwendigerweise Fragen der Ordnung des Betriebes und des Verhaltens der Beschäftigten (§ 87 Abs. 1 Nr. 1 BetrVG/§ 75 Abs. 3 Nr. 15 BPersVG). Sofern die gesetzlichen Regelungen den Beschäftigten das Einlegen einer Beschwerde vollständig freistellen, wirkt sich das Angebot der Nutzung nur geringfügig auf das Ordnungsverhalten der Beschäftigten aus, so dass § 87 Abs. 1 Nr. 1 BetrVG nicht einschlägig ist.<sup>31</sup> Wenn bei Verstößen nach dem HinSchG und dem LkSG Reputationschäden drohen, geht es bei entsprechenden Hinweisen auf zumindest „gravierende“ drohende Risiken oder Rechtsverstöße jedoch um eine Nebenpflicht der Beschäftigten. Der Mitbestimmung unterliegt ferner die technische Ausgestaltung des Meldeverfahrens zumeist auch, da sie i.d.R. unter dem Einsatz von technischen Einrichtungen erfolgt, die objektiv geeignet sind, Leistung und Verhalten von Beschäftigten zu kontrollieren (§ 87 Abs. 1 Nr. 6 BetrVG; § 80 Abs. 1 Nr. 21 BPersVG).

## 6. Das – zunächst – gescheiterte Verbandssanktionengesetz

Ein kurzer Rückblick ist im Rahmen des erörterten Themas auf das in der vergangenen Legislaturperiode im deutschen Bundestag wegen Nicht-Behandlung gescheiterte Verbandssanktionengesetz angezeigt.<sup>32</sup> Mit dem Gesetz sollte einerseits der Sanktionierung von Straftaten wirtschaftlich Tätiger eine eigenständige gesetzliche Grundlage erhalten.<sup>33</sup> Andererseits sollten Unternehmen aber durch Sanktionsmilderungen beim Nachweis angemessener und wirksamer organisatorischer Vorkehrungen zur Vermeidung von Verbandstaten – also einem auch Anzeigepflichten enthaltenen Compliance-System – zur Schaffung solcher Systeme motiviert werden.<sup>34</sup> Ob der Gesetzgeber das Thema in dieser Legislaturperiode noch mal aufgreift ist offen.<sup>35</sup> Der Koalitionsvertrag trifft hierzu keine Aussage.<sup>36</sup> Das noch angesprochene Lieferkettensorgfaltspflichtengesetz<sup>37</sup> bietet nur bedingt eine Alternative zum Verbandsklagerecht.<sup>38</sup>

## II. Das HinSchG als neues Whistleblowing - „Stammgesetz“

### 1. Die Vorgeschichte

#### a) Das Gesetzgebungsverfahren

Der Bundestag hatte zunächst am 16.12.2022 ein Gesetz zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden,<sup>39</sup> beschlossen. Nachdem der Bundesrat dieser Fassung in seiner Sitzung am 10.02.2023 die Zustimmung versagte, hatten die Koalitionsparteien dem Bundestag das HinSchG unter Verzicht auf die Regelungen, die die Zustimmungsbedürftigkeit des Bundesrats begründet hatten, und ansonsten in weitgehendst un-

veränderter Fassung erneut vorgelegt;<sup>40</sup> sich dann jedoch dazu entschlossen, den Vermittlungsausschuss einzuschalten, der sich am 09.05.2023 auf einen Kompromiss einigte.<sup>41</sup> Der Gesetzgebungsprozess wurde letztendlich mit der Veröffentlichung des Gesetzes im BGBl. I Nr. 140 v. 02.06.2023 abgeschlossen.

#### b) Die Kompromissregelung in der Zusammenfassung

Die verabschiedete Kompromissfassung enthält insbesondere die Stärkung interner Meldewege, den Wegfall des Zwangs zur Schaffung von Meldewegen für anonyme Hinweise und die Reduzierung von Bußgeldern. Informationen über Verstöße fallen zudem nur noch in den Anwendungsbereich des Gesetzes, wenn sie sich auf den Beschäftigungsgeber oder eine andere Stelle, mit der die hinweisgebende Person beruflich im Kontakt stand, beziehen.

Whistleblower können Hinweise sowohl – und dies nunmehr möglichst vorrangig – an eine von ihrem Beschäftigungsgeber einzurichtende interne Meldestelle oder an eine – u.a. bei dem Bundesamt für Justiz etablierte – externe Meldestelle geben. Auch anonymen Hinweisen soll nachgegangen werden. Ein spezielles Verfahren ist hierzu nicht mehr einzurichten.

Wird ein Hinweis abgegeben, muss die Meldestelle tätig werden, diesen dokumentieren und über die Bearbeitung unter Beachtung vorgegebener Frist dem Whistleblower berichten.

Wenn die hinweisgebende Person meint und geltend macht, wegen ihrer Whistleblower-Aktivität bei ihrer beruflichen Tätigkeit benachteiligt zu werden, stehen ihr ein mit einer Beweislastumkehr versehenes Benachteiligungsverbot nebst Schadensersatzregelung zur Seite. Das ursprünglich vorgesehene Schmerzensgeld für die „immateriellen Schäden“ ist nicht mehr Teil des Gesetzes.

Die in § 11 Abs. 5 HinSchG vorgesehene Lösungsfrist dokumentierter Meldungen wurde entsprechend Art. 17 Abs. 1 lit. a DS-GVO praxisbezogen flexibel festgelegt.

Der Bußgeldrahmen wurde von 100.000,- auf 50.000,- Euro abgesenkt.

31 Schneider, Die arbeitsrechtliche Implementierung von Compliance- und Ethikrichtlinien, S. 198.

32 Gesetz zur Sanktionierung von verbandsbezogenen Straftaten (Verbands-sanktionengesetz –VerSanG); BT-Drs. 19/23568 v. 21.10.2020.

33 Zu den möglichen Konsequenzen des VerSanG auf den betrieblichen Datenschutz vgl. Gola, RDV 2021, 212.

34 Schulz, Wirksames Compliancemanagement: Anreize und Orientierungshilfen zur Vermeidung von (Verbands)Sanktionen, CCZ 2020, 49.

35 Schweiger, Status quo und status futurus der Verbandssanktionierung in Deutschland nach dem gescheiterten Verbandssanktionengesetz, LRZ 2022, Rn. 439.

36 Verbandssanktionengesetz – endgültig vom Tisch? [https://www.haufe.de/.../verbandssanktionengesetz\\_230132\\_515536](https://www.haufe.de/.../verbandssanktionengesetz_230132_515536).

37 Koch, Das Lieferkettensorgfaltspflichtengesetz – Compliance; Sorgfaltspflichten und zivilrechtliche Haftung, MDR 2022, 1.

38 Vgl. bei Klein, Das Lieferkettensorgfaltspflichtengesetz als Alternative zum Verbandsklagerecht?, ZIP 2023, 1053.

39 Zur Kritik: Caracas, Das geplante Verbandssanktionengesetz gibt Hungern den einen Mantel, CCZ 2020, 331.

40 BT-Drs. 20/5992 v. 14.03.2023 S. 25.

41 Vgl. die beschlossenen Änderungen in BT-Drs. 20/6700 v. 09.05.2023.

## 2. Das HinSchG im Einzelnen

### a) Grundsätzliches

Ziel des HinSchG ist es, Personen, die unternehmens-/behördeninterne Rechtsverstöße i.S.d. § 2 HinSchG melden oder offenlegen (vgl. Definition in § 3 Abs. 4 und 5 HinSchG), vor negativen Konsequenzen vornehmlich seitens des als „Beschäftigungsgeber“ (§ 3 Abs. 9 HinSchG) benannten Arbeitgebers aber auch seitens der gemeldeten „Rechtsverletzer“ zu schützen und ihnen damit die Entscheidung für eine Meldung zu erleichtern.<sup>42</sup> Das HinSchG soll neben fortbestehenden Einzelregelungen das „Stammgesetz“ zur Regelung des Whistleblowings<sup>43</sup> sein.

### b) Gesetzesadressaten

Nach § 12 HinSchG sind Beschäftigungsgeber zur Einrichtung von Meldesystemen und internen Meldestellen verpflichtet, sofern in der Regel – Abweichungen nach unten regelt Abs. 3 – mindestens 50 Beschäftigungen vorliegen.<sup>44</sup> Die in § 3 Abs. 8 HinSchG getroffene Definition des Beschäftigten entspricht bedauerlicherweise und ohne Grund nicht der des § 26 Abs. 8 BDSG. Zur Feststellung der regelmäßigen Beschäftigtenzahl bedarf es eines Rückblicks auf die bisherige personelle Stärke und einer Einschätzung der zukünftigen Entwicklung.<sup>45</sup> Es soll nicht eine auf einen bestimmten Stichtag abgestellte Betrachtung erfolgen.

### c) Der tangierte Personenkreis

Das Gesetz will ein faires Meldeverfahren sicherstellen und schützt sowohl Meldende (§ 33 – § 39 HinSchG) als auch Gemeldete – wenngleich auch deutlich unausgewogen – vor unzulässigen Eingriffen (§ 1 HinSchG).

Potenzielle Hinweisgeber<sup>46</sup> sollen zu entsprechendem Handeln motiviert werden und werden daher auch dann von einer Haftung freigestellt, wenn sie nicht grob fahrlässig falsch beschuldigen (§ 38 HinSchG). Art. 6 lit. a der Richtlinie setzt eine hinreichend begründete Annahme des Whistleblowers voraus.<sup>47</sup>

Daneben wird aber auch der „Gegenpart“ geschützt, d.h. Personen, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind (§ 1 Abs. 2 HinSchG). Der Schadensersatz bei einer Falschmeldung (§ 38 HinSchG) beschränkt sich jedoch auf grob fahrlässiges Verhalten und sieht kein Schmerzensgeld vor.

Als „hinweisgebende Personen“ (§ 1 Abs. 1 HinSchG) geschützt sind neben Arbeitnehmern auch Beamte, Anteilseigner, Mitarbeiter von Lieferanten und Personen, die bereits vor Beginn eines Arbeitsverhältnisses Kenntnisse von Verstößen erlangt hatten.

### d) Zur Meldung berechtigende Sachverhalte

Zu den zu meldenden Rechtsverletzungen gehören zunächst Handlungen, die straf- oder (mit einigen Einschränkungen) bußgeldbewehrt sind (§ 2 Abs. 1 Nr. 1 und 2 HinSchG).

Unter dem Aspekt des Datenschutzes relevant sind nach § 2 Abs. 1 Nr. 3 HinSchG Verstöße gegen die in lit. o) und p) genannten Vorschriften zum Schutz der Privatsphäre und personenbezogener Daten in der elektronischen Kommunikation, zum Schutz vor unzumutbaren Belästigungen durch elektronische

Werbung oder auch zum Schutz personenbezogener Daten im Anwendungsbereich der Datenschutz-Grundverordnung.

Der in § 1 Abs. 1 HinSchG geforderte „Zusammenhang des gemeldeten Vorgangs mit der beruflichen Tätigkeit“ ist weit zu verstehen. Er umfasst nicht nur das formale Arbeits- oder Dienstverhältnis, sondern z.B. auch Tätigkeiten von Arbeitnehmervertretungen. Es genügt, wenn laufende oder auch frühere berufliche Tätigkeiten betroffen sind.

Nicht mehr geschützt sind jedoch Meldungen über privates Fehlverhalten, auch wenn die hinweisgebende Person im beruflichen Zusammenhang davon erfährt. Dies gilt auch – trotz der ihrer außerdienstlichen Wohlverhaltenspflicht – für Beamte.<sup>48</sup>

### e) Melderecht und Meldepflicht

Eine Meldepflicht enthält das Gesetz nicht. Ob eine solche besteht, hängt – sofern interne Complianceregelungen<sup>49</sup> nicht eine solche im zulässigen Rahmen enthalten, – von der Reichweite der Treuepflicht der Beschäftigten ab.<sup>50</sup> Diese umfasst keine Pflicht zur Selbstbelastung.<sup>51</sup>

Eine Pflicht zum Whistleblowing besteht nur in den Grenzen billigen Ermessens und hängt insofern auch von den Gegebenheiten des Einzelfalls ab. Im Direktionsrecht erfolgte Anordnungen zum Whistleblowing dürfen die Grenze billigen Ermessens nicht überschreiten.<sup>52</sup> Das gilt auch für eine zu dieser Thematik, d.h. für eine zu betrieblichen Ethik-Regelungen abgeschlossene Betriebsvereinbarung.<sup>53</sup>

Andererseits ist eine Behinderung oder vertragliche Einschränkung der gesetzlichen Meldebefugnisse unzulässig (§ 7 Abs. 2 HinSchG).

42 Vgl. z.B. Ammon, Das Hinweisgeberschutzgesetz für Unternehmen – Umsetzung der EU-Whistleblower-Richtlinie; PinG 2023, 67; Beukelmann, Schutz von Hinweisgebern, NJW-Spezial 2029, 312; Gerdemann, Neuer Entwurf für ein Hinweisgeberschutzgesetz; ZRP 2022, 98; Junker, Das Gesetz für einen besseren Schutz hinweisgebender Personen, EuZA 2023,1; Ibel, Whistleblowing über Verstöße gegen die Pflicht zur Verfassungstreue, NJOZ 2023, 321; Quast/Ohtlo, Der Regierungsentwurf des Hinweisgeberschutzgesetzes, CCZ 2022, 303; Schoch/Kumar, Der neue Entwurf eines Hinweisgeberschutzgesetzes, CB 2022, 181; Scholz, Hinweisgeberschutz zwischen Legalitäts- und Legalitätskontrollpflicht, Die Aktiengesellschaft 2022, 553; Rosner, Entwurf des HinSchG geht weit über die Umsetzung der EU-Richtlinie hinaus, NWB 2022, 3173; Schmolke, Die neue Whistleblower-Richtlinie ist da! Und nun?, NZG 2020, 5; Zimmer/Humphrey, Petzen? Ja, bitte! Meldesysteme nach der Whistleblower-Richtlinie der EU, BB 2021, 372.

43 Gesetzesbegründung; BT-Drs. 20/3442 v. 19.09.2022, 34.

44 Gortan, Berechnung der Beschäftigtenanzahl und Begriff der Organisationseinheit im RefE des HinSchG, NZA 2022, 838.

45 BAG, Urt. v. 31.01.1991 – 2 AZR 356/90 und v. 24.01.2013 – 2 AZR 140/12.

46 Gola, HinSchG; HR-Performance 1/2023, 68.

47 Vgl. Zimmer/Schwung, Hilfe für Hinweisgeber – Beweislastumkehr nach § 36 II HinSchG-RegE, NZA 2022, 1167; Siemes, Die hinreichend begründete Annahme des Whistleblowers nach Art. 6 Abs. 1 lit. a Richtlinie (EU) 2019/1937 – Auslegung und Umsetzung, CCR 2022, 29.

48 BT-Drs. 20/5992, 39.

49 Teichmann/Weber, Die Whistleblower-Richtlinie, ihr Missbrauchspotenzial und Implikationen für den Compliance-Beauftragten, CB 2022, 157.

50 Gola, HinSchG; HR-Performance 1/2023, 68.

51 BGH Urt. v. 23.02.1989 – IX ZR 236, 86.

52 Vgl. bereits Mengel/Hahnemeister, Compliance und arbeitsrechtliche Implementierung im Unternehmen, BB 2007, 1386; Schuster/Darsow, Einführung von Ethikrichtlinien durch Direktionsrecht, NZA 2005, 273; zum Meinungsstand: Thüsing/Forst in Thüsing, Beschäftigtendatenschutz und Compliance, § 6 Whistleblowing, Rn. 52; Schulz, Compliance – Internes Whistleblowing, BB 2011, 629.

53 BAG, Beschl. v. 22.07.2008 – 1 ABR 40/07.

Nach § 12 Abs. 1 S. 1 HinSchG müssen die internen Meldekanäle mindestens den eigenen Beschäftigten offenstehen. Die zur Einrichtung verpflichteten Unternehmen können selbst entscheiden, ob das Meldeverfahren darüber hinaus auch von (außenstehenden) Personen, die im Kontakt zum Unternehmen stehen, genutzt werden kann.

#### f) Die Meldewege

Beschäftigungsgeber haben den hinweisberechtigten Personen zwei gesetzlich definierte und gleichwertig nebeneinanderstehende Möglichkeiten zur Mitteilung von Meldungen (§ 3 Abs. 4 HinSchG) anzubieten. Offen stehen muss der Weg zu internen (§ 12 HinSchG) oder externen Meldestellen (§§ 19 bis 24 HinSchG).

In der Fassung des Vermittlungsausschusses wieder aufgegriffen wurde der Vorrang des Versuchs der innerbetrieblichen Klärung.<sup>54</sup> Nach § 7 Abs. 1 S. 2 HinSchG „sollten“ Beschäftigte, wenn keine Repressalien zu befürchten seien, die Meldung an eine interne Meldestelle bevorzugen. Wenn einem intern gemeldeten Verstoß nicht abgeholfen wird, bleibt es der hinweisgebenden Person unbenommen, sich an eine externe Meldestelle zu wenden.

Fraglich ist, ob eine externe Meldestelle befugt ist, den sich bei ihr unmittelbar Meldenden ggf. an den internen Meldeweg zu verweisen. Im Regelfall wird das jedoch ausgeschlossen sein, da der Vorrang der internen Meldung von der externen Meldestelle nicht nachprüfbar Kriterien abhängt. So soll der Vorrang nur für Fälle gelten, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und der Whistleblower keine Repressalien zu befürchten hat.

Während die Einrichtung des internen Meldekanals Sache des Beschäftigungsgebers ist, sind die externen Meldestellen gesetzlich u.a. als Einrichtung beim Bundesamt für Justiz oder bei Behörden mit speziellen Zuständigkeitsbereichen wie der Bundesanstalt für Finanzdienstleistungsaufsicht und dem Bundeskartellamt etabliert.

Die durch das Gesetz eingeführten externen Meldestellen sind abzugrenzen bzw. zu trennen von „ausgelagerten“ internen Meldestellen im Rahmen von Konzernlösungen<sup>55</sup> oder z.B. der Beauftragung eines Vertrauensanwalts.<sup>56</sup>

#### g) Anonyme Meldungen

Die Mehrheit der in Deutschland eingerichteten Hinweisgebermeldesysteme sehen die Möglichkeit eines anonymen Hinweises vor (siehe § 4d Abs. 1 S. 2 FinDAG, § 3b Abs. 1 S. 2 BörsG, § 34d Abs. 12 S. 2 GewO, § 53 Abs. 1 S. 3 GwG).

Der zum HinSchG gefundene Kompromiss verzichtet jedoch auf eine zunächst vorgesehene Pflicht, die Abgabe anonymer Meldungen<sup>57</sup> sowohl für interne als auch für externe Meldestellen zu ermöglichen.<sup>58</sup> Gleichwohl „sollten“ dennoch anonym eingehende Meldungen bearbeitet werden (§ 16 Abs. 1 S. 4., § 27 Abs. 1 S. 2 HinSchG), obwohl zur Regelung dieser Meldeart keine Notwendigkeit nach Art. 6 Abs. 2 HinSch-RL bestand. Es besteht allerdings keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonyme Meldungen ermöglichen.

Die Sinnhaftigkeit von anonymen Hinweisen im Meldeverfahren bleibt umstritten.<sup>59</sup> Aus Compliance-Sicht sind anonymer Meldungen begrüßenswert, da sie eine weitere potenzielle Hemmschwelle für Hinweisgeber abbauen. Aus der Sicht unberechtigt „Verleumdeter“ gilt das Gegenteil.

Jedoch unabhängig davon, ob das HinSchG Unternehmen ausdrücklich zur Entgegennahme von anonymen Meldungen verpflichtet, müssen Unternehmen einer anonymen Meldung – freilich nur einer substantiierten Meldung – ohnehin im Rahmen ihrer Legalitätspflicht nachgehen. Die Pflicht zur Entgegennahme anonymer Meldungen führt also zu keiner Mehrbelastung. Anders wäre es gewesen bei der Pflicht, Meldekanäle für die anonyme Kommunikation vorzuhalten.

### 3. Regelungen zu den Datenverarbeitungen der Meldestellen

#### a) Erlaubnistatbestände

Bei einer Meldung über ein Hinweisgebersystem werden regelmäßig personenbezogene Daten verarbeitet. Eine Meldung enthält zumeist sowohl Daten zum Hinweisgeber als auch von Beschuldigten und betroffenen Personen. Interne und externe Meldestellen erhalten in § 10 HinSchG die bereichsspezifische geregelte Befugnis gemäß Art. 4 DS-GVO personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 HinSchG bezeichneten Aufgaben erforderlich ist (Art. 6 Abs. 1 lit. c DS-GVO). Abweichend von Art. 9 DS-GVO sind auch erforderliche Verarbeitungen besonderer Kategorien personenbezogener Daten durch eine Meldestelle zulässig. In diesem Fall hat die Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 22 Abs. 2 S. 2 HinSchG). Die spezielle Verarbeitungsbefugnis gilt für zur Implementierung eines Hinweisgebersystems verpflichtete Unternehmen. Unternehmen mit weniger als 50 Mitarbeitern werden sich auf Art. 6 Abs. 1 lit. f DS-GVO stützen.

#### b) Vertraulichkeit der Meldung

Meldestellen haben die Daten der involvierten Personen vertraulich zu behandeln (§ 8 HinSchG), d.h. sie dürfen nur den mit der Bearbeitung des Meldevorgangs zulässigerweise betrauten Personen zugänglich sein. Nach der Gesetzesbegründung<sup>60</sup> sind – „soweit erforderlich“ – die für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zuständigen Personen zur Vertraulichkeit zu verpflichten. Die Erforderlichkeit ergibt sich aus den parallel geltenden Vorschriften der DS-GVO und des BDSG.

Das Gebot der Vertraulichkeit bedingt aber auch Einschränkungen der datenschutzrechtlichen Auskunfts- und Informationsrechte. Ausnahmen vom Vertraulichkeitsgebot gelten für vorsätzlich oder grob fahrlässig handelnde Hinweisgeber (§ 9 Abs. 1 HinSchG) oder im Rahmen der Untersuchungen durch nationale Behörden oder in Gerichtsverfahren

54 BAG, Urt. v. 03.07.2003 – 2 AZR 235/02.

55 Vgl. nachstehend 4.2.

56 Fassbach/Hülsberg/Spamer, Hinweisgeberschutz durch Vertrauensanwälte, CB 2022, 151.

57 Krit. ggü. anonymen Meldungen exempl. bei Thüsing/Forst in Thüsing, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 6 Rn. 24; Thüsing, Effektiver Hinweiserschutz mit Augenmaß, DB 2022, 1066; Wiedmann/Seyfert, Richtlinienentwurf der EU-Kommission zum Whistleblowing, CCZ 2019, 12.

58 Vgl. aber die positive Stellungnahme gegenüber dieser Regelung von Transparency international Deutschland, www.transparency.de.

59 Befürwortend hingegen exempl. Dilling, Cat's Gold-Plating – Der neue Referentenentwurf zum Hinweisgeberschutzgesetz, CCZ 2022, 145.

60 BT-Drs. 20/3442 v. 19.09.2022, S. 74.

– und hier auch im Hinblick auf die Wahrung der Verteidigungsrechte der betroffenen Person. Die Vertraulichkeit seiner Person kann von dem Hinweisgeber dadurch sichergestellt werden, dass seine Meldung anonym erfolgt.

### c) Dokumentationspflicht

Internen und externen Meldestellen wird in § 11 HinSchG vorgegeben, alle eingehenden Meldungen in dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots (§ 8 HinSchG) schriftlich oder – mit Einwilligung des Betroffenen – auch technisch zu dokumentieren und fallgerecht befristet (§ 11 Abs. 5 HinSchG) aufzubewahren.

## 4. Interne Meldestelle

### a) Der Handlungsspielraum

Nach § 14 HinSchG hat der Beschäftigungsgeber bei der Organisation interner Meldestellen einen weiten Spielraum. Voraussetzung für die Funktionsfähigkeit des Meldesystems ist allerdings, dass die Person oder Organisationseinheit, die mit der Aufgabe betraut wird, die nötige Unabhängigkeit hat und ohne Interessenkonflikte für eine gewisse Dauer arbeiten kann.

Die interne Meldestelle kann auch „extern“ sein, d.h. es können, so wie dies auch bereits in der Praxis teilweise mittels Ombudspersonen<sup>61</sup> gehandhabt wird, externe Dritte mit der Einrichtung und dem Betreiben der internen Meldestelle beauftragt werden, wobei der Dritte jedoch nicht losgelöst von dem betreffenden Unternehmen oder der jeweiligen Institution agieren kann. Seine Tätigkeit sollte demgemäß als Auftragsdatenverarbeitung geregelt werden.<sup>62</sup> Insbesondere für Folgemaßnahmen zur Prüfung der Stichhaltigkeit einer Meldung und der Abstellung eines Verstoßes bedarf es einer Kooperation zwischen der Meldestelle und dem Beschäftigungsgeber.

### b) Konzernregelungen

Auch Konzernregelungen sind zulässig.<sup>63</sup> Dem konzernrechtlichen Trennungsprinzip entsprechend kann auch eine andere Konzerngesellschaft (zum Beispiel Mutter-, Schwester-, oder Tochtergesellschaft) eine unabhängige und vertrauliche Stelle als „Dritter“ im Sinne von § 14 HinSchG sein, die dann für mehrere selbstständige Unternehmen in dem Konzern tätig wird. Die Bearbeitung von Meldungen kann konzentriert bei der ausgelagerten internen Meldestelle erfolgen. Sie kann auch interne Ermittlungen in den jeweils betroffenen Konzernteilen durchführen. Notwendig ist es allerdings, dass die Verantwortung dafür, einen festgestellten Verstoß zu beheben und weiterzuverfolgen, immer bei dem jeweiligen beauftragenden Tochterunternehmen verbleibt.

### c) Verfahren bei internen Meldungen

Nach § 16 Abs. 3 HinSchG müssen interne Meldekanäle Meldungen in mündlicher oder in Textform ermöglichen unter der Voraussetzung, dass bei dem gewählten Übertragungsweg die Vertraulichkeit der Identität der von der Meldung betroffenen Personen gewahrt ist.

Mündliche Meldungen müssen per Telefon oder mittels einer anderen Art der Sprachübermittlung möglich sein. Meldekanäle, die Meldungen in Textform ermöglichen, können sein: IT-gestütztes Hinweisgebersystem, wie etwa eine

Plattform im Internet oder Intranet oder eine eigens hierfür eingerichtete E-Mail-Adresse. Meldekanäle, die Meldungen ausschließlich in Schriftform ermöglichen (z.B. ein Beschwerde-Briefkasten oder Meldungen über den Postweg) dürften nicht ausreichen.

Auf Ersuchen der hinweisgebenden Person ist für eine Meldung innerhalb einer angemessenen Zeit eine persönliche Zusammenkunft mit einer für die Entgegennahme einer Meldung zuständigen Person der internen Meldestelle zu ermöglichen. Mit Einwilligung der hinweisgebenden Person kann die Zusammenkunft auch im Wege der Bild- und Tonübertragung erfolgen.

### d) Reaktion des Meldeempfängers

Welche Konsequenzen der Meldeempfänger, d.h. i.d.R. der Arbeitgeber aus der Meldung zieht, bleibt – abgesehen davon, dass er rechtswidriges Verhalten abstellen muss – ihm überlassen. Schenkt er einer „Verdachtsmeldung“ keinen Glauben, so muss er der Sache nicht nachgehen. Stellt er eine Verfehlung eines Mitarbeiters fest, kann er versuchen die Angelegenheit intern zu regeln. Ob er Behörden bezüglich strafrechtlicher Konsequenzen informiert bzw. Strafanzeige stellt, ist ebenfalls ihm überlassen.

Eine Reaktionspflicht besteht allein gegenüber dem Einmeldenden beginnend mit der Eingangsinformation und endend mit der Mitteilung, ob bzw. welche Maßnahmen ergriffen wurden (§ 17 HinSchG).

### e) Datenschutzbeauftragte als interne Meldestelle

#### aa) Allgemeines

Die internen Meldestellen müssen unabhängig sein, die nötige Fachkunde haben und ihrer Tätigkeit ohne Interessenkonflikte nachgehen können (§ 15 HinSchG). Erfordert der für sie anfallende Arbeitsbedarf keine fulltime Beschäftigung, so kann der Inhaber der Meldestelle noch weitere Aufgaben wahrnehmen. Gleiches gilt für einen internen und auch einen externen Datenschutzbeauftragten.<sup>64</sup> Sowohl nach Art. 38 Abs. 6 S. 1 DS-GVO als auch nach § 15 Abs. 1 S. 2 HinSchG steht es einem Datenschutzbeauftragten oder der Person, der die Aufgaben einer internen Meldestelle übertragen sind, ausdrücklich frei, neben dieser Tätigkeit zusätzlich andere Aufgaben und Pflichten innerhalb oder auch außerhalb des Unternehmens wahrzunehmen. In ähnlichem Wortlaut zeigen HinSchG und DS-GVO jedoch auch die Grenze zusätzlicher Aufgabenübertragungen auf. In beiden Regelungen wird verankert, dass die parallele Wahrnehmung von Aufgaben nicht zu Interessenskonflikten führen darf (§ 15 Abs. 1 S. 3 HinSchG bzw. Art. 38 Abs. 6 S. 2 DS-GVO). Wird die interne Meldestelle und die Position des Datenschutzbeauftragten einer Person

61 Feger, EU-Hinweisgeberrichtlinie und HinSchG-E: Möglichkeiten und Nutzen der Einbindung von Ombudspersonen, CB 2022, 187.

62 Vgl. auch Gesetzesbegründung zu § 14 Abs. 1 HinSchG, BT-Drs. 20/3442, S. 78.

63 Kappen/Cho/Gaertner, Konzernlösung des HinSchG-E – Unionsrechtswidrig?, CB 2022, 237; Bürkle, Zur Unionsrechtskonformität zentraler Konzernmeldestellen für Hinweisgeber, CCZ 2022, 335; Dilling, Die Konzernlösung gemäß § 14 Abs. 1 S. 1 HinSchG im Spannungsfeld zwischen europarechtlichen Vorgaben und den praktischen Bedürfnissen der von der Umsetzung betroffenen Unternehmensverbände, CCZ 2023, 91.

64 Im Internet finden sich u.a. hinreichend Angebote zur Bestellung eines externen DSB als Hinweisempfänger.

übertragen, muss gewährleistet werden, dass beide Funktionen unabhängig ausgeübt werden können.

#### bb) Interessenkonflikte

Voraussetzung zur Wahrnehmung der Funktionen von DSB und Meldestelle ist somit gleichermaßen zum einem, dass ausreichend (zeitliche) Ressourcen für beide Aufgaben zur Verfügung stehen und dass hierbei keine Interessenkonflikte vorliegen.<sup>65</sup>

Trotz dieser Ausschlussregelung sehen die Gesetzesbegründung und auch die Whistleblower-Richtlinie ausdrücklich die Möglichkeit den Datenschutzbeauftragten mit der Aufgabe der Meldestelle zu betrauen,<sup>66</sup> was nicht nur bedeutet, dass Konflikte in der Regel nicht bestehen, sondern dass sich die Personalunion sogar in Betrachtung des Anforderungsprofils beider Tätigkeiten und den personellen Möglichkeiten eines kleineren Unternehmens vielfach geradezu anbietet. Dabei spielt es keine Rolle, ob eine interne oder externe DSB-Bestellung vorliegt.

Ein zu vermeidender Konflikt kann eventuell auftreten, wenn der Datenschutzbeauftragte seine Arbeit als interne Meldestelle unter datenschutzrechtlichem Bezug kontrollieren muss. Im Regelfall werden durch die Einbindung einer weiteren Person<sup>67</sup> und eine ausgewogene und klar abgesteckte Rollenverteilung Interessenkonflikte erheblich verringert bzw. ausgeschlossen werden. Häufig wird die Wahrscheinlichkeit solcher Interessenkonflikte derart gering sein, dass sie bei der Übernahme der Meldestelle durch den DSB vernachlässigt werden können.

#### f) Sonstige datenschutzrechtliche Auswirkungen

Jede Meldung über natürliche Personen hat auch datenschutzrechtliche Auswirkungen, welche bei ihrer Bearbeitung zu berücksichtigen sind. Gegenüber der einmeldenden Person besteht die Informationspflicht nach Art. 13 DS-GVO.<sup>68</sup> Werden personenbezogene Daten in Hinweisgebermeldungen ohne Kenntnis der betroffenen Personen verarbeitet, so sind diese grundsätzlich nach Art. 14 DS-GVO über die Umstände der Datenverarbeitung zu unterrichten.<sup>69</sup> Außerdem kann es bei einem Auskunftsanspruch eines Beschuldigten nach Art. 15 DS-GVO zu datenschutzrechtlichen Fragestellungen hinsichtlich der Auskunftspflicht im konkreten Fall kommen. Hinsichtlich des Inhalts einer Meldung kann daneben der Ausnahmetatbestand in Art. 14 Abs. 5 lit. b DS-GVO zum Tragen kommen. Demnach besteht die Informationspflicht nicht, sofern sie voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, sodass bei internen Ermittlungen mit einer Verdunklungsfahr argumentiert werden kann.

### 5. Externe Meldestelle

Die zentrale externe Meldestelle auf Ebene des Bundes wird beim Bundesamt für Justiz (BfJ) angesiedelt (§ 19 HinSchG). Daneben sollen in speziellen Zuständigkeitsbereichen, wie z.B. denen der BaFin oder des Bundeskartellamtes dort existente Meldestellen bestehen bleiben. Den Ländern steht es frei, für die Meldungen, die die jeweiligen Landesverwaltung und die jeweiligen Kommunalverwaltungen betreffen, eigene externe Meldestellen einzurichten.

Das Verfahren bei externen Meldestellen regeln im Einzelnen die §§ 27 bis 31 HinSchG. Die externe Meldestelle kann

Auskünfte einholen und erteilt der hinweisgebenden Person Rückmeldungen.

### 6. Meldung an die Öffentlichkeit

Schließlich kann – sofern eine der hierfür geltenden Voraussetzungen vorliegt – als Hinweismöglichkeit der Weg an die Öffentlichkeit, d.h. die „Offenlegung“ (§ 3 Abs. 5 HinSchG) der Information gewählt werden (§ 32 HinSchG). Wenn die hinweisgebende Person zulässig den Weg der „Offenlegung“ des Vorgangs wählt, darf sie hierbei nicht behindert werden (§ 7 Abs. 2 HinSchG). Dem Weg an die Öffentlichkeit Grenzen aufzuzeigen, steht im Einklang mit der Rechtsprechung des EGMR.<sup>70</sup> Demgemäß gestattet § 32 HinSchG die Offenlegung, u.a. wenn die hinweisgebende Person nach der Meldung eines Verstoßes an eine externe Meldestelle nicht fristgemäß eine Rückmeldung erhalten hat, im Fall einer externen Meldung Repressalien zu befürchten sind oder aufgrund sonstiger besonderer Umstände die Aussichten gering sind, dass die externe Meldestelle wirksame Folgemaßnahmen nach § 29 HinSchG einleiten wird. Das Offenlegen unrichtiger Informationen über Verstöße ist verboten (§ 32 Abs. 2 HinSchG).

### 7. Schadenersatz und Sanktionen zum Schutz der hinweisgebenden Personen

Das Hinweisgeberschutzgesetz enthält zudem eigene Bestimmungen zu Schadenersatzansprüchen und Sanktionen: Bei einem Verstoß gegen das Repressalienverbot ist der hinweisgebenden Person der materielle Schaden zu ersetzen (§ 37 HinSchG).

§ 32 Abs. 2 HinSchG enthält ein spezielles Verbot des Offenlegens unrichtiger Informationen. Bei einer vorsätzlichen oder grob fahrlässigen Falschmeldung ist hingegen die hinweisgebende Person zur Erstattung des dadurch eingetretenen Schadens verpflichtet (§ 38 HinSchG).

Verstöße gegen die wesentlichen Vorgaben des Gesetzes können als Ordnungswidrigkeiten mit einer Geldbuße in Höhe von bis zu 50.000,- Euro geahndet werden (§ 40 HinSchG). Dies ist z.B. der Fall für Behinderungen von Meldungen aber auch für das wissentliche Offenlegen unrichtiger Informationen. Auch das Nichtbetreiben einer internen Meldestelle ist logischerweise bußgeldbewehrt.

## III. Das Beschwerdeverfahren nach dem LkSG

### 1. Schutzziel des LkSG

#### a) Allgemeines

Neu zu dem Kreis der Gesetze, die Hinweisgeberregelungen enthalten, zählt neben dem als „Stammgesetz“ des Themenbereichs konzipierten HinSchG ab Beginn 2023 auch

65 Gola, in: Gola/Heckmann, DS-GVO/BDSG § 7 BDSG, Rn. 13 ff.; vgl. auch bei Schneider/Brower/Scholz-Fröhling, Der Mehrfachbeauftragte – Vorüberlegungen zu einem allgemeinen Recht des Beauftragten, CCZ 2023, 133.

66 Vgl. Erwägungsgrund 56 HinSch-RL sowie BT-Drs. 20/5992 v. 14.03.2023, 66.

67 Zur Bestellung eines Vertreters des DSB im Verhinderungs- und Konfliktfall vgl. Gola, in: Gola/Heckmann, DS-GVO/BDSG § 5 BDSG, Rn. 23.

68 Vgl. auch das Beispiel der Hinweise zum LkSG nach Art. 13 der BAFA; <https://www.bafa.delskg-datenschutzerklärung-de>.

69 Torpediert Art. 14 DS-GVO den Hinweisgeberschutz?, <https://www.q-perior.com>.

70 Vgl. aktuell zur Berechtigung von Whistleblowing: EGMR, Urt. v. 14.02.2023 – Nr. 21884/18.

das Lieferkettensorgfaltspflichtengesetz – LkSG.<sup>71</sup> Ge-regelt werden die Verantwortung für die Einhaltung der Menschenrechte und des Schutzes der Umwelt in globalen Lieferketten (§ 2 LkSG)<sup>72</sup> und die diesbezüglichen Sorgfaltspflichten, wozu die Einrichtung eines in § 8 LkSG geregelten Beschwerdeverfahrens gehört (§ 3 Abs. 1 S. 2 Nr. 8 LkSG).<sup>73</sup>

### b) Die Gesetzesadressaten

Adressat des Gesetzes sind zunächst Unternehmen mit mindestens 3.000 Mitarbeitern, ab 2024 auch Unternehmen mit mindestens 1.000 Arbeitnehmern im Inland. Auch auf Körperschaften des öffentlichen Rechts findet das Gesetz Anwendung. Nach aktuellen Informationen der Bundesregierung wird das Gesetz einschließlich der ausländischen Unternehmen ab 2023 für über 900 Unternehmen gelten und ab 2024 für ca. 4.800.<sup>74</sup>

Zu beachten ist jedoch, dass darüber hinaus auch mittelbare und unmittelbare Zulieferer auf die Einhaltung menschenrechtlicher und umweltbezogener Standards zu überprüfen sind, so dass auch KMU indirekt betroffen sind,<sup>75</sup> weil deren Auftraggeber auch von ihnen die Umsetzung der Pflichten aus dem LkSG verlangen.<sup>76</sup> Liegen einem Unternehmen tatsächliche Anhaltspunkte vor, die eine Verletzung einer menschenrechtsbezogenen oder einer umweltbezogenen Pflicht eines Zulieferers möglich erscheinen lassen, so muss das Unternehmen anlassbezogen auch gegenüber einem mittelbaren Zulieferer tätig werden.<sup>77</sup> Die Verantwortung der Unternehmen endet nicht am eigenen Werkstor, sondern besteht entlang der gesamten Lieferkette.

Auch juristische Personen des öffentlichen Rechts fallen unter das Gesetz soweit sie unternehmerisch am Markt tätig sind, was der Fall ist, wenn der unternehmerisch tätige Teil der juristischen Person die Voraussetzungen des § 1 LkSG (eigenständig) erfüllt. Die erforderliche unternehmerische Tätigkeit am Markt liegt vor, wenn Dritten eine Dienstleistung oder ein Produkt (auch unentgeltlich) in Konkurrenz zu anderen Konkurrenten angeboten wird.

### c) Der Schutzauftrag im Konkreten

Konkret geht es um den Schutz von in § 2 LkSG umfangreich aufgelisteten Rechtsgütern. Beispielhaft ist der Schutz vor Kinderarbeit, das Recht auf faire Arbeitsbedingungen oder den Schutz der Umwelt. Das Gesetz legt dar, welche Präventions- und Abhilfemaßnahmen zur Gewährleistung der Rechtskonformität notwendig sind. Eine zur Gewährleistung dieses Schutzes speziell vorgegebene Pflicht ist die Einrichtung von Beschwerdekanälen für die in Lieferketten involvierten Menschen.

## 2. Das unternehmensinterne Beschwerdeverfahren

### a) Der Gesetzauftrag

Ein Kernelement der vom LkSG geforderten Sorgfallsmaßnahmen ist die Einrichtung eines „angemessenen unternehmensinternen und von dem Nutzer nachteilsfrei nutzbaren Beschwerdeverfahrens“ (§ 8 Abs. 1 LkSG).<sup>78</sup> Hingewiesen werden können soll auf menschenrechtliche und umweltbezogene Risiken und Rechtsverletzungen, die durch das wirtschaftliche Handeln eines Unternehmens im eigenen Geschäftsbereich oder eines unmittelbaren oder auch mittelbaren Zulieferers entstehen oder entstanden sind (§ 9 Abs. 1 LkSG).

### b) Die Organisation des Beschwerdeverfahrens

Bei der Ausgestaltung des Beschwerdeverfahrens haben die verpflichteten Unternehmen einen weiten Handlungs- und Ermessensspielraum. Die Unternehmen können sich statt interne Verfahren zu wählen auch an einem entsprechenden externen Beschwerdeverfahren beteiligen (§ 8 Abs. 1 S. 6 LkSG). In Betracht kommt etwa ein Beschwerdemechanismus, der unternehmensübergreifend von einem Branchenverband eingerichtet wurde. Konzernlösungen sind damit möglich.<sup>79</sup>

Es besteht auch keine Pflicht, allen Zielgruppen Zugang zu dem gleichen Beschwerdeverfahren zu geben. So können Unternehmen mehrere Verfahren einrichten, so z.B. eines nur für interne Personen.

### c) Der Kreis der Beschwerdeführer

Eine Besonderheit des Beschwerdeverfahrens nach dem LkSG ist seine weitgefaste Zielgruppe. Während bestehende Hinweisgebersysteme meist vordergründig auf die Nutzung durch die eigenen Beschäftigten ausgerichtet sind, soll ein Beschwerdeverfahren nach dem LkSG einem deutlich weiter gefassten Personenkreis, d.h. sowohl internen als auch externen Beschwerdeführenden zugänglich sein. Auch Menschen, die nicht direkt betroffen sind, aber von Menschenrechtsverletzungen oder Umweltgefährdungen Kenntnis erlangen, müssen Zugang zu Meldekanälen haben. Dies können beispielsweise Mitarbeitende von direkten oder indirekten Lieferanten sein oder Anwohner der Standorte.

### d) Der Schutz der Beschwerdeführer

Im Beschwerdeverfahren sind Vorkehrungen zu treffen, um die Vertraulichkeit der Identität von hinweisgebenden Per-

71 Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten (Lieferkettensorgfaltspflichtengesetz–LkSG); verabschiedet als Art. 1 des Gesetzes über die unternehmerischen Sorgfaltspflichten in Lieferketten v. 16.07.2021, BGBl. I v. 21.07.2021, S. 2959.

72 Dohrmann, Das deutsche Lieferkettensorgfaltspflichtengesetz als Vorbild für den europäischen Gesetzgeber? – Eine kritische Analyse, CCZ 2021, 265; Ehmann/Berg, Das Lieferkettensorgfaltspflichtengesetz (LkSG): ein erster Überblick, GWR 2021, 287; Freund/Krüger, Das neue Lieferkettensorgfaltspflichtengesetz, NVwZ 2022, 665; Fleischer, Grundstrukturen der lieferkettenrechtlichen Sorgfaltspflichten, CCZ 2022, 205; Gehling/Ott/Lüneborg, Das neue Lieferkettensorgfaltspflichtengesetz – Umsetzung in der Unternehmenspraxis, CCZ 2021, 230; Helck, Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten: Worauf sich Unternehmen zukünftig vorbereiten müssen, BB 2021, 1603; Leuring/Rubner, Lieferkettensorgfaltspflichtengesetz, NJW-Spezial 2021, 399; Saga/Schmidt, Das Lieferkettensorgfaltspflichtengesetz, NZA-RR 2022, 281; Wagner/Ruttloff, Das Lieferkettensorgfaltspflichtengesetz – Eine erste Einordnung, NJW 2021, 2145; Wais, Die vertragliche Seite des LkSG, JZ 2023, 429.

73 Siehe hierzu Bundesamt für Wirtschaft und Ausfuhrkontrolle, Handreichung „Beschwerdeverfahren nach dem Lieferkettensorgfaltsgesetz“, 1. Auflage, Oktober 2022.

74 Fragen und Antworten zum neuen Lieferkettengesetz; Eine Veröffentlichung der Initiative Lieferkettengesetz, Oktober 2021, 3.

75 Hess, Die Folgen des Lieferkettensorgfaltspflichtengesetz für KMU, NWB 2021, 2981.

76 Baldauf, Das Lieferkettensorgfaltspflichtengesetz findet auch auf Körperschaften des öffentlichen Rechts Anwendung, CCZ 2023, 81.

77 BMWK, Wissenschaftlicher Beirat, Gutachten: Menschenrechte und unternehmerische Sorgfaltspflichten 2022.

78 Das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) hat – entsprechend seinem gesetzlichen Auftrag (§ 20 LkSG) – die Handreichung „Beschwerdeverfahren organisieren, umsetzen und evaluieren“ veröffentlicht.

79 Nicolas/Ott/Lüneborg/Schmelzeisen, Zur Anwendung des Lieferkettensorgfaltspflichtengesetzes im Konzern, DB 2022, 238; Rothenburg/Rogg, Die Umsetzung des Lieferkettensorgfaltspflichtengesetzes im Konzern, AG 2022, 257.

sonen sowie den Schutz ihrer personenbezogenen Daten zu gewährleisten, wozu anonyme Verfahren beitragen. Unternehmen müssen festlegen und kommunizieren, wie hinweisgebende Personen vor Benachteiligung oder Bestrafung aufgrund der Nutzung eines Beschwerdeverfahrens geschützt sind. Dazu gehört die Verpflichtung, Vergeltungsmaßnahmen aufgrund von Beschwerden oder Hinweisen nicht zu tolerieren.

#### e) „Beschwerdebeauftragte“ als interne Ansprechpersonen

Für die Entgegennahme und Verarbeitung von Hinweisen muss mindestens eine „unparteiische“, zur Verschwiegenheit verpflichtete Person bestimmt werden. Zu benennen ist somit zumindest ein „Beschwerdebeauftragter“, der die ordnungsgemäße Durchführung des Verfahrens zu überwachen und eingegangene Hinweise zu dokumentieren hat. § 8 Abs. 3 LkSG gibt insbesondere vor, dass er nicht an Weisungen gebunden ist und die Gewähr für unparteiisches Handeln bietet, was den Ausschluss von Interessenkonflikten gebietet. Unternehmen müssen daher die strukturellen Voraussetzungen für unparteiisches Handeln schaffen. Daher stellt sich die Frage, ob – auch wenn das LkSG keinen besonderen Schutz des Beschwerdebeauftragten vor Abberufung, Benachteiligung oder Kündigung enthält – ein solcher vertraglich verankert werden sollte. So wird die Auffassung vertreten, dass – solange der Gesetzgeber einen solchen Schutz nicht kodifiziert – nur eine externe Lösung für das Beschwerdeverfahren möglich sei.<sup>80</sup>

#### f) Zugänglichkeit und Transparenz des Verfahrens

Sichergestellt sein muss, dass das Beschwerdeverfahren für potenzielle Beteiligte unschwer zugänglich, die Vertraulichkeit der Identität der Beschwerdeführer gewahrt und wirksamer Schutz vor Benachteiligung oder Bestrafung aufgrund einer Beschwerde gewährleistet ist (§ 8 Abs. 4 LkSG).

Um die spezifischen Zugangsbarrieren zu überwinden, kann es notwendig sein, unterschiedliche Beschwerdekanaäle (telefonisch, Online-Systeme, lokale Ansprechpersonen) und diese ggf. auch in mehreren Sprachen bereitzustellen.

In jedem Falle muss die Verfahrensweise transparent sein. In geeigneter Weise sind klare und verständliche Informationen zur Erreichbarkeit, Zuständigkeit und Durchführung des Beschwerdeverfahrens öffentlich zugänglich zu machen.<sup>81</sup> Die Nutzer müssen regelmäßig darüber informiert werden, wie mit ihren Informationen verfahren wird. Dies beginnt mit der Bestätigung des Eingangs des Hinweises und ggf. seiner Erörterung mit den Hinweisgebern (§ 8 Abs. 1 S. 3 LkSG).

Die genannten Verfahrensregelungen müssen ihren Niederschlag finden in einer Verfahrensordnung (§ 8 Abs. 2 LkSG), die einen vorhersehbaren zeitlichen Rahmen für jede Verfahrensstufe sowie klare Aussagen zu den vorgegebenen Abläufen festlegt.

### 3. Der fakultative Menschenrechtsbeauftragte

#### a) Überwachung des Risikomanagements

Nach § 4 LkSG haben vom Gesetz tangierte Unternehmen ein angemessenes und wirksames Risikomanagement zur Einhaltung der ihnen obliegende Sorgfaltspflichten (§ 3 Abs. 1

LkSG) einzurichten, das einer Überwachung bedarf. Nach Abs. 3 ist festzulegen, wer innerhalb des Unternehmens hierfür zuständig ist. Mit der Aufgabe können auch mehrere konkrete Personen betraut werden und von Nöten sein, da die Anforderungen an Überwachungs- und Kontrollaufgaben in der praktischen Umsetzung umfangreiche Ausmaße annehmen können. Aus dem Wortlaut des § 17 Abs. 2 LkSG ist zu entnehmen, dass eine Aufgabendelegation auf verschiedene Personen bzw. Geschäftsabläufe sinnvoll sein soll.

#### b) Ein neuer „Beauftragter“

Als eine organisatorische Möglichkeit der Kontrolle bietet das Gesetz die Benennung eines Menschenrechtsbeauftragten an.<sup>82</sup> Ihm obliegt – ähnlich einem Datenschutzbeauftragten – eine Überwachungsfunktion hinsichtlich der Etablierung und Funktionsfähigkeit des Risikomanagements nebst Beschwerdeverfahren. In seinen Aufgabenbereich fällt die Abgabe konkreter oder allgemeiner Empfehlungen im Hinblick auf die Präventions-/Abhilfemaßnahmen. Hierzu gehört unter anderem die Überprüfung der Risikoanalyse (§ 5 LkSG) und die Abhilfe- und Präventionsmaßnahmen (§§ 6, 7 LkSG). Ermittelte Risiken muss er bewerten und der Geschäftsleitung anlassbezogen bzw. jedenfalls einmal im Jahr in einem Bericht mitteilen. Die Verantwortung für die Erfüllung der Sorgfaltspflichten und für die Umsetzung der vorstehenden Maßnahmen sind originäre Pflichten der Geschäftsleitung.

Das Lieferkettengesetz spricht bei dem Menschenrechtsbeauftragten nicht explizit von einer Einzelperson. Jedoch ist hier wie in der Regel bei dem Datenschutzbeauftragten von einer Einzelperson auszugehen, der natürlich ggf. Mitarbeiter zugordnet werden können. Nur bei Trennung der Aufgabengebiete können Menschenrechtsbeauftragte parallel tätig sein.

Eine Personalunion zwischen dem Beschwerdebeauftragten und dem Menschenrechtsbeauftragten scheidet aus, da zu der Überwachungsfunktion des Menschenrechtsbeauftragten auch die Tätigkeit des Beschwerdebeauftragten gehört. Die Umsetzung des LkSG im Unternehmen hat somit eine duale Struktur. Der Beschwerdebeauftragte wirkt bei der Umsetzung mit und der Menschenrechtsbeauftragte kontrolliert, ob dies in angemessener Weise geschieht.

Menschenrechtsbeauftragte werden freiwillig bestellt und genießen keine abgesicherte Rechtsstellung etwa in Gestalt eines besonderen Kündigungs- oder Diskriminierungsschutzes.

### 4. Kontrolle und Sanktionen

Die Umsetzung des LkSG wird durch das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) überwacht. Das BAFA ist mit Eingriffsbefugnissen ausgestattet und kann Zwangs- und Bußgelder verhängen oder den Ausschluss von öffentlichen Ausschreibungen verfügen.

80 Zimmer, Das Lieferkettensorgfaltspflichtengesetz – Handlungsempfehlungen für Mitbestimmungsakteure und Gewerkschaften, Bund Verlag, HSI-Schriftenreihe BD 48, 65.

81 Vgl. Verfahrensordnung der Zurich AG, [https://www.zurich.de/br/>...>lksg-verfahrensverordnung\\_2022\\_12](https://www.zurich.de/br/>...>lksg-verfahrensverordnung_2022_12); sowie <https://www.prosiebensat1.com/uploads/Verfahrensordnung/Verfahrensordnung-ProSiebenSat1MediaSE,KlinikenLudwigshafen,https://www.klilu.de/>...>e44350>e44367/Verfahrensordnung>.

82 Häfeli, Der Menschenrechtsbeauftragte im Lieferkettensorgfaltspflichtengesetz – ein weiterer betrieblicher Beauftragter?, ARP 2021, 229.

U.a. handelt ordnungswidrig, wer entgegen § 8 Abs. 1 S. 1 LkSG auch in Verbindung mit § 9 Abs. 1 LkSG nicht dafür sorgt, dass ein Beschwerdeverfahren eingerichtet wird. Das Bußgeld kann bis zu 800.000,- Euro betragen (§ 24 LkSG).

#### IV. Abschlussbemerkung

Die Beschäftigten eines Unternehmens oder einer Behörde sind zunächst im Rahmen ihrer Treuepflicht im Regelfall gehalten, von Kollegen verursachte gravierende Schädigungen des Arbeitgebers/Dienstherrn durch entsprechende Meldung abzuwenden bzw. zu beenden. Das gilt unabhängig davon, ob die Schäden unmittelbar beim Arbeitgeber/Dienstherrn oder zunächst bei Dritten, also z.B. bei Kunden mit Rückwirkung auf den Arbeitgeber eintreten. Die Treuepflicht geht aber ins Leere, wenn Rechtsverstöße vom Arbeitgeber selbst initiiert oder jedenfalls gebilligt werden. Beide Situationen erfassend bieten nunmehr spezielle und allgemeine Whistleblower-Regelungen einen Verbund von Schutzwirkungen, die zur Motivation von Hinweisgebern beitragen sollen. Je nach dem Tätigkeitsbereich eines Unternehmens sind

ggf. mehrere Melderegeln gleichzeitig zu beachten bzw. umzusetzen, wobei die gesetzlich vorgegebenen Verfahren teilweise übereinstimmen bzw. sich überschneiden und abgestimmt vereinheitlicht werden können. Das gilt u.a. für das HinSchG und das LkSG. Häufig wird es sinnvoll sein, den beiden Regelwerken in einem Verfahren und Kanal zu genügen, wobei jedoch die jeweils strengeren Anforderungen der einzelnen Verfahren umzusetzen sind.



#### Prof. Peter Gola

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

Prof. Dr. Lorenz Franck

# Zertifizierungsstellen nach der DS-GVO als Beliehene?

Das Verfahren nach den Art. 42 und 43 DS-GVO kennt neben der Datenschutzaufsichtsbehörde eine weitere Akteurin, welche Zertifizierungen erteilen kann: Die akkreditierte Zertifizierungsstelle. Ob diese hoheitlich tätig wird und insofern selbst als Behörde dem allgemeinen Verwaltungsverfahrensrecht unterliegt, ist bislang nicht abschließend geklärt. Dabei hängen von der Beantwortung dieser Vorfrage maßgebliche Weichenstellungen u.a. für den Ablauf des Verfahrens und den Widerruf von Zertifizierungen ab.

## I. Überblick

Certificāre aus dem Spät- bzw. Kirchenlateinischen bedeutet so viel wie vergewissern, jemandem etwas versichern, sicherstellen (von certus „sicher, gewiss“ und facere „machen, tun“). Die hergebrachte Arbeitsdefinition der International Standards Organisation (ISO) für den Vorgang der Zertifizierung lautet: „the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.“<sup>1</sup> Gefordert wird also gemeinhin eine von unabhängiger dritter Seite herrührende Bestätigung, dass ein Prüfungsgegenstand bestimmten zuvor festgelegten Prüfkriterien entspricht.

## II. Zertifizierung im Datenschutzrecht

Die datenschutzrechtliche Zertifizierung ist maßgeblich in den Artt. 42 und 43 DS-GVO geregelt. In der VO 2018/1725/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union (EUIBA) wird unmittelbar auf die DS-GVO-Vorschriften verwiesen und somit ein Gleichlauf erzeugt. Demgegenüber kennt die RL 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von

<sup>1</sup> <https://www.iso.org/certification.html>.

Straftaten oder der Strafvollstreckung (JI-RL) keine Zertifizierung.

## 1. Gegenstand der Zertifizierung

Unsicherheit besteht hinsichtlich des eigentlichen Gegenstands, der zertifiziert werden soll. Während Erwägungsgrund 100 DS-GVO Produkte und Dienstleistungen in den Blick nimmt, werden im regelnden Teil entweder Verarbeitungsvorgänge (Art. 42 Abs. 2 DS-GVO), Verarbeitungen<sup>2</sup> (Art. 42 Abs. 6 DS-GVO) oder Verarbeitungstätigkeiten<sup>3</sup> (Art. 42 Abs. 6 DS-GVO) angesprochen. Nach Auffassung des Europäischen Datenschutzausschusses kommt hier vor dem Hintergrund der ISO 17065 ein weites Verständnis zum Tragen, indem die tatbestandlichen Verarbeitungsvorgänge zu Produkten, Dienstleistungen und Prozessen gebündelt werden können.<sup>4</sup>

Unabhängig von etwaigen Meinungsstreitigkeiten wird zumindest deutlich, was nicht Gegenstand der Zertifizierung sein kann: Personenzertifizierungen (etwa zum behördlichen oder betrieblichen Datenschutzbeauftragten) oder sonstige personengebundene Nachweise, etwa zugunsten von Anbietern, Herstellern oder Importeuren, scheiden von vornherein aus. Taugliche Antragssteller sind insoweit gem. Art. 42 Abs. 7 S. 1 DS-GVO ausschließlich Verantwortliche oder Auftragsverarbeiter.<sup>5</sup>

Ausweislich Art. 42 Abs. 1 DS-GVO ist (mindestens) die Einhaltung der Verordnung als Zertifizierungsmaßstab festgelegt.<sup>6</sup> Zur Ermittlung und Festlegung von Zertifizierungskriterien haben sowohl der Europäische Datenschutzausschuss<sup>7</sup> als auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder<sup>8</sup> Papiere veröffentlicht.

## 2. Wirkungen und Vorteile der Zertifizierung

Gem. Art. 42 Abs. 2 DS-GVO muss die Zertifizierung stets freiwillig erfolgen. Es handelt sich daher nicht um einen Erlaubnisvorbehalt für das Inverkehrbringen von Produkten. Zu den „Soft-Benefits“ gehören zweifellos Marketing und PR. Öffentliche Stellen könnten u.U. eine bestehende Zertifizierung bei der Ausschreibung und Beschaffung voraussetzen<sup>9</sup> oder zumindest berücksichtigen. Zum Teil wird außerdem vermutet, dass Aufsichtsbehörden ihre Kontrolltätigkeit nach dem Opportunitätsprinzip eher auf nicht-zertifizierte Verantwortliche und Auftragsverarbeiter konzentrieren werden („Fliegen unterm Radar“).<sup>10</sup>

Einige Gründe für das Durchlaufen eines Zertifizierungsverfahrens<sup>11</sup> lassen sich dagegen unmittelbar in der DS-GVO ablesen. Zunächst erleichtert eine bestehende Zertifizierung den Nachweis der Rechtmäßigkeit der Verarbeitung.<sup>12</sup> Die Zertifizierung wird ausdrücklich genannt im Zusammenhang mit der Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 Abs. 3 DS-GVO), den Grundsätzen von privacy by design/privacy by default (Art. 25 Abs. 3 DS-GVO), der Auftragsverarbeitung (Art. 28 Abs. 3 DS-GVO) sowie der Sicherheit der Verarbeitung (Art. 32 Abs. 3 DS-GVO). Auch im Rahmen einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) wird einer Zertifizierung bestätigende Wirkung zukommen,<sup>13</sup> zumindest im Falle einer Folgeprüfung nach Art. 35 Abs. 11 DS-GVO.

Bei Drittstaatstransfers erleichtert die Zertifizierung nicht nur den Nachweis der Rechtmäßigkeit, sondern kann selbst Teil der Rechtfertigung (Art. 46 Abs. 2 lit. f DS-GVO) sein.<sup>14</sup>

Kommt es zum Rechtsverstoß, kann eine Haftungsminimierung zum Tragen kommen, dies einerseits bei der Bemessung eines Bußgelds (Art. 83 Abs. 2 lit. j DS-GVO), andererseits beim Schadensersatzrechtlichen Exkulpationsversuch<sup>15</sup> (Art. 82 Abs. 3 DS-GVO).

Die DS-GVO besitzt unterdessen keine Sperrwirkung für freie, nicht-akkreditierte Zertifizierungsprogramme.<sup>16</sup> Letztere entfalten jedoch keine besonderen Rechtswirkungen und sind allenfalls zu Werbezwecken einsetzbar. Eine Beleihung nicht-akkreditierter Zertifizierer kommt daher nicht in Frage.

## 3. Akteure im Zertifizierungsverfahren

Der Weg zur Zertifizierung, wie er in der DS-GVO vorgezeichnet ist, weist einige Verzweigungen auf.

Zunächst bedarf es bestimmter Zertifizierungskriterien, diese werden gem. Art. 42 Abs. 5 S. 1 i.V.m. Art. 58 Abs. 3 lit. f Alt. 2 DS-GVO grds. von der Aufsichtsbehörde genehmigt. Sofern stattdessen der Europäische Datenschutzausschuss die Kriterien genehmigt (Art. 42 Abs. 5 S. 1 und 2 i.V.m. Art. 63 DS-GVO), ist der Weg zum sog. Europäischen Datenschutzsiegel eröffnet.

2 Art. 4 Nr. 2 DS-GVO: „Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe“.

3 In Anlehnung an Art. 18 Abs. 1 RL 95/467EG: Bündel von Verarbeitungsschritten mit hinreichender Komplexität und einheitlicher Zweckbestimmung. Siehe auch LfDI Baden-Württemberg, 34. TB 2018, 11 mit Blick auf den Geschäftsprozess.

4 Europäischer Datenschutzausschuss, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Version 3.0 vom 04.06.2019, 16, online unter <https://t1p.de/fsu9i>; vgl. auch Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 22; Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 36 ff.

5 Ein etwaiges Sponsoring wie bei anderen IT-Zertifizierungen (vgl. etwa § 8 Abs. 1 S. 2 BSIZertV) ist nicht vorgesehen.

6 Nach vorzugswürdiger Auffassung kann freilich ein strengerer Maßstab zertifiziert werden, Bergt/Pesch, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 42 Rn. 15; Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 26; Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 48.

7 Europäischer Datenschutzausschuss, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Version 3.0 vom 04.06.2019, online unter <https://t1p.de/fsu9i>.

8 Datenschutzkonferenz, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 2.0 vom 21.06.2022, online unter <https://t1p.de/trhj6>.

9 Befürwortend Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 83; ablehnend Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 9; Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 30; kritisch Eckhardt, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. 2021, Art. 42 DS-GVO Rn. 41; Bergt/Pesch, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 42 Rn. 9 f.

10 Bergt/Pesch, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 42 Rn. 2/27.

11 Zu den Erwartungen der Branche vgl. Potthoff/Schrief, DuD 2021, 326 ff.

12 Zum Grundprinzip der Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO eingehend Veil ZD 2018, 9 ff.

13 Kritisch Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 7; Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 9; Scholz in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 52.

14 Hierzu Europäischer Datenschutzausschuss, Guidelines 07/2022 on certification as a tool for transfers v. 14.06.2022, online unter <https://t1p.de/grh5c>.

15 Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 9; Hornung in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 79.

16 Müllmann/Spiecker gen. Döhmann, DVBl 2022, 208, 213 f.; Will in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 10; Bergt/Pesch, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 42 Rn. 17; Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 3.

Die Zertifizierung selbst erfolgt gem. Art. 42 Abs. 5 S. 1 DS-GVO durch die Aufsichtsbehörde oder durch eine akkreditierte Zertifizierungsstelle. Die zuvor erforderliche Akkreditierung wird gem. Art. 43 Abs. 1 S. 2 DS-GVO entweder durch die Aufsichtsbehörde oder durch die nationale Akkreditierungsstelle erteilt.<sup>17</sup> In Deutschland ist die nationale Akkreditierungsstelle nach § 1 Abs. 1 AkkStelleGBV die Deutsche Akkreditierungsstelle GmbH (DAKKS). Gem. § 39 S. 1 BDSG erteilt die Aufsichtsbehörde nach erfolgreicher Akkreditierung durch die DAKKS der Zertifizierungsstelle die Befugnis, ihre Tätigkeit auszuüben.

Die Erteilung oder Verweigerung einer Zertifizierung durch eine Zertifizierungsstelle erfolgt gem. Art. 43 Abs. 5 DS-GVO erst nach vorheriger Notifizierung der Aufsichtsbehörde. Aufsichtsbehörden und Zertifizierungsstellen können nötigenfalls Zertifizierungen widerrufen (Art. 42 Abs. 7 S. 2 DS-GVO, Art. 58 Abs. 2 lit. h DS-GVO).

### III. Hoheitliches Handeln

Bemerkenswert ist zunächst, dass durch den Einsatz privat verfasster Zertifizierungsstellen parallele Strukturen zur Datenschutzaufsicht aufgebaut werden. Die Zertifizierung erfolgt keineswegs allein im wirtschaftlichen Interesse der Antragsteller, sondern ausweislich Erwägungsgrund 100 DS-GVO im Interesse der Transparenz zugunsten der betroffenen Personen. Zugleich ist mit der erfolgreichen Zertifizierung eine Erweiterung des Rechtskreises sowie eine Verbesserung der Rechtsstellung der jeweiligen Antragsteller verbunden (siehe oben Pkt. II. 2.). Das Zertifizierungsverfahren wird folglich sowohl von Aufsichtsbehörden als auch Zertifizierungsstellen gleichermaßen im öffentlichen Interesse durchgeführt.<sup>18</sup>

#### 1. Beliehene

Das Verwaltungsrecht kennt seit jeher Privatrechtssubjekte, welche hoheitliche Aufgaben wahrnehmen. Beliehene (oder: beliehene Unternehmer) sind eigenständige Verwaltungsträger und somit Teil der mittelbaren Staatsverwaltung. Sie sind Behörden im Sinne von § 1 Abs. 4 VwVfG. Diese Sonderstellung ist notwendig, da gem. Art. 33 Abs. 4 GG die Ausübung hoheitsrechtlicher Befugnisse als ständige Aufgabe grds. dem Privatsektor entzogen und in der Regel Angehörigen des öffentlichen Dienstes zu übertragen ist, welche in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.<sup>19</sup> Die Beleihung bedarf daher aus verfassungsrechtlicher Sicht einer restriktiven Handhabung.

Der Beliehene ist zunächst eine Figur des nationalen Verwaltungsrechts. Er kann dennoch in unionsrechtlichen Zusammenhängen Bedeutung erlangen.<sup>20</sup> Die Union ist mangels umfassenden Verwaltungsunterbaus für die Durchführung des Unionsrechts auf die Mitwirkung der Mitgliedstaaten angewiesen (sog. indirekter Vollzug). Das Unionsrecht statuiert dabei für die Mitgliedstaaten kein Allgemeines Verwaltungsrecht. Es existiert also keine eigenständige Kodifikation eines „Unionsverwaltungsrechts“.<sup>21</sup> Stattdessen ist anerkannt, dass in Ermangelung unionsrechtlicher Vorgaben stets das jeweilige mitgliedstaatliche Verwaltungsrecht bei der Durchsetzung des Unionsrechts maßgeblich ist.<sup>22</sup> Der Behördenbegriff ist insofern ebenfalls mitgliedstaatlich zu bestimmen.<sup>23</sup>

#### 2. Folgen einer etwaigen Beleihung im Zertifizierungsumfeld

Würde es sich bei den Zertifizierungsstellen um Beliehene und somit um Behörden handeln, hätte dies weitreichende Folgen für das Zertifizierungsverfahren. Die Zertifizierungsstelle wäre selbst unmittelbar grundrechtsverpflichtet<sup>24</sup> (Art. 1 Abs. 3, 20 Abs. 3 GG) und müsste verwaltungsverfahrensrechtliche Vorschriften beachten. Die (Nicht-)Erteilung der Zertifizierung erfolgte im Wege des Verwaltungsakts gem. § 35 S. 1 VwVfG.<sup>25</sup> Dementsprechend wäre eine Rechtsbehelfsbeleihung gem. § 37 Abs. 6 VwVfG anzufügen. Rechtsschutz wäre grds. nur innerhalb einer Monatsfrist möglich<sup>26</sup> und nicht etwa innerhalb der zivilrechtlichen Verjährungsfrist von drei Jahren.<sup>27</sup> Die gerichtliche Auseinandersetzung fände vor dem Verwaltungsgericht und nicht vor dem Zivilgericht statt. Verwaltungsgebühren würden per Bescheid festgesetzt und nötigenfalls vollstreckt, nicht etwa per privater Rechnung beigetrieben. Die Aufhebung eines Zertifizierungsverwaltungsaktes richtete sich grds. nach den §§ 48, 49 VwVfG.<sup>28</sup> Wäre die Zertifizierungsstelle eine Behörde, könnte gegen sie wegen Art. 83 Abs. 7 DS-GVO i.V.m. § 43 Abs. 3 BDSG kein Bußgeld nach Art. 83 Abs. 4 lit. b DS-GVO verhängt werden, es sei denn, sie nähme gem. § 2 Abs. 5 S. 1 BDSG am Wettbewerb teil.<sup>29</sup> Schadenersatzrechtlich griffe gem. Art. 34 S. 2 GG die Amtshaftung. Darüberhinaus wäre das Informationsfreiheitsrecht einschlägig. Die Frage nach der Belieheneneigenschaft besitzt deshalb unmittelbare praktische Bedeutung.<sup>30</sup>

17 Zu den Akkreditierungsvoraussetzungen siehe Art. 43 Abs. 2 und 3 DS-GVO, näher Europäischer Datenschutzausschuss, Guidelines 4/2018 on the accreditation of certification bodies, Version 3 v. 04.06.2019, online unter <https://t1p.de/gt5yf>; Datenschutzkonferenz, Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065, Version 1.4 v. 08.10.2020, online unter <https://t1p.de/x5bpy>.

18 Daher der Förderauftrag in Art. 42 Abs. 1 und Art. 57 Abs. 1 lit. n DS-GVO.

19 BVerwG NVwZ 2011, 368, 370.

20 Vgl. Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, 10. Aufl. 2023, § 1 Rn. 256 zur möglichen Beleihung von unionsrechtlich vorgesehenen Konformitätsbewertungsstellen.

21 Zu entsprechenden Entwürfen näher Guckelberger, NVwZ 2013, 601; Kahl, JuS 2018, 1025, 1029 ff.

22 EuGH NJW 1984, 2024 f. Rn. 17 (Deutsche Milchkontor); EuGH NVwZ 2004, 593, 597 Rn. 67 (Wells). Vgl. Franck ZD 2021, 247, 247 f. zur Ausstrahlungswirkung des Unionsrechts auf das Unionsverwaltungsrecht der Mitgliedstaaten.

23 Für das Datenschutzrecht ausdrücklich Art.-29-Datenschutzgruppe, Guidelines on Data Protection Officers (DPOs) – WP 243 rev01 v. 05.04.2017, 6, online unter <https://t1p.de/1ozi0>.

24 Zur Grundrechtsbindung öffentlich beherrschter Unternehmen vgl. BVerfG, NJW 2011, 1201 ff.

25 Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 31; Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 13c; Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 86.

26 Widerspruch: § 70 Abs. 1 S. 1 VwGO; Verpflichtungsklage: § 74 Abs. 2 VwGO.

27 Regelmäßige Verjährung: § 195 BGB.

28 Zur unionsrechtlichen Überlagerung insb. hinsichtlich Ermessensspielraums und Vertrauensschutzaspekten Bergt/Pesch, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 42 Rn. 24 f.

29 Was wegen der Konkurrenzsituation mit nicht-akkreditierten Zertifizierern gesondert zu prüfen wäre.

30 Im Zusammenhang mit anerkannten Prüf- und Bestätigungsstellen nach § 18 Abs. 1 SigG a.F. wurde die praktische Bedeutung apodiktisch verneint, BT-Dr. 14/4662, 30.

### 3. Beleihung der Zertifizierungsstelle

Eine gesetzliche Definition fehlt im VwVfG,<sup>31</sup> doch gilt als Beliehener jede natürliche oder juristische Person des Privatrechts, die durch oder aufgrund Gesetzes hoheitliche Aufgaben im eigenen Namen und in eigener Verantwortung mit hoheitlichen Mitteln unter staatlicher Aufsicht wahrnimmt.<sup>32</sup> Im datenschutzrechtlichen Schrifttum wird – soweit ersichtlich – vertreten, bei der Zertifizierungsstelle im Sinne von Art. 43 DS-GVO handele es sich um eine rein privatrechtliche Figur.<sup>33</sup> Eine Begründung bleiben die Verfasser schuldig.<sup>34</sup>

#### a) Unproblematisches

Als Zertifizierungsstellen kommen zunächst unzweifelhaft natürliche oder juristische Personen des Privatrechts in Betracht. Es fehlt an einer Verwendung des Begriffs „Beleihung“ im Gesetzeswortlaut. Zum Vergleich: Die DAkKS wird gem. § 8 Abs. 1 S. 1 AkkStelleG i.V.m. § 1 Abs. 1 AkkStelleGBV ausdrücklich zur Beliehenen erklärt. Ähnlich verhält es sich mit Beleihungen in anderen Rechtsgebieten.<sup>35</sup> Das Fehlen der Bezeichnung im Gesetzestext ist jedoch unschädlich,<sup>36</sup> wie etwa der Vergleich mit der Hauptuntersuchung von Kraftfahrzeugen (§ 29 Abs. 2 S. 2 StVZO), einem klassischen Schulbeispiel der Beleihung, zeigt. Zudem ist nicht zu erwarten, dass sich der Unionsgesetzgeber des Sprachgebrauchs nationalen Verwaltungsrechts bedient.<sup>37</sup> Das argumentum e silentio geht daher ins Leere.

Die Zertifizierungsstelle handelt von vornherein im eigenen Namen und in eigener Verantwortung, dies folgt aus der formalen Gleichrangigkeit der Zertifizierungen von Zertifizierungsstelle bzw. Aufsichtsbehörde in Art. 42 Abs. 5 S. 1 DS-GVO. Die Bewertung durch die Zertifizierungsstelle erfolgt gem. Art. 43 Abs. 4 S. 1 DS-GVO abschließend und in eigener Verantwortlichkeit. Dass dann zwei Behörden mit identischer Zuständigkeit agierten, wäre unschädlich. Hinsichtlich der vorgelagerten Akkreditierung ist bereits eine vergleichbare Parallelität von Aufsichtsbehörde und beliehener Akkreditierungsstelle in Art. 43 Abs. 1 S. 2 DS-GVO angelegt. Auch in anderen verwaltungsrechtlichen Zusammenhängen können sich u.U. Mehrfachzuständigkeiten ergeben.<sup>38</sup> Es entspricht geradezu dem Wesen, „dass dem Beliehenen etwas übertragen wird, [...] was der Beleihende aber nicht endgültig aufgibt.“<sup>39</sup>

Die Aufgabenübertragung erfolgt durch Befugniserteilung gem. § 39 S. 1 BDSG und somit aufgrund gesetzlicher Regelung (mittels Verwaltungsakts).

#### b) Staatliche Aufsicht

Zugleich unterliegt die Zertifizierungsstelle der staatlichen Aufsicht. Staatliche Aufsicht meint regelmäßig Fach- und/oder Rechtsaufsicht.<sup>40</sup> Zertifizierungsstellen sehen sich potenziell gleich mehreren aufsichtsrechtlichen Maßnahmen ausgesetzt. Die Aufsichtsbehörde genehmigt allgemein die Akkreditierungsvoraussetzungen gem. Art. 43 Abs. 3 S. 1 DS-GVO und sodann die konkreten Zertifizierungskriterien gem. Art. 42 Abs. 5 S. 1 DS-GVO. Die Erteilung und der Widerruf – nicht jedoch die Verweigerung – der Zertifizierung durch eine Zertifizierungsstelle erfolgen jeweils gem. Art. 43 Abs. 5 DS-GVO erst nach vorheriger Notifizierung der Aufsichtsbehörde. Hierbei ist der Aufsicht hinreichend Zeit einzuräumen, damit diese nötigenfalls von ihren Befugnissen Gebrauch machen kann.<sup>41</sup> Zu letzteren gehört u.a. die

Anweisung, die Zertifizierung zu verweigern (Art. 58 Abs. 2 lit. h Var. 3 DS-GVO). Gleichwohl kann die Aufsichtsbehörde nicht anweisen, eine Zertifizierung wie beantragt zu erteilen oder einen Widerruf zu unterlassen. Das aufsichtsrechtliche Instrumentarium ist an dieser Stelle unvollständig. Die Zertifizierungsstelle kann angewiesen werden, eine bereits erteilte Zertifizierung zu widerrufen (Art. 58 Abs. 2 lit. h Var. 2 DS-GVO) oder die Aufsichtsbehörde kann den Widerruf unmittelbar selbst vornehmen (Art. 58 Abs. 2 lit. h Var. 1 DS-GVO)<sup>42</sup>. Die Aufsichtsbehörde kann gem. Art. 43 Abs. 7 DS-GVO die Akkreditierung als solche widerrufen und so die Voraussetzung für die Aufhebung der Befugnis nach § 39 S. 1 BDSG schaffen. Zu guter Letzt besteht die bereits angesprochene Sanktionsmöglichkeit gem. Art. 83 Abs. 4 lit. b) DS-GVO.

Diese besondere Sanktionsmöglichkeit trifft unterdessen keine grundsätzliche Aussage über eine möglicherweise fehlende Behördeneigenschaft der Zertifizierungsstelle. Dem Unionsrecht ist die Sanktionierung von Behörden und öffentlichen Stellen insgesamt nicht fremd.<sup>43</sup>

#### c) Hoheitsgewalt

Der Tätigkeit der Zertifizierungsstelle haftet das Odium des Öffentlichen Rechts an (siehe oben, Pkt. II. 2.). Hinsichtlich der Erleichterung von Rechenschaftspflichten, der Ermöglichung von Drittstaatstransfers sowie der Haftungserleichterung wird man eine öffentlich-rechtliche Grundbedeutung der Zertifizierung nicht in Abrede stellen können. Immerhin wird ein von einer Zertifizierungsstelle herrührendes Zertifikat z.T. „als besonders geschützte öffentliche Urkunde“ aufgefasst.<sup>44</sup> Es handele sich bei der Zertifikats-

31 Siehe stattdessen § 24 LVwG SH.

32 Ronellenfitsch, in: Bader/Ronellenfitsch, BeckOK VwVfG, 58. Ed. 2020, § 1 Rn. 71; Schoch, in: Schoch/Schneider, Verwaltungsrecht, 3. EL 2022, § 1 VwVfG Rn. 162.

33 Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 47; Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 9; Scholz, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2019, Art. 43 DS-GVO Rn. 1/32; Raschauer, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, Art. 42 Rn. 35; Kinast, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 42 Rn. 55; Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 88.

34 Allein Kinast, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 42 Rn. 55 begnügt sich mit einem knappen Verweis auf die Freiwilligkeit der Zertifizierung.

35 Vgl. § 33 Abs. 1 S. 2 PostG; § 12 Abs. 1 LuftSiG; § 16a LuftSiG, § 6 IfrGG; § 28 UAG; § 31c SGB V u.u.a.

36 Kiefer, LKRZ 2009, 441, 443 konstatiert generell sehr unterschiedliche Regelungsintensitäten in Bezug auf die Beleihung je nach Fachrecht.

37 Zur „benannten Stelle“ stattdessen Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, 10. Aufl. 2023, § 1 Rn. 256. Rennert, JZ 2009, 976 Fn. 10 verneint wohl eine Beleihung unmittelbar durch Unionsrecht und verlangt eine mitgliedstaatliche Umsetzung. Ob sich eine Beleihung unmittelbar aus dem Unionsrecht ergeben kann oder ob den Mitgliedstaat lediglich eine Verpflichtung trifft, eine Beleihung vorzunehmen, kann für hiesige Zwecke dahinstehen.

38 Vgl. etwa die parallelen bundesweiten Zuständigkeiten der an sich nach örtlichen Zuständigkeiten gegliederten Bundespolizeidirektionen gem. § 2 Abs. 2 BPolZV.

39 Ronellenfitsch, in: Bader/Ronellenfitsch, BeckOK VwVfG, 58. Ed. 2020, § 1 Rn. 71.

40 Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, 10. Aufl. 2023, § 1 Rn. 246.

41 Arg. ex Art. 43 Abs. 1 S. 1 a.E. DS-GVO.

42 Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 42; zweifelnd Eckhardt, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. 2021, Art. 42 DS-GVO Rn. 68; Paal/Kumkar, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, Art. 42 Rn. 21.

43 Vgl. Art. 83 Abs. 7 DS-GVO, Art. 57 RL 2016/680/EU (II-RL) bzw. Art. 66 VO 2018/1725/EU (EUIBA).

44 Raschauer, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, Art. 42 Rn. 35; Kinast, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 42 Rn. 55.

erteilung um einen „öffentlich-rechtlich überformten privaten Rechtsakt“.<sup>45</sup> Eine Zertifizierungsstelle (auch) in öffentlich-rechtlicher Rechtsform wird zumindest in Betracht gezogen.<sup>46</sup>

Die Zertifizierungsstellen im Datenschutz dürften den Umweltgutachtern nach der VO 1221/2009/EU nachgebildet sein.<sup>47</sup> Auch diese müssen nach § 9 UAG zugelassen sein. Sie nehmen ihre Aufgaben „halbhoheitlich“ wahr,<sup>48</sup> oder in „zumindest quasi-öffentlich-rechtlicher Stellung“,<sup>49</sup> aber wohl nicht als Beliehene.<sup>50</sup>

Zu prüfen bleibt daher, ob zum Zwecke des Zertifizierungsverfahrens nach Artt. 42, 43 DS-GVO spezifisch-hoheitliche Befugnisse übertragen werden. Bei der Beleihung werden Hoheitsbefugnisse „ausgeliehen“, maßgebliches Kriterium für die Abgrenzung von privatem und öffentlichem Recht und somit der Einordnung als Beleihung ist daher die Hoheitsgewalt.<sup>51</sup> Nicht nur das „Ob“ der Beleihung, sondern auch Art und Umfang der dem Privatrechtssubjekt verliehenen Hoheitsbefugnisse müssen sich aus der gesetzlichen Regelung ergeben.<sup>52</sup> Die bloße Wahrnehmung von Aufgaben im öffentlichen Interesse genügt nicht.<sup>53</sup>

### aa) Historie und Systematik

Die frühere Datenschutzrichtlinie 95/46/EG enthielt keine Vorgaben zur datenschutzrechtlichen Zertifizierung. Die Vorabkontrolle gem. Art. 20 RL 95/46/EG<sup>54</sup> ist mit dem heutigen Konzept der Zertifizierung nicht zu vergleichen. Die Genese des Zertifizierungsverfahrens lässt sich anhand der Vorentwürfe zur DS-GVO nachvollziehen.<sup>55</sup>

Art. 39 des Kommissionsentwurfs der DS-GVO sprach die Zertifizierung zwar an, überwies Detailregelungen allerdings an die Kommission, welche per delegiertem Rechtsakt u.a. Kriterien sowie Bedingungen für die Erteilung und den Entzug der Zertifizierung festlegen sollte.

Der Parlamentsentwurf (ParLE) ging deutlich mehr in die Tiefe. Es fällt auf, dass sich die Behörde gem. Art. 39 Abs. 1 d) S. 1 ParLE akkreditierter Prüfer bedienen durfte. Die Alleinständigkeit für die Erteilung der Zertifizierung lag dennoch gem. Art. 39 Abs. 1 d) S. 4 ParLE bei der Aufsichtsbehörde. Der Schwerpunkt lag insoweit auf dem hoheitlichen Charakter.

Im Trilog hat sich diesbezüglich allerdings der Ratsentwurf (RatsE) durchgesetzt. Art. 39 Abs. 2 a) RatsE stellte Zertifizierungsstelle und Aufsichtsbehörde nebeneinander, wobei auffällt, dass die Zertifizierungsstelle an erster Stelle genannt wird.<sup>56</sup> Eine Zertifizierung sollte nach Art. 39 Abs. 2 RatsE nicht die Verantwortung des Verantwortlichen oder Auftragsverarbeiters mindern und zudem die Aufgaben und Befugnisse der Aufsichtsbehörde unberührt lassen.<sup>57</sup> Hier schimmert jeweils eine Hinwendung zur Selbstregulierung durch, welche losgelöst vom hoheitlichen Bereich wirkt. Folgerichtig wurden die Vorgaben für Zertifizierungsstellen in den neuen Art. 39a RatsE ausgegliedert.<sup>58</sup>

Gem. Art. 39a Abs. 2 litt. b und c RatsE legte die Zertifizierungsstelle im Rahmen der Akkreditierung selbst fest, welche Verfahren für die Erteilung, regelmäßige Überprüfung sowie den Widerruf greifen, bzw. welche Verfahren und Strukturen im Falle von Beschwerden oder Verletzungen der Zertifizierung umgesetzt werden.<sup>59</sup> Sofern eine Behörde zertifiziert, gelten schlichtweg die Grundsätze des Unionsverwaltungsrechts (siehe oben, Pkt. III. 1.). Wäre die Tätigkeit der Zertifizierungsstelle als hoheitliches Handeln konzipiert, hätte es der eigenständigen (und möglicherweise abweichenden) „Rechtssetzung“ im Rahmen der Akkreditierung gar nicht bedurft.

zierungsstelle als hoheitliches Handeln konzipiert, hätte es der eigenständigen (und möglicherweise abweichenden) „Rechtssetzung“ im Rahmen der Akkreditierung gar nicht bedurft.

### bb) Grundrechtsrelevanz und Reichweite der Maßnahmen

Die Erteilung, die Verweigerung und der Widerruf der Zertifizierung sowie die dem jeweiligen Zertifizierungsschema zugrunde liegenden Kriterien berühren ohne Weiteres grundrechtlich geschützten Positionen wie die Berufsfreiheit. Es stellt sich dennoch die Frage, ob die Tätigkeit der Zertifizierungsstelle wirklich auf den Eintritt unmittelbar spürbarer hoheitlicher Rechtsfolgen gerichtet ist.<sup>60</sup>

Wegen der inhärenten Freiwilligkeit kann es sich zunächst nicht um eine Marktzugangsvoraussetzung handeln.<sup>61</sup> Die Zertifizierung darf sich nicht als Vorabgenehmigungsverfahren auswirken.

Wenn die Zertifizierung dazu dient, die Einhaltung der Verordnung „nachzuweisen“, ist damit keine eigenständige Regelungswirkung im Sinne einer öffentlich-rechtlichen „Feststellung“ der Einhaltung verbunden.<sup>62</sup> Die datenschutzrechtliche Verantwortung wird ausweislich Art. 42 Abs. 4 DS-GVO gerade nicht eingeschränkt. Dies zeigt sich an weiteren Stellen im Verordnungstext: Hinsichtlich der Verantwortung des für die Verarbeitung Verantwortlichen kann eine bestehende Zertifizierung „als Gesichtspunkt herangezogen werden“ (Art. 24 Abs. 3 DS-GVO). In Bezug auf die Grundsätze privacy by design/privacy by default kann sie für den Nachweis „als Faktor herangezogen werden“ (Art. 25 Abs. 3 DS-GVO). Bei der Auftragsverarbeitung kann die Zertifizierung „als Faktor heran-

45 Horning, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 88.

46 Lepperhoff, in: Gola/Heckmann, DS-GVO/BDSG, 3. Aufl. 2022, Art. 42 Rn. 16.

47 Einhellig Raschauer, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, Art. 42 Rn. 3; Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 4; Kinast, in: Taeger/Gabel, DS-GVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 42 Rn. 78.

48 Vgl. die Website des Umweltgutachterausschusses beim Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, <https://www.emas.de/umweltgutachter-in>.

49 Schottelius, BB 1995, 1549, 1551.

50 Scherzberg, NVwZ 2006, 377, 380 f.; Lütke, NVwZ 1996, 230, 234; Höland, ZEuP 1998, 30, 44 f., a.A. Ossenbühl/Cornils, Staatshaftungsrecht, 6. Aufl. 2013, Teil 2, 17 als „moderner Fall der Beleihung privater Sachverständiger“.

51 Ronellenfitsch, in: Bader/Ronellenfitsch, BeckOK VwVfG, 58. Ed. 2020, § 1 Rn. 7; Schoch, in: Schoch/Schneider, Verwaltungsrecht, 3. EL 2022, § 1 VwVfG Rn. 162.

52 Schoch, in: Schoch/Schneider, Verwaltungsrecht, 3. EL 2022, § 1 VwVfG Rn. 164; BVerwG NVwZ 2011, 368, 370.

53 Grundlegend Terrahe, Die Beleihung als Rechtsinstitut der Staatsorganisation, 1961, S. 64 ff. Im Europäischen Datenschutzrecht unterscheidet Art. 6 Abs. 1 lit. e DS-GVO nicht zwischen Hoheitsträgern und Privatrechtssubjekten, vgl. auch Art.-29-Datenschutzgruppe, Guidelines on Data Protection Officers (DPOs) – WP 243 rev01 v. 05.04.2017, 6, online unter <https://t1p.de/tozi0>.

54 Umsetzung in § 4d Abs. 5 BDSG a.F.

55 Bayerisches Landesamt für Datenschutzaufsicht, Trilog-Synopse der DS-GVO, 2016, 420 ff.

56 So jetzt auch Art. 42 Abs. 5 S. 1 DS-GVO.

57 Jetzt Art. 42 Abs. 4 DS-GVO.

58 Jetzt Art. 43 DS-GVO.

59 Jetzt Art. 43 Abs. 2 lit. c DS-GVO.

60 Hierzu Kiefer LKRZ 2009, 441, 444 für die Feststellung der Vorschriftsmäßigkeit eines Kfz.

61 Zu Belieheneneigenschaft wegen staatlichen Erlaubnisvorbehalts für das Inverkehrbringen von Produkten vgl. BGH, NJW 1978, 2548, 2549.

62 Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 13. Ein feststellender Verwaltungsakt wird sich eher auf die Befugnis des Antragsstellers kaprizieren, das entsprechende Datenschutzzertifikat führen zu dürfen.

gezogen werden“, um hinreichende Garantien nachzuweisen (Art. 28 Abs. 3 DS-GVO). Im Hinblick auf die Sicherheit der Verarbeitung kann sie „als Faktor herangezogen werden“, um die Erfüllung der technischen Sicherheitsmaßnahmen nachzuweisen (Art. 32 Abs. 3 DS-GVO). Bei Drittstaatstransfers erspart die Zertifizierung lediglich die Genehmigung der Behörde, es müssen jedoch rechtsverbindliche und durchsetzbare Verpflichtungen des Verantwortlichen bzw. Auftragsverarbeiters im Drittland hinzutreten (Art. 46 Abs. 2 lit. f DS-GVO), und die übrige Verarbeitung muss ihrerseits rechtmäßig erfolgen. Bei der Bemessung eines Bußgelds wird die bestehende Zertifizierung neben einer erklecklichen Reihe weiterer Kriterien „gebührend berücksichtigt“ (Art. 83 Abs. 2 lit. j DS-GVO). Eine bestehende Zertifizierung besitzt demnach nur „sehr begrenzte materiellrechtliche Wirkungen“.<sup>63</sup> Sie sind mehr als Anreizwirkungen zu verstehen.

Nun begründet die Teilnahme am Zertifizierungsverfahren umfassende Mitwirkungs- und Duldungspflichten, die für einen hoheitlichen Charakter sprechen könnten. Gem. Art. 42 Abs. 6 DS-GVO stellt der Antragsteller der Zertifizierungsstelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung und gewährt ihr den erforderlichen Zugang zu seinen Verarbeitungstätigkeiten. Dies wird mitunter als Vor-Ort-Zutrittsrecht verstanden.<sup>64</sup> Verstöße hiergegen können gem. Art. 83 Abs. 4 lit. a DS-GVO sogar mit Bußgeldern geahndet werden. Gleichwohl besitzt die Zertifizierungsstelle keinerlei eigene Untersuchungsbefugnisse, die hoheitlich durchgesetzt werden könnten. Auch die Sanktionsmöglichkeit wegen Verstoßes gegen die Verpflichtungen aus Art. 42 und 43 DS-GVO steht der Aufsichtsbehörde zu und nicht der Zertifizierungsstelle. Letztlich ist es dem Zertifizierungskandidaten jederzeit möglich, sich der Mitwirkungs- und Duldungsverpflichtung durch Verzicht auf eine Zertifizierung zu entziehen.

Die Mitwirkungs- und Duldungspflichten sind daher ebenso schwach ausgeprägt, wie die materiellrechtlichen Wirkungen der Zertifizierung an sich.

### cc) Ergebnis

Die Einordnung der Zertifizierungsstelle als Beliehene sollte nicht von vornherein als abwegig abgetan werden. Gleichwohl ist bei wertender Gesamtschau unter Berücksichtigung der Stellung und der Befugnisse sowie der Rechtswirkungen der Zertifizierung festzuhalten, dass der hoheitliche Charakter ausgesprochen schwach ausgeprägt ist. Dies genügt nach hiesiger Auffassung nicht, um von einer Beleihung im Sinne des deutschen öffentlichen Rechts ausgehen zu dürfen.

## IV. Zusammenfassung und Ausblick

Die Zertifizierungsstelle nach Art. 43 Abs. 1 DS-GVO ist keine Beliehene. Sie tritt nicht als Behörde auf und ergreift keine hoheitlichen Maßnahmen. Sie arbeitet im Wesentlichen nach den gem. Art. 43 Abs. 2 litt. b, c und d DS-GVO festgelegten Verfahrensvorgaben. Insbesondere das Verfahren für die Erteilung, die regelmäßige

Überprüfung und den Widerruf der Datenschutzzertifizierung legt die Zertifizierungsstelle im Rahmen der Akkreditierung selbst fest. Die Zertifizierungsstelle verfügt nicht über nennenswerte Eingriffsbefugnisse und die Zertifizierung als solche zeitigt keine erheblichen hoheitlichen Rechtswirkungen. Das Rechtsverhältnis zwischen Antragssteller und Zertifizierungsstelle ist folglich rein privatrechtlicher Natur.

Der hiesige Ausflug ins Unionsverwaltungsrecht hat unterdessen gezeigt, dass die etwaige Beliehenenqualität von den konkreten Gegebenheiten des jeweiligen Zertifizierungsregimes abhängt. Andere Zertifizierungs- oder Konformitätsbewertungsstellen mögen abweichend zu beurteilen sein. So wird z.B. auch die Zertifizierung von qualifizierten elektronischen Signatur- bzw. Siegelerstellungseinheiten gem. Artt. 30 bzw. 39 VO 910/2014/EU (eIDAS-VO) sowohl von öffentlichen als auch privaten Stellen vorgenommen.<sup>65</sup> Die Cybersicherheitszertifizierung nach Artt. 46 ff. VO 2019/881/EU (Cyber Security Act, CSA) kennt ebenfalls ein Nebeneinander von nationaler Cybersicherheitsbehörde<sup>66</sup> und Konformitätsbewertungsstelle. Der Entwurf<sup>67</sup> des EU Artificial Intelligence Acts (AIA) sieht schließlich eine Zertifizierung von Hochrisiko-KI-Systemen vor, welche u.a. durch eine behördlich notifizierte Konformitätsbewertungsstelle vorgenommen wird.

In diesen und vergleichbaren Fallkonstellationen ist stets konkret zu prüfen, ob die Wesensmerkmale für eine Beleihung vorliegen oder nicht.<sup>68</sup>



### Prof. Dr. Lorenz Franck

ist Professor für IT-Recht an der Hochschule des Bundes für öffentliche Verwaltung in Brühl.

<sup>63</sup> Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 35.

<sup>64</sup> Lepperhoff, in: Gola/Heckmann, DS-GVO/BDSG, 3. Aufl. 2022, Art. 42 Rn. 14; Will, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 42 Rn. 40; Scholz, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 41; Hornung, in: Eßer/Kramer/von Lewinski, Auernhammer DS-GVO/BDSG, 7. Aufl. 2020, Art. 42 Rn. 64.

<sup>65</sup> BSI als öffentliche Stelle gem. § 17 Abs. 4 VdG, von BNetzA benannte private Stelle gem. § 17 Abs. 1 VdG.

<sup>66</sup> BSI gem. § 9a BSIg.

<sup>67</sup> Proposal for a Regulation of the European Parliament and of the Council laying down harmonised Rules on Artificial Intelligence (Artificial Intelligence Act, COM/2021/206 final, online unter <https://t1p.de/r4lr>.

<sup>68</sup> Vgl. § 3 Abs. 1 S. 1 und 2 ÖLG, wonach einige Aufgaben nach VO 2018/848/EU nur von beliehenen Kontrollstellen erfüllt werden dürfen, die Zertifizierung nach Art. 35 Abs. 1 S. 1 der VO 2018/848/EU aber gerade nicht dazugehört. Vgl. auch die AnerkV für Konformitätsbewertungsstellen im Bereich der elektromagnetischen Verträglichkeit, welche seit 2006 auf die Beleihung verzichtet, BT-Drs. 16/3658, 22.

Tim Wybitul

# Wie geht es weiter mit DS-GVO-Bußgeldern?

## Analyse der Schlussanträge in der EuGH-Rechtssache C-807/21\*

Datenschutzbehörden fordern bei DS-GVO-Verstößen eine verschuldensunabhängige Haftung von Unternehmen („strict liability“). Mittlerweile ist diese Frage der Unternehmenshaftung nach Art. 83 DS-GVO Gegenstand zweier Verfahren. In diesen Verfahren haben die zuständigen Generalanwälte beim EuGH bereits ihre Schlussanträge gestellt. Beide Generalanwälte sprechen sich klar gegen die von den Behörden angenommene „strict liability“ aus. Der vorliegende Überblick fasst die für Bußgeldverfahren wesentlichen Aussagen der Schlussanträge in der Rechtssache C-807/21 zusammen und bewertet sie aus Sicht der Verteidigung, für die der Verfasser das Plädoyer in der mündlichen Verhandlung vor dem EuGH gehalten hat. Zudem greift er einige wesentliche Aussagen aus dem Parallelverfahren C-683/21 auf, soweit diese die Verhängung von Bußgeldern wegen Datenschutzverstößen betreffen. Abschließend fasst der vorliegende Beitrag die möglichen Folgen der Schlussanträge für das laufende EuGH-Verfahren C-807/21 und die weitere DS-GVO-Bußgeldpraxis zusammen.

### I. Bußgelder gegen Unternehmen wegen Verstößen gegen die DS-GVO

Die von den europäischen Datenschutzbehörden verhängten Geldbußen haben mittlerweile die Milliardengrenze überschritten.<sup>1</sup> Zudem haben die Behörden bereits eine ganze Reihe von Bußgeldern in dreistelliger Millionenhöhe verhängt. Auch in Deutschland gab es bereits mehrere Geldbußen nach Art. 83 DS-GVO im zweistelligen Millionenbereich.<sup>2</sup> Gerade bei hohen Geldbußen stehen Unternehmen und nicht einzelne natürliche Personen im Fokus. Dabei ist umstritten, nach welchen Regeln Behörden Unternehmen wegen DS-GVO-Verstößen sanktionieren können.<sup>3</sup> Insbesondere muss der EuGH bei der Beantwortung der in der Rechtssache C 807/21 vom Kammergericht gestellten Vorlagefragen entscheiden, ob der Nachweis eines schuldhaften Handelns nötig ist und nach welchen Kriterien Verstöße Unternehmen zugerechnet werden.

#### 1. Verfahrensautonomie der Mitgliedstaaten

Die DS-GVO enthält kein prozessuales Bußgeldrecht.<sup>4</sup> Für die prozessuale Umsetzung der materiellrechtlichen Vorgaben der DS-GVO gilt wegen der Verfahrensautonomie der Mitgliedstaaten grundsätzlich nationales Recht.<sup>5</sup> Dabei dürfen die nationalen Regelungen die Umsetzung des Unionsrechts nicht übermäßig erschweren (Effektivitätsgrundsatz).<sup>6</sup> Zudem dürfen die nationalen Verfahrensregeln nicht ungünstiger sein, als die, die gleichartige Sachverhalte innerstaatlicher Art regeln (Äquivalenzgrundsatz).<sup>7</sup>

Auch Art. 83 Abs. 8 DS-GVO verweist bekanntlich auf die Verfahrensgarantien der Union und der Mitgliedstaaten.<sup>8</sup> Dies sind insbesondere die Justizgrundrechte in Art. 47 ff. der GRCh und als mitgliedstaatliche Regelungen in Deutschland die Vorschriften des BDSG und des OWiG.<sup>9</sup>

#### 2. Forderungen der Datenschutzbehörden nach Erleichterungen bei der Verhängung von Bußgeldern

Die Datenschutzbehörden<sup>10</sup> und Teile der Fachliteratur argumentieren, dass das deutsche Ordnungswidrigkeitenrecht nicht hinreichend wirksam sei, um die Vorgaben der DS-GVO gegenüber Unternehmen umzusetzen.<sup>11</sup> Die Konferenz der

unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 18.01.2023 eine Stellungnahme zu dem Verfahren C-807/21 veröffentlicht.<sup>12</sup> Darin fordert sie eine „Erleichterung für die Datenschutzaufsichtsbehörden“ bei der Verhängung von Geldbußen.<sup>13</sup> Die Anwendung des deutschen Rechts würde die Durchsetzung der DS-GVO erheblich

\* Hinweis: Der Verfasser verteidigt das in dem hier besprochenen Verfahren vor dem EuGH beschuldigte Unternehmen. Die hier vertretenen Auffassungen und Aussagen sind allein die des Verfassers und nicht des von ihm vertretenen Unternehmens.

1 Die irische Datenschutzbehörde DPC hat im Mai 2023 eine Geldbuße in Höhe von 1,2 Milliarden Euro verhängt, vgl. Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), abrufbar unter: [https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission\\_en](https://edpb.europa.eu/our-work-tools/consistency-findings/register-decisions/2023/decision-data-protection-commission_en) (zuletzt abgerufen am 24.05.2023).

2 Einen Überblick über entsprechende Geldbußen gibt etwa IHWas CCZ 2023, 23.

3 Vgl. hierzu nachstehend, Abschnitt I; vgl. Wybitul/König ZD 2022, 591.

4 Venn/Wybitul NStZ 2021, 204 (206); Pentzien/Haak CB 2022, 105 (107); Schwartmann/Burckhard RDV 2022, 237 (240).

5 Vgl. Art. 4 EUV sowie EuGH Urt. v. 21.01.2016, Rs. C-74/14, ECLI:EU:C:2016:42, Rn. 32 – E-turas u.a.; vgl. Nietsch/Osmanovic BB 2021, 1858 (1862).

6 Vgl. EuGH Urt. v. 21.01.2016, Rs. C-74/14, ECLI:EU:C:2016:42, Rn. 32 – E-turas u.a.

7 Vgl. EuGH Urt. v. 21.01.2016, Rs. C-74/14, ECLI:EU:C:2016:42, Rn. 32 – E-turas u.a.; vgl. auch Nietsch/Osmanovic BB 2021, 1858 (1862) mwN.

8 Art. 83 Abs. 8 DS-GVO: „Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.“

9 Vgl. etwa BeckOK DatenschutzR/Holländer, 43. Ed. 01.11.2021, DS-GVO Art. 83 Rn. 82, Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 83 Rn. 29; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 83 Rn. 56; Taeger/Gabel/Moos/Schefzig, 4. Aufl. 2022, DS-GVO Art. 83 Rn. 159 ff.

10 Vgl. zu den Positionen der Datenschutzbehörden nachstehend Fußnote 14.

11 Vgl. BeckOK Datenschutzrecht/Holländer, 40. Ed. 01.11.2021, DS-GVO Art. 83 Rn. 14.1; LG Bonn ZD 2021, 154 Rn. 32 f. mAnm von dem Bussche.

12 „Stellungnahme zu Grundsatzfragen zur Sanktionierung von Datenschutzverstößen von Unternehmen – EuGH-Rechtssache C-807/21“, nachstehend bezeichnet als „DSK-Stellungnahme“, abrufbar unter [https://www.datenschutzkonferenz-online.de/media/st/20230118\\_DSK\\_Stellungnahme\\_Datenschutzverstoesse\\_von\\_Unternehmen.pdf](https://www.datenschutzkonferenz-online.de/media/st/20230118_DSK_Stellungnahme_Datenschutzverstoesse_von_Unternehmen.pdf) (zuletzt abgerufen am 21.05.2023).

13 DSK-Stellungnahme, I.

erschweren.<sup>14</sup> Die Behörden gehen dabei davon aus, dass „im Grundsatz bereits ein dem Unternehmen zuzuordnender objektiver Pflichtenverstoß ausreicht („strict liability“).“<sup>15</sup>

Im Kern argumentiert die DSK, dass die Anwendung des deutschen Bußgeldrechts bei der Umsetzung von Art. 83 DS-GVO gegen den Wirksamkeitsgrundsatz verstoße, weil die Ermittlung der Verantwortlichkeit im Unternehmen zu aufwendig sei: „Schlimmstenfalls entstehen Sanktionslücken, weil trotz enormem Ermittlungsaufwands eine Leitungsperson, der ein Vorwurf zu machen ist, nicht ermittelt werden kann, obschon ein Verstoß des Unternehmens anhand der übrigen Beweise ansonsten zweifelsfrei feststeht.“<sup>16</sup> Dabei lässt die Stellungnahme klar erkennen, dass es den Behörden nicht allein um Fragen der Zurechnung geht, sondern um den Nachweis eines Verstoßes: „Der Nachweis ist regelmäßig mit einem erheblichen Aufwand verbunden.“<sup>17</sup>

Die DSK fordert somit Erleichterungen bei der Feststellung und der Zurechnung von Verstößen gegen die DS-GVO. Diese Forderung begründen die Behörden damit, dass das deutsche Recht eine wirksame Sanktionierung von Unternehmen nicht ermögliche.<sup>18</sup> Vor diesem Hintergrund wird die Wirkung des deutschen Bußgeldrechts bei der Sanktionierung von Unternehmen in den folgenden Abschnitten genauer untersucht.

### III. Sanktionierung von Unternehmen nach deutschem Recht

Das deutsche Recht fordert für die Sanktionierung von Unternehmen eine schuldhaft (beziehungsweise vorwerfbare) Pflichtverletzung einer Leitungsperson.<sup>19</sup> Diese Pflichtverletzung kann in einer Verletzung der Aufsichtspflichten der Unternehmensleitung nach § 130 OWiG liegen. In der Praxis ist die Verletzung von Aufsichtspflichten sogar der häufigste Fall der Sanktionierung von Unternehmen. Der wohl führende Kommentar zum deutschen Ordnungswidrigkeitenrecht formuliert dies klar: „Die Aufsichtspflichtverletzung nach § 130 ist die in der Praxis bedeutsamste Anknüpfungstat des § 30.“<sup>20</sup> Die Vorschrift des § 130 OWiG dient dabei gerade der Schließung möglicher Zurechnungslücken.<sup>21</sup> Eine vorherige oder parallele Sanktionierung der Unternehmensleitung ist hingegen keine Voraussetzung für die Verhängung einer sogenannten Verbandsgeldbuße gegen das Unternehmen. Vielmehr kann die Geldbuße gegen das Unternehmen selbstständig nach § 30 Abs. 4 OWiG festgesetzt werden.

### IV. Analyse der Positionen der DSK

Die oben zitierte Aussage der DSK, es drohen Sanktionslücken, weil eine Leitungsperson, der ein Vorwurf zu machen ist, nicht ermittelt werden könnte, obwohl ein Verstoß des Unternehmens anhand der übrigen Beweise ansonsten zweifelsfrei feststehe,<sup>22</sup> ist nachweislich falsch. Denn es ist überhaupt nicht nötig, eine einzelne Person zu ermitteln.<sup>23</sup> Vielmehr wäre die von der DSK beschriebene Fallkonstellation geradezu ein Beispielfall für ein selbstständiges Verfahren gegen das Unternehmen nach § 30 Abs. 4 OWiG. Ein selbstständiges Verfahren gegen das Unternehmen ist typischerweise gerade dann einzuleiten, „wenn die Ermittlung des Täters einer als Ordnungswidrigkeit einzustufenden Zuwiderhandlung voraussichtlich nicht oder nur mit unverhältnismäßigem Aufklärungsaufwand möglich sein wird.“<sup>24</sup> Die

genannte Aussage der DSK steht auch in klarem Widerspruch zur Rechtsprechung des BGH: „Die Verhängung einer Geldbuße gegen eine juristische Person oder Personenvereinigung hängt deshalb auch nicht davon ab, dass festgestellt wird, welcher von mehreren in Frage kommenden Verantwortlichen die Aufsichtspflicht nicht erfüllt hat. Notwendig ist allein die Feststellung, dass ein i.S.v. § 30 OWiG Verantwortlicher die Zuwiderhandlung vorwerfbar begangen hat.“<sup>25</sup>

Zudem werden die Behauptungen der mangelnden Wirksamkeit in der DSK-Stellungnahme weder empirisch noch statistisch belegt.<sup>26</sup> In der Praxis ist die Verhängung von Geldbußen gegen Unternehmen nach §§ 30, 130 OWiG keineswegs an hohe Anforderungen geknüpft. Vielmehr verhängen deutsche Behörden auf dieser Basis regelmäßig und ohne erkennbare Schwierigkeiten – teilweise auch sehr hohe – Geldbußen gegen Unternehmen.<sup>27</sup> Auch der BGH hat in seiner Rechtsprechung bislang keinerlei Zweifel an der hinreichenden Wirksamkeit der geltenden Fassung des § 130 OWiG erkennen lassen.<sup>28</sup>

Auch ein Vergleich mit der Bußgeldpraxis des Bundeskartellamts spricht gegen einen Wirksamkeitsmangel der Bußgeldverhängung nach §§ 30, 130 OWiG.<sup>29</sup> Die im Vorjahr der COVID-19 Pandemie durch das Bundeskartellamt festgesetzten Bußgelder erreichten insgesamt etwa 847,4 Mio. Euro. Davon wurden Bußgelder mit einem Volumen von 846,8 Mio. Euro auf der Grundlage von §§ 30, 130 OWiG gegen juristische Personen verhängt.<sup>30</sup> Der Vollständigkeit halber sei erwähnt, dass bei einer Sanktionierung eines Unternehmens nach §§ 30, 130 OWiG auch der konkrete Täter der für die Aufsichtspflichtverletzung nötigen Anknüpfung-

14 DSK-Stellungnahme, 1: „Die Notwendigkeit der Feststellung eines Leitungsverschuldens würde unter Verletzung des Effektivitätsgebots („effet utile“) den Vollzug des Art. 83 DS-GVO in Deutschland ansonsten erheblich erschweren.“

15 DSK-Stellungnahme, 1.

16 DSK-Stellungnahme, 15.

17 DSK-Stellungnahme, 15 f.

18 DSK-Stellungnahme, 15.

19 In § 130 Abs. 1 S.1 OWiG heißt es: „Wer als Inhaber eines [...] Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig [...]“ (Auslassungen durch den Verfasser).

20 KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 30 Rn. 92.

21 KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 130 Rn. 4.

22 Vgl. DSK-Stellungnahme, 15.

23 Vgl. Krenberger/Krumm, 7. Aufl. 2022, OWiG § 30 Rn. 10 m.w.N.

24 KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 30 Rn. 166.

25 BGH, Beschluss vom 08.02.1994 – KRB 25/93 NSTZ 1994, 346, vgl. auch Krenberger/Krumm, 7. Aufl. 2022, OWiG § 30 Rn. 10: „Die Bezugstat muss weder geahndet werden noch geahndet worden sein (Abs. 4). Auch wird die Feststellung des konkreten Täters nicht für erforderlich angesehen, sofern nur feststeht, dass die Ahndungsvoraussetzungen des § 30 für JP oder PV sämtlich vorliegen.“ So etwa auch OLG Düsseldorf GewArch 2000, 341; OLG Hamm NJW 1979, 1312; wistra 2000, 393; OLG Köln GewArch 1974, 141, 143; BayObLG NJW 1972, 1771 f.; Göhler/Gürtler Rn. 40; RRH/Förster Rn. 52; Müller, S. 89 f.; Eidam wistra 2003, 454.

26 Wybitul DSB, 2023, 75 (77).

27 Das Gesamtvolumen der von den Datenschutzbehörden verhängten Geldbußen betrug bspw. im Jahr 2021 knapp 1,3 Mrd. Euro, vgl.: <https://de.statista.com/infografik/26629/strafen-auf-grund-von-verstoessen-gegen-die-datenschutz-grundverordnung/> (zuletzt abgerufen am 24.05.2023).

28 Vgl. zur Rechtsprechung des BGH zu § 130 OWiG etwa KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 30 Rn. 88 ff.

29 Wybitul DSB, 2023, 75 (77).

30 Vgl. Bundeskartellamt, Tätigkeitsbericht 2019/2020, BT-Drs. 19/30775, 38, 41.

tat nicht ermittelt werden muss.<sup>31</sup> Diese ist lediglich eine objektive Bedingung der Ahndbarkeit nach § 130 OWiG.<sup>32</sup>

Im Ausgangsverfahren hatte auch das LG Berlin sehr klar festgestellt, dass entsprechende Feststellungen der zuständigen Behörde ohne übermäßigen Aufwand möglich gewesen wären: „Insoweit wären Ausführungen dazu möglich und notwendig gewesen, aus welchen Umständen die Behörde eine Verantwortlichkeit der Betroffenen herleiten möchte.“<sup>33</sup>

Dementsprechend hatte sich auch die Bundesrepublik Deutschland in ihrer Stellungnahme in der Rechtssache C-807/21 zur Wirksamkeit des deutschen Bußgeldrechts bei der Sanktionierung von Unternehmen sehr deutlich positioniert. Danach „ermöglicht das deutsche Recht die Verhängung wirksamer, verhältnismäßiger und abschreckender Geldbußen gegen juristische Personen oder Personenvereinigungen bei Verstößen gegen die DS-GVO.“<sup>34</sup>

Im Ergebnis spricht eine Analyse der Wirkweise des deutschen Rechts somit klar gegen die – auch empirisch nicht begründete – Wertung, dass §§ 30, 130 OWiG keine wirksame Sanktionierung von Unternehmen erlaubten. Vor diesem Hintergrund wurden die Schlussanträge des Generalanwalts zu diesen Fragen mit großer Spannung erwartet.

## II. Positionen und Wertungen des Generalanwalts in der Rechtssache C-807/21

Der Generalanwalt beim EuGH Campos Sánchez-Bordona hat am 27.04.2023 seine Schlussanträge<sup>35</sup> in diesem Verfahren gestellt. Die Schlussanträge sind für den Gerichtshof nicht verbindlich.<sup>36</sup> In der ganz überwiegenden Anzahl der Fälle folgen die Richter aber den Entscheidungsvorlagen der Generalanwälte.<sup>37</sup> Der folgende Überblick fasst die für die Praxis wichtigsten Aussagen und Wertungen der Schlussanträge zusammen.<sup>38</sup>

### 1. Unternehmen können Täter und Sanktionsadressaten des Art. 83 DS-GVO sein

Der Generalanwalt argumentiert, dass im Unionsrecht nichts dagegen spricht, ein Unternehmen „als Täterin und als Schuldnerin der verhängten Sanktion anzusehen.“<sup>39</sup> Bereits an dieser Stelle macht der Generalanwalt deutlich, dass er eine Zurechnung von festgestellten Verstößen gegenüber einem Unternehmen für möglich, für eine Sanktionierung aber auch für nötig hält.<sup>40</sup> Aus dem Wortlaut der Artt. 4, 58 und 83 DS-GVO ergebe sich „ohne Auslegungsschwierigkeiten“, dass Sanktionen wegen Verstößen gegen die DS-GVO unmittelbar gegen eine juristische Person als Täterin verhängt werden können.<sup>41</sup> Aus dem Zusammenspiel dieser Bestimmungen ergebe sich ganz selbstverständlich, dass nach der DS-GVO eine juristische Person unmittelbare Adressatin der Geldbußen wegen eines Verstoßes gegen diese Verordnung sein kann.<sup>42</sup>

Der Generalanwalt differenziert in seinen Schlussanträgen anders als das deutsche Recht nicht zwischen Tätern und Sanktionsadressaten. Er stellt lediglich klar, dass Sanktionen nach Art. 83 DS-GVO unmittelbar gegen Unternehmen und andere juristische Personen verhängt werden können.<sup>43</sup> Dies sieht aber auch das deutsche Recht vor. Auch hier kann wegen der Verletzung der DS-GVO oder sonstiger Pflichten einer juristischen Person „gegen diese eine Geldbuße festgesetzt werden.“<sup>44</sup> Die für das Aus-

gangsverfahren maßgebliche Frage, ob ein Unternehmen nicht als „Nebenbeteiligte“ i.S.d. Art. 88 DS-GVO, sondern als „Betroffene“ und damit als unmittelbare Beschuldigte eines DS-GVO-Verstoßes behandelt werden kann, lässt der Generalanwalt im Ergebnis offen. Zwar spricht er in der deutschen Sprachfassung vom Unternehmen als Täterin. Gleichzeitig macht er aber deutlich, dass dem Unternehmen die Handlungen natürlicher Personen zugerechnet werden müssen,<sup>45</sup> was eher gegen eine Einordnung als Täter im Sinne einer ordnungswidrigkeitsrechtlich Betroffenen spricht. Es steht zu hoffen, dass der EuGH hier in seinem Urteil mehr Klarheit schafft.

### 2. Keine Prüfung der Zurechnung in Konzernstrukturen

Im Zusammenhang mit der Einordnung von Unternehmen als Sanktionsadressaten des Art. 83 DS-GVO führt der General-

31 KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 130 Rn. 110: „Die Feststellung eines bestimmten Täters, der die Zuwiderhandlung begangen hat, ist allgemeiner Ansicht nach nicht notwendig (vgl. dazu nur RRH/Förster Rn. 9; Rotberg Rn. 11; Senge OWiG Rn. 24; BeckOK OWiG/Beck Rn. 89; HK-OWiG/Ziegler Rn. 58; Bohmert/Krenberger/Krumm Rn. 27).“

32 BeckOK OWiG/Beck, 38. Ed. 01.04.2023, OWiG § 130 Rn. 79: „Das Vorliegen einer Zuwiderhandlung i.S.d. Norm ist objektive Bedingung der Ahndbarkeit (BGH wistra 1982, 35; 1984, 187; 2003, 465; OLG Hamm VRS 92, 235; Krenberger/Krumm Rn. 24; Göhler/Gürtler/Thoma Rn. 17).“ So übrigens auch die Wertung der Bundesrepublik Deutschland in ihrer Stellungnahme in der Rechtssache C-807/21 v. 08.04.2022, Rn. 25: „Die Festsetzung der Verbands-geldbuße setzt nicht voraus, dass gegen die für die juristische Person oder Personenvereinigung handelnde natürliche Person ein Verfahren eingeleitet und ihr Verstoß festgestellt wird. Es ist noch nicht einmal erforderlich, dass die handelnde natürliche Person identifiziert wird. Dies gilt zum einen für Verstöße von Leitungspersonen, bei denen die handelnde natürliche Person nicht identifiziert werden muss, solange feststeht, dass irgendeine Leitungsperson der juristischen Person oder Personenvereinigung den Verstoß begangen hat. In diesen Fällen ist die Festsetzung einer sogenannten „anonymen Geldbuße“ in einem Verfahren gegen das Unternehmen möglich. Dies gilt zum anderen aber auch bei Verstößen von Nicht-Leitungspersonen im Zusammenhang mit Aufsichtspflichtverletzungen: hier muss weder die Nicht-Leitungsperson, die den Verstoß begangen hat, noch die für Aufsichtspflichtverletzung verantwortliche Leitungsperson identifiziert werden. Auch in diesen Fällen kann eine „anonyme Geldbuße“ festgesetzt werden und die Identität von Leitungsperson und Nicht-Leitungsperson offenbleiben.“

33 LG Berlin, Beschl. v. 18.02.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), im Volltext unter BeckRS 2021, 2985, Rn. 32.

34 Stellungnahme der Bundesrepublik Deutschland in der Rechtssache C-807/21 v. 08.04.2022, Rn. 23.

35 Schlussanträge des Generalanwalts Manuel Campos Sánchez-Bordona vom 27.04.2023 in der Rechtssache C-807/21, ECLI:EU:C:2023:360, (nachstehend „Schlussanträge C-807/21“).

36 EuGH Ur t. v. 11.11.2010, Rs. C-229/09, ECLI:EU:C:2010:673, Rn. 26 – Hogan Lovells/Bayer CropScience; EuGH Ur t. v. 17.03.2011, Rs. C-221/09, ECLI:EU:C:2010:673, Rn. 45 – AJD Tuna.

37 Vgl. etwa Bergmann, Handlexikon EU, 6. Auflage 2022, Generalanwalt (EuGH).

38 Soweit inhaltlich einschlägig, geht der Überblick dabei auch auf die Schlussanträge in dem Verfahren C 683/21 ein.

39 Schlussanträge C-807/21, Rn. 37.

40 Zum vorliegenden Fall bezieht der Generalanwalt sich auf die Angaben des KG im Vorlagebeschluss. Danach hatte die Behörde die streitgegenständliche Geldbuße gegen das Unternehmen „wegen einer Reihe von Verstößen gegen die DS-GVO verhängt, die dieser Gesellschaft als dem für die Datenverarbeitung Verantwortlichen zugerechnet wurden“, Schlussanträge C-807/21, Rn. 37 (Hervorhebung durch den Verfasser).

41 Schlussanträge C-807/21, Rn. 38.

42 Schlussanträge C-807/21, Rn. 39.

43 Schlussanträge C-807/21, Rn. 39.

44 § 30 Abs. 1 a.E. OWiG.

45 Schlussanträge C-807/21, Rn. 58: „In Wirklichkeit bilden und definieren jene natürlichen Personen den Willen der juristischen Person, indem sie ihm durch individuelle und konkrete Handlungen Ausdruck verleihen. Diese individuellen Handlungen als konkreter Ausdruck jenes Willens sind letztlich der juristischen Person selbst zuzurechnen.“

walt überraschenderweise auch aus, dass er das am Verfahren beteiligte Unternehmen selbst und nicht deren Konzerngesellschaften als Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO bewerte.<sup>46</sup> Fragen nach einer möglichen Zurechnung im Konzern prüft der Generalanwalt daher trotz entgegenstehenden Aussagen des vorlegenden Kammergerichts nicht.<sup>47</sup> Das Kammergericht hatte dies dagegen wie folgt formuliert: „Am 23. Juni 2017 hat die Berliner Beauftragte für den Datenschutz (im Folgenden: „Behörde“) im Rahmen einer Vor-Ort-Kontrolle das betroffene Unternehmen darauf hingewiesen, dass ihre Konzerngesellschaften personenbezogene Daten von Mietern in einem elektronischen Archivsystem speicherten, bei dem nicht nachvollzogen werden könne, ob die Speicherung erforderlich und gewährleistet sei, dass nicht mehr erforderliche Daten gelöscht würden.“<sup>48</sup> Auch die Voraussetzungen einer möglichen gemeinsamen Verantwortlichkeit haben weder das Kammergericht noch der Generalanwalt geprüft.

### 3. Keine verschuldensunabhängige Unternehmenshaftung

Die Frage einer möglichen „strict liability“ hält der Generalanwalt für die vorliegende Entscheidung (noch) nicht für maßgeblich. Vielmehr könne sie erst im Falle einer Zurückverweisung der Sache an das erstinstanzliche Gericht für dessen zukünftige Entscheidung maßgeblich werden.<sup>49</sup> Unabhängig von dieser Frage spricht sich der Generalanwalt klar gegen die Möglichkeit einer objektiven Unternehmenshaftung ohne Feststellung eines schuldhaften Verstoßes aus.<sup>50</sup> Auch in diesem Kontext spricht der Generalanwalt ein „Überwachungs- und Auswahlverschulden“ als mögliche Zurechnungsgrundlage an.<sup>51</sup> Die Beurteilung der Frage, ob die Vorgaben der DS-GVO eingehalten wurden, setze „einen komplexen Bewertungs- und Beurteilungsprozess voraus, der über die bloße Feststellung eines formalen Verstoßes hinausgeht.“<sup>52</sup>

Gegen die von den Datenschutzbehörden geforderte verschuldensunabhängige Unternehmenshaftung sprächen der Grundsatz der Verhältnismäßigkeit und der Grundsatz der Gesetzmäßigkeit der Strafen nach Art. 49 Abs. 1 GRCh und die Regelungen in Art. 83 Abs. 2 lit. b) sowie Abs. 3 DS-GVO, die Fahrlässigkeit und Vorsatz ansprechen, aber keine andere Tatbestandsverwirklichung in Form eines rein objektiven Verstoßes.<sup>53</sup> Im Interesse einer einheitlichen Geltung der DS-GVO in der EU könne einzelnen Mitgliedstaaten auch nicht gestattet werden, ein System zu regeln, das auch eine rein objektive Verantwortlichkeit umfasse.<sup>54</sup>

Im Ergebnis erteilt der Generalanwalt der Forderung der DSK nach einer verschuldensunabhängigen „strict liability“ damit eine deutliche Absage. Mit ganz ähnlichen Argumenten spricht sich auch Generalanwalt Nicholas Emiliou in der Rechtssache C-683/21 gegen eine unmittelbare Unternehmenshaftung im Rahmen von Art. 83 DS-GVO aus.<sup>55</sup> Der Wortlaut von Art. 83 Abs. 2 lit. b) und lit. k) DS-GVO lege gerade nicht nahe, dass eine Geldbuße auch beim Fehlen eines Verschuldens verhängt werden könnte.<sup>56</sup> Auch Art. 83 Abs. 3 DS-GVO setze voraus, dass ein Verstoß vorsätzlich oder fahrlässig begangen sein muss.<sup>57</sup> Zudem gelte für Geldbußen nach Art. 83 DS-GVO der Grundsatz der Gesetzmäßigkeit der Strafen nach Art. 49 Abs. 1 GRCh.<sup>58</sup> Gegen diesen Grundsatz, aber auch gegen die in Art. 83 Abs. 1 DS-GVO geforderte Verhältnismäßigkeit, würde die Annahme einer unmittelbaren

Unternehmenshaftung verstoßen.<sup>59</sup> Es wäre unverhältnismäßig, Geldbußen in Fällen zu verhängen, in denen nicht zu mindest Fahrlässigkeit nachgewiesen sei.<sup>60</sup>

Sollte der EuGH den Generalanwälten folgen, bleibt die von den Behörden propagierte „Erleichterung“<sup>61</sup> bei der Verhängung von Geldbußen nach Art. 83 DS-GVO wohl aus.

### 4. Erwägungsgrund 150 S. 3 DS-GVO betrifft nur die Festlegung des Bußgeldrahmens

Die Datenschutzbehörden und Teile der Fachliteratur bewerten Erwägungsgrund 150 S. 3 DS-GVO als umfassenden Verweis auf die Rechtsprechung des EuGH zum Wettbewerbsrecht der Union.<sup>62</sup> Er lautet: „Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff ‚Unternehmen‘ im Sinne der Artt. 101 und 102 AEUV verstanden werden.“ Aus dem Verweis auf die genannten Vorschriften des EU-Wettbewerbsrecht folge nach dieser Ansicht eine weitgehende Anwendung der Kasuistik des EuGH zu Verstößen nach Art. 23 der VO 1/2003 (Kartellverfahrensverordnung).

Der Begriff „Unternehmen“ wird in Art. 83 Abs. 4 bis Abs. 6 DS-GVO im Zusammenhang mit der Festlegung des maximalen Bußgeldrahmens verwendet. Soweit als Höchstbetrag für Sanktionen ein Prozentsatz des Vorjahresumsatzes festgelegt sei, gelte als Bezugsgröße für dessen Festsetzung nicht der Umsatz der juristischen Person, sondern der der „wirtschaftlichen Einheit“ im Sinne des EU-Wettbewerbsrechts.<sup>63</sup> Nach Art. 83 Abs. 1 DS-GVO müssten Geldbußen „wirksam, verhältnismäßig und abschreckend“ sein.<sup>64</sup> Diese Anforderungen erfüllten nach Auffassung des Generalanwalts nur

46 Schlussanträge C-807/21, Fn. 9: „Ungeachtet der in der mündlichen Verhandlung erhobenen Einwände von Deutsche Wohnen gegen ihre diesbezügliche Einstufung steht fest, dass ihr Profil der Definition des für die Verarbeitung „Verantwortlichen“ in Art. 4 DS-GVO entspricht.“

47 Schlussanträge C-807/21, Fn. 10: „Eine andere Frage ist, inwieweit bei der Festsetzung der Höhe der betreffenden Sanktion gegebenenfalls die etwaige Integration von Deutsche Wohnen und ihrer Tochtergesellschaften in eine übergeordnete wirtschaftliche Einheit zu berücksichtigen ist. Entgegen dem Anschein bestehen die klassischen Probleme der Haftungszurechnung zwischen Mutter- und Tochtergesellschaften oder innerhalb von Konzernen als solche im vorliegenden Fall nicht.“

48 KG Beschl. v. 06.12.2021 – 3 Ws 250/21, BeckRS 2021, 39748 Rn. 3 (Hervorhebung durch den Verfasser).

49 Schlussanträge C-807/21, Rn. 67.

50 Schlussanträge C-807/21, Rn. 70 ff.

51 Schlussanträge C-807/21, Rn. 77.

52 Schlussanträge C-807/21, Rn. 80.

53 Schlussanträge C-807/21, Rn. 81.

54 Schlussanträge C-807/21, Rn. 82.

55 Schlussanträge des Generalanwalts Nicholas Emiliou vom 04.05.2023 in der Rechtssache C-683/21, ECLI:EU:C:2023:376, (nachstehend „Schlussanträge C-683/21“), Rn. 55 ff.

56 Schlussanträge C-683/21, Rn. 66.

57 Schlussanträge C-683/21, Rn. 71.

58 Schlussanträge C-683/21, Rn. 74.

59 Schlussanträge C-683/21, Rn. 75.

60 Schlussanträge C-683/21, Rn. 75.

61 Vgl. DSK-Stellungnahme, 1.

62 Vgl. DSK-Stellungnahme, 9; Dannecker NZWIST 2022, 85 (94); LG Bonn ZD 2021, 154 Rn. 31 m. Anm. von dem Bussche, Spindler/Schuster/Eckhardt, 4. Aufl. 2019, DS-GVO Art. 83 Rn. 6.

63 Schlussanträge C-807/21, Rn. 46.

64 Schlussanträge C-807/21, Rn. 47.

Geldbußen, deren Höhe anhand der tatsächlichen oder materiellen Leistungsfähigkeit des Sanktionsadressaten festgesetzt würden.<sup>65</sup> Daher könnten bei der Berechnung der Sanktion materielle oder wirtschaftliche Kriterien anstelle eines rein formellen Unternehmensbegriffs zugrunde gelegt werden.<sup>66</sup> Dabei stellt der Generalanwalt unmissverständlich klar, dass sich der in Erwägungsgrund 150 S. 3 DS-GVO genannte Unternehmensbegriff ausschließlich auf die Festlegung des maximalen Bußgeldrahmens bezieht: „Die tatsächliche oder materielle Definition von „Unternehmen“, die für das Wettbewerbsrecht kennzeichnend ist, wird somit vom europäischen Gesetzgeber für die Festsetzung der Höhe der Geldbußen wegen eines Verstoßes gegen die DS-GVO herangezogen. Ich möchte jedoch wiederholen, dass die DS-GVO auf diesen Begriff nur zu diesem Zweck Bezug nimmt.“<sup>67</sup>

Der Generalanwalt setzt sich in seinen Schlussanträgen nicht mit der Frage auseinander, ob eine derart weitreichende Erweiterung des Bußgeldrahmens, wie er sie in seiner Auslegung vorschlägt, überhaupt in einem Erwägungsgrund geregelt werden kann.<sup>68</sup> Auch die Frage, ob eine solche Auslegung von Art. 83 DS-GVO nicht gegen den Grundsatz der Gesetzmäßigkeit der Strafen nach Art. 49 Abs. 1 GRCh verstößt, lässt er offen.<sup>69</sup> Jedenfalls ist zu begrüßen, mit welcher Deutlichkeit der Generalanwalt klarstellt, dass sich Erwägungsgrund 150 S. 3 DS-GVO allein auf die Festlegung des Bußgeldrahmens bezieht.

## 5. Analoge Anwendung des EU-Kartellrechts möglich

Bei unionsrechtlichen Strafen oder strafähnlichen Sanktionen gelten der Bestimmtheitsgrundsatz und das daraus folgende Analogieverbot.<sup>70</sup> Auch in der Rechtsprechung des EuGH nimmt der Bestimmtheitsgrundsatz eine zentrale Rolle ein: „Aus dem in Art. 49 I der Charta verankerten Grundsatz der Gesetzmäßigkeit im Zusammenhang mit Straftaten und Strafen, der nach der Rechtsprechung des EuGH eine besondere Ausprägung des allgemeinen Grundsatzes der Rechtssicherheit darstellt, folgt unter anderem, dass das Gesetz die Straftaten und die für sie angedrohten Strafen klar definieren muss (vgl. i.d.S. EuZW 2017, 529 Rn. 162 m.w.N. – Rosneft).“<sup>71</sup>

Dennoch hält der Generalanwalt ohne nähere Begründung oder Befassung mit Art. 49 Abs. 1 GRCh bei Sanktionen nach Art. 83 DS-GVO eine Analogie zur Rechtsprechung des EuGH zum EU-Wettbewerbsrecht für möglich: „Dies schließt nicht aus, dementsprechend die allgemeinen Grundsätze, die für Sanktionen im Wettbewerbsrecht gelten (das vom Gerichtshof bereits umfassend ausgelegt worden ist), im Bereich der Verantwortlichkeit juristischer Personen für Verstöße gegen Vorschriften zum Schutz personenbezogener Daten analog anzuwenden.“<sup>72</sup>

Diese Aussage ist zum einen deshalb überraschend, weil eine Analogie zu „den allgemeinen Grundsätzen“ einer (teilweise durchaus unklaren) Rechtsprechung zu einem anderen Rechtsgebiet im Widerspruch zu Art. 49 Abs. 1 GRCh stehen dürfte.<sup>73</sup> Zum anderen ist erstaunlich, dass der Generalanwalt diese Aussage trifft, ohne überhaupt auf den Grundsatz der Gesetzmäßigkeit der Strafen einzugehen – der inhaltlich einer der absoluten Schwerpunkte der mündlichen Verhandlung war.<sup>74</sup> Dies erstaunt auch vor dem Hintergrund, dass in der Literatur bereits ohne die Annahme einer solchen möglichen Analogie teilweise erhebliche Zweifel an der Vereinbarkeit von

Art. 83 DS-GVO mit dem Bestimmtheitsgrundsatz geäußert werden.<sup>75</sup> Denn bereits die materiellen Rechtmäßigkeitsvorschriften an die Art. 83 DS-GVO anknüpft, sind teilweise sehr vage.<sup>76</sup> Dieser Mangel an Bestimmtheit würde durch eine solche Analogie noch massiv verstärkt. Dies hatte etwa auch die Bundesrepublik Deutschland in ihrer Stellungnahme zu dem Verfahren ausgeführt: „Überdies wäre eine anderweitige Auslegung auch nicht mit der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta der Grundrechte) vereinbar. Nach Art. 49 Abs. 1 S. 1 der Charta der Grundrechte darf niemand wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach innerstaatlichem oder internationalem Recht nicht strafbar war. Dieser Grundsatz erfordert nach der Rechtsprechung des Europäischen Gerichtshofs, dass eine Unionsregelung Straftaten und die für sie angedrohten Sanktionen klar definieren muss. (...). Dieser Grundsatz gilt auch für die Bußgeldtatbestände. Art. 83 DS-GVO genügt diesem Maßstab nicht.“<sup>77</sup>

Insofern steht zu erwarten, dass der Gerichtshof in seinem anstehenden Urteil hier eine gründlichere Prüfung vornimmt und dann auch eine entsprechende – und hoffentlich ausführlichere – Begründung vorgibt.

## 6. Keine Prüfung der Wirksamkeit des deutschen Rechts

Selbst wenn man eine Anwendung der allgemeinen Grundsätze der Rechtsprechung zum Wettbewerbsrecht der Union anders als der Generalanwalt<sup>78</sup> nicht als (strafbegründende?) Analogie sondern nur als „Rückgriff“<sup>79</sup> auf diese Rechtspre-

65 Schlussanträge C-807/21, Rn. 47.

66 Schlussanträge C-807/21, Rn. 47 und 49.

67 Schlussanträge C-807/21, Rn. 47 (Hervorhebung durch den Verfasser).

68 Zudem sind Erwägungsgründe nicht rechtsverbindlich, vgl. etwa EuGH Urt. v. 19.06.2014 – C-345/13 ECLI:EU:C:2014:2013, Rn. 31 – Karen Millen Fashions Ltd.; EuGH Urt. v. 24.11.2005 C-136/04 ECLI:EU:C:2005:716, Rn. 32 Deutsches Milch-Kontor; Wybitul/König, in: ZD 2022, 591 (593) aA Jandt/Steidle, Datenschutz im Internet/Ambrock, 2018, B.VII, Rn. 49.

69 Vgl. Calliess/Ruffert/Blanke, 6. Aufl. 2022, EU-GRCharta Art. 49 Rn. 6: „Um einen Täter auf einer innerstaatlichen oder internationalen Rechtsgrundlage verurteilen zu können, muss ein hinreichend klar und bestimmt formuliertes Gesetz den Straftatbestand enthalten und eine Strafe androhen. Ein von einem Straftatbestand nicht erfasstes Verhalten darf nicht im Wege des Analogieschlusses als strafbar bewertet werden (Analogieverbot).“

70 Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, GRCh Art. 49 Rn. 25: „Unter Analogie versteht man eine Methode richterlicher Rechtsfortbildung zur Auffindung und Auffüllung von (planwidrigen und nicht schon durch Auslegung schließbaren) Regelungslücken.“

71 Vgl. etwa auch EuGH (Große Kammer), Urt. v. 08.03.2022 – C-205/20, EuZW 2022, 606 Rn. 47: „Der Grundsatz der Gesetzmäßigkeit der Straftatbestände und der Strafen besagt, dass die Gemeinschaftsvorschriften klar die Straftaten und die für sie angedrohten Strafen definieren müssen.“

72 Schlussanträge C-807/21, Rn. 50.

73 Zur Diskussion zum Gesetzlichkeitsprinzip vgl. Schwartmann/Burkhardt RDV 2022, 237 (245) m.w.N.

74 Der Verfasser dieses Beitrags hielt in der mündlichen Verhandlung das Plädoyer für die Verteidigung, ein Erfahrungsbericht findet sich unter Wybitul DSB, 2023, 75.

75 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2020, Art. 83 Rn. 45.

76 Bergt, in: Kühling/Buchner, DS-GVO BDSG, 3. Auflage 2020, Art. 83 Rn. 45.

77 Stellungnahme der Bundesrepublik Deutschland in der Rechtssache C-807/21 v. 08.04.2022, Rn. 21 f.

78 Schlussanträge C-807/21, Rn. 50.

79 Die DSK geht hingegen von einem „Rückgriff“ auf das nach der Verfahrensautonomie der Mitgliedstaaten, Art. 83 Abs. 8 DS-GVO und § 41 BDSG anwendbare deutsche Recht aus. „Es bedarf daher im Datenschutzrecht grundsätzlich keines Rückgriffs auf nationale Befugnissnormen“, DSK-Stellungnahme, 10.

chung im Wege einer Auslegung bezeichnen wollte, käme dies nur dann in Betracht, wenn das deutsche Recht keine hinreichend wirksame Anwendung von Art. 83 DS-GVO gewährleisten würde. Dementsprechend befasst sich der Generalanwalt auch recht ausführlich mit dieser Frage.<sup>80</sup> Er selbst prüft die Wirksamkeit des deutschen Bußgeldrechts bei der Sanktionierung von Unternehmen nicht. In seinen Schlussanträgen weist er zunächst darauf hin, dass das Kammergericht ausgeführt hat, dass allein ein Verstoß einer Leitungsperson einem Unternehmen zugerechnet werden könnte.<sup>81</sup> Wie bereits gezeigt, ist das falsch.<sup>82</sup>

Verstöße von Mitarbeitern unterhalb der Leitungsebene können Unternehmen ohne Weiteres nach §§ 30, 130 OWiG wegen Aufsichtspflichtverletzungen ihrer Leitungspersonen zugerechnet werden.<sup>83</sup> Dieser Widerspruch bleibt dem Generalanwalt nicht verborgen. Er weist in seinen Schlussanträgen ausdrücklich darauf hin, dass das beschuldigte Unternehmen „und die deutsche Regierung dieser Auffassung entgegen“ treten.<sup>84</sup> „Ihrer Ansicht nach ist § 30 OWiG in Verbindung mit den §§ 9 und 130 OWiG auszulegen, mit denen er ein kohärentes Sanktionssystem bilde. Nach diesem System könnten Verwaltungsanktionen gegen ein Unternehmen verhängt werden, ohne dass ein Verfahren gegen die natürliche Person eingeleitet werden müsse, die für das Unternehmen gehandelt habe.“<sup>85</sup>

Erstaunlicherweise hatte das Kammergericht es in seinem Vorlagebeschluss nicht einmal für nötig gehalten, § 130 OWiG auch nur in der Aufzählung der maßgeblichen Vorschriften des nationalen Rechts zu nennen.<sup>86</sup> Der EuGH hatte das Kammergericht daher um eine entsprechende Klarstellung zum Einfluss von § 130 OWiG gebeten.<sup>87</sup> Hierauf hatte das vorliegende Kammergericht geantwortet, dass diese Vorschrift vorliegend nicht erheblich sei.<sup>88</sup> „Zwar ermögliche diese Bestimmung neben §§ 9, 30 OWiG die Verhängung von Bußgeldern gegen Unternehmen, aber der durch § 130 OWiG erreichbare Schutz von Rechtsgütern sei gegenüber dem aus Art. 101 und 102 AEUV abgeleiteten Haftungsregime deutlich eingeschränkt.“<sup>89</sup> Worauf das Kammergericht diese rechtsvergleichende Wertung stützt, bleibt leider offen.

Wie die nachstehend dargelegten Ausführungen des Generalanwalts zur Zurechnung zeigen,<sup>90</sup> könnte auch er bei der Abfassung seiner Schlussanträge die Aussagen des Kammergerichts durchaus bezweifeln haben. Zu einer Überprüfung der Wertungen zum nationalen Recht sei dennoch allein das vorliegende Gericht des Mitgliedstaats befugt. „Der Gerichtshof hat sich an den vom vorlegenden Gericht beschriebenen nationalen rechtlichen Rahmen zu halten, denn dieses Gericht ist das zur Auslegung seines innerstaatlichen Rechts befugte Organ. Die Fragen des nationalen Gerichts zur Auslegung des Unionsrechts sind in dem rechtlichen und sachlichen Rahmen zu beantworten, den es in eigener Verantwortung festlegt und dessen Richtigkeit der Gerichtshof nicht zu prüfen hat.“<sup>91</sup>

Hierfür verweist der Generalanwalt auf die Rechtsprechung des Gerichtshofs.<sup>92</sup> Dort heißt es: „Es ist jedoch darauf hinzuweisen, dass in einem Verfahren nach Art. 267 AEUV, das auf einer klaren Aufgabentrennung zwischen den nationalen Gerichten und dem Gerichtshof beruht, allein das nationale Gericht für die Feststellung und Beurteilung des Sachverhalts des Ausgangsrechtsstreits sowie die Auslegung und Anwendung des nationalen Rechts zuständig ist [...]“.<sup>93</sup> Ob das

deutsche Ordnungswidrigkeitenrecht den unionsrechtlichen Effektivitätsgrundsatz wahrt, ist jedoch keine Frage der Auslegung des nationalen Rechts. Auch für den hier angesprochenen Vergleich der §§ 9, 30, 130 OWiG mit Artt. 101, 102 AEUV ist nicht das nationale Recht, sondern das Unionsrecht maßgeblich.<sup>94</sup> Die hierzu getroffenen Wertungen der Schlussanträge überzeugen vor diesem Hintergrund nicht.

## 7. Vorgaben zur Zurechnung von Verschulden

Falls der EuGH dem Generalanwalt in Bezug auf eine mögliche Analogie folgt, muss das Kammergericht im weiteren Verfahren die Wirksamkeit von Verbandsgeldbußen nach §§ 130, 30, 9 OWiG mit derjenigen der Rechtsprechung des EuGH zu Art. 101, 102 AEUV vergleichen. Der Generalanwalt macht hierzu in seinen Schlussanträgen Vorgaben für diesen Rechtsvergleich. Er geht davon aus, dass eine „juristische Person, die als für die Verarbeitung personenbezogener Daten Verantwortliche [...] eingestuft werden kann, [...] die Folgen – in Gestalt von Sanktionen – von Verstößen gegen die DS-GVO nicht nur tragen [muss], wenn diese von ihren Vertretern, Leitern oder Geschäftsführern begangen wurden [...]“.<sup>95</sup> Dies gelte vielmehr „auch, wenn die Verstöße von natürlichen Personen (Mitarbeitern im weiteren Sinne) begangen wurden, die im Rahmen der unternehmerischen Tätigkeit des Unternehmens und unter der Aufsicht der zuerst genannten Personen handeln.“<sup>96</sup> Der Generalanwalt setzt für die Zurechnung folgerichtig eine Aufsichtspflichtverletzung der Leitungsebene voraus. Das belegen auch seine weiteren Ausführungen. Demnach erfolgt eine Zurechenbarkeit zu der juristischen Person, „soweit der Verstoß des Mitarbeiters, der unter der Aufsicht ihrer Leitungsorgane handelt, auf einen Mangel des Kontroll- und Überwachungssystems zurückgeht, für den die Leitungsorgane unmittelbar verantwortlich sind“.<sup>97</sup>

## III. Weiteres Verfahren

Der EuGH wird vermutlich noch in diesem Jahr sein Urteil fällen. Das Kammergericht wird dann im Anschluss auf der Basis der Entscheidung des EuGH über die sofortige Beschwerde der Staatsanwaltschaft Berlin entscheiden. Wenn der Ge-

80 Vgl. Schlussanträge C-807/21, Rn. 54 ff.

81 Schlussanträge C-807/21, Rn. 31.

82 Siehe dazu vorstehend A.III.

83 Vgl. KK-OWiG/Rogall, 5. Aufl. 2018, OWiG § 130 Rn. 38.

84 Schlussanträge C-807/21, Rn. 32.

85 Schlussanträge C-807/21, Rn. 32.

86 Das KG Berlin nennt in seinem Vorlagebeschluss vom 06.12.2021 – 3 Ws 250/21, Rn. 9 lediglich §§ 9, 30 OWiG und § 41 BDSG.

87 Vgl. Schlussanträge C-807/21, Rn. 33.

88 Schlussanträge C-807/21, Rn. 33.

89 Schlussanträge C-807/21, Rn. 33.

90 Siehe dazu nachstehend unter B.VII.

91 Schlussanträge C-807/21, Rn. 35.

92 Schlussanträge C-807/21, Rn. 35 i.V.m. Fn. 7.

93 EuGH, Urt. v. 26.04.2017, Rs. C-564/15, ECLI:EU:C:2017:302, Rn. 37 – Farkas m.w.N. aus der eigenen Rechtsprechung des Gerichtshofs (Auslassungen durch den Verfasser).

94 Wybitul/Hager, MMR 2023, 321.

95 Schlussanträge C-807/21, Rn. 57 (Auslassungen durch den Verfasser).

96 Schlussanträge C-807/21, Rn. 57 (Hervorhebung durch den Verfasser).

97 Schlussanträge C-807/21, Rn. 59 (Hervorhebung durch den Verfasser).

richtshof dem Generalanwalt folgt und eine „strict liability“ ablehnt, spricht dies dafür, die Entscheidung des Landgerichts Berlin zu bestätigen.

Dieses hatte in seinem Beschluss zur Einstellung des Bußgeldverfahrens klar ausgeführt, dass der dem Verfahren zugrunde liegende Bußgeldbescheid gegen die Vorgaben von § 66 OWiG verstoße. Nach dieser Vorschrift muss die Behörde die dem Betroffenen zur Last gelegte Tat hinreichend konkretisieren. Daran fehlte es: „Der Bußgeldbescheid vom 30. Oktober 2019 erfüllt diese Abgrenzungsfunktion nicht. Der Tatvorwurf ist nicht bestimmt. Es fehlt etwa die Angabe von Tatzeit und -ort sowie des Organmitgliedes, das schuldhaft und der Betroffenen zurechenbar die Einrichtung eines den datenschutzrechtlichen Anforderungen genügenden EDV-Systems unterlassen oder aber eine rechtzeitige Löschung relevanter Daten nicht veranlasst haben soll. Der Bescheid enthält – mit Blick auf die Rechtsauffassung der Behörde konsequent – auch sonst keine Angaben zur konkreten Tathandlung selbst oder ihrer Unterlassung. Ihm lässt sich nicht entnehmen, worauf ein Vorwurf, die datenschutzrechtlichen Anforderungen seien nicht eingehalten worden, gestützt wird.“<sup>98</sup> Die Frage nach der Vereinbarkeit des § 66 OWiG hatte das Kammergericht dem EuGH nicht vorgelegt, sondern sich auf die Frage nach der „strict liability“ beschränkt. Ohne diese geforderte „Erleichterung“<sup>99</sup> in Form einer unmittelbaren Unternehmenshaftung leidet ein Bescheid, der weder konkrete Tathandlungen noch Feststellungen zu einer möglichen Aufsichtspflichtverletzung enthält, auch im Rahmen einer Analogie zum Wettbewerbsrecht der Union – in den Worten des Landgerichts Berlin –<sup>100</sup> „unter derart gravierenden Mängeln, dass er nicht Grundlage des Verfahrens sein kann.“

Wenn das Kammergericht dies anders sehen sollte, muss es die Frage der hinreichenden Wirksamkeit des deutschen

Rechts als Voraussetzung für eine mögliche Analogie unter Berücksichtigung der Positionen des Generalanwalts beziehungsweise des EuGH prüfen. Dabei geht es nicht um einen bloßen Vergleich der jeweiligen Wirksamkeit. Vielmehr wäre zu prüfen, ob die Anwendung von §§ 130, 30, 9 OWiG „die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren.“<sup>101</sup>

#### IV. Fazit

Auch mehr als fünf Jahre nach Geltung der Verordnung bleiben wesentliche Fragen der Verhängung von Bußgeldern nach Art. 83 DS-GVO ungeklärt. Der EuGH sollte die vorliegende Rechtssache C-807/21 zum Anlass nehmen, viele offene Fragen zu klären. Es wäre wünschenswert, dass er der Praxis deutlich klarere Vorgaben als bislang gibt.



#### Tim Wybitul

ist Rechtsanwalt und Partner der Sozietät Latham & Watkins LLP in Frankfurt a.M. und berät umfassend im Datenschutzrecht. Insbesondere verteidigt er Unternehmen auch in Bußgeldverfahren und sonstigen behördlichen oder gerichtlichen Verfahren im Datenschutz.

<sup>98</sup> LG Berlin Beschl. v. 18.02.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), BeckRS 2021, 2985 Rn. 32.

<sup>99</sup> Vgl. oben Fn. 13.

<sup>100</sup> Vgl. LG Berlin Beschl. v. 18.02.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), BeckRS 2021, 2985 Rn. 9.

<sup>101</sup> Vgl. etwa EuGH, Urt. v. 22.04.2021 – C-485/19, BKR 2021, 629 Rn. 52.

## KURZBEITRÄGE

# Praxisfälle zum Datenschutzrecht XXIII: Fotografieren und Anzeige von Falschparkern durch Privatpersonen

RAin Yvette Reif, LL.M.\*

### I. Sachverhalt

K lebt in München und fährt regelmäßig Fahrrad. Dabei fotografierte er mehrfach Fahrzeuge, an denen er vorbeifuhr und die verbotswidrig geparkt waren. Die Lichtbilder leitete er

anschließend, verbunden mit der Anzeige als Ordnungswidrigkeit, per E-Mail bzw. über ein entsprechendes Onlinetool an die zuständige Polizeidienststelle weiter. Auf den Lichtbildern sind Fahrzeuge, die im absoluten Halteverbot parken,

mit Kfz-Kennzeichen zu sehen. Teils stehen die Fahrzeuge auf der Straße, teils so auf einem Gehweg, dass ein Passieren auf dem Gehweg an dieser Stelle nicht mehr möglich wäre. Menschen oder Kfz-Kennzeichen anderer Fahrzeuge sind auf den Fotos nicht zu erkennen.

Die Texte der E-Mails bzw. Nachrichten über das Onlinetool enthalten ebenfalls das betroffene Kfz-Kennzeichen, außerdem Ort und Zeit der Fotoaufnahme sowie Marke und Typ des Fahrzeugs. Insgesamt handelt es sich um sechs Anzeigen durch K. Eine konkrete eigene Betroffenheit als Verkehrsteilnehmer aufgrund der Parkverstöße hat K in keiner der Nachrichten an die Polizei dargelegt. Die Anzeigen durch K gelangen der örtlich zuständigen Datenschutzaufsichtsbehörde zur Kenntnis, die diesen daraufhin nach vorheriger Anhörung aufgrund der Annahme eines Datenschutzverstößes verwarnt.

Zur Begründung führt die Behörde u.a. aus, dass das Fotografieren und Weiterleiten der Kfz-Kennzeichen eine Datenverarbeitung i.S.d. DS-GVO darstelle, für die kein Erlaubnistatbestand des Art. 6 Abs. 1 DS-GVO bestehe, insbesondere liege kein hinreichend berechtigtes Interesse i.S.d. Art. 6 Abs. 1 lit. f) DS-GVO vor. Die aus § 158 StPO folgende Befugnis für jedermann Anzeigen zu erstatten, umfasse nur die Übermittlung von Daten, die zur Einleitung von Ermittlungen benötigt würden, bei Parkverstößen also den Tatort, das Kennzeichen des Fahrzeugs sowie die Identität von Tatzeugen. Die Übermittlung von Fotos werde vom Anzeigenrecht nicht erfasst. Da K außerdem weder eine konkrete eigene Gefährdung vorgetragen noch einen allgemeinen Anspruch auf ungestörte Nutzung des Verkehrsraums habe, liege auch insoweit kein berechtigtes Interesse vor, so die Datenschutzbehörde.

Hat die Behörde K zu Recht verwarnt?<sup>1</sup>

## II. Musterlösung

### 1. Allgemeines

Damit die Datenschutzaufsichtsbehörde K zu Recht verwarnt hat, ist es zunächst erforderlich, dass diese überhaupt die Befugnis besitzt, Verwarnungen auszusprechen, ihr also diese Handlungsform im Grundsatz zur Verfügung steht. Sofern dies der Fall ist, müsste ein Verstoß gegen die DS-GVO durch K vorliegen. Fraglich ist insofern bereits, ob die DS-GVO auf Verarbeitungen des K überhaupt anwendbar ist, denn es handelt sich nicht um Verarbeitungen eines Unternehmens oder einer öffentlichen Stelle, sondern um solche einer Privatperson. Gemäß Art. 2 Abs. 2 lit. c) DS-GVO sind Datenverarbeitungen im Zusammenhang mit rein persönlichen oder familiären Tätigkeiten aber vom Anwendungsbereich der DS-GVO ausgeschlossen (sog. „Haushaltsausnahme“). Sollte die DS-GVO anwendbar sein, bleibt schließlich zu beantworten, ob die Aufsichtsbehörde die Interessen von K und diejenigen der Falschparker in einen angemessenen Ausgleich gebracht hat.

### 2. Befugnis der Behörde zur Aussprache von Verwarnungen

In Art. 58 DS-GVO sind Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse der jeweils zuständigen Datenschutzaufsichtsbehörde normiert. Zu den Abhilfebefugnissen nach Abs. 2 der Regelung gehört dabei u.a. auch, „einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat“ (lit. b). Voraussetzung der Verwarnung

durch die Aufsichtsbehörde ist, dass eine bereits begonnene Datenverarbeitung eines Verantwortlichen bzw. Auftragsverarbeiters gegen die DS-GVO verstößt. Die Verwarnung ist zu unterscheiden von der Warnung nach Art. 58 Abs. 2 lit. a) DS-GVO, die sich auf „beabsichtigte Verarbeitungsvorgänge“ bezieht, die „voraussichtlich“ gegen die DS-GVO verstoßen werden. Im Verhältnis zu anderen Befugnissen der Behörde nach Art. 58 Abs. 2 DS-GVO, insbes. den Befugnissen nach lit. d) (Anweisung hinsichtlich der Durchführung von Verarbeitungsvorgängen) bzw. lit. f) (Beschränkung oder Verbot einer Verarbeitung), handelt es sich bei der Verwarnung um eine mildere Maßnahme.<sup>2</sup> Von Anweisungen nach lit. d) und Verboten bzw. Beschränkungen nach lit. f) unterscheidet sich die Verwarnung dadurch, dass sie keine unmittelbare Rechtspflicht des Adressaten auslöst, die Verarbeitung abzustellen oder zu ändern.<sup>3</sup> Umstritten ist insofern, ob die Verwarnung einen feststellenden Verwaltungsakt darstellt.<sup>4</sup> Hierfür spricht, dass, auch wenn aus der Verwarnung keine unmittelbaren Rechtspflichten resultieren, die mit der Verwarnung verbundene Feststellung eines Rechtsverstoßes für den Adressaten belastende Wirkung hat.<sup>5</sup> So kann sie etwa im Wiederholungsfall für ein Bußgeldverfahren herangezogen werden.<sup>6</sup>

Unproblematisch ist, dass es sich bei K dem Grundsatz nach um einen Verantwortlichen i.S.v. Art. 4 Nr. 7 DS-GVO handeln kann, denn er entscheidet über die Zwecke und Mittel der Datenverarbeitung. Fraglich ist lediglich, ob dessen Handeln im Hinblick auf die Tatsache, dass er eine Privatperson ist, überhaupt in den Anwendungsbereich der DS-GVO fällt. Die Anwendbarkeit der DS-GVO soll daher im Folgenden näher geprüft werden.

### 3. Anwendbarkeit der DS-GVO auf die Datenübermittlungen durch die Privatperson K

#### a) Allgemeines

Zweifel im Hinblick auf die räumliche Anwendbarkeit der DS-GVO (Art. 3) bestehen im vorliegenden Fall nicht. Art. 2 Abs. 1 DS-GVO knüpft die Eröffnung des sachlichen Anwendungsbereichs der DS-GVO an die Verarbeitung personenbezogener Daten, soweit diese ganz oder teilweise automatisiert erfolgt (Alt. 1) oder zwar keine automatisierte Verarbeitung erfolgt, aber Daten verarbeitet werden, die in einem „Dateisystem“ gespeichert sind oder gespeichert werden sollen (Alt. 2). Was eine Verarbeitung i.S.d. DS-GVO darstellt, ist in Art. 4 Nr. 2 DS-GVO legaldefiniert. Verarbeitung i.S.d. DS-GVO ist demnach jeder mit oder ohne Hilfe auto-

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

1 Der Praxisfall inklusive Sachverhaltsdarstellung basiert auf der Entscheidung des Verwaltungsgericht (VG) Ansbach v. 02.11.2022 – verbundene Verfahren AN 14 K 22.00468 und AN 14 K 21.01431.

2 BeckOK DatenschutzR/Eichler/Matzke, 44. Ed. (01.05.2023), DS-GVO Art. 58 Rn. 20.

3 Paal/Pauly/Körffler, DS-GVO BDSG, 3. Aufl., DS-GVO Art. 58 Rn. 18; Simitis/Hor-nung/Spiecker gen. Döhmann/Polenz, Datenschutzrecht, DS-GVO Art. 58 Rn. 29.

4 Zum Streitstand vgl. bei Paal/Pauly/Körffler, DS-GVO Art. 58 Rn. 18.

5 Paal/Pauly/Körffler, a.a.O.; für das Vorliegen eines feststellenden Verwaltungsaktes auch VG Hannover, Urt. v. 27.11.2019 – 10 A 820/19; VG Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ sowie das VG Ansbach in der diesem Praxisfall zugrundeliegenden Entscheidung (vgl. Fn. 1).

6 Paal/Pauly/Körffler, a.a.O.

matisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Letztere Aufzählung ist nicht abschließend und bringt zum Ausdruck, dass schon aufgrund des Schutzzwecks der DS-GVO jeglicher Umgang mit personenbezogenen Daten eine Verarbeitung i.S.d. DS-GVO darstellt.

Art. 2 Abs. 2 DS-GVO regelt Ausnahmen von dem durch Abs. 1 vorgegebenen sachlichen Anwendungsbereich, wobei vorliegend ein Eingreifen der bereits angesprochenen sog. „Haushaltsausnahme“ nach Art. 2 Abs. 2 lit. c) DS-GVO in Betracht kommt.

#### b) Vorliegen der Anforderungen nach Art. 2 Abs. 1 DS-GVO

Bei Kfz-Kennzeichen handelt es sich um Informationen, die sich auf eine identifizierbare natürliche Person beziehen, und somit um personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO, denn es ist möglich, anhand des Kfz-Kennzeichens eine Person, den Halter, zu ermitteln und zu identifizieren, wenn auch unter Zuhilfenahme behördlicher Auskünfte.<sup>7</sup> Da die fotografierten Kfz-Kennzeichen Personenbezug aufweisen, gilt das in der Konsequenz auch für von K zusätzlich übermittelte Informationen zu Ort und Zeit der Fotoaufnahme sowie Marke und Typ des Fahrzeugs.

In den Nachrichten des K per E-Mail bzw. über das Online-tool an die zuständige Polizeidienststelle liegt eine automatisierte Verarbeitung personenbezogener Daten in Form der Datenübermittlung. Die Voraussetzungen des Art. 2 Abs. 1 Alt. 1 DS-GVO sind damit erfüllt.

#### c) Eingreifen der „Haushaltsausnahme“?

Art. 2 Abs. 2 lit. c) DS-GVO sieht eine Ausnahme von einer grundsätzlich gegebenen sachlichen Anwendbarkeit der DS-GVO gemäß Art. 2 Abs. 1 vor, sofern die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“ erfolgt. Diese als „Haushaltsausnahme“ bezeichnete Regelung verfolgt den Zweck, einen angemessenen Ausgleich zwischen den Grundrechten des Datenverarbeiters und der betroffenen Personen zu erzielen.<sup>8</sup> Sofern die Datenverarbeitung auf den Bereich persönlicher oder familiärer Tätigkeiten des Datenverarbeiters beschränkt ist, erscheinen die Risiken für die Grundrechte und Freiheiten der betroffenen Person so überschaubar, dass es vertretbar erscheint, durch Nichtanwendung der DS-GVO die private Sphäre gegen eine übermäßige Regulierung zu schützen.<sup>9</sup>

Zu beachten ist allerdings zum einen, dass das Eingreifen der Haushaltsausnahme nur zum Ausschluss der Anwendbarkeit der DS-GVO und der dort geltenden „einzelfallübergreifenden prozeduralen Vorgaben“ führt.<sup>10</sup> Personenbezogene Daten verarbeitende Privatpersonen sind in jedem Fall an die allgemeinen zivil- und strafrechtlichen Vorgaben gebunden.<sup>11</sup> Hierzu gehört insbesondere die Verpflichtung zur Achtung des allgemeinen Persönlichkeitsrechts (APR), dessen Verletzung Schadensersatzansprüche des Betroffenen

auslösen kann. Zum anderen ist die Regelung in Art. 2 Abs. 2 lit. c) DS-GVO wegen ihres Ausnahmeharakters, vor allem aber wegen des resultierenden Risikos für die Gewährleistung eines effektiven Datenschutzes eng auszulegen.<sup>12</sup>

Für die notwendige Abgrenzung zwischen rein privaten und nicht rein privaten Tätigkeiten ist ein Bündel an Kriterien maßgeblich, welches sich insbesondere an räumlichen und sozialen Gesichtspunkten sowie den Zwecken der Datenverarbeitung orientiert.<sup>13</sup> Nach dem EuGH kann eine Verarbeitung dann nicht mehr als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden, wenn sie sich auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet.<sup>14</sup>

Die von K getätigten Aufnahmen von Kfz einschließlich Kennzeichen sind von diesem sämtlich im öffentlichen Verkehrsraum erstellt worden. Die Aufnahmen wurden auch nicht nur für die persönliche Nutzung erstellt, sondern mit der Zweckbestimmung, diese an die Polizeiinspektion zur Verfolgung der darauf abgebildeten Ordnungswidrigkeiten weiterzuleiten. Folglich sind die Aufnahmen nicht ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten des Klägers verarbeitet worden und die Ausnahme nach Art. 2 Abs. 2 lit. c) DS-GVO findet keine Anwendung.<sup>15</sup>

Zwischenergebnis: Die DS-GVO ist auf den vorliegenden Sachverhalt anwendbar.

#### 4. Vorliegen einer rechtswidrigen Verarbeitung

Zu beantworten bleibt damit die Frage, ob die Datenübermittlungen durch K an die Polizei rechtswidrige Verarbeitungen darstellen und damit eine Verwarnung nach Art. 58 Abs. 2 lit. b) DS-GVO rechtfertigen oder aber die Übermittlungen durch eine entsprechende Rechtsgrundlage legitimiert sind.

Als Rechtsgrundlage für die Übermittlungen kommt nur die sog. Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f) DS-GVO in Betracht. Hiernach ist eine Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Zur diesbezüglichen Argumentation der zuständigen Datenschutzaufsichtsbehörde vgl. die Ausführungen im Sachverhalt. Das Verwaltungsgericht (VG) Ansbach hat in der diesem Praxisfall zugrunde liegenden Entscheidung jedoch die Datenübermittlungen durch K als rechtmäßig und die Verwarnung der Behörde damit als rechtswidrig angesehen.

7 VG Ansbach v. 02.11.2022 – verbundene Verfahren AN 14 K 22.00468 und AN 14 K 21.01431 m.w.N.

8 Vgl. etwa Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel, DS-GVO Art. 2 Rn. 23 m.w.N.

9 BeckOK DatenschutzR/Bäcker, 44. Ed. (01.11.2021), DS-GVO Art. 2 Rn. 12.

10 BeckOK DatenschutzR/Bäcker, 44. Ed. (01.11.2021), DS-GVO Art. 2 Rn. 12.

11 BeckOK DatenschutzR/Bäcker, 44. Ed. (01.11.2021), DS-GVO Art. 2 Rn. 12.

12 Simitis/Hornung/Spiecker gen. Döhmann/Roßnagel, DS-GVO Art. 2 Rn. 23 m.w.N.

13 BeckOK DatenschutzR/Bäcker, 44. Ed. (01.11.2021), DS-GVO Art. 2 Rn. 14.

14 EuGH, Urt. v. 11.12.2014 – C-212/13; die Entscheidung bezieht sich noch auf die Richtlinie 95/46/EG (Datenschutzrichtlinie), ist aber auf die DS-GVO übertragbar.

15 VG Ansbach v. 02.11.2022 – verbundene Verfahren AN 14 K 22.00468 und AN 14 K 21.01431.

Seine Entscheidung begründete das Gericht im Einzelnen wie folgt:

Der Begriff des berechtigten Interesses i.S.v. Art. 6 Abs. 1 S. 1 lit. f DS-GVO sei weit zu verstehen und könne rechtliche, tatsächliche, wirtschaftliche oder ideelle Interessen umfassen. Im konkreten Fall sei insofern insbes. Erwägungsgrund 50 S. 9<sup>16</sup> der DS-GVO zu berücksichtigen, so das VG Ansbach. Bei den Erwägungsgründen der DS-GVO handle es sich zwar nicht um eigenständige Rechtsnormen mit Regelungscharakter, vielmehr werde in den Erwägungsgründen nur die Zielsetzung ausgeführt, die durch den Verordnungsgeber verfolgt wurde. Die Erwägungsgründe seien insofern aber maßgeblich für die Auslegung der Regelungen der DS-GVO.

Trotz der Verortung im Zusammenhang mit der Weiterverarbeitung von Daten seien die Wertungen von Erwägungsgrund 50 S. 9 DS-GVO auch generell und nicht nur im Zusammenhang mit zweckändernden Verarbeitungen zu berücksichtigen. Auch sei unbedenklich, dass die genannte Bestimmung nur auf Straftaten abstelle und Ordnungswidrigkeiten, um dies es vorliegend aber ausschließlich geht, nicht erwähne. Anders als nach dem deutschen Verständnis seien vom unionsrechtlichen Begriff der Straftaten auch solche Tatbestände umfasst, welche eine Ordnungswidrigkeit i.S. des deutschen Rechts verwirklichen würden.

Diene die Übermittlung personenbezogener Daten an eine Polizeiinspektion dem Hinweis auf eine begangene Ordnungswidrigkeit, bestehe also grundsätzlich ein berechtigtes Interesse an der Datenverarbeitung i.S.v. Art. 6 Abs. 1 S. 1 lit. f) DS-GVO, so das VG. Eine persönliche Betroffenheit des Anzeigenerstatters durch die Verkehrsordnungswidrigkeit sei für das Vorliegen eines berechtigten Interesses nicht erforderlich. K habe folglich ein berechtigtes Interesse, Ordnungswidrigkeiten auch unter Übermittlung von Lichtbildern der Polizei anzeigen zu können. Auf die Frage, ob dieses Verständnis eine unbegrenzte Übermittlung von Daten an die Polizei ermöglicht, komme es vorliegend nicht an, so das Gericht. Jedenfalls im konkreten Fall liege angesichts der geringen Zahl an Übersendungen keine Datenverarbeitung in unbegrenztem Maße vor, sodass über die Frage eines Rechtsmissbrauchs nicht entschieden werden müsse. Ob die durch K gemeldeten Verstöße gegen ordnungsrechtliche Vorschriften tatsächlich verfolgt werden, entscheide die Polizei als Verfolgungsbehörde gemäß dem im Ordnungswidrigkeitenrecht geltenden Opportunitätsprinzip unter Ausübung ihres pflichtgemäßen Ermessens (§ 47 Abs. 1 S. 1 Ordnungswidrigkeitengesetz – OWiG).

Aufgrund des weiten Verständnisses des Begriffs des berechtigten Interesses ergebe sich ein solches im Übrigen auch aus der zumindest abstrakten Gefährdung der körperlichen Unversehrtheit des K. Diese Gefährdung erhöhe sich durch Parkverstöße, bei denen z.B. die Gehwege teilweise blockiert und dadurch verengt werden oder die Einsicht in eine Kreuzung erschwert wird.

Bzgl. der Erforderlichkeit der Datenverarbeitung zur Wahrung des berechtigten Interesses führt das VG aus, dass eine Anzeigenerstattung nur durch eine Beschreibung der Umstände nicht in gleichem Maße wie ein Bild geeignet sei, eine Ahndung des Verstoßes herbeizuführen: Ein Lichtbild gebe die tatsächlichen Umstände des Verstoßes wieder, nämlich das verbotswidrig parkende Fahrzeug samt Kennzeichen sowie die Situation, aus welcher der verantwortliche Anzei-

generstatter darauf schließt, dass eine Ordnungswidrigkeit begangen worden ist. Hierdurch werde es der Polizei im Vergleich zu einer meist durch subjektive Eindrücke geprägten Schilderung einer begangenen Ordnungswidrigkeit erleichtert, ihr Ermessen bezüglich der Verfolgung von Ordnungswidrigkeiten auszuüben.

Zugunsten der Fahrzeughalter berücksichtigte das Gericht deren Interesse, im Straßenverkehr anonym zu bleiben, sowie das Interesse, nicht aufgrund des durch K dokumentierten Verstoßes wegen der Begehung einer Ordnungswidrigkeit belangt zu werden. Im Rahmen der Abwägung kam es aber zu dem Ergebnis, dass diese Interessen die berechtigten Interessen des K nicht überwiegen bzw. die Interessen des Halters nicht schutzwürdig sind.

Zwar könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine Person vernünftigerweise nicht mit einer Verarbeitung rechnen muss (Erwägungsgrund 47 S. 4 DS-GVO). Dies sei vorliegend aber gerade nicht der Fall, da die betroffenen Personen damit rechnen müssen, dass ihre Daten zum Zwecke der Verfolgung einer Ordnungswidrigkeit verarbeitet werden.

Auch bestehe gerade kein Anspruch auf Anonymität im Straßenverkehr, vielmehr muss das Kennzeichen eines Fahrzeugs stets gut lesbar (§ 23 Abs. 1 S. 3 StVO) und mithin öffentlich zugänglich sein (vgl. BVerwG, Urt. v. 22.10.2014 – 6 C 7/13). Dass eine solche Anzeige nicht nur durch die Verfolgungsbehörden, sondern auch durch Privatpersonen erfolgen könne, zeige § 46 OWiG i.V.m. § 158 Abs. 1 StPO.

Der Eingriff in das Recht auf Schutz personenbezogener Daten durch die Übermittlung der Lichtbilder, auf denen das Kfz-Kennzeichen und die Situation des Parkverstoßes zu erkennen sind, sei schließlich als „denkbar geringfügig“ anzusehen, so die Urteilsbegründung, während dem Interesse des K, eine Ordnungswidrigkeit anzuzeigen, schon deshalb einiges Gewicht zuzusprechen sei, weil sich dieses berechnete Interesse explizit in einem Erwägungsgrund der DS-GVO wiederfindet. Daneben komme auch dem beschriebenen Interesse des K an dem Schutz der körperlichen Unversehrtheit einiges Gewicht zu. Das Interesse der betroffenen Personen, nicht aufgrund der Begehung einer Ordnungswidrigkeit belangt zu werden, müsse dagegen ebenfalls zurückstehen, da diesem ein rechtswidriges Verhalten zugrunde liege und das Interesse nicht schutzwürdig sei.

Die Abwägung der beiderseitigen Interessen ergab daher nach Auffassung des Gerichts, dass die Interessen von K als Verantwortlichem an der Datenverarbeitung diejenigen der betroffenen Fahrzeughalter überwiegen, die Voraussetzungen von Art. 6 Abs. 1 S. 1 lit. f) DS-GVO also erfüllt waren.

Ergebnis: Folgt man der dargestellten Argumentation des VG Ansbach, sind die Datenübermittlungen des K an die Polizei nicht rechtswidrig und die Verwarnung des K durch die Aufsichtsbehörde ist unzulässig erfolgt.

<sup>16</sup> Erwägungsgrund 50 S. 9 DS-GVO hat folgenden Inhalt: „Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten.“

# Erstattung von Rechtsanwaltskosten im kirchengerichtlichen Datenschutzverfahren

Robert Gmeiner\*

## I. Einleitung

Eine Erstattung von Rechtsanwaltskosten für das kirchengerichtliche Datenschutzverfahren der katholischen Kirche sieht das Prozessrecht nur vor, sofern ein materiell-rechtlicher Anspruch besteht, § 16 S. 2 KDSGO. In seiner bisherigen Rechtsprechungspraxis lehnte das Interdiözesane Datenschutzgericht eine Erstattung der notwendigen Rechtsverfolgungskosten, insbesondere für die Mandatierung eines Rechtsanwalts, auch im Falle des Obsiegens des Antragstellers ab. Materiell-rechtliche Anspruchsgrundlagen seien nicht ersichtlich.<sup>1</sup> Das zweitinstanzliche Datenschutzgericht der Deutschen Bischofskonferenz bestätigte jüngst diese Ansicht: „Angesichts der ausdrücklichen eigenständigen Normierung in § 16 KDSGO scheidet eine Anwendung von Kostenträgungsgrundsätzen des staatlichen Rechts für diese Frage aus.“<sup>2</sup> Dies führt zu der Frage, aufgrund welcher materiell-rechtlicher Vorschriften eine Erstattung von Anwaltskosten möglich ist.

## II. Materiell-rechtliche Ansprüche

§ 16 S. 2 KDSGO setzt für eine Auslagenerstattung eine materiell-rechtliche Grundlage voraus. Sie kann sich aus Vertrag, Verzug, positiver Vertragsverletzung, culpa in contrahendo, Geschäftsführung ohne Auftrag oder Delikt ergeben.<sup>3</sup> Nachfolgend interessieren lediglich Ansprüche aus dem Kirchenrecht (§ 50 Abs. 1 KDG, c. 128 CIC) und aus Delikt (§ 839 Abs. 1 BGB).

### 1. Anspruch aus § 50 Abs. 1 KDG

Nach § 50 Abs. 1 KDG hat jede Person, der wegen eines Verstoßes gegen das kirchliche Datenschutzrecht ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen die kirchliche Stelle als Verantwortliche oder Auftragsverarbeiter. Sie sind nach § 7 Abs. 1 KDSGO am gerichtlichen Verfahren beteiligt.

Stellt eines der beiden kirchlichen Datenschutzgerichte fest, dass eine Datenschutzverletzung durch die kirchliche Stelle stattgefunden hat, so liegt der tatbestandlich erforderliche und rechtswidrige KDG-Verstoß vor. Abgesehen vom Mitverschulden (§ 50 Abs. 7 KDG i.V.m. § 254 BGB) enthält das Gesetz aber keine Vorgaben über den Umfang des Schadenersatzes. Wie bereits in § 50 Abs. 7 KDG angedeutet, bietet es sich an, den Umfang des Schadenersatzes anhand des staatlichen Rechts (§§ 249 ff. BGB) zu bestimmen. Danach hat der Schädiger gem. § 249 Abs. 1 BGB den Zustand wiederherzustellen, der ohne das schädigende Ereignis bestünde, wobei nach § 249 Abs. 2 S. 1 BGB auch die Herstellungskosten verlangt werden können. Zu diesem erstattungsfähigen Schaden zählen unstreitig auch erforderliche und zweckmäßige Rechtsverfolgungskosten.<sup>4</sup> Keiner Hinzuziehung eines Rechtsanwalts bedarf es hingegen, wenn es sich um einfache Fälle handelt, die der Geschädigte selbst regeln kann.<sup>5</sup>

Ob die Beauftragung eines Rechtsanwalts erforderlich und zweckmäßig ist, ist eine vom Anspruchsteller darzulegende Tatsache.<sup>6</sup> Zwar kann man nicht pauschal die Erforderlichkeit und Zweckmäßigkeit der Hinzuziehung eines Anwalts bejahen. Gerade im Datenschutzrecht wird man es in den meisten Fällen annehmen müssen. So enthält es zum einen zahlreiche unbestimmte und ausfüllungsbedürftiger Rechtsbegriffe, wie Wahrnehmung kirchlicher Interessen in § 6 Abs. 1 lit. f) KDG, die Wahrung erheblicher Belange des Gemeinwohls in § 6 Abs. 2 lit. f) KDG und die Glaubwürdigkeit der Kirche in § 6 Abs. 2 lit. j) KDG. Zudem erfordert das Datenschutzrecht einzelfallbezogene Interessenabwägungen, wie berechtigten Interessen des Verantwortlichen im Verhältnis zu den Interessen der betroffenen Person nach § 6 Abs. 1 lit. g) KDG oder die Abwehr schwerwiegende Beeinträchtigungen der Rechte eines Dritten, lit. h), § 17 Abs. 4 KDG.<sup>7</sup> Zudem ist selbst im Fall einer Rechtsverletzung zu prüfen, ob die verletzte Norm drittschützenden Charakter hat.<sup>8</sup> Teilweise spielen auch allgemeine verfassungs- und kirchenrechtliche Erwägungen eine entscheidungserhebliche Rolle.<sup>9</sup> Hinzu kommt, dass das Prozessrecht nur fragmentarisch geregelt ist und keine (ausdrücklichen) normativen Vorgaben für die Lückenschließung bereithält.<sup>10</sup>

Stellt ein kirchliches Datenschutzgericht eine Datenschutzverletzung fest, so kann grundsätzlich davon ausgegangen werden, dass die erforderlichen und zweckmäßigen Rechtsanwaltskosten gem. § 50 Abs. 1 KDG vom Antragsgegner zu erstatten ist.

### 2. Deliktsrecht

Neben dem Schadenersatzanspruch aus § 50 Abs. 1 KDG kommt auch ein Schadenersatzanspruch aus § 839 Abs. 1 BGB in Be-

\* Der Autor ist Rechtsreferendar am LG Ellwangen (Jagst) und wissenschaftliche Hilfskraft am Lehrstuhl für Öffentliches Recht, Finanz- und Steuerrecht (Prof. Dr. Hellermann) an der Universität Bielefeld.

1 IDSG, Beschl. v. 14.12.2020 – IDSG 01/2020, Rn. 55; Beschl. v. 02.02.2021 – IDSG 09/2020, Rn. 64; Beschl. v. 01.03.2021 – IDSG 27/2020, Rn. 54; Beschl. v. 19.04.2021 – IDSG 14/2020, Rn. 59; Beschl. v. 29.11.2021 – IDSG 04/2019, Rn. 50; Beschl. v. 09.12.2021 – IDSG 03/2020, Rn. 78; Beschl. v. 25.04.2022 – IDSG 10/2021, Rn. 72; Beschl. v. 24.05.2022 – IDSG 01/2021, Rn. 45.

2 DSG-DBK, Beschl. v. 08.02.2023 – DSG-DBK 02/2022, Rn. 117, zu beachten jedoch auch Rn. 60.

3 Vgl. BGHR BGB § 280 Abs. 3 Kostenerstattungsanspruch 1 Rn. 7 = BGHR BGB § 823 Kostenerstattungsanspruch 1 Rn. 7 = JurBüro 2007, 249 (250); Hergert, in: Zöller, ZPO, 34. Aufl. 2022, Vor § 91 Rn. 11 m.w.N.

4 BGHZ 127, 348 (350); BGHR BGB § 249 Abs. 2 S. 1 Rechtsverfolgungskosten 3 Rn. 21 = NJW 2020, 144 (146 f.); BGHR BGB § 249 Rechtsverfolgungskosten 10 Rn. 10 = NJW 2021, 243 f.

5 BGHZ 127, 348 (352); BGHR BGB § 249 Abs. 2 Rechtsverfolgungskosten 3 Rn. 21 = NJW 2020, 144 (147).

6 BGHR BGB § 249 Rechtsverfolgungskosten 10 Rn. 10 = NJW 2021, 243 (244).

7 So zum Beispiel im Verfahren IDSG, Beschl. v. 25.02.2022 – IDSG 23/2020, Rn. 20–22.

8 DSG-DBK, Beschl. v. 03.01.2023 – DSG-DBK 04/2022, Rn. 15, 22.

9 So zum Beispiel im Verfahren IDSG, Beschl. v. 09.12.2020 – IDSG 05/2019, Rn. 38, 40.

10 DSG-DBK, Beschl. v. 08.02.2023 – DSG-DBK 02/2022, Rn. 60.

tracht. Jedenfalls in der Rechtsprechung ist anerkannt, dass öffentlich-rechtliche Religionsgemeinschaften – wie die römisch-katholische Kirche – ein öffentliches Amt i.S.v. Art. 34 S. 1 GG ausüben können.<sup>11</sup> Ist dies der Fall, setzt der Schadenersatzanspruch voraus, dass der Beamte im haftungsrechtlichen Sinn die ihm einem Dritten gegenüber obliegende Amtspflicht verletzt.

Zunächst muss der Beamte seine Amtsgeschäfte im Einklang mit dem objektiven Recht führen.<sup>12</sup> Verstößt ein Beamter gegen Bestimmungen des Datenschutzrechts, steht die Entscheidung nicht im Einklang mit der objektiven Rechtsordnung und stellt somit eine Amtspflichtverletzung dar. Eine Gesetzesverletzung reicht jedoch noch nicht aus. Erforderlich ist, dass eine drittgerichtete Amtspflicht verletzt wurde. Dies ist der Fall, wenn die Amtspflicht einen individualisierten Schutz gewährleistet.<sup>13</sup> Da das Datenschutzrecht eine Ausprägung des allgemeinen Persönlichkeitsrechts darstellt,<sup>14</sup> sind (materielle) datenschutzrechtliche Vorgaben drittgerichtete Amtspflichten.

Die Rechtsfolge des Schadenersatzanspruchs ergibt sich ebenfalls aus § 249 Abs. 2 S. 1 BGB. Insoweit kann auf die obigen Ausführungen verwiesen werden.

### 3. Allgemeiner kirchenrechtlicher Schadenersatzanspruch

Das Kirchenrecht enthält in c. 128 CIC einen eigenständigen Schadenersatzanspruch. Danach ist zur Schadenswiedergutmachung verpflichtet, wer einen anderen durch einen unrechtmäßigen Rechtsakt vorsätzlich oder fahrlässig einen Schaden zufügt.<sup>15</sup> Da es sich bei dem Schadenersatzanspruch aus c. 128 CIC um ein naturrechtliches Prinzip handelt, kommt es auf Seiten der Geschädigten nicht darauf an, ob es sich um Kirchenmitglieder, sonstige Christen oder Ungetaufte handelt.<sup>16</sup>

Zu den Rechtsakten, die einen Schadenersatzanspruch auslösen können, zählen auch Rechtsakte kirchlicher Autoritäten,<sup>17</sup> die gegen geltendes Recht verstoßen.<sup>18</sup> Verstöße gegen datenschutzrechtliche Bestimmungen stellen in jedem Fall Verletzungen des geltenden Rechts dar.

Die Wiedergutmachungspflicht aus c. 128 CIC erfasst jedenfalls auch den Ausgleich finanzieller Schäden.<sup>19</sup> Nach den obigen Ausführungen können Rechtsanwaltskosten einen erstattungsfähigen Schaden darstellen. Zwar ist der staatliche § 249 Abs. 2 BGB nicht Maßstab für den universalkirchlichen c. 128 CIC. Jedoch ergeben sich gem. c. 1649 § 1, 4 CIC wertungsmäßig keine Unterschiede.

### 4. Verschulden

Voraussetzungen für alle drei Anspruchsgrundlagen ist ein Verschulden des Handelnden.<sup>20</sup> Erforderlich ist nach § 276 Abs. 1 BGB grundsätzlich Vorsatz oder Fahrlässigkeit. Zum staatshaftungsrechtlichen Anspruch aus § 839 Abs. 1 BGB ist anerkannt, dass eine rechtsfehlerhafte, aber vertretbare, Rechtsanwendung dann nicht schuldhaft ist, wenn der Beamte im haftungsrechtlichen Sinn die Rechtslage sorgfältig und gewissenhaft prüft.<sup>21</sup> Ist dies der Fall, scheidet eine Amtshaftung aus. Nichts anderes dürfte zunächst für Schadenersatzansprüche aus § 50 Abs. 1 KDG und c. 128 CIC gelten.

Fraglich ist jedoch, ob dies mit dem Unionsrecht vereinbar ist. Nach Art. 91 Abs. 1 DS-GVO müssen Regeln zum Schutz natürlicher Personen mit denjenigen der DS-GVO im Einklang stehen. Zwar steht das Recht auf effektiven Rechtsschutz in Art. 78, 79 DS-GVO einer Kostentragungspflicht für den Fall

des Unterliegens nicht entgegen.<sup>22</sup> Allerdings ist es mit dem grundgesetzlichen Rechtsstaatsprinzip, welches nach Art. 23 Abs. 1 S. 3 GG durch das Unionsrecht nicht überlagert werden darf, unvereinbar, wenn unbemittelten Personen der Zugang zu Gericht im Verhältnis zu bemittelten Personen erschwert wird.<sup>23</sup> Der Zugang zu Gericht darf nicht davon abhängig sein, ob der Rechtsschutzsuchende sich die Hinzuziehung eines Anwalts leisten kann.<sup>24</sup> Dabei macht es keinen Unterschied, ob vor dem Gericht Anwaltszwang besteht oder nicht.<sup>25</sup>

Für das Unionsrecht dürfte nichts anderes gelten. Denn für das geistige Eigentum hat der EuGH anerkannt, dass ein fehlender Kostenerstattungsanspruch im Obsiegens-Fall einen Geschädigten davon abhalten könnte, seine Rechte gerichtlich geltend zu machen.<sup>26</sup> Dabei dürfte es sich hierbei nicht nur um eine Sonderrechtsprechung des IP-Rechts handeln, sondern um einen allgemeinen Grundsatz des Unionsrechts, Art. 6 Abs. 3 EUV. So hat der EGMR ebenfalls entschieden, dass ein unangemessenes Prozesskostenrisiko mit Art. 6 Abs. 1 EMRK unvereinbar ist.<sup>27</sup>

Das kirchliche Datenschutzprozessrecht sieht in § 16 S. 2 KDSGO keinen allgemeinen Kostenerstattungsanspruch für eine obsiegende Partei vor, sondern nur für den Fall, dass über das Obsiegen hinaus ein materieller Erstattungsanspruch besteht. Für den Fall der Beauftragung eines Rechtsanwalts fehlt für unbemittelte Personen jedoch die Möglichkeit, Prozesskostenhilfe bewilligt zu bekommen und sich einen Rechtsanwalt beordnen zu lassen.<sup>28</sup> Dies führt nach dem derzeitigen (formellen) Prozessrecht dazu, dass ein Antragsteller stets die Kosten eines Rechtsanwalts tragen muss. Dies gilt auch dann, wenn das Gericht zwar einen Datenschutzverstoß feststellt, der beteiligte Verantwortliche bzw. Datenverarbeiter aber vorträgt, sich mit der Rechtslage gewissenhaft ausei-

11 BGHZ 22, 383 (388) = KirchE 3, 430 (433 f.); BGHZ 154, 54 (57 f.) = KirchE 43, 105 (107 f.); BGH, VersR 1961, 437; a.A. OLG Düsseldorf, KirchE 38, 425 (430) = NVwZ 2001, 1449 (1450) mit unzutreffendem Verweis auf BGHSt 37, 191 (192 f.) = KirchE 28, 241 (242), da der BGH den Amtsträgerbegriff des § 11 Abs. 1 Nr. 2 StGB und nicht § 839 Abs. 1 BGB, Art. 34 GG zum Gegenstand hatte.

12 Sprau, in: Grüneberg (Hrsg.), BGB, 82. Aufl. 2023, § 839 Rn. 32.

13 BGHZ 223, 72 (84 f.) m.w.N.

14 DSG-DBK, Beschl. v. 03.01.2023 – DSG-DBK 04/2022, Rn. 19; Sydow, in: ders. (Hrsg.), Kirchliches Datenschutzrecht, 2021, § 1 Rn. 5 f.

15 Quicumque illegitime actu iuridico, immo quovis alio actu dolo vel culpa posito, alteri damnum infert, obligatione tenetur damnum illatum reparandi.

16 Pree, in: Lüdicke (Hrsg.), Münsterischer Kommentar zum Codex Iuris Canonici, Stand: 29. Erg.-Lfg. 1998, c. 128 Rn. 2 i.V.m. Rn. 3.

17 Pree (Fn. 16), c. 128 Rn. 2 f.

18 Pree (Fn. 16), c. 128 Rn. 7.

19 Pree (Fn. 16), c. 128 Rn. 10.

20 Für § 50 KDG: Herrlein, in: Sydow (Hrsg.), Kirchliches Datenschutzrecht, 2021, § 50 Rn. 17; für c. 128 CIC: Pree (Fn. 16), c. 128 Rn. 2.

21 BGHZ 119, 365 (369); 223, 72 (88); BGHR BGB § 839 Abs. 1 S. 1 Verschulden 47 Rn. 16; jüngst: BGH, Urt. v. 19.01.2023 – III ZR 234/21, Rn. 31 (juris).

22 Schaffland/Holthaus, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Stand: Lfg. 7/20, DS-GVO Art. 78 Rn. 14; Bergmann/Möhrlé/Herb, Datenschutzrecht, Stand: 56. Erg.-Lfg. 2018, DS-GVO Art. 78 Rn. 54.

23 BVerfGE 81, 347 (358); BVerfGK 1, 111 (114); 20, 187 (192); jüngst: BVerfG (K), Beschl. v. 27.12.2022 – 1 BvR 1791/22, Rn. 16 (juris).

24 BVerfGE 1, 109 (111).

25 BVerfGE 85, 337 (348).

26 EuGH, Urt. v. 16.07.2015 – C-681/13 (Diageo Brands), Rn. 77; Urt. v. 28.04.2022 – C-531/20 (NovaText), Rn. 37.

27 EGMR, Urt. v. 19.06.2001 – 28249/95 (Kreuz), § 66.

28 Zur ungeschriebenen Prozesskostenhilfe: BVerfGE 1, 109 (110 f.).

nandergesetzt zu haben. Insbesondere unbemittelte Personen können aufgrund der allgemeinen Kostenpflicht daher davon abgehalten werden, durch die Hinzuziehung eines Rechtsanwalts ihre Rechte wahrzunehmen. Der strenge Verschuldensmaßstab des § 839 Abs. 1 BGB für eine fehlerhafte Gesetzesanwendung kann daher nicht für das datenschutzrechtliche Verfahren übernommen werden.

### III. Fazit

Obsiegt eine Partei vor dem Interdiözesanen Datenschutzgericht bzw. dem Datenschutzgericht der Deut-

schen Bischofskonferenz, so sind ihm die Kosten für einen Rechtsanwalt aus § 50 Abs. 1 KDG, § 839 Abs. 1 BGB, c. 128 CIC zu erstatten. Der allgemeine staatshaftungsrechtliche Verschuldensmaßstab des § 839 Abs. 1 BGB für eine fehlerhafte Gesetzesanwendung kann dabei nicht maßgeblich sein. Andernfalls würden unbemittelte Rechtsschutzsuchende mangels eines anderweitigen Kostenerstattungsanspruch unangemessen benachteiligt.

## Die Anonymisierung im Kontext von Krisenresilienzplattformen

Sakyi Mannah\*

### I. Einleitung

Eine komplexe und dynamische Umwelt im weiteren Sinne bietet immer weniger Reaktionszeit und nur eingeschränkt Raum für eine Lösung zur Bewältigung einer Krise. Wie sich durch den Konflikt in der Ukraine oder andere Krisen in der Vergangenheit zeigt, werden von Unternehmen in solchen Situationen immer wieder angemessene und wirksame Reaktionen auf relevante Umweltveränderungen erwartet.

Genau dieses Problem der komplexen wirtschaftlichen Herausforderungen in Krisensituationen wird durch sog. Krisenresilienzplattformen angegangen. Ein Projekt, welches dieses Thema mittels einer KI basierten Plattform zur Integration, Strukturierung, Vernetzung, Analyse und Bewertung von Daten (aus wirtschaftlichen Wertschöpfungsnetzen sowie dem Branchenumfeld und gesellschaftlichem Kontext) adressiert, ist das vom Bundesministerium für Wirtschaft und Klimaschutz geförderte Projekt CoyPu (Cognitive Economy Intelligence Plattform für die Resilienz wirtschaftlicher Ökosysteme).<sup>1</sup> Um eine möglichst genaue Analyse durchzuführen, werden mithilfe solcher Plattformen, ganz- und/oder teilautomatisiert, große Mengen an personen- und nichtpersonenbezogenen Informationen aus unterschiedlichen Datenquellen verarbeitet.

Die Verarbeitung personenbezogener Daten untersteht hierbei den Vorschriften der Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO).<sup>2</sup> Ziel und Zweck der DS-GVO ist gemäß Art. 1 Abs. 1 DS-GVO der Schutz natürlicher Personen bei der Verarbeitung ihrer Daten und der freie Verkehr solcher Daten. Eine Methode, welche i.d.R. zur Erreichung dieses Schutzzweckes genutzt wird, ist die Anonymisierung personenbezogener Daten. Diese stellt bislang für Unternehmen eine attraktive Methode zur Datenverarbeitung dar. Allerdings besteht nach wie vor Uneinigkeit darüber, was unter

einer „korrekten“ Anonymisierung zu verstehen ist. Diese Uneinigkeit stellt nicht nur für datenverarbeitende Unternehmen, sondern auch für beaufsichtigende Datenschutzbehörden eine große Herausforderung im Bereich der Datenverarbeitung dar. Vor diesem Hintergrund werden im Folgenden der Begriff der Anonymisierung und mit Blick auf die Anforderungen der DS-GVO die Begriffe der Nicht- und Re-Identifizierung thematisiert. Zwar wäre es naheliegend anzunehmen, dass das Konzept der Re-Identifizierung bei einer Anonymisierung, mangels Identifizierbarkeit einzelner Personen, ausgeschlossen wäre. Mit Blick auf die immer schneller wachsende und komplexer werdende Informationstechnologie wird jedoch deutlich, dass aufgrund des derzeitigen technischen Standes die Wahrscheinlichkeit einer Re-Identifizierung bei anonymen Daten nicht ganz ausgeschlossen werden könnte. Im Rahmen der Anforderungen an anonymisierte Daten wird deshalb weiter kontextualisiert auf die grundlegende Architektur der Krisenresilienzplattformen Bezug genommen. Des Weiteren wird eine Studie zum Erfolg von Re-Identifizierungen in unvollständigen Datensätzen unter Verwendung eines generativen Modells beleuchtet.

\* Der Autor ist Wissenschaftlicher Mitarbeiter des Selbstregulierung Informationswirtschaft e.V.

<sup>1</sup> <https://coypu.org>.

<sup>2</sup> Art. 2 Abs. 1 DS-GVO: Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

## II. Begriff der Anonymisierung

### 1. Was ist unter einer Anonymisierung zu verstehen?

Der Begriff der Anonymisierung ist anders als der Begriff der Pseudonymisierung in Art. 4 Nr. 5 DS-GVO nicht legaldefiniert. Auch im Bundesdatenschutzgesetz (BDSG), welches die DS-GVO auf nationaler Ebene ergänzt und präzisiert, findet sich eine solche Definition nicht, wobei an dieser Stelle klarzustellen ist, dass die DS-GVO mangels entsprechender Öffnungsklausel konkretisierende Definitionen wie z.B. des Begriffs der Anonymisierung nicht ausdrücklich gestattet. Ausdrücklich wird die Anonymisierung lediglich in den Erwägungsgründen<sup>3</sup> der DS-GVO in Abgrenzung zur Pseudonymisierung genannt. Demnach sollen die Vorschriften der DS-GVO nicht für anonyme Informationen, d.h. Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, gelten. Dies gelte auch, wenn anonyme Daten für statistische oder für Forschungszwecke verarbeitet werden.<sup>4</sup> Dass bereits anonyme Daten nicht vom Geltungsbereich der DS-GVO erfasst sind, überrascht nicht. Vielmehr verdeutlicht das bereits den im Art. 1 Abs. 1 DS-GVO verankerten Rechtsgedanken. Die Vorschriften der DS-GVO finden lediglich Anwendung auf die Verarbeitungen von Informationen identifizierter oder identifizierbarer Personen.<sup>5</sup> Das Merkmal der Nichtidentifizierbarkeit einzelner natürlicher Personen ist, anders als bei pseudonymisierten Daten, gerade charakteristisch für bereits anonymisierte Daten.

Historisch gesehen befand sich, anders als in der DS-GVO und der aktuellen Fassung des BDSG, im § 3 Abs. 6 BDSG a.F. eine allgemeine Definition der Anonymisierung als Form einer Verarbeitung. Demnach sei unter der Anonymisierung das Verändern personenbezogener Daten derart zu verstehen, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden könnten. Der Aspekt der De-Identifizierung von personenbezogenen Informationen – ein Prozess bei dem Informationen, die zur Identifizierung einer Person verwendet werden könnten, entfernt werden<sup>6</sup> – spielt mithin eine sehr wichtige Rolle bei der Einordnung eines Datenverarbeitungsvorgangs als Anonymisierungsprozess.

### 2. Nichtidentifizierbarkeit der Daten

Im Kontrast zum Aspekt der De-Identifizierung von personenbezogenen Daten spielt im Kontext anonymisierter Daten auch der Aspekt der Nichtidentifizierbarkeit eine entscheidende Rolle. Noch recht unklar ist, ob die DS-GVO zumindest abstrakt Anforderungen an die Nichtidentifizierbarkeit anonymisierter Daten stellt, und mithin inhärent bereits eine absolute Anonymisierung ausschließen würde. Eine Antwort betreffend diese Frage könnte sich zunächst aus den Erwägungsgründen der DS-GVO ergeben.

Gemäß den Erwägungsgründen der DS-GVO sollten zur Feststellung einer Identifizierbarkeit einer Person alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine einzelne Person direkt oder indirekt zu identifizieren.<sup>7</sup> Die Identifizierbarkeit einer von der Verarbei-

tung betroffenen Person hänge demnach zum einen davon ab, mit welchen Mitteln oder Informationen eine betroffene Person identifiziert werden könnte. Zum anderen hänge sie davon ab, wie wahrscheinlich es wäre, dass diese Mittel oder Informationen tatsächlich zur Identifizierung genutzt werden würden. Darüber hinaus sollten, entsprechend den Erwägungsgründen der DS-GVO, alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, zur Berücksichtigung der Identifizierbarkeit herangezogen werden.<sup>8</sup> Ebenfalls maßgebend hierfür seien die zum Zeitpunkt der Verarbeitung verfügbaren Technologien und technischen Innovationen.<sup>9</sup>

Auf den ersten Blick scheinen sich die dort beschriebenen Anforderungen im Kontext der vorherigen Sätze des Erwägungsgrundes 26 vielmehr auf die Pseudonymisierung zu beziehen. Anonymisierte Daten werden erstmals im S. 5 des Erwägungsgrundes, wenn auch nur im Kontext der Rechtsfolgen, beschrieben.

Dies hätte zur Folge, dass eine direkte Anwendung dieser Anforderungen auf die Anonymisierung zunächst erst einmal nicht in Betracht käme. Entsprechende Anforderungen betreffend die Anonymisierung und wann eine solche nach der DS-GVO als solche anzunehmen wäre, würden ergo in den Erwägungsgründen nicht ausdrücklich erwähnt. Es stellt sich mithin die Frage, ob die in den Erwägungsgründen der DS-GVO befindlichen Anforderungen an die Identifizierbarkeit bei der Pseudonymisierung ebenfalls Anwendung auf die Anonymisierung finden. Von großer Tragweite ist hierbei auch die Frage der Wahrscheinlichkeit einer Re-Identifizierung einzelner Personen anhand anonymer Datensätze. Ein Blick auf die Datenverarbeitung mittels KI-basierter Krisenresilienzplattformen, bei denen es unter anderem auch zu Überschneidungen von Daten aus verschiedenen öffentlichen und privaten Datenquellen kommt, könnte hier etwas Klarheit bringen. Dies erfordere zunächst einen genaueren Blick auf die Architektur derartiger Plattformen insb. auf die Art und Weise, wie die Daten in die Plattform eingebracht, miteinander verknüpft und/oder gespeichert werden.

#### a) Krisenresilienzplattformen

Mithilfe von Krisenresilienzplattformen sollen krisenresiliente Strukturen für Krisenbetroffene wie z.B. KMUs aufgebaut werden. Zur Entwicklung dieser Plattformen tragen im wesentlichen Technologien Künstlicher Intelligenz (KI) wie das Machine Learning und Deep Learning bei.

Machine Learning – zu Deutsch maschinelles Lernen – ist eine Art KI, die es Softwareanwendungen ermöglicht automatisch aus Erfahrungen (Daten) zu lernen und sich zu verbessern, ohne explizit dafür programmiert zu sein.<sup>10</sup> Diese Art von

<sup>3</sup> ErwG. 26 S. 5 (EU) 2016/679.

<sup>4</sup> ErwG. 26 S. 6 (EU) 2016/679.

<sup>5</sup> Siehe dazu Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 DS-GVO.

<sup>6</sup> So auch Kathriner/Ruch/Schmidlin in: DE-Identifikation, unter: [https://www.awk.ch/resources/E-Paper\\_DE-Identifikation\\_DE.pdf](https://www.awk.ch/resources/E-Paper_DE-Identifikation_DE.pdf) (2021).

<sup>7</sup> ErwG. 26 S. 3 (EU) 2016/679.

<sup>8</sup> ErwG. 26 S. 4 (EU) 2016/679.

<sup>9</sup> S. Fn. 8.

<sup>10</sup> Wuttke, Laurenz: Machine Learning: Definition, Algorithmen, Methoden und Beispiele, <https://datasolut.com/was-ist-machine-learning/> (Stand: 13.03.2023, 15:39 Uhr).

KI kann dann automatisiert Wissen generieren, Algorithmen trainieren, Zusammenhänge identifizieren und unbekannte Muster erkennen.<sup>11</sup> Diese identifizierten Zusammenhänge und Muster lassen sich dann auf einen neuen, noch unbekanntem Datensatz anwenden, um so Vorhersagen zu treffen und eigene Prozesse zu optimieren.<sup>12</sup> Schwerpunkt des Machine Learnings liegt auf dem selbstständigen Lernen des Algorithmus aus Daten und der alleinigen Erstellung des Programmcodes.<sup>13</sup>

In Bezug auf das eben Gesagte, stellt das Deep Learning eine besondere Form von Machine Learning dar. Hierbei werden neuronale Netze verwendet, um den Computer so zu trainieren, dass dieser aus den Daten lernt.<sup>14</sup> Bei beiden KI-Technologien werden im Kontext der Krisenresilienz i.d.R. Daten aus öffentlichen oder nicht öffentlichen Datenquellen insb. der Domäne Krisenevents, Naturkatastrophen, Informationen zum Unternehmenseigentum und Firmendaten verwendet. Dies ermöglicht es valide, wirtschaftlich verwertbare Einsichten zu generieren oder konkrete krisenbezogene Maßnahmen für Unternehmen abzuleiten.<sup>15</sup> Maßgebend für die Frage der hohen Wahrscheinlichkeit einer Re-Identifizierung anonymisierter Daten ist jedoch nicht bloß die Technologie der KI, die verwendet wurde. Vielmehr ist die Art und Weise, wie diese Daten in diesen Technologien eingebracht, gespeichert und miteinander verknüpft werden, von größerer Wichtigkeit.

#### aa) Knowledge Graphen

Basis für die mithilfe der KI durchgeführten krisenbezogenen Analysen, wie sie etwa auf der CoyPu-Plattform durchgeführt werden sollen, bilden die sog. Knowledge Graphs – zu Deutsch Wissensgraphen. Unter einem Wissensgraphen ist eine Wissens-Datenbank zu verstehen, in der Informationen so strukturiert aufgearbeitet sind, dass aus ihnen Wissen entsteht.<sup>16</sup> Hierbei werden die sog. Entitäten über Kanten ins Verhältnis zueinander gestellt, mit Attributen versehen und in einen thematischen Kontext bzw. eine Ontologie gebracht.<sup>17</sup> Als Entitäten werden in der Informatik einzelne, identifizierbare und separate Objekte bezeichnet.<sup>18</sup> Diese können insb. Systeme, Systemkomponenten aber auch Informationen zu Einzelpersonen oder Organisationen abbilden.<sup>19</sup> Eine derartige Verknüpfung einzelner Entitäten ermöglicht es dann Antworten auf Abfragen zu erteilen, in denen ein Thema oder eine Entität gesucht wird, die in der eigentlichen Abfrage nicht ausdrücklich genannt ist.<sup>20</sup>

Als Grundlage für den Wissensgraphen dienen im Wesentlichen zwei Ebenen: die Ebene des Entitäten-Kataloges und die Ebene des sog. Knowledge repository – zu Deutsch Wissens-Depot. Im Entitäten-Katalog werden alle Entitäten gespeichert, die mit der Zeit identifiziert worden sind.<sup>21</sup> Im Knowledge repository hingegen geht es um die Zusammenführung und Speicherung von Beschreibungen und die Bildung semantischer Klassen bzw. Gruppen in Form von Entitätsgruppen.<sup>22</sup> Hierbei werden die Entitäten in einem Depot mit den Informationen bzw. Attributen aus den verschiedenen Quellen zusammengeführt.<sup>23</sup> Folglich käme es innerhalb dieser Ebenen auch zur Verknüpfung einzelner Informationen, welche aus verschiedenen Datenquellen stammen.

Für die Frage der Identifizierbarkeit einzelner Personen anhand von anonymen Daten bedeutet dies, dass eine Re-Identifizierbarkeit, bei ausreichend komplexer Vernetzung einzelner Entitäten, zumindest nicht vollständig ausgeschlossen werden kann und durchaus (gering) wahrschein-

lich ist. Auch mit Blick auf das Ergebnis einer durchgeführten Studie zum Erfolg von Re-Identifizierungen in unvollständigen Datensätzen unter Verwendung generativer Modelle<sup>24</sup> könnte diese Ansicht bekräftigt werden.

#### bb) Bedenken an der Anonymisierung

Die Anonymisierung stellt bei groß angelegten Verarbeitungen detaillierter Daten im Rahmen der Medizin, Sozialwissenschaft und KI ein wichtiges Instrument zur Übertragung von Informationen bzw. Daten dar. Hierbei erfolgt die Übertragung der Informationen allgemeiner Auffassung nach i.d.R. mit hinreichendem Schutz der Rechte betroffener Personen.<sup>25</sup> In vergangenen Jahren kam es jedoch vermehrt zu Vorfällen, in denen vermeintlich nicht identifizierbare Personen über anonymisierte Daten wieder identifizierbar gemacht wurden. So kam es bspw. dazu, dass Journalisten Politiker zzgl. ihrer Gesundheitsinformationen und sexuellen Präferenzen aus 3 Millionen anonymisierten Datensätzen über deutsche Bürger identifizieren konnten.<sup>26</sup> Dies löste Bedenken hinsichtlich der Einhaltung datenschutzrechtlicher Rahmenbedingungen und den damit einhergehenden Gefahren wie z.B. potenzielle Massenüberwachungen oder Identitätsdiebstahl aus.<sup>27</sup> Diese Bedenken boten der Wissenschaft Anlass dazu sich in einer Studie näher mit der Wahrscheinlichkeit der Re-Identifizierbarkeit einzelner Personen bei stark unvollständigen Datensätzen zu befassen.

Bei der Studie wurde ein generatives grafisches Modell verwendet, welches mit unvollständigen Informationen aus soziodemografischen Umfrage- und Gesundheitsdatensätzen trainiert wurde.<sup>28</sup> Mithilfe dieses Modells wurden dann ein von einer Organisation freigegebener Datensatz und eine Probe von Individuen, welche nach dem Zufallsprinzip aus einer Population von Individuen (z.B. der US-Bevölkerung) ex-

11 S. Fn. 10.

12 S. Fn. 10.

13 S. Fn. 10.

14 Kopp, Olaf: Machine-Learning einfach erklärt: Definition, Unterschied zu Artificial Intelligence, Funktionsweise ..., <https://www.sem-deutschland.de/online-marketing-glossar/was-ist-maschinen-learning-definition-funktionsweise-bedeutung/>, 01.08.2022 (Stand: 13.03.2023, 15:44 Uhr).

15 Wie bei CoyPu <https://datasets.coypu.org/>.

16 Kopp, Olaf: Google Knowledge Graph einfach erklärt: Definition & FAQ, <https://www.sem-deutschland.de/seo-glossar/knowledge-graph/>, 06.09.2019 (Stand: 13.03.2023, 15:35 Uhr).

17 S. Fn. 16.

18 <https://www.seobility.net/de/wiki/Entit%C3%A4t> (Stand: 28.03.2023, 11:09 Uhr).

19 S. Fn. 18.

20 S. Fn. 16.

21 S. Fn. 16.

22 S. Fn. 16.

23 S. Fn. 16.

24 Rocher, Luc, Hendrickx, Julien M., de Montjoye, Yves-Alexandre: Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications* 10, 3069 (veröffentlicht am 23.07.2019). <https://doi.org/10.1038/s41467-019-10933-3>.

25 S. Fn. 24; Polonetsky, J., Tene, O. & Finch, K. Shades of gray: seeing the full spectrum of practical data De-Identification. *Santa Clara Law Rev.* 56, 593–629 (2016); Office for Civil Rights, HHS. Standards for privacy of individually identifiable health information. *Federal Register*. <https://ncbi.nlm.nih.gov/pubmed/12180470> (2002); Malin, B., Benitez, K. & Masys, D. Never too old for anonymity: a statistical stand-ard for demographic data sharing via the HIPAA privacy rule. *J. Am. Med. Inform. Assoc.* 18, 3–10 (2011).

26 Hern, A. 'Anonymous' browsing data can be easily exposed, researchers reveal., *The Guardian* (01.08.2017).

27 S. Fn. 24.

28 S. Fn. 24.

trahiert wurden, betrachtet.<sup>29</sup> Das Modell bezifferte dann infolgedessen, basierend auf diesen Komponenten, die Wahrscheinlichkeit der Re-Identifizierbarkeit jedes Individuums.<sup>30</sup>

### cc) Ergebnis der herangezogenen Studie

Die Ergebnisse der Studie zeigten, dass eine Re-Identifizierung eines Individuums anhand des vorgeschlagenen statistischen Modells, unter Berücksichtigung weniger Basisattribute, wie z.B. Geschlecht, Postleitzahl oder Geburtsdatum, bei einer Wahrscheinlichkeit von ca. 95 % möglich wäre. Daraus ließe sich weiter ableiten, dass eine absolute Anonymität von personenbezogenen Daten nie garantiert werden könne und die Re-Identifizierbarkeit einzelner Personen trotz durchgeführter Anonymisierung der personenbezogenen Datensätze weiterhin ein praktisches Risiko darstellt.

Der Ansicht der Forschenden an der Studie nach ließe sich zwar die Behauptung aufstellen, dass eine geringe Einzigartigkeit der betrachteten Population von Individuen und die bereits fortgeschrittenen De-Identifizierungsverfahren ausreichen, um einen Schutz der Privatsphäre einzelner Personen zu gewährleisten.<sup>31</sup> Dies schließe allerdings nicht die abstrakte Gefahr, dass einzelne Personen dennoch über dieses oder vergleichbare Modelle erfolgreich identifiziert werden könnten, aus. Auch die Möglichkeit einer zufälligen Re-Identifizierung bliebe davon unberührt. Mit Blick auf die Zukunft eröffne dies im Weiteren auch die Frage, ob die derzeitigen De-Identifizierungspraktiken den Standards einschlägiger Datenschutzgesetze entsprechen bzw. genügen. Voraussetzung hierfür wäre allerdings, dass die von den Datenschutzgesetzen gestellten Anforderungen an eine Anonymisierung unmissverständlich bzw. klar gestellt sind.

### b) Missverständnis betreffend die Anforderungen der Datenschutzgesetze

Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) adressierte die Thematik der potenziellen Re-Identifizierung von einzelnen Personen in einem Positionspapier zur Thematik Anonymisierung unter der DS-GVO in Berücksichtigung der TK-Branche<sup>32</sup>. Demnach sei eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden mehr möglich ist, häufig nicht durchführbar.<sup>33</sup> Es wird jedoch auch klargestellt, dass eine absolute De-Identifizierung bzw. Anonymisierung im Regelfall auch datenschutzrechtlich nicht gefordert ist.<sup>34</sup> Vielmehr soll eine sog. faktische Anonymisierung ausreichen. Diese läge vor, wenn der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch gesehen nicht durchführbar ist, weil der Personenbezug nur mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann.<sup>35</sup> Dies entspräche auch der im § 3 Abs. 6 BDSG a.F. befindlichen Definition der Anonymisierung. Weiter zeigt auch die Praxis, dass eine Ermittlung der potenziellen Re-Identifizierung von personenbezogenen Informationen besonders bei Grenzfällen in der Realität meist sehr schwer oder sogar unmöglich erscheint.<sup>36</sup> Ob eine Re-Identifizierung auf Grund von Zeit, Arbeitsaufwand oder Kosten praktisch nicht durchführbar ist, ließe sich demnach anhand des aktuellen Standes der Technik<sup>37</sup> ermitteln. Hierbei wären auch vorhandene und vernünftigerweise einsetzbare rechtliche Mittel wie z.B. Akteneinsichtsrechte zu berücksichtigen.<sup>38</sup>

Problematisch erscheint hierbei allerdings, dass sich der technische Stand mit technischem Fortschritt der Informa-

tionssysteme ständig neu definiert. Weniger problematisch hingegen erscheint, wie sich dieser Umstand auf die Anforderungen der DS-GVO an die Anonymisierung auswirken könnte. Wie bereits unter Ziffer 2.2 dargestellt, beziehen sich die Anforderungen aus den Erwägungsgründen an die Nichtidentifizierbarkeit lediglich auf den Prozess der Pseudonymisierung und nicht auf die Anonymisierung. Eine feste Definition der Voraussetzungen für die Annahme einer Anonymisierung wäre folglich unter dem Aspekt der technischen Entwicklung mancher Ansicht nach nicht sinnvoll gewesen.<sup>39</sup> Dadurch besteht für die Verantwortlichen i.S.d. Art. 24 DS-GVO oder die zuständigen Aufsichtsbehörden die Möglichkeit Anonymisierungsmaßnahmen im Einzelfall flexibel und unter Berücksichtigung des derzeitigen technischen Standes zu beurteilen.<sup>40</sup>

Weiter werden mit hoher Wahrscheinlichkeit zukünftig innovativere Datenverarbeitungstechniken entwickelt werden, welche die derzeitigen Anonymisierungstechniken in ihrer Wirkung beeinträchtigen könnten.<sup>41</sup> Die Open Data Initiative zeigt, dass zukünftig, mit dem Ziel die Innovation im gesamten deutschen Raum zu fördern, mit großer Wahrscheinlichkeit immer mehr Datensätze für die Öffentlichkeit freigegeben werden. Diese freie Zugänglichkeit von Daten könnte einen Quervergleich zwischen Datensätzen ermöglichen, sodass einzelne Datensätze trotz aller Anonymisierungstechniken miteinander verknüpft und letztlich Einzelpersonen identifiziert werden könnten.<sup>42</sup> Mithin wird zum einen deutlich, dass auch zukünftig der Bedarf an vertrauensvollen Anonymisierungsprozessen bestehen wird und zum anderen, derartige Anonymisierungsprozesse nicht innovationshemmend wirken sollen.

29 S. Fn. 24.

30 S. Fn. 24.

31 Rocher, Luc, Hendrickx, Julien M., de Montjoye, Yves-Alexandre, (S. Fußn. 25); so auch: El Emam, K. & Arbuckle, L. Anonymizing Health Data (O'Reilly, Newton, MA, 2013); Cavoukian, A. & Castro, D., Big data and innovation, setting the record straight: de-identification does work., <http://www2.itif.org/2014-big-data-deidentification.pdf> (2014).

32 Positionspapier des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zur Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, unter: [https://www.bfdi.bund.de/Shared-Docs/Downloads/DE/Konsultationsverfahren/1\\_Anonymisierung/Positionspapier-Anonymisierung.pdf?\\_\\_blob=publicationFile&v=4](https://www.bfdi.bund.de/Shared-Docs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4), (Stand: 29.06.2020).

33 Ziebarth, in: Sydow/Marsch, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 Rn. 24 f.

34 S. Fn. 33.

35 Vgl. EuGH, Urt. v. 19.10.2016 – C-582/14 – Breyer, ZD 2017, 24 (26) = MMR 2016, 842 (843); Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019, § 98 TKG Rn. 13.

36 So auch in: Information Commissioner's Office (ICO), Anonymisation: managing data protection risk code of practice, November 2012, 20.

37 „Der 'Stand der Technik' ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind.“ (vgl. Handbuch der Rechtsförmlichkeit v. 22.09.2008, Rn. 256).

38 Roßnagel, ZD 2018, 243, 245; Koyuncu, Kügel/Müller/Hofmann, Arzneimittelgesetz, 3. Auflage 2022, Rn. 12-14.

39 Vgl. Schewior, Christoph, Anonymisierung von Daten – Der BfDI informiert, 30.06.2020, unter: <https://www.dr-datenschutz.de/anonymisierung-von-daten-der-bfdi-informiert/>.

40 S. Fn. 37.

41 Vgl. An Coimisiún um Chosaint Sonraí (Datenschutz Kommission Irland), Guidance Note: Guidance on Anonymisation and Pseudonymisation, 2019, Page 7, unter: <https://www.dataprotection.ie/en/dpc-guidance/anonymisation-and-pseudonymisation> (Stand: 24.03.2023, 16:51 Uhr).

42 S. Fn. 41.

### c) Verhaltensregeln i.S.v. Art. 40 DS-GVO

Besonders für Verantwortliche nach Art. 24 DS-GVO und Auftragsverarbeiter besteht deshalb weiterhin betreffend die eindeutige datenschutzrechtliche Einordnung etwaiger Anonymisierungsprozesse und der an diese zu stellenden Anforderungen große Unklarheit. Über diesen Bedarf an regulatorischer Klarheit betreffend die datenschutzkonforme Anonymisierung, könnten Verhaltensregeln (oder auch sog. Codes of Conduct) i.S.d. Art. 40 der DS-GVO hinweghelfen.

Gemäß Art. 40 Abs. 1 DS-GVO und den Erwägungsgründen der DS-GVO<sup>43</sup> sollen Verbände oder andere Vereinigungen mithilfe des Art. 40 DS-GVO gerade dazu ermutigt werden, innerhalb der Grenzen der DS-GVO Verhaltensregeln auszuarbeiten, um eine wirksame Anwendung der datenschutzrechtlichen Anforderungen zu erleichtern. Zwar wird die Anonymisierung im Art. 40 DS-GVO nicht ausdrücklich erwähnt, jedoch bestünde mit Blick auf die Erwägungsgründe der DS-GVO ein berechtigtes Interesse daran die Anwendung der DS-GVO auf die Anonymisierung (in Abgrenzung zur Pseudonymisierung) durch Verhaltensregeln zu präzisieren. Hierbei ist auch zu beachten, dass die DS-GVO lediglich eine nicht abschließende Liste besonders drängender Themen vorsieht, die letztlich Auswahl der von einer Verhaltensregel abgebildeten Themen aber in der Entscheidungshoheit und Verantwortung der sog. Code-Owner liegt.<sup>44</sup>

Das solche Verhaltensregeln für regulatorische Klarheit sorgen können zeigt z.B. der von SCOPE Europe<sup>45</sup> betreute EU Cloud Code of Conduct<sup>46</sup>. Dieser wurde entwickelt, um die Anforderungen der DS-GVO betreffend Cloud-Dienste abzudecken und wurde nach einer positiven Stellungnahme<sup>47</sup> des Europäischen Datenschutzausschusses im Mai 2021 von der belgischen Datenschutzbehörde genehmigt<sup>48</sup>. Auch der thematisch die Anonymisierung im Kontext der „Verpixelung“ zumindest teilweise tangierende Geodatenkodex konnte die aufsichtsbehördliche Praxis und Diskussion bereits zu Zeiten der Richtlinie beruhigen.<sup>49</sup> Ein Verhaltenskodex für die Anonymisierung, welcher künftig entsprechend Art. 40 Abs. 5 DS-GVO von der zuständigen Datenschutzbehörde genehmigt bzw. anerkannt werden würde, würde gewiss mehr Sicherheit für die Datenverarbeiter und zuständigen Aufsichtsbehörden bei der Beurteilung etwaiger Anonymisierungsprozesse mit sich bringen. Konkrete Anforderungen der Verhaltensregeln könnten so insb. Risikoanalysen betreffend die Anonymisierung verbessern. Etwa könnten diese beispielshalber Kriterien der Risikoanalyse wie z.B. der Grad des Interesses eines Angreifers an einer Re-Identifizierung des anonymen Datensatzes umfassen.<sup>50</sup> Hierbei wären jedoch nicht alle Anonymisierungen gleich zu beurteilen. Konkret am Kriterium des Grades des Interesses an einer Re-Identifizierung wird deutlich, und das gilt es klarzustellen, dass nicht bei jedem anonymisierten Datensatz ein solches Interesse des Angreifers vorliegt und somit auch nicht bei jeder Anonymisierung ein Risiko der Re-Identifizierung besteht.

### III. Fazit

Zusammenfassend lässt sich feststellen, dass der Aspekt einer Re-Identifizierung einzelner Personen bei anonymen Datensätzen aufgrund der bestehenden Wahrscheinlichkeit auch zukünftig eine sehr wichtige Rolle spielen wird. Deutlich wird auch, dass besonders

automatisierte Datenverarbeitungssysteme wie die Krisenresilienzplattformen, welche krisenresiliente Lösungsoptionen anbieten möchten und somit auf große Mengen an (auch anonymen) Datensätzen angewiesen sind, von einer Klärung dieser Problematik profitieren würden. Zwar stellt insb. die Anonymisierung ein geeignetes De-Identifizierungsinstrument dar, um den Personenbezug der Daten bestmöglich aufzuheben und so einen hinreichenden Schutz der Rechte betroffener Personen zu gewährleisten. Allerdings bliebe mit Blick auf die Weiterentwicklung des derzeitigen technischen Standes stets ein Restrisiko der Re-Identifizierung, welche die Verantwortlichen und Datenverarbeiter fortwährend berücksichtigen sollten. Nach jetzigem Stand der Wissenschaft und behördlichen Stellungnahmen, ist eine rechtskonforme Anonymisierung möglich. Dieser grundsätzliche Umstand sollte auch im Sinne des Datenschutzes (privacy-by-design) aufrechterhalten werden, ungeachtet der künftigen technischen Entwicklungen. Im Übrigen würde jeder Anreiz für Unternehmen verloren gehen, in datensparsamere, anonymisierte Verarbeitungsprozesse zu investieren.

Über die dennoch im Einzelfall verbleibende Unklarheit betreffend die DS-GVO konformen Anforderungen an eine Anonymisierung könnten anerkannte Verhaltensregeln nach Art. 40 DS-GVO hinweghelfen. Diese könnten grundsätzliche Anforderungen an Anonymisierungsprozess und abwägungsrelevante Aspekte definieren; soweit erforderlich könnten Verhaltensregeln auch für bestimmte Verarbeitungskontexte konkrete Maßgaben treffen, die eine sachgerechte und Innovationspotenzial aufrechterhaltene Interessenabwägung sowie den Schutz der Betroffenen im Sinne der DS-GVO gewährleisten. Entsprechend sollte bei Erstellung der Verhaltensregeln stets der Aspekt des Restrisikos einer Re-Identifizierung berücksichtigt werden, so dass es Verantwortlichen, Datenverarbeitern und zuständigen Datenschutzaufsichtsbehörden ermöglicht wird, Anonymisierungsmaßnahmen auch zukünftig rechtssicher einzuordnen.

43 ErwG. 98 S. 1 (EU) 2016/679.

44 So auch Wittmann/Ingenrieth in: Plath, DS-GVO – BDSG – TTDSG, 4. Auflage 2023, Rn. 12; Paal/Pauly/Paal/Kumkar, DS-GVO, Art. 40 Rn. 13; Jungkind in: Wolff/Brink, BeckOK DatenschutzR, 43. Ed. 01.11.2021, DS-GVO, Art. 40 Rn. 13.

45 SCOPE Europe ist die Tochtergesellschaft des Selbstregulierung Informationswirtschaft e.V. welcher es sich zum Ziel gemacht hat, durch glaubwürdige und wirkungsvolle Selbst- und Ko-Regulierung, vor allem im Bereich des Daten- und Verbraucherschutzes, eine innovationsfreundliche und moderne Politikgestaltung zu etablieren. Mehr dazu unter: <https://sriw.de/der-sriw>.

46 Mehr unter: <https://eucoc.cloud/en/home>.

47 Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the “EU Data Protection Code of Conduct for Cloud Service Providers” submitted by Scope Europe, 19.05.2021, unter: [https://edpb.europa.eu/system/files/2021-05/edpb\\_opinion\\_202116\\_eucloudcode\\_en.pdf](https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf).

48 Siehe <https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf>.

49 Näheres unter <https://geodatenkodex.de/home>; Die Erstfassung stammt aus 2011 und wurde 2015 erstmalig überarbeitet; [https://geodatenkodex.de/fileadmin/gdk/files/Datenschutz-Kodex\\_f%C3%BCr\\_Geodatendienste.pdf](https://geodatenkodex.de/fileadmin/gdk/files/Datenschutz-Kodex_f%C3%BCr_Geodatendienste.pdf). Per 2023 wurde eine an die DS-GVO angepasste Fassung (2.1) veröffentlicht: [https://geodatenkodex.de/fileadmin/gdk/files/Geodatenkodex\\_v2-1.pdf](https://geodatenkodex.de/fileadmin/gdk/files/Geodatenkodex_v2-1.pdf).

50 So auch Schwartmann/Jaspers/Lepperhoff/Weiß/Meier, Praxisleitfaden zum Anonymisieren personenbezogener Daten – Anforderungen, Einsatzklassen und Vorgehensmodell, Dezember 2022, 27.

# RECHTSPRECHUNG

## Highlights für den betrieblichen Datenschutz:

### Voraussetzungen eines immateriellen Schadenersatzanspruchs nach Art. 82 DS-GVO

(EuGH, Urteil vom 4. Mai 2023 – C-300/21 –)

#### Relevanz für die Praxis

Unter welchen Voraussetzungen Betroffene Schadenersatz nach Art. 82 DS-GVO für immaterielle Schäden verlangen können, ist seit Inkrafttreten der DS-GVO eine der meist umstrittenen Fragen im Datenschutzrecht. Nun hat der EuGH in einem lang ersehnten Urteil in einigen Punkten für Klarheit gesorgt.

Ein bloßer Verstoß gegen die DS-GVO reicht dem neuesten Urteil zufolge nicht aus, um einen Schadenersatzanspruch zu begründen. Die betroffene Person muss einen immateriellen Schaden erlitten haben und vor Gericht darlegen. Eine Erheblichkeitsschwelle kennt die DS-GVO hingegen nicht, so der EuGH. Damit erleichtert die Entscheidung die Geltendmachung von Schadenersatzansprüchen erheblich.

Die Ermittlung der Höhe des Schadenersatzes legt der EuGH in die Hände der einzelnen Mitgliedstaaten. Hier bleibt also die hiesige Praxis weiterhin entscheidend.

1. **Art. 82 Abs. 1 der Verordnung (EU) 2016/679 [...] ist dahin auszulegen, dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung nicht ausreicht, um einen Schadenersatzanspruch zu begründen.**
2. **Art. 82 Abs. 1 der Verordnung 2016/679 ist dahin auszulegen, dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.**
3. **Art. 82 der Verordnung 2016/679 ist dahin auszulegen, dass die nationalen Gerichte bei der Festsetzung der Höhe des Schadenersatzes, der aufgrund des in diesem Artikel verankerten Schadenersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden haben, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden.**

#### Zu den Vorlagefragen:

##### Zur ersten Frage:

Mit seiner ersten Frage möchte das vorliegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DS-GVO dahin auszu-

legen ist, dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung ausreicht, um einen Schadenersatzanspruch zu begründen.

Insoweit ist darauf hinzuweisen, dass nach ständiger Rechtsprechung die Begriffe einer Bestimmung des Unionsrechts, die für die Ermittlung ihres Sinnes und ihrer Tragweite nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten müssen (Urt. v. 22. Juni 2021, Latvijas Republikas Saeima [Strafpunkte], C-439/19, EU:C:2021:504, Rn. 81, und vom 10. Februar 2022, ShareWood Switzerland, C-595/20, EU:C:2022:86, Rn. 21), die insbesondere unter Berücksichtigung des Wortlauts der betreffenden Bestimmung und des Zusammenhangs, in den sie sich einfügt, zu ermitteln ist (vgl. in diesem Sinne Urt. v. 15. April 2021, The North of England P & I Association, C-786/19, EU:C:2021:276, Rn. 48, sowie vom 10. Juni 2021, KRONE – Verlag, C-65/20, EU:C:2021:471, Rn. 25).

Die DS-GVO verweist für den Sinn und die Tragweite der in ihrem Art. 82 enthaltenen Begriffe, insbesondere in Bezug auf die Begriffe „materieller oder immaterieller Schaden“ und „Schadenersatz“, nicht auf das Recht der Mitgliedstaaten. Daraus folgt, dass diese Begriffe für die Anwendung der DS-GVO als autonome Begriffe des Unionsrechts anzusehen sind, die in allen Mitgliedstaaten einheitlich auszulegen sind.

Was als Erstes den Wortlaut von Art. 82 DS-GVO betrifft, ist darauf hinzuweisen, dass nach Abs. 1 dieses Artikels „[j]ede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, ... Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter [hat]“.

Zum einen geht aus dem Wortlaut dieser Bestimmung klar hervor, dass das Vorliegen eines „Schadens“ eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadenersatzanspruch darstellt, ebenso wie das Vorliegen eines Verstoßes gegen die DS-GVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind.

Daher kann nicht davon ausgegangen werden, dass jeder „Verstoß“ gegen die Bestimmungen der DS-GVO für sich genommen den Schadenersatzanspruch der betroffenen Person im Sinne von Art. 4 Nr. 1 dieser Verordnung eröffnet. Eine solche Auslegung liefe dem Wortlaut von Art. 82 Abs. 1 DS-GVO zuwider.

Zum anderen ist hervorzuheben, dass die gesonderte Erwähnung eines „Schadens“ und eines „Verstoßes“ in Art. 82 Abs. 1 DS-GVO überflüssig wäre, wenn der Unionsgesetzgeber davon ausgegangen wäre, dass ein Verstoß gegen die Bestimmungen der DS-GVO für sich allein in jedem Fall ausreichend wäre, um einen Schadenersatzanspruch zu begründen.

Als Zweites wird die vorstehende Wortauslegung durch den Zusammenhang bestätigt, in den sich diese Bestimmung einfügt.

Art. 82 Abs. 2 DS-GVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt nämlich die drei Voraussetzungen für die Entstehung des Schadenersatzanspruchs, nämlich eine Verar-

beitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DS-GVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden.

Diese Auslegung wird auch durch die Erläuterungen in den Erwägungsgründen 75, 85 und 146 der DS-GVO bestätigt. Zum einen bezieht sich der 146. Erwägungsgrund der DS-GVO, der speziell den in Art. 82 Abs. 1 dieser Verordnung vorgesehenen Schadenersatzanspruch betrifft, in seinem ersten Satz auf „Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht“. Zum anderen heißt es in den Erwägungsgründen 75 und 85 der DS-GVO, dass „[d]ie Risiken ... aus einer Verarbeitung personenbezogener Daten hervorgehen [können], die zu einem ... Schaden führen könnte“ bzw. dass eine „Verletzung des Schutzes personenbezogener Daten ... einen ... Schaden ... nach sich ziehen [kann]“. Daraus ergibt sich erstens, dass der Eintritt eines Schadens im Rahmen einer solchen Verarbeitung nur potenziell ist, zweitens, dass ein Verstoß gegen die DS-GVO nicht zwangsläufig zu einem Schaden führt, und drittens, dass ein Kausalzusammenhang zwischen dem fraglichen Verstoß und dem der betroffenen Person entstandenen Schaden bestehen muss, um einen Schadenersatzanspruch zu begründen.

Die Wortauslegung von Art. 82 Abs. 1 DS-GVO wird auch durch einen Vergleich mit anderen Bestimmungen bestätigt, die ebenfalls in Kapitel VIII der DS-GVO enthalten sind, das u.a. die verschiedenen Rechtsbehelfe regelt, mit denen die Rechte der betroffenen Person im Fall einer Verarbeitung ihrer personenbezogenen Daten, die gegen die Bestimmungen dieser Verordnung verstoßen soll, geschützt werden können.

Hierzu ist festzustellen, dass die in diesem Kapitel enthaltenen Artt. 77 und 78 DS-GVO im Fall eines behaupteten Verstoßes gegen diese Verordnung Rechtsbehelfe bei einer bzw. gegen eine Aufsichtsbehörde vorsehen, wobei sie – anders als Art. 82 DS-GVO in Bezug auf Schadenersatzklagen – keinen Hinweis darauf enthalten, dass der betroffenen Person ein „Schaden“ entstanden sein müsste, um solche Rechtsbehelfe einlegen zu können. Dieser Unterschied in der Formulierung offenbart die Bedeutung des Kriteriums „Schaden“ und damit seine Eigenständigkeit gegenüber dem Kriterium „Verstoß“ für die Zwecke der auf die DS-GVO gestützten Schadenersatzansprüche.

Auch haben die Artt. 83 und 84 DS-GVO, die die Verhängung von Geldbußen und anderen Sanktionen erlauben, im Wesentlichen einen Strafzweck und hängen nicht vom Vorliegen eines individuellen Schadens ab. Das Verhältnis zwischen den in Art. 82 DS-GVO und den in den Artt. 83 und 84 DS-GVO enthaltenen Vorschriften zeigt, dass zwischen diesen beiden Kategorien von Bestimmungen ein Unterschied besteht, sie einander aber als Anreiz zur Einhaltung der DS-GVO auch ergänzen, wobei das Recht jeder Person, den Ersatz eines Schadens zu verlangen, die Durchsetzungskraft der in dieser Verordnung vorgesehenen Schutzvorschriften erhöht und geeignet ist, von der Wiederholung rechtswidriger Verhaltensweisen abzuschrecken.

Schließlich ist darauf hinzuweisen, dass nach dem vierten Satz des 146. Erwägungsgrundes der DS-GVO die Vorschriften der DS-GVO unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten gelten.

Nach alledem ist auf die erste Frage zu antworten, dass Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung nicht ausreicht, um einen Schadenersatzanspruch zu begründen.

#### Zur dritten Frage:

Mit seiner dritten Frage, die vor der zweiten Frage zu prüfen ist, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.

Insoweit ist auf die oben gemachten Ausführungen hinzuweisen, wonach der Begriff „Schaden“ und im vorliegenden Fall speziell der Begriff „immaterieller Schaden“ im Sinne von Art. 82 DS-GVO in Anbetracht des Fehlens jeglicher Bezugnahme auf das innerstaatliche Recht der Mitgliedstaaten eine autonome und einheitliche unionsrechtliche Definition erhalten müssen.

Als Erstes ist in der DS-GVO der Begriff „Schaden“ für die Zwecke der Anwendung dieses Instruments nicht definiert. Art. 82 DS-GVO beschränkt sich auf die ausdrückliche Feststellung, dass nicht nur ein „materieller Schaden“, sondern auch ein „immaterieller Schaden“ Anspruch auf Schadenersatz eröffnen kann, ohne dass eine wie auch immer geartete Erheblichkeitsschwelle genannt wird.

Als Zweites deutet auch der Zusammenhang, in den sich diese Bestimmung einfügt, darauf hin, dass der Schadenersatzanspruch nicht davon abhängt, dass der betreffende Schaden eine gewisse Erheblichkeit erreicht. Nach dem dritten Satz des 146. Erwägungsgrundes der DS-GVO sollte „[d]er Begriff des Schadens ... im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht“. Es stünde jedoch zu dem vom Unionsgesetzgeber gewählten weiten Verständnis des Begriffs „Schaden“ im Widerspruch, wenn dieser Begriff auf Schäden mit einer gewissen Erheblichkeit beschränkt wäre.

Als Drittes und Letztes wird diese Auslegung durch die mit der DS-GVO verfolgten Ziele bestätigt. Insoweit ist darauf hinzuweisen, dass im dritten Satz des 146. Erwägungsgrundes der DS-GVO ausdrücklich gefordert wird, bei der Definition des Begriffs „Schaden“ im Sinne dieser Verordnung „den Zielen dieser Verordnung in vollem Umfang“ zu entsprechen.

Insbesondere geht aus dem zehnten Erwägungsgrund der DS-GVO hervor, dass diese namentlich darauf abzielt, innerhalb der Union ein gleichmäßiges und hohes Niveau des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten und zu diesem Zweck für eine unionsweit gleichmäßige und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten dieser Personen bei der Verarbeitung personenbezogener Daten zu sorgen (vgl. in diesem Sinne Ur. v. 16. Juli 2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 101, sowie vom 12. Januar 2023, Österreichische Post [Informationen über die Empfänger personenbezogener Daten], C-154/21, EU:C:2023:3, Rn. 44 und die dort angeführte Rechtsprechung).

Würde aber der Ersatz eines immateriellen Schadens von einer Erheblichkeitsschwelle abhängig gemacht, könnte dies die Kohärenz der mit der DS-GVO eingeführten Regelung beeinträchtigen, da die graduelle Abstufung einer solchen Schwelle, von der die Möglichkeit, Schadenersatz zu erhalten, abhinge, je nach Beurteilung durch die angerufenen Gerichte unterschiedlich hoch ausfallen könnte.

Allerdings bedeutet diese Auslegung nicht, dass eine Person, die von einem Verstoß gegen die DS-GVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 dieser Verordnung darstellen.

Nach alledem ist auf die dritte Frage zu antworten, dass Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.

#### Zur zweiten Frage:

Mit seiner zweiten Frage möchte das vorliegende Gericht im Wesentlichen wissen, ob Art. 82 DS-GVO dahin auszulegen ist, dass die nationalen Gerichte bei der Festsetzung der Höhe des Schadenersatzes, der aufgrund des in diesem Artikel verankerten Schadenersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung unter Beachtung nicht nur der unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität anzuwenden haben.

Insoweit ist darauf hinzuweisen, dass es nach ständiger Rechtsprechung mangels einschlägiger Unionsregeln nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaates ist, die verfahrensrechtlichen Modalitäten der Rechtsbehelfe, die zum Schutz der Rechte der Bürger bestimmt sind, festzulegen, vorausgesetzt allerdings, dass diese Modalitäten bei unter das Unionsrecht fallenden Sachverhalte nicht ungünstiger sind als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz), und dass sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz) (vgl. in diesem Sinne Urt. v. 13. Dezember 2017, El Hassani, C-403/16, EU:C:2017:960, Rn. 26, und vom 15. September 2022, Uniqa Versicherungen, C-18/21, EU:C:2022:682, Rn. 36).

Im vorliegenden Fall ist festzustellen, dass die DS-GVO keine Bestimmung enthält, die sich den Regeln für die Bemessung des Schadenersatzes widmet, auf den eine betroffene Person im Sinne von Art. 4 Nr. 1 dieser Verordnung nach deren Art. 82 Anspruch hat, wenn ihr durch einen Verstoß gegen diese Verordnung ein Schaden entstanden ist. Daher sind die Ausgestaltung von Klageverfahren, die den Schutz der dem Einzelnen aus Art. 82 DS-GVO erwachsenden Rechte gewährleisten sollen, und insbesondere die Festlegung der Kriterien für die Ermittlung des Umfangs des in diesem Rahmen geschuldeten Schadenersatzes in Ermangelung einschlägiger unionsrechtlicher Vorschriften Aufgabe des Rechts des einzelnen Mitgliedstaates, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten sind (vgl. entsprechend

Urt. v. 13. Juli 2006, Manfredi u.a., C-295/04 bis C-298/04, EU:C:2006:461, Rn. 92 und 98).

Was den Äquivalenzgrundsatz betrifft, verfügt der Gerichtshof im vorliegenden Verfahren über keinerlei Anhaltspunkte, die einen Zweifel an der Vereinbarkeit einer auf den Ausgangrechtsstreit anwendbaren nationalen Regelung mit diesem Grundsatz aufkommen lassen und somit darauf hindeuten könnten, dass sich dieser Grundsatz im Rahmen dieses Rechtsstreits konkret auswirken könnte.

Was den Effektivitätsgrundsatz betrifft, ist es Sache des vorlegenden Gerichts, festzustellen, ob die im österreichischen Recht vorgesehenen Modalitäten für die gerichtliche Festsetzung des Schadenersatzes, der aufgrund des in Art. 82 DS-GVO verankerten Schadenersatzanspruchs geschuldet wird, die Ausübung der durch das Unionsrecht und insbesondere durch diese Verordnung verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren.

In diesem Zusammenhang ist darauf hinzuweisen, dass der sechste Satz des 146. Erwägungsgrundes der DS-GVO besagt, dass dieses Instrument einen „vollständigen und wirklichen Schadenersatz für den erlittenen Schaden“ sicherstellen soll.

Wie der Generalanwalt in den Nrn. 39, 49 und 52 seiner Schlussanträge im Wesentlichen ausgeführt hat, ist in Anbetracht der Ausgleichsfunktion des in Art. 82 DS-GVO vorgesehenen Schadenersatzanspruchs eine auf diese Bestimmung gestützte finanzielle Entschädigung als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen, ohne dass ein solcher vollumfänglicher Ausgleich die Verhängung von Strafschadenersatz erfordert.

Nach alledem ist auf die zweite Frage zu antworten, dass Art. 82 DS-GVO dahin auszulegen ist, dass die nationalen Gerichte bei der Festsetzung der Höhe des Schadenersatzes, der aufgrund des in diesem Artikel verankerten Schadenersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden haben, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden.

#### Zur Vertiefung

*Wybitul/Brams/Zhou, Der EuGH erleichtert Massenklagen im Datenschutz = RDV 3/2023.*

*Meyer, Rechtsmissbräuchliche Schadenersatzforderungen = RDV 6/2022.*

*[Urteil] BAG-EuGH-Anfrage zu immateriellem Schadenersatz wegen der Übermittlung personenbezogener Daten an die ehemalige Konzernmutter der Arbeitgeberin in den USA aufgrund einer Betriebsvereinbarung = RDV 6/2022.*

*[Urteil] 10.000,- € Schadenersatz wegen einer verspäteten Auskunft nach Art. 15 DS-GVO = RDV 3/2023.*

*[Urteil] Zur Höhe eines Anspruchs auf immateriellen Schadenersatz bei Verstoß gegen die DS-GVO = RDV 5/2022.*

*[Urteil] Ein immaterieller Schadenersatz nach Art. 82 DS-GVO muss konkretisiert sein (Ls) = RDV 1/2022.*

## Reichweite des Rechts auf Kopie aus Art. 15 Abs. 3 S. 1 DS-GVO

(EuGH, Urteil vom 4. Mai 2023 – C-487/21 –)

### Relevanz für die Praxis

Das Urteil schafft Klarheit in einer der seit dem Inkrafttreten der DS-GVO bestehenden Fragen im Kontext des Art. 15 Abs. 3 S. 1 DS-GVO, dem Umfang des Rechts auf Kopie. Der EuGH spricht dem Betroffenen in der vorliegenden Entscheidung das Recht zu, eine „originalgetreue und verständliche Reproduktion der verarbeiteten personenbezogenen Daten“ zu erhalten. Um seiner Pflicht aus Art. 15 Abs. 3 S. 1 DS-GVO gerecht zu werden, kann es für den Verantwortlichen daher erforderlich sein, dem Betroffenen eine Kopie von Auszügen aus Dokumenten oder sogar von ganzen Dokumenten zu übermitteln. Dies ist der Fall, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten. Eine aggregierte Auflistung der verarbeiteten personenbezogenen Daten ist in diesem Fall zur Erfüllung der Pflicht aus Art. 15 Abs. 3 S. 1 DS-GVO nicht ausreichend. Etwas anderes kann sich aber dann ergeben, wenn das Recht auf Kopie der personenbezogenen Daten im Konflikt mit Rechten oder Freiheiten anderer Personen steht. Dann ist der Umfang des Rechts aus Art. 15 Abs. 3 S. 1 DS-GVO im Einzelfall durch eine Abwägung der widerstreitenden Rechte und Freiheiten zu bestimmen. Diese Abwägung darf nicht zu einer Verweigerung jeglicher Auskunft führen.

1. Art. 15 Abs. 3 S. 1 der [...] [DS-GVO] ist dahin auszulegen, dass das Recht, vom für die Verarbeitung Verantwortlichen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zu erhalten, bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten ausgefolgt wird. Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u.a. diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, [...].
2. Art. 15 Abs. 3 S. 3 der Verordnung 2016/679 ist dahin auszulegen, dass sich der im Sinne dieser Bestimmung verwendete Begriff „Informationen“ ausschließlich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäß S. 1 dieses Absatzes eine Kopie zur Verfügung stellen muss.

### Zu den Vorlagefragen:

#### Zu den Vorlagefragen 1 bis 3:

Mit den Fragen 1 bis 3, die zusammen zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 3 S. 1 DS-GVO im Licht des in Art. 12 Abs. 1 dieser Verordnung vorgesehenen Transparenzgrundsatzes dahin auszulegen ist, dass das Recht auf Ausfolgung einer Kopie der perso-

nenbezogenen Daten, die Gegenstand der Verarbeitung sind, bedeutet, dass der betroffenen Person nicht nur eine Kopie dieser Daten ausgefolgt wird, sondern auch eine Kopie der Auszüge aus Dokumenten oder gar eine Kopie von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u.a. diese Daten enthalten. Das vorlegende Gericht wirft insbesondere die Frage nach dem Umfang dieses Rechts auf. [...]

Was den Wortlaut von Art. 15 Abs. 3 S. 1 DS-GVO betrifft, so heißt es in dieser Bestimmung, dass der Verantwortliche „eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung [stellt]“.

Auch wenn die DS-GVO keine Definition des so verwendeten Begriffs „Kopie“ enthält, ist der gewöhnliche Sinn dieses Begriffs zu berücksichtigen, der, wie der Generalanwalt in Nr. 30 seiner Schlussanträge ausgeführt hat, die originalgetreue Reproduktion oder Abschrift bezeichnet, so dass eine rein allgemeine Beschreibung der Daten, die Gegenstand der Verarbeitung sind, oder ein Verweis auf Kategorien personenbezogener Daten nicht dieser Definition entspreche. Außerdem ergibt sich aus dem Wortlaut von Art. 15 Abs. 3 S. 1 dieser Verordnung, dass sich die Mitteilungspflicht auf die personenbezogenen Daten bezieht, die Gegenstand der in Rede stehenden Verarbeitung sind. [...]

In der Verwendung des Ausdrucks „alle Informationen“ im Zusammenhang mit der Bestimmung des Begriffs „personenbezogene Daten“ in [...] [Art. 4 Nr. 1 DS-GVO] kommt das Ziel des Unionsgesetzgebers zum Ausdruck, diesem Begriff eine weite Bedeutung beizumessen, die potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen umfasst, unter der Voraussetzung, dass es sich um Informationen „über“ die in Rede stehende Person handelt (vgl. entsprechend Ur. v. 20. Dezember 2017, Nowak, C 434/16, EU:C:2017:994, Rn. 34). [...]

In diesem Zusammenhang ist hinzuzufügen, dass der Unionsgesetzgeber den Begriff „Verarbeitung“, wie er in Art. 4 Nr. 2 DS-GVO definiert ist, durch eine nicht erschöpfende Aufzählung von Vorgängen weit fassen wollte (vgl. in diesem Sinne Ur. v. 24. Februar 2022, Valsts ierņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C 175/20, EU:C:2022:124, Rn. 35).

Daher folgt aus der wörtlichen Auslegung von Art. 15 Abs. 3 S. 1 DS-GVO, dass diese Bestimmung der betroffenen Person das Recht verleiht, eine originalgetreue Reproduktion ihrer personenbezogenen Daten im Sinne einer weiten Bedeutung zu erhalten, die Gegenstand von Vorgängen sind, die als Verarbeitung durch den für diese Verarbeitung Verantwortlichen eingestuft werden müssen.

Allerdings ist festzustellen, dass der Wortlaut dieser Bestimmung für sich genommen die Beantwortung der ersten drei Fragen nicht ermöglicht, da er keinen Hinweis auf ein etwaiges Recht enthält, nicht nur eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sondern auch eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder Auszügen aus Datenbanken, die u.a. diese Daten enthalten, zu erlangen.

Zum Kontext von Art. 15 Abs. 3 S. 1 DS-GVO ist festzustellen, dass Art. 15 („Auskunftsrecht der betroffenen Person“) Abs. 1 DS-GVO den Gegenstand und den Anwendungsbereich des der betroffenen Person zustehenden Auskunftsrechts festlegt und darin deren Recht verankert, von dem für die

Verarbeitung Verantwortlichen Auskunft über ihre personenbezogenen Daten sowie die in den Buchst. a) bis h) dieses Absatzes genannten Informationen zu erhalten.

Art. 15 Abs. 3 DS-GVO legt die praktischen Modalitäten für die Erfüllung der dem für die Verarbeitung Verantwortlichen obliegenden Verpflichtung fest [...].

Daher kann Art. 15 DS-GVO nicht so ausgelegt werden, dass er in seinem Abs. 3 S. 1 ein anderes Recht als das in seinem Abs. 1 vorgesehene gewährt. Im Übrigen bezieht sich, wie die Europäische Kommission in ihren schriftlichen Erklärungen betont hat, der Begriff „Kopie“ nicht auf ein Dokument als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen. Die Kopie muss daher alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind.

Zu den mit Art. 15 DS-GVO verfolgten Ziele ist festzustellen, dass die DS-GVO, wie sich aus ihrem elften Erwägungsgrund ergibt, den Zweck hat, die Rechte der betroffenen Personen zu stärken und präzise festzulegen. Im Unterschied zu Art. 12 Buchst. a) zweiter Gedankenstrich der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31), der lediglich eine „Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind“ verlangt, sieht Art. 15 dieser Verordnung insoweit ein Recht auf Erhalt einer Kopie vor. Im 63. Erwägungsgrund der DS-GVO wird wiederum klargestellt: „[E]ine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.“ [...]

Somit muss es der betroffenen Person durch die Ausübung des in Art. 15 DS-GVO vorgesehenen Auskunftsrechts nicht nur ermöglicht werden, zu überprüfen, ob sie betreffende Daten richtig sind, sondern auch, ob sie in zulässiger Weise verarbeitet werden (vgl. in diesem Sinne Urt. v. 12. Januar 2023, Österreichische Post [Informationen über die Empfänger personenbezogener Daten], C 154/21, EU:C:2023:3, Rn. 37 und die dort angeführte Rechtsprechung).

Dieses Auskunftsrecht ist insbesondere erforderlich, um es der betroffenen Person zu ermöglichen, gegebenenfalls ihr Recht auf Berichtigung, ihr Recht auf Löschung („Recht auf Vergessenwerden“) und ihr Recht auf Einschränkung der Verarbeitung, die ihr nach den Artt. 16, 17 bzw. 18 DS-GVO zukommen, sowie ihr in Art. 21 DS-GVO vorgesehenes Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten oder im Schadensfall ihr in den Artt. 79 und 82 DS-GVO vorgesehenes Recht auf Einlegung eines gerichtlichen Rechtsbehelfs auszuüben (Urt. v. 12. Januar 2023, Österreichische Post [Informationen über die Empfänger personenbezogener Daten], C 154/21, EU:C:2023:3, Rn. 38 und die dort angeführte Rechtsprechung).

Im Übrigen muss gemäß dem vom vorlegenden Gericht erwähnten Grundsatz der Transparenz, auf den im 58. Erwägungsgrund der DS-GVO Bezug genommen wird und der in Art. 12 Abs. 1 dieser Verordnung ausdrücklich verankert ist, eine für die betroffene Person bestimmte Information prä-

zise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sein.

Wie der Generalanwalt in den Nrn. 54 und 55 seiner Schlussanträge ausgeführt hat, ergibt sich aus dieser Bestimmung, dass der Verantwortliche geeignete Maßnahmen zu treffen hat, um der betroffenen Person alle u.a. in Art. 15 DS-GVO genannten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, und dass die Übermittlung der Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch zu erfolgen hat, es sei denn, die betroffene Person verlangt, dass diese mündlich erteilt werden.

Daraus folgt, dass die vom Verantwortlichen nach Art. 15 Abs. 3 S. 1 DS-GVO zur Verfügung zu stellende Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, alle Merkmale aufweisen muss, die es der betroffenen Person ermöglichen, ihre Rechte aus dieser Verordnung wirksam auszuüben, und diese Daten daher vollständig und originalgetreu wiedergeben muss. [...]

Um zu gewährleisten, dass die so bereitgestellten Informationen leicht verständlich sind, wie es Art. 12 Abs. 1 i.V.m. dem 58. Erwägungsgrund der DS-GVO verlangt, kann sich [...], wie der Generalanwalt in den Nrn. 57 und 58 seiner Schlussanträge ausgeführt hat, die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die u.a. personenbezogene Daten enthalten, die Gegenstand der Verarbeitung sind, als unerlässlich erweisen, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten.

Insbesondere wenn personenbezogene Daten aus anderen Daten generiert werden oder wenn sie auf freien Feldern beruhen, d.h. einer fehlenden Angabe, aus der eine Information über die betroffene Person hervorgeht, ist der Kontext, in dem diese Daten Gegenstand der Verarbeitung sind, unerlässlich, damit die betroffene Person eine transparente Auskunft und eine verständliche Darstellung dieser Daten erhalten kann.

Außerdem sollte nach Art. 15 Abs. 4 DS-GVO i.V.m. dem 63. Erwägungsgrund der DS-GVO das Recht auf Erhalt einer Kopie gemäß Abs. 3 die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen.

Daher sind, wie der Generalanwalt in Nr. 61 seiner Schlussanträge ausgeführt hat, im Fall eines Konflikts zwischen der Ausübung des Rechts auf vollständige und umfassende Auskunft über die personenbezogenen Daten zum einen und den Rechten oder Freiheiten anderer Personen zum anderen die fraglichen Rechte gegeneinander abzuwägen. Nach Möglichkeit sind Modalitäten der Übermittlung der personenbezogenen Daten zu wählen, die die Rechte oder Freiheiten anderer Personen nicht verletzen, wobei diese Erwägungen „nicht dazu führen [dürfen], dass der betroffenen Person jegliche Auskunft verweigert wird“, wie sich aus dem 63. Erwägungsgrund DS-GVO ergibt. [...]

#### Zur Vorlagefrage 4:

Mit dieser Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 3 S. 3 DS-GVO dahin auszulegen

ist, dass sich der im Sinne dieser Bestimmung verwendete Begriff „Informationen“ ausschließlich auf personenbezogene Daten bezieht, von denen der für die Verarbeitung Verantwortliche gemäß S. 1 dieses Absatzes eine Kopie zur Verfügung stellen muss, oder ob er sich auch auf alle in Abs. 1 dieses Artikels genannten Informationen bezieht oder gar darüber hinausgehende Einzelheiten wie etwa Metadaten umfasst. [...]

Insoweit beschränkt sich Art. 15 Abs. 3 S. 3 DS-GVO zwar auf den Hinweis, dass „die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen [sind]“, wenn „die betroffene Person den Antrag elektronisch [stellt]“, ohne dass erläutert wird, was unter dem Begriff „Informationen“ zu verstehen ist, doch heißt es in S. 1 dieses Absatzes: „Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.“

Somit ergibt sich aus dem Kontext von Art. 15 Abs. 3 S. 3 DS-GVO, dass die von ihm erfassten „Informationen“ zwangsläufig den personenbezogenen Daten entsprechen, von denen der für die Verarbeitung Verantwortliche gemäß S. 1 dieses Absatzes eine Kopie zur Verfügung stellen muss. [...]

### Zur Vertiefung

Peisker, *Die Kopie nach Art. 15 Abs. 3 S. 1 DS-GVO – Gedanken zur EuGH-Entscheidung in der Rs. C-487/21 = RDV 3/2023.*

Allgayer, *Die Datenschutz-Grundverordnung in der Rechtsprechung des Bundesgerichtshofs und des Bundesarbeitsgerichts = RDV 1/2023.*

Nowak/Bornholdt, *Zum Recht auf Kopie und zur rechtlichen Weite eines Anspruchs gemäß Art. 15 Abs. 3 der Datenschutz-Grundverordnung = RDV 4/2020.*

[Beschluss] *Vorlagefrage zum Anspruch gegen einen Arzt auf kostenfreie Zurverfügungstellung der Patientenakte nach Art. 15 Abs. 3 DS-GVO = RDV 4/2022.*

[Urteil] *Zur Reichweite des Auskunftsanspruchs nach Art. 15 Abs. 1 DS-GVO = RDV 4/2021.*

[Urteil] *Zum Recht auf kostenlose Kopie der juristischen Staatsprüfung = RDV 5/2021.*

## Erlöschen von ungenutzten Einwilligungserklärungen

(AG München, Urteil vom 14. Februar 2023 – 161 C 12736/22 –)

### Praxishinweis

Das Urteil befasst sich mit der zunehmend für Verantwortliche relevanten Frage, ob Einwilligungserklärungen nach der DS-GVO auch ein „Verfallsdatum“ haben können. Die DS-GVO selbst enthält hierzu keine Angaben. Die vorliegende Entscheidung setzt die derzeit wohl herrschende und vom Gericht zitierte Rechtsprechung und Rechtsauffassung in der Sache konsequent um und prüft, ob zum Zeitablauf weitere Umstände hinzutreten,

die anzeigen, dass die Einwilligung nicht mehr gültig ist. Mit Blick auf die vom Gericht zitierten Entscheidungen, die letztlich vielfach kürzere Zeiträume betreffen als den streitgegenständlichen Zeitraum, ist für die Praxis relevant, welche Leitlinien sich daraus ergeben und wann eine Aktualisierung einer einmal eingeholten Einwilligung ratsam ist.

- Nach den Umständen des Einzelfalls kann das Erlöschen einer ursprünglich erteilten Einwilligung in die Zusendung von E-Mail-Werbung anzunehmen sein. Dies ist jedenfalls dann der Fall, wenn in einem Zeitraum von vier Jahren ein Account, bei dessen Erstellung ein Newsletter abonniert wurde, nicht mehr genutzt und in Kenntnis hiervon auch keine weitere Werbung übersandt wurde. [...]**
- In einem solchen Fall muss sich der Werbende vor der neuerlichen Zusendung von E-Mail-Werbung bei dem Empfänger erkundigen, ob die ursprüngliche Einwilligung fortbesteht. [...]**

### Aus den Gründen:

Der Kläger hat gegen die Beklagte einen Anspruch auf Unterlassung der Zusendung werblicher E-Mails aus S. 823 Abs. 1 i.V.m. S. 1004 Abs. 1 S. 2 BGB analog wegen eines rechtswidrigen Eingriffs in sein allgemeines Persönlichkeitsrecht, Art. 2 Abs. 1, 1 Abs. 1 GG. [...]

b) Die Zusendung der E-Mail erfolgte ohne Einverständnis des Klägers. Die ursprünglich erteilte Einwilligung war angesichts der Umstände des Einzelfalls infolge Zeitablaufs nicht mehr wirksam.

aa) Ob und ab wann eine ursprünglich erteilte Einwilligung nicht mehr wirksam ist, ist in Rechtsprechung und Literatur umstritten und bisher nicht abschließend geklärt.

(1) Der BGH (BGH, Urt. v. 01.02.2018 – III ZR 196/17 –, juris 31) führt hierzu aus (Hervorhebungen seitens des Gerichts):

„Eine zeitliche Begrenzung einer einmal erteilten Einwilligung sieht weder die RL 2002/58/EG noch S. 7 UWG vor. Hieraus ergibt sich, dass diese – ebenso wie eine Einwilligung nach 183 BGB – grundsätzlich nicht allein durch Zeitablauf erlischt (vgl. OLG Stuttgart, BeckRS 2007, 10540; OLG Köln, GRUR-RR 2013, 219, 221; LG Berlin, BeckRS 2012, 08644; Köhler/Bornkamm/Köhler, UWG, 35. Aufl., 7 Rn. 148 und 186; jurisPK-UWG/Koch, 4. Aufl., 7 Rn. 245 und 376; Schöler, in: Harte-Bavendamm/Henning-Bodewig, UWG, 4. Aufl., 7 Rn. 243). Vor diesem Hintergrund bestehen jedenfalls gegen die gegenständliche Regelung [sic!] zur Geltungsdauer keine Bedenken, da diese eingegrenzt ist auf die Zeit während des laufenden Vertragsverhältnisses bis zu höchstens zwei Jahre ab Vertragsbeendigung und zumindest während dieses überschaubaren Zeitraums bei einem Verbraucher, der seine Einwilligung im Rahmen des Vertragsschlusses erteilt, von seinem fortbestehenden Interesse an einer Information über neue Services und Angebote der Beklagten ausgegangen werden kann (siehe auch zum Datenschutzrecht 95 Abs. 2 und Abs. 3 S. 1 TKG).“

Der BGH wendet sich also im Grundsatz gegen das Erlöschen einer Einwilligung mit Zeitablauf.

Er schränkt dies nachfolgend jedoch insoweit ein, als dass dies jedenfalls für die dort streitgegenständliche Regelung gelte, die sich auf höchstens zwei Jahre nach Vertragsbeendigung beziehe. In diesem überschaubaren Zeitraum sei bei einem Verbraucher von seinem fortbestehenden Interesse an Informationen auszugehen.

Ein Teil der instanzgerichtlichen Rechtsprechung befürwortet das Erlöschen einer Einwilligung mit der Zeit, so beispielsweise das LG München I ab einem Zeitraum von mehr als 1,5 Jahren (LG München I, Urt. v. 8. April 2010 – 17 HK O 138/10 –, juris Rz. 21), das LG Berlin bei einem Zeitraum von zwei Jahren später (LG Berlin, Beschl. v. 2. Juli 2004 – 15 O 653/03 –) und das LG Hamburg bei einem Zeitraum von zehn Jahren später (LG Hamburg, Urt. v. 17. Februar 2004 – 312 O 645/02 –, <https://openjur.de/u/30531.html>, Rz. 63).

Gegen ein Erlöschen der Einwilligung wenden sich das OLG Stuttgart (OLG Stuttgart, Urt. v. 22. März 2007 – 2 U 159/06 –, juris Rz. 34) bei einem Zeitraum von einem Jahr und drei Monaten sowie das OLG Köln bei einem Zeitraum von einem Jahr und vier Monaten (OLG Köln, Urt. v. 7. Dezember 2012 – I-6 U 69/12 –, juris Rz. 15).

(2) In der Literatur wurde die Linie des BGH aufgegriffen, nach der zwar nicht im Grundsatz, aber nach den Umständen des Einzelfalls durchaus von einem Erlöschen der Einwilligung ausgegangen werden kann.

Köhler (Köhler/Bornkamm/Feddersen, 41. Aufl. 2023, UWG S. 7 Rn. 182) hält fest, dass die Einwilligung an sich unbefristet sei und demnach nicht mit Zeitablauf erlösche. Etwas anderes könne sich jedoch aus dem mutmaßlichen Willen des Verbrauchers ergeben. Es komme auf die Umstände des Einzelfalls an, insbesondere den konkreten Zweck der Einwilligung, darauf, ob von der Einwilligung erst nach längerer Zeit Gebrauch gemacht wurde sowie darauf, ob der Werbende davon ausgehen dürfe, der Verbraucher habe noch Kenntnis von der Einwilligung und Interesse an der Kontaktaufnahme. [...]

bb) Selbst wenn man davon ausgeht, dass eine Einwilligung grundsätzlich zeitlich unbegrenzt gilt, so ist hier nach den Umständen des Einzelfalls nicht mehr von einem Fortbestehen der Einwilligung des Klägers auszugehen.

Der Kläger hatte die Newsletter der Beklagten 2015 und 2017 abonniert, seinen Account auf der Website der Beklagten aber seit Dezember 2017 nicht mehr genutzt. Seit Dezember 2017 hatte der Kläger infolge seines Austritts aus einem Golfclub keine Newsletter mehr erhalten. Der Austritt aus dem Club und die anschließende Nichtnutzung waren der Beklagten ausweislich ihrer Stellungnahme in Anlage K7 auch bekannt. Die Beklagte nahm nach eigenen Angaben in Anlage K7 erst im Dezember 2021 wieder Kontakt auf, nachdem die Kooperation mit dem Deutschen Golf Verband ausgelaufen war.

Zu berücksichtigen ist daher, dass eine ausdrückliche Einwilligung zunächst unstrittig vorlag. Das Abonnement war zunächst wohl mit einer Mitgliedschaft des Klägers in einem Golfclub gekoppelt. Diese Mitgliedschaft endete Ende 2017. Hiervon hatte die Beklagte auch Kenntnis und sandte dem Kläger entsprechend keine E-Mails mehr zu. Als sich die internen Regelungen der Beklagten Ende 2021 änderten, hatte der Kläger seit vier Jahren weder seinen Account bei der Beklagten genutzt noch E-Mails der Beklagten erhalten. Die Beklagte hatte auch keine positive Kenntnis von einer erneuten Anmeldung des Klägers für den Newsletter oder für einen weiteren mit der Beklagten verbundenen Golfclub. Vor dem

Hintergrund der erheblichen Zeit von vier Jahren sowie dem Ende der Zusendung infolge des Austritts des Klägers aus einem Golfclub durfte die Beklagte nicht davon ausgehen, die Einwilligung des Klägers bestehe fort. Sie hätte sich vielmehr zunächst erkundigen müssen, ob dies noch der Fall war (vgl. LG Berlin, Beschl. v. 2. Juli 2004 – 15 O 653/03 –).[...]

### Zur Vertiefung

*Retzbach, Die unverschlüsselte E-Mail als Gegenstand einer datenschutzrechtlichen Einwilligungserklärung = RDV 4/2022.*

*Schwartzmann/Benedikt, = Einwilligungsmanagementsysteme nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) – Lösungen und Chancen für einen fairen Online-datenschutz = RDV 5/2021.*

*[Urteil] Unzulässige Einwilligung in E-Mail-Werbung = RDV 2/2023.*

*[Urteil] Unzulässige Einwilligung bei „Cookie-Banner“ = RDV 2/2023.*

## Wichtiges aus der Rechtsprechung:

### Kein Recht auf Löschung bei Verstößen gegen Artt. 26 und 30 DS-GVO

(EuGH, Urteil vom 4. Mai 2023 – C-60/22 –)

- Art. 17 Abs. 1 Buchst. d) und Art. 18 Abs. 1 Buchst. b) der [...] [DS-GVO] sind dahin auszulegen, dass der Verstoß eines Verantwortlichen gegen die Pflichten aus den Artt. 26 und 30 dieser Verordnung über den Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung für die Verarbeitung bzw. das Führen eines Verzeichnisses von Verarbeitungstätigkeiten keine unrechtmäßige Verarbeitung darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht, weil dieser Verstoß als solcher nicht bedeutet, dass der Verantwortliche gegen den Grundsatz der „Rechenschaftspflicht“ im Sinne von Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchst. a) und Art. 6 Abs. 1 UAbs. 1 dieser Verordnung verstößt.**
- Das Unionsrecht ist dahin auszulegen, dass dann, wenn ein für die Verarbeitung personenbezogener Daten Verantwortlicher gegen seine Pflichten aus den Artt. 26 oder 30 der [...] [DS-GVO] verstoßen hat, die Einwilligung der betroffenen Person keine Voraussetzung dafür darstellt, dass die Berücksichtigung dieser Daten durch ein nationales Gericht rechtmäßig ist.**

### Zu den Vorlagefragen:

#### Zur ersten Vorlagefrage:

Mit seiner ersten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 17 Abs. 1 Buchst. d) und Art. 18 Abs. 1 Buchst. b) der DS-GVO dahin auszulegen sind, dass der Verstoß eines Verantwortlichen gegen die Pflichten aus den

Artt. 26 und 30 dieser Verordnung über den Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung für die Verarbeitung bzw. das Führen eines Verzeichnisses von Verarbeitungstätigkeiten eine unrechtmäßige Verarbeitung darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht, weil ein solcher Verstoß bedeutet, dass der Verantwortliche gegen den Grundsatz der „Rechenschaftspflicht“ des Art. 5 Abs. 2 der DS-GVO verstößt. [...]

Nach dem Wortlaut von Abs. 2 des Art. 5 der DS-GVO ist der Verantwortliche nach dem in dieser Bestimmung verankerten Grundsatz der „Rechenschaftspflicht“ für die Einhaltung des Abs. 1 dieses Artikels verantwortlich und muss nachweisen können, dass jeder der dort genannten Grundsätze eingehalten worden ist; mithin obliegt ihm hierfür die Beweislast (vgl. in diesem Sinne Urt. v. 24. Februar 2022, Valsts ierņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C 175/20, EU:C:2022:124, Rn. 77, 78 und 81).

Hieraus folgt, dass der Verantwortliche nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchst. a) der DS-GVO sicherstellen muss, dass die von ihm durchgeführte Datenverarbeitung „rechtmäßig“ ist.

Die Rechtmäßigkeit der Verarbeitung wird aber, wie sich aus der Überschrift von Art. 6 der DS-GVO selbst ergibt, gerade in ebendiesem Artikel geregelt. Dieser sieht vor, dass die Verarbeitung nur rechtmäßig ist, wenn mindestens eine der in seinem Abs. 1 UAbs. 1 Buchst. a) bis f) aufgeführten Bedingungen erfüllt ist [...].

In Übereinstimmung mit allen Regierungen, die schriftliche Erklärungen abgegeben haben, sowie mit der Europäischen Kommission ist jedoch festzustellen, dass die Einhaltung der in Art. 26 der DS-GVO vorgesehenen Pflicht zum Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung und der in Art. 30 dieser Verordnung verankerten Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, nicht zu den in Art. 6 Abs. 1 UAbs. 1 genannten Gründen für die Rechtmäßigkeit der Verarbeitung zählen.

Darüber hinaus besteht das Ziel der Artt. 26 und 30 der DS-GVO im Unterschied zu den Artt. 7 bis 11 dieser Verordnung nicht darin, den Umfang der in Art. 5 Abs. 1 Buchst. a) und Art. 6 Abs. 1 der Verordnung genannten Anforderungen näher zu bestimmen.

Daher lässt sich aus dem Wortlaut von Art. 5 Abs. 1 Buchst. a) und Art. 6 Abs. 1 UAbs. 1 der DS-GVO ableiten, dass ein Verstoß des Verarbeiters gegen die in den Artt. 26 und 30 dieser Verordnung vorgesehenen Pflichten keine „unrechtmäßige Verarbeitung“ im Sinne von Art. 17 Abs. 1 Buchst. d) und Art. 18 Abs. 1 Buchst. b) der Verordnung darstellt, die sich aus einem Verstoß des Verarbeiters gegen den in Art. 5 Abs. 2 der DS-GVO genannten Grundsatz der „Rechenschaftspflicht“ ergeben würde.

Diese Auslegung wird zweitens durch den Kontext dieser verschiedenen Bestimmungen untermauert. Aus der Struktur der DS-GVO und mithin aus ihrer Systematik geht nämlich eindeutig hervor, dass sie zum einen zwischen den „Grundsätzen“, die in ihrem Kapitel II, das u.a. die Artt. 5 und 6 dieser Verordnung umfasst, geregelt werden, und zum anderen den „allgemeinen Pflichten“ unterscheidet, die zu Abschnitt 1 des Kapitels IV der Verordnung gehören, das die Verantwort-

lichen betrifft; zu diesen Pflichten zählen die Pflichten nach den Artt. 26 und 30 ebendieser Verordnung. [...]

Drittens wird schließlich die [...] dargelegte wörtliche Auslegung der DS-GVO durch das mit dieser Verordnung verfolgte Ziel bestätigt, das sich aus ihrem Art. 1 sowie ihren Erwägungsgründen 1 und 10 ergibt. Es besteht insbesondere darin, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres in Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union und in Art. 16 Abs. 1 AEUV verankerten Rechts auf Privatleben – bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. in diesem Sinne Urt. v. 1. August 2022, Vyriausioji tarnybinės etikos komisija, C 184/20, EU:C:2022:601, Rn. 125 und die dort angeführte Rechtsprechung).

Das Fehlen einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung nach Art. 26 der DS-GVO oder eines Verzeichnisses von Verarbeitungstätigkeiten im Sinne von Art. 30 dieser Verordnung reicht nämlich für sich genommen nicht aus, um nachzuweisen, dass ein Verstoß gegen das Grundrecht auf den Schutz personenbezogener Daten vorliegt. Insbesondere stellen zwar, wie aus den Erwägungsgründen 79 und 82 der DS-GVO hervorgeht, die klare Aufteilung der Verantwortlichkeiten zwischen den gemeinsam Verantwortlichen und das Verzeichnis von Verarbeitungstätigkeiten Mittel dar, um sicherzustellen, dass die Verantwortlichen die von dieser Verordnung vorgesehenen Garantien für den Schutz der Rechte und Grundfreiheiten der betroffenen Personen wahren. Gleichwohl belegt das Fehlen eines solchen Verzeichnisses oder einer solchen Vereinbarung für sich genommen nicht, dass diese Rechte und Grundfreiheiten verletzt wurden.

Hieraus ergibt sich, dass ein Verstoß gegen die Artt. 26 und 30 der DS-GVO durch den Verantwortlichen keine „unrechtmäßige Verarbeitung“ im Sinne von Art. 17 Abs. 1 Buchst. d) oder Art. 18 Abs. 1 Buchst. b) dieser Verordnung i.V.m. ihren Art. 5 Abs. 1 Buchst. a) und Art. 6 Abs. 1 UAbs. 1 darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung gewährt.

### Zur dritten Vorlagefrage:

Mit seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob das Unionsrecht dahin auszulegen ist, dass dann, wenn ein für die Verarbeitung personenbezogener Daten Verantwortlicher gegen seine Pflichten aus den Artt. 26 oder 30 der DS-GVO verstoßen hat, die Einwilligung der betroffenen Person die Voraussetzung dafür darstellt, dass die Berücksichtigung dieser Daten durch ein nationales Gericht rechtmäßig ist. [...]

Wenn ein Gericht die ihm durch das nationale Recht übertragenen gerichtlichen Befugnisse ausübt, ist davon auszugehen, dass die von diesem Gericht durchzuführende Verarbeitung personenbezogener Daten für den in Art. 6 Abs. 1 UAbs. 1 Buchst. e) der DS-GVO genannten Zweck – Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde – erforderlich ist.

Da es zum einen ausreicht, dass eine der in Art. 6 Abs. 1 der DS-GVO aufgestellten Voraussetzungen erfüllt ist, damit eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann und zum anderen [...] ein Verstoß

gegen die Artt. 26 und 30 der DS-GVO keine unrechtmäßige Verarbeitung darstellt, ist die Einwilligung der betroffenen Person nicht Voraussetzung dafür, dass die Berücksichtigung personenbezogener Daten, die vom Bundesamt unter Verstoß gegen die in den letztgenannten Bestimmungen vorgesehenen Pflichten verarbeitet worden sein sollen, durch das vorliegende Gericht rechtmäßig ist.

## Kein Personenbezug bei fehlenden Mitteln des Datenempfängers zur Re-Identifizierung

(EuG, Urteil vom 26. April 2023 – T-557/20 –)

- 1. Sichtweisen und persönliche Meinungen stellen nicht per se personenbezogene Daten dar. Es ist vielmehr im Einzelfall zu prüfen, ob sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sind.**
- 2. Werden pseudonymisierte Informationen an Dritte übermittelt, handelt es sich aus Sicht des Empfängers nur dann um personenbezogene Daten, wenn der Datenempfänger über Mittel verfügt, die betroffenen Personen zu re-identifizieren. Eine solche Identifizierbarkeit ist insbesondere dann abzulehnen, wenn die Identifizierung der betreffenden Person aus Sicht des Datenempfängers gesetzlich verboten oder praktisch nicht durchführbar ist.**

*(Nicht amtliche Leitsätze)*

### Zur Begründetheit:

Art. 3 Nr. 1 der Verordnung 2018/1725 bestimmt den Begriff personenbezogene Daten als „alle Informationen[,] die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen[, wobei] als identifizierbar ... eine natürliche Person angesehen [wird], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Gemäß dieser Begriffsbestimmung sind Informationen u.a. dann personenbezogene Daten, wenn zwei kumulative Voraussetzungen erfüllt sind, nämlich zum einen die, dass sich diese Informationen auf eine natürliche Person „beziehen“, und zum anderen, dass dies eine „identifizierte oder identifizierbare“ Person ist. [...]

Zur Voraussetzung nach Art. 3 Nr. 1 der Verordnung 2018/1725, wonach die Informationen sich auf eine natürliche Person „beziehen“ müssen

Nach der Rechtsprechung kommt in der Verwendung des Ausdrucks „alle Informationen“ im Zusammenhang mit der Bestimmung des Begriffs „personenbezogene Daten“ in Art. 3 Nr. 1 der Verordnung 2018/1725 das Ziel des Unionsgesetzgebers zum Ausdruck, diesem Begriff eine weite Bedeutung beizumessen. Er ist nicht auf sensible oder private Infor-

mationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen „über“ die in Rede stehende Person handelt (vgl. entsprechend Ur. v. 20. Dezember 2017, Nowak, C 434/16, EU:C:2017:994, Rn. 34).

Was diese letztgenannte Voraussetzung betrifft, so hat der Gerichtshof entschieden, dass sie erfüllt ist, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (Ur. v. 20. Dezember 2017, Nowak, C 434/16, EU:C:2017:994, Rn. 35).

In der überarbeiteten Entscheidung hat der EDSB aber weder den Inhalt noch den Zweck noch die Auswirkungen der an Deloitte übermittelten Informationen geprüft.

Vielmehr hat er sich auf den Hinweis beschränkt, dass die von den Beschwerdeführern während der Konsultationsphase eingereichten Stellungnahmen deren Meinungen oder Sichtweisen widerspiegeln, und kam allein auf dieser Grundlage zu dem Ergebnis, dass es sich bei den Stellungnahmen um Informationen über diese Personen handele, was für ihre Einstufung als personenbezogene Daten ausreiche. [...]

Zwar kann nicht ausgeschlossen werden, dass persönliche Sichtweisen oder Meinungen personenbezogene Daten darstellen. Doch aus [...] [dem Urteil des EuGH] vom 20. Dezember 2017, Nowak (C 434/16, EU:C:2017:994), geht hervor, dass eine solche Stellungnahme nicht auf eine Annahme wie die oben [...] beschriebene gestützt werden darf, sondern auf der Prüfung beruhen muss, anhand deren bestimmt werden soll, ob eine Sichtweise aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist. [...]

Zur Voraussetzung nach Art. 3 Nr. 1 der Verordnung 2018/1725, wonach die Informationen sich auf eine „identifizierte oder identifizierbare“ natürliche Person“ beziehen müssen. Gemäß dieser Vorschrift wird als „identifizierbare natürliche Person“ eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann. [...]

Da der 16. Erwägungsgrund der Verordnung 2018/1725 auf die Mittel Bezug nimmt, die vernünftigerweise entweder von dem Verantwortlichen oder von einem „Dritten“ eingesetzt werden könnten, ist sein Wortlaut ein Indiz dafür, dass es für die Einstufung eines Datums als „personenbezogenes Datum“ im Sinne von Art. 3 Nr. 1 der Verordnung 2018/1725 nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden (vgl. entsprechend Ur. v. 19. Oktober 2016, Breyer, C 582/14, EU:C:2016:779, Rn. 43).

Der Gerichtshof führte jedoch weiter aus, dass der Umstand, dass über die zur Identifizierung des Nutzers einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten verfügt, sondern der Internetzugangsanbieter dieses Nutzers, daher nicht ausschließen vermag, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn personenbezogene Daten darstellen (Ur. v. 19. Oktober 2016, Breyer, C 582/14, EU:C:2016:779, Rn. 44).

Zu prüfen war nach Auffassung des Gerichtshofs jedoch, ob die Möglichkeit, eine dynamische IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfügt, ein Mittel darstellt, das vernünftigerweise zur Bestim-

mung der betreffenden Person eingesetzt werden kann (Urt. v. 19. Oktober 2016, Breyer, C 582/14, EU:C:2016:779, Rn. 45).

Der Gerichtshof wies darauf hin, dass dies nicht der Fall gewesen wäre, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar gewesen wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordert hätte, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschienen wäre (Urt. v. 19. Oktober 2016, Breyer, C 582/14, EU:C:2016:779, Rn. 46). [...]

Wie der EDSB [...] ausführlich, schließt die Tatsache, dass nicht Deloitte, sondern der SRB über die zur Identifizierung der Verfasser der während der Konsultationsphase abgegebenen Stellungnahmen erforderlichen zusätzlichen Informationen verfügte, zwar nicht von vornherein aus, dass es sich bei den an Deloitte übermittelten Informationen für Deloitte um personenbezogene Daten handelte.

Doch geht aus dem Urt. v. 19. Oktober 2016, Breyer (C 582/14, EU:C:2016:779), auch hervor, dass für die Bestimmung, ob es sich bei den an Deloitte übermittelten Informationen um personenbezogene Daten handelte, auf das Verständnis abzustellen ist, das Deloitte bei der Bestimmung der Frage hatte, ob die ihr übermittelten Informationen sich auf „identifizierbare Personen“ beziehen. [...]

Somit war es gemäß [...] des Urt. v. 19. Oktober 2016, Breyer (C 582/14, EU:C:2016:779), Sache des EDSB, zu prüfen, ob für Deloitte die an sie übermittelten Stellungnahmen personenbezogene Daten waren. [...]

Somit durfte der EDSB, weil er nicht geprüft hat, ob Deloitte das Recht hatte, auf die für die Rückidentifizierung der Verfasser der Stellungnahmen erforderlichen zusätzlichen Informationen zuzugreifen, und ob dieser Zugriff auch praktisch durchführbar war, nicht zu dem Ergebnis gelangen, dass die an Deloitte übermittelten Informationen sich auf eine „identifizierbare natürliche Person“ im Sinne von Art. 3 Nr. 1 der Verordnung 2018/1725 beziehen.

## Anmerkung zum EuG-Urteil

Die Entscheidung nimmt zur Frage der anonymisierenden Wirkung einer Pseudonymisierung Stellung und bejaht diese Möglichkeit im Ergebnis grundsätzlich. Das Gericht der Europäischen Union (EuG) ist ein eigenständiges europäisches Gericht, das dem Europäischen Gerichtshof (EuGH) nachgeordnet ist, und unter anderem für direkte Klagen natürlicher oder juristischer Personen gegen Maßnahmen oder Unterlassen von Maßnahmen der Gemeinschaftsorgane zuständig ist.

### 1. Bedeutung der Entscheidung für die Datenschutzpraxis

Die Entscheidung ergeht zu einer Entscheidung des europäischen Datenschutzbeauftragten (EDSB) gegen eine europäische Behörde. Rechtsentscheidend sind daher hauptsächlich Bestimmungen der Verordnung (EU) 2018/1725, die nach deren Art. 2 Abs. 1 für die Verarbeitung personenbezogener Daten durch alle Organe und Einrichtungen der Union gilt. Sie geht als speziellere Norm der DS-GVO vor und ersetzt die dort noch in Art. 2 Abs. 3 genannte Verordnung (EG) Nr. 45/2001. Die DS-GVO sieht ihrerseits die Anpassung der Ver-

ordnung (EG) Nr. 45/2001 vor, um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu gewährleisten.

Zwar nimmt die Entscheidung nicht direkt zu Bestimmungen der DS-GVO Stellung, sie ist dennoch inhaltlich von Bedeutung, da die streitentscheidenden Normen der Verordnung (EU) 2018/1725 wortgleich zu den entsprechenden Normen der DS-GVO sind. Ohnehin diene die DS-GVO der Verordnung (EU) 2018/1725 in Inhalt und Wortlaut als Vorbild, was eine reibungslose parallele Anwendung der Normen ermöglichen sollte (Erwägungsgrund 4 VO 2018/1725). Insbesondere wortgleich sind die Begriffsdefinitionen „personenbezogene Daten“ in Art. 3 Nr. 1 VO 2018/1725 respektive Art. 4 Nr. 1 DS-GVO und „Pseudonymisierung“ in Art. 3 Nr. 6 VO 2018/1725 respektive Art. 4 Nr. 5 DS-GVO. Wortgleich sind auch Erwägungsgrund 16 VO 2018/1725 und Erwägungsgrund 26 DS-GVO, die die Relativität des Personenbezugs betreffen und klarstellen, dass die jeweiligen Verordnungen keine anonymen Daten betreffen.

Die Entscheidung setzt sich auch ausführlich mit der Breyer-Entscheidung des EuGH auseinander (ECLI:EU:C:2016:779 = RDV 6/2016), die wesentliche Hinweise für die grundrechtskonforme Auslegung von unionalen Datenschutzbestimmungen enthält und auch zum Begriff des Personenbezugs Stellung nimmt [Rn. 88 ff.]. Auch wenn sich jenes Urteil noch auf die Datenschutz-Richtlinie (RL 1995/46/EG – DS-RL) bezog, haben die dort getroffenen Erwägungen Gewicht, insbesondere weil die Definition in Art. 2 lit. a DS-RL sowie Erwägungsgrund 26 fast wortgleich in die DS-GVO respektive die VO 2018/1725 übernommen worden sind.

## 2. Anonymisierende Wirkung der Pseudonymisierung

### a) Pseudonymisieren

Pseudonymisieren ist nach Art. 3 Nr. 6 VO 2018/1725 respektive Art. 4 Nr. 5 DS-GVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Fraglich ist insbesondere, ob eine Pseudonymisierung durch einen Verarbeiter für einen Dritten eine anonymisierende Wirkung hat, so dass die Daten an jenen übermittelt werden können. Anonyme oder anonymisierte Daten unterliegen nicht (mehr) der VO 2018/1725, der DS-GVO oder den Datenschutzgesetzen des Bundes und der Länder. Der EuG bejaht diese Möglichkeit in der vorliegenden Entscheidung i.E. grundsätzlich. Der EuG nimmt damit insbesondere die Aufsichtsbehörde, aber auch Verarbeiter in die Pflicht, zu prüfen, ob die an Dritte übermittelten pseudonymisierten Daten für den Dritten tatsächlich personenbeziehbar sind [Rn. 100].

Die anonymisierende Wirkung der Pseudonymisierung ist nicht unumstritten. Nach einem Teil der Literatur soll Pseudonymisierung keinen Einfluss auf die Personenbeziehbarkeit eines Datums haben (Eckhardt/Kramer, DuD 2013, 287 (288 f.); Karg, DuD 2015, 520 (521 f.); PDK Hessen § 2 Rn. 17; Schild, in: BeckOK DatenschutzR, 42. Ed. 01.11.2022, DS-GVO, Art. 4, Rn. 77; Ernst, in: Paal/Pauly, DS-GVO/BDSC, 3. Aufl 2021, Art. 4 Rn. 40;

Piltz, K&R 2016, 557 (562); Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Rn. 26 ff., 31.; nach Weichert, in: Däubler/Wedde/Weichert/Sommer, EU-DS-GVO und BDSG, 2. Aufl. 2020, Art. 4 Rn. 80, soll die Datenverarbeitung weiterhin der DS-GVO unterliegen soll, wenn die Re-Identifizierung nicht absolut ausgeschlossen ist). Pseudonymisierung sei bestenfalls eine technisch-organisatorische Maßnahme zum Schutz der weiterhin personenbezogenen Daten (Karg, DuD 2015, 520 (521f.); Albrecht/Jotzo, DatenschutzR, 2017, Teil 3, Rn. 4, Teil 5, Rn. 8).

Die zutreffende herrschende Meinung liegt jedoch auf der Argumentationslinie des EuGH. Nach ihr kann einer Pseudonymisierung eine anonymisierende Wirkung gegenüber Dritten zukommen (mit weiteren Nennungen, insb. zum BDSG aF, Ziebarth, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 2022, Art. 4 Rn. 97 f.; s.a. Bischoff, PharmR 2020, 309 (314); Roßnagel, ZD 2018, 243 (245f.); Eßer, in: Eßer/Kramer/Lewinski (Hrsg.), DS-GVO/BDSG, 7. Aufl. 2020, Art. 4, Rn. 71; Gierschmann, ZD 2021, 482 (483); Hofmann/Johannes, ZD 2017, 221 (224); Johannes, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, § 7 Rn. 249; Johannes/Geminn MedR 2023, 368; Pötters, in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 89 Rn. 13). Die Bewertung der Anonymität bestimmter Daten ist dann vom konkreten Verarbeitungskontext abhängig. Zunächst darf der Dritte die Zuordnungsregel nicht kennen. Außerdem darf er nicht über Zusatzwissen verfügen, die eine Re-Identifizierung zuließe.

Dies liegt im Einklang mit Breyer-Entscheidung des EuGH, zu der der EuGH in der vorliegenden Entscheidung ausführlich Stellung nimmt und sichtlich bemüht ist Einklang herzustellen. In jener Entscheidung hatte der EuGH allgemein festgestellt, dass das Wissen anderer Personen oder Stellen für den Verantwortlichen ein Mittel darstellt, das dieser „vernünftigerweise“ zur Bestimmung der betreffenden Person einsetzen kann, wenn er über rechtliche Möglichkeiten verfügt, um an das identifizierende Zusatzwissen zu gelangen. Ein Mittel kann dagegen nicht „vernünftigerweise“ zur Bestimmung einer natürlichen Person eingesetzt werden, wenn die Identifizierung der Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung de facto vernachlässigbar erschiene (s.a. Johannes/Geminn MedR 2023, 368).

Für die Feststellung einer Identifizierbarkeit der betroffenen Person ist nach Art. 3 Nr. 1 VO 2018/1725 respektive Art. 4 Nr. 1 DS-GVO zufolge maßgeblich, ob die vorhandene Information als solche bereits für eine Identifizierung ausreicht oder ob die Heranziehung oder Verknüpfung weiterer Informationen zur Bestimmung erforderlich ist. Hierbei sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffene Person zu identifizieren.

## b) Risikoprognose zur Re-Identifizierung

Ob eine Pseudonymisierung daher für Dritte eine anonymisierende Wirkung hat hängt also davon ab, ob der Dritte – als potenzieller weiterer Verantwortlicher – mittels der ihm zur Verfügung stehenden Mittel, Kenntnisse und Möglichkeiten die (Re-)Identifikation vornehmen kann. Die muss im Wege einer Risikoprognose bewertet werden. Diese muss sowohl das Interesse möglicher Datenverarbeiter als auch die von ihnen mobilisierbaren Mittel der Zuordnung berücksichtigen

(siehe auch Schwartmann/Jaspers/Lepperhof/Weiß/Meier, Praxisleitfaden für die Anonymisierung personenbezogener Daten, 2022). Die Zuordnung der Daten zu einer identifizierbaren Person muss im Verhältnis zu dem dazu notwendigen Aufwand so unverhältnismäßig sein, dass eine Identifizierung nach allgemeiner Lebenserfahrung oder dem Stand der Wissenschaft und Technik nicht zu erwarten ist. Dabei muss das vorhandene oder erwerbbar Zusatzwissen des Verantwortlichen, die aktuelle und künftige technische Möglichkeiten der Verarbeitung sowie der mögliche Aufwand und die verfügbare Zeit berücksichtigt werden. Eine absolut sichere Unmöglichkeit der Zuordnung ist nicht erforderlich (siehe zum Beispiel. Art. 29-Datenschutzgruppe, Stellungnahme 5/2014 vom 10.04.2014, WP 216, S. 10; Gola, in: Gola/Heckmann, DS-GVO/BDSG, 3. Aufl. 2022, Art. 4 Rn. 40; Ziebarth, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 2022, Art. 4 Rn. 97 f.; Husemann, in: Roßnagel (Hrsg.), Das neue Datenschutzrecht, 2018, § 3 Rn. 7; Roßnagel, in: Roßnagel (Hrsg.), HDSIG, 2021, § 2 Rn. 40 ff.; Roßnagel/Scholz, MMR 2000, 721 (723 f.).

Eine Risikoprognose muss die Gesamtumstände bewerten. Entscheidend kommt es auf das Wissen und die dem empfangendem Dritten zur Verfügung stehenden Mittel an. Das Risiko einer Re-Identifizierung lässt sich auch nie vollständig ausschließen. Aufdeckungen des Personenbezugs lassen sich insbesondere dann nicht ausschließen, wenn die Daten vielen Verantwortlichen mit unterschiedlichem mobilisierbarem Zusatzwissen zur Verfügung stehen und langfristig aufbewahrt und damit dem künftigen technischen Fortschritt ausgesetzt sein werden. Wenn ausreichendes Vertrauen in die Anonymisierung und damit in die wesentliche Voraussetzung gerade auch für das Trainieren, Testen und Evaluieren von KI-Systemen erreicht werden soll, müssen ergänzende – insbesondere rechtliche – Maßnahmen in die Beständigkeit der Anonymität ergriffen werden (Roßnagel/Geminn, ZD 2019, 487 (488), Johannes/Geminn, MedR 2023, 368).

Tatsachen, die für eine anonymisierende Wirkung der Pseudonymisierung sprechen sind u.a.:

- Den zu übermittelten Daten ist keine Information zur Identifizierung inhärent. Zum Beispiel sind Porträtaufnahmen, biometrische oder genetische Daten in der Regel eindeutig und aussagekräftig genug, um eine Person individualisierbar zu machen und zu identifizieren.
- Der Dritte hat auch keine tatsächliche Möglichkeit zur Einsichtnahme der Daten bei dem pseudonymisierenden Verarbeiter, insbesondere nicht über die verwendeten IT-Anwendungen.
- Randomisierte Pseudonyme ermöglichen einen schwereren Rückschluss auf eine natürliche Person.
- Die Pseudonyme sind keiner anderen Stelle bekannt. So ist das Risiko einer Re-Identifizierung größer, je mehr Verarbeiter das Pseudonym einer bestimmten Person zuordnen können oder auch nur kennen. Das Risiko ist auch größer, je weiter verbreitet der pseudonymisierte Datensatz ist.
- Die Pseudonyme wurden vor Übermittlung an den Dritten vom Verarbeiter verschlüsselt, so dass der Dritte nur die verschlüsselten Pseudonyme kennen würde.
- Der Dritte verfügt auch über keine rechtlichen Mittel, an das Wissen zu den Pseudonymen zu gelangen. Es dürften, anders als zum Beispiel in der Breyer-Entscheidung

zu IP-Adressen, keine gesetzlichen oder vertraglichen Auskunftsrechte gegenüber dem Verarbeiter oder Dritten bestehen, die eine Re-Identifizierung ermöglichen.

- Die Informationen zum Pseudonym unterliegen beim pseudonymisierenden Verarbeiter einer berufsrechtlichen Geheimhaltungspflicht.
- Zu berücksichtigen sind auch spezifische organisatorische Maßnahmen zur Wahrung der Interessen der betroffenen Person, die auch darauf abzielen das Risiko einer Re-Identifizierung weiter zu verringern. Konkrete Beispiele für Maßnahmen, die ein entsprechender Verarbeiter treffen könnte und mit einem Dritten vereinbaren könnte und die für eine Anonymität der pseudonymisierten Daten bei dem Dritten streiten würden sind zum Beispiel:
  - die Verpflichtung von Mitarbeitern auf Wahrung von Geschäftsgeheimnissen und Datenschutz, die auch die Re-Identifizierung und ungenehmigte Weitergabe anonymisierter Daten umfassen;
  - die Prüfung der an den Dritten übermittelten Daten durch den Dritten bei Eingang darauf, dass identifizierende Merkmale durch den übermittelnden Verarbeiter entfernt wurden;
  - die Einschaltung eines Datentreuhänders oder Datenvermittlungsdienstes, der Zuordnungsschlüssel für Verarbeiter und Dritte verwaltet, die Qualität der Anonymisierung prüft und ggf. nicht benötigte identifizierende Merkmale entfernt und
  - konkrete weitere Maßnahmen zur Anonymisierung der Datensätze bei Verarbeiter und/oder Dritten (auch nach Übermittlung), ggf. schrittweise oder nach bestimmten Fristablauf, zum Beispiel durch Löschung der ID zur Übernahme in KI-Trainingsdaten, Verschleierung oder Löschung von Metadaten zur Herkunft und Eingangszeitpunkt.

### 3. Fazit

Das Konzept der anonymisierenden Wirkung der Pseudonymisierung verbreitet in der Praxis mitunter große Unsicherheit. Dies folgt aus der Komplexität der Konstruktion und dem seit langem bestehendem Streit um das Konzept an sich. Bezogen auf die anonymisierende Wirkung der Pseudonymisierung bestehen wirksame Instrumente in Form von technischen und organisatorischen Maßnahmen, um die verbleibenden Risiken zu adressieren können. Auch im Kontext der Anonymisierung geht es nicht um eine Reduktion bestehender Risiken auf null. Ein Restrisiko der Re-Identifizierung besteht hier wie da, insbesondere mit Blick auf möglicherweise in der Zukunft entstehende Auswertungsmethoden (Johannes/Geminn, MedR 2023, 368, 372).

Bisher finden sich in der Judikatur nur wenig vergleichbare Fälle oder Entscheidungen, die im Anwendungsbereich der DS-GVO spielen (vgl. z.B. VG Hamburg, ZD 2023, 300 m. Anm. Petri). Es ist davon auszugehen, dass sich das zukünftig ändern wird, da die Weitergabe von pseudonymisierten Daten ein verbreitetes Phänomen der Datenwirtschaft ist und sich nicht alle diese Weitergaben durch eine Auftragsverarbeitung lösen las-

sen können. Die vorliegende Entscheidung des EuG gibt einen Hinweis darauf, wie diese Konstellationen zu bewerten sind: Nicht mittels pauschalierter Bewertungen, sondern durch einzelfallbezogene Prüfungen und Risikobewertungen.

*(Paul C. Johannes, LL.M.)*

## Ein Schmerzensgeldanspruch setzt keine objektiv nachvollziehbare Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht voraus

(OLG Hamm, Urteil vom 20. Januar 2023 – 11 U 88/22 –)

1. Der Eintritt eines immateriellen Schadens setzt nicht voraus, dass dem Betroffenen durch den Verstoß gegen die DS-GVO ein spürbarer Nachteil entstanden ist oder es zu einer objektiv nachvollziehbaren Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht gekommen ist.
2. Ausgehend von diesem Begriff des immateriellen Schadens entsteht ein solcher schon dadurch, dass personenbezogene Daten offenbart werden und die betroffene Person dadurch die Kontrolle über die gegenüber Dritten offenbarten Daten verliert.

*(Nicht amtliche Leitsätze)*

### Aus den Gründen:

1. Die Beklagte haftet dem Kläger aus Art. 82 Abs. 1 DS-GVO. [...]
  - aa) Es liegt ein Verstoß gegen Art. 5 Abs. 1 Buchst. a) DS-GVO vor.

Danach müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Die Verarbeitung der personenbezogenen Daten des Klägers, die in ihrem Versand als Anhang zu der E-Mail an deren Empfänger zu erblicken ist, und damit ihre Offenlegung gegenüber Dritten war rechtswidrig. Denn die Verarbeitung ist nach Art. 6 Abs. 1 UAbs. 1 DS-GVO nur rechtmäßig, wenn mindestens eine der dort genannten Bedingungen erfüllt ist. Dies ist hier nicht ersichtlich. Weder lag eine Einwilligung des Klägers im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. a) DS-GVO vor, noch war die Verarbeitung in Gestalt der Übermittlung als Anhang zu der E-Mail für einen der in Art. 6 Abs. 1 UAbs. 1 Buchst. b) bis f) DS-GVO genannten Zwecke erforderlich.

- bb) Es liegt auch ein Verstoß gegen Art. 5 Abs. 1 Buchst. f) DS-GVO vor. [...]

Die Vorschrift stellt auf eine angemessene Sicherheit personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen ab. Nach Erwägungsgrund 39 S. 12 zur DS-GVO gehört hierzu unter anderem auch, dass unbefugte Personen weder Zugang zu den Daten noch zu den Geräten haben, mit denen sie verarbeitet werden [...].

Die von der Beklagten in zweiter Instanz vorgetragene und vom Kläger nicht bestrittene Tatsache zu den Abläufen im Zusammenhang mit dem Versand der E-Mail vom 18.08.2021 machen deutlich, dass die Beklagte die diesbezüglichen Anforderungen grundsätzlich beachtet hat, da die entsprechenden Daten der Terminbuchungen nur von bestimmten Personen eingesehen, bearbeitet und nur auf bestimmten Geräten gespeichert werden durften. Außerdem wurde, wie von Seiten der Beklagten im Senatstermin am 09.12.2022 noch einmal glaubhaft dargestellt, ein Vier-Augen-Prinzip praktiziert, mit dem einem Missbrauch von personenbezogenen Daten und auch unbeabsichtigten Fehlern bei der Datenverarbeitung entgegengewirkt werden konnte.

Dennoch war die konkrete Datenverarbeitung nicht ausreichend abgesichert, weil der Versand der E-Mails von den beiden damit befassten Mitarbeitern mit der versehentlich nicht entfernten, unverschlüsselten Excel-Datei erfolgte, die den Empfängern nicht zu offenbarende personenbezogene Daten Dritter enthielt. Diese Verarbeitung bewirkte einen unbeabsichtigten Datenschutzverstoß, der bereits eine Verletzung des Art. 5 Abs. 1 Buchst. f) DS-GVO darstellt. [...]

cc) Zudem liegt ein Verstoß gegen Art. 9 Abs. 1 DS-GVO vor. [...]

Gesundheitsdaten sind hier die Informationen über die Anzahl der Impfungen und den vorgesehenen Impfstoff. [...]

Eine Ausnahme im Sinne von Art. 9 Abs. 2 DS-GVO greift vorliegend nicht ein. Weder lag eine Einwilligung des Klägers im Sinne von Art. 9 Abs. 2 Buchst. a) DS-GVO vor, noch war die Verarbeitung in Gestalt der Übermittlung als Anhang zu der E-Mail für einen der in Art. 9 Abs. 2 Buchst. b) bis j) DS-GVO genannten Zwecke erforderlich.

dd) Ob auch ein Verstoß gegen Art. 32 Abs. 1 DS-GVO gegeben ist, den das Landgericht bejaht hat, kann der Senat offen lassen. Ein eventueller Verstoß hätte ein geringes Gewicht und viele neben den Verstößen gegen Art. 5 Abs. 1 Buchst. a) und f) und 9 Abs. 1 DS-GVO nicht ins Gewicht. [...]

Wie bereits ausgeführt, hat die Beklagte Maßnahmen zur Einhaltung der Anforderungen des Datenschutzes bei der Datenverarbeitung in ihrem Impfzentrum getroffen, die grundsätzlich geeignet waren, personenbezogene Daten vor einem unbefugten Zugriff, unrechtmäßiger Verarbeitung und auch unbeabsichtigten Pflichtverletzungen zu schützen. So erfolgte die Verarbeitung durch eine begrenzte Anzahl eingewiesener Mitarbeiter allein auf dienstlichen Computern nach dem beschriebenen Vier-Augen-Prinzip.

Ob es dann letztlich, um den an die Integrität und Vertraulichkeit der zu bearbeitenden Daten gem. Art. 32 DS-GVO zu stellenden Anforderungen zu genügen, noch der Anweisung bedurft hätte, (Excel-)Dateien mit personenbezogenen Daten mit einem Passwortschutz zu versehen, bedarf keiner abschließenden Bewertung. Nähme man einen Verstoß an, fiel er bei dem im vorliegenden Fall zu beurteilenden Datenschutzverstoß nicht erheblich ins Gewicht.

Die in Frage stehende Excel-Datei musste kurzzeitig erstellt werden, um die E-Mail-Adressen der Impfwilligen zu ermitteln, die von den geänderten Öffnungszeiten des Impfzentrums betroffen waren und deswegen informiert werden sollten. [...] Dass bei der Erledigung dieser Aufgabe eine Situation entstand, in der es zum versehentlichen Versand der Datei als E-Mail-Anhang kommen konnte, in dem der streitgegenständliche Datenschutzverstoß liegt, ist nach den auch insoweit glaub-

haften Angaben der Beklagten den bei der Bearbeitung auftretenden technischen Schwierigkeiten geschuldet. Diese führten dazu, dass die Excel-Datei mit einem anderen Rechner, als dem Rechner, mit dem sie erstellt worden war, bearbeitet werden musste und deswegen als E-Mail-Anhang zunächst verschickt wurde, um E-Mail und Excel-Datei an einem anderen Rechner bearbeiten zu können. Dass diese nur für einen kurzen Zeitraum benötigte Excel-Datei, die an sich auch nicht als E-Mail-Anhang benötigt wurde, bei ihrer Erstellung nicht verschlüsselt wurde, ist kein Umstand, der bei dem in Frage stehenden Datenschutzverstoß erheblich ins Gewicht fällt. Maßgeblich ist insoweit, wie bereits ausgeführt, dass sie von den mit dem Versand der E-Mail befassten Mitarbeitern als E-Mail-Anhang übersehen und deswegen vor dem Abschieken der E-Mail nicht entfernt wurde, was insbesondere einen Verstoß gegen Art. 5 Abs. 1 Buchst. a) und f) und 9 Abs. 1 DS-GVO darstellt.

e) Die Beklagte ist nicht gemäß Art. 82 Abs. 3 DS-GVO von der Haftung befreit. [...]

Das Verschulden wird nach dem Wortlaut der Norm grundsätzlich vermutet. Um die Feststellung treffen zu können, der Verantwortliche sei „in keinerlei Hinsicht“ verantwortlich, hat der Verantwortliche nachzuweisen, dass er alle Sorgfaltspflichten erfüllt hat und ihm damit nicht die geringste Fahrlässigkeit vorgeworfen werden kann [...]. Dies wäre etwa der Fall, wenn von allen mit der Datenverarbeitung befassten Personen alle erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen eingehalten wurden und es dennoch zu einem unbefugten Datenzugriff kommt [...].

aa) Diesen Nachweis hat die Beklagte indes nicht zu führen vermocht. Im Hinblick auf die Verstöße gegen Art. 5 Abs. 1 Buchst. a) und f) sowie 9 Abs. 1 DS-GVO liegt ein der Beklagten zuzurechnendes Verschulden ihrer Mitarbeiter vor, die die E-Mail abgesandt haben. Die allgemeinen Grundsätze des § 278 BGB gelten auch hier [...]. Die Absendung der E-Mail ohne das vorherige Entfernen der angehängten Excel-Datei ist zumindest als fahrlässig im Sinne von § 276 Abs. 2 BGB einzustufen. [...] Für das Verhalten ihrer Mitarbeiter haftet die Beklagte als Verantwortliche, ohne sich entlasten zu können [...].

f) Dem Kläger ist auch ein immaterieller Schaden entstanden.

Einen solchen sieht der Kläger insbesondere in dem mit dem Versand der Excel-Datei verbundenen Kontrollverlust seiner in der Datei aufgeführten personenbezogenen Daten und dem späteren Erhalt einer Phishing-E-Mail am 18.08.2021, den er auf diesen Kontrollverlust zurückführt. [...]

dd) Der Eintritt eines Schadens setzt auch nicht voraus, dass dem Betroffenen durch den Verstoß gegen die DS-GVO ein spürbarer Nachteil entstanden ist oder es zu einer objektiv nachvollziehbaren Beeinträchtigung von persönlichkeitsbezogenen Belangen mit gewissem Gewicht gekommen ist. Insoweit wird vertreten, dass für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung bzw. für eine bloß individuell empfundene Unannehmlichkeit kein Schmerzensgeld zu gewähren sei (LG Essen, Urt. v. 23.09.2021 – 6 O 190/21, juris Rn. 53; AG Diez, Urt. v. 07.11.2018 – 8 C 130/18, juris Rn. 6; Schaffland/Holthaus, in: Schaffland/Wiltfang, DS-GVO/BDSG, Stand: August 2022, Art. 82 DS-GVO Rn. 5 und 11a – hier: eine unwillkommene Mail konnte vom Betroffenen ohne großen Aufwand gelöscht werden). Auch wird vertreten, ein Schadener-

satzanspruch bestehe nicht bei bloßen Bagatellschäden, die vorliegen sollen bei der Verbreitung von Name, Geburtsdatum, Geschlecht, E-Mail-Adresse und Telefonnummer einer Person (LG Karlsruhe, Urt. v. 09.02.2021 – 4 O 67/20, juris Rn. 38; Schaffland/Holthaus, in: Schaffland/Wiltfang, DS-GVO/BDSG, Stand: August 2022, Art. 82 DS-GVO Rn. 14a).

Nach Überzeugung des Senats findet eine derartige Einschränkung des Anspruchs in der DS-GVO keine Grundlage und ist auch aus sonstigen Gründen nicht geboten. Es handelt sich auch hierbei letztlich ebenfalls um eine Erheblichkeitsschwelle, die weder in der DS-GVO noch in der Rechtsprechung des EuGH eine Stütze findet (vgl. Buchner/Wessels, in ZD 2022, 251 (254)).

ee) Ausgehend von dem vorstehend beschriebenen Begriff des immateriellen Schadens ist dem Kläger im vorliegenden Fall ein solcher dadurch entstanden, dass die in der Excel-Datei enthaltenen personenbezogenen Daten des Klägers offenbart wurden und der Kläger die Kontrolle über diese gegenüber Dritten offenbarten Daten verloren hat. Zu Recht macht der Kläger den ihn belastenden Kontrollverlust bezüglich seiner Daten geltend, was als Schaden zu bewerten ist. [...]

Soweit der Kläger weiter geltend macht, bei der E-Mail vom 18.08.2021 habe es sich um eine Phishing-Mail gehandelt, mit der weitere Daten des Klägers „abgegriffen“ oder sein PC „gehackt“ hätte werden sollen, begründet dies jedoch keinen weitergehenden Schaden. Es ist schon nicht erkennbar, dass es tatsächlich zu einem weiteren Abfluss von Daten des Klägers gekommen ist oder sein PC tatsächlich gehackt wurde. Auch soweit der Kläger mit seinem Vorbringen offenbar geltend machen will, er könne Gefahren durch „militante Impfgegner“ ausgesetzt sein, zumal die Befürwortung der Corona-Impfung und der vollständige Name des Klägers und seine Anschrift unter anderem auch Kriminellen bekannt geworden seien, vermag dieses rein spekulative Vorbringen nicht die Annahme eines weitergehenden Schadens zu rechtfertigen. [...]

## (Mit-)Verantwortlichkeit von Google Ireland neben Google LLC aus den USA bei Löschanträgen nach Art. 17 Abs. 1 DS-GVO

(LG Heidelberg, Urteil vom 31. März 2023 – 6 S 1/22 –)

- Nach dem weiten Verarbeitungsbegriff des Art. 4 Nr. 2 DS-GVO stellt bereits die Anzeige einer Seite mit Suchergebnissen eine Verarbeitung von Daten dar. Ein Unternehmen, das den Nutzern Informationen anzeigt, die ein anderes Unternehmen gefunden, indexiert und gespeichert hat, ist daher als (Mit-)Betreiber der Suchmaschine und damit als (Mit-)Verantwortlicher im Sinne von Art. 17 Abs. 1 DS-GVO anzusehen.**
- Ein Suchmaschinenbetreiber muss einem Auslistungsantrag stattgeben, wenn die betroffene Person Nachweise vorlegt, aus denen sich offensichtlich ergibt, dass die in dem aufgelisteten Inhalt enthaltenen Informationen unrichtig sind oder zumindest ein für diesen gesam-**

**ten Inhalt nicht unbedeutender Teil dieser Informationen offensichtlich unrichtig ist.**

- 3. Sofern vorgerichtlich keine Nachweise für die offensichtliche Unrichtigkeit der beanstandeten Inhalte vorgelegt wurden, hat eine Abwägung der widerstreitenden Interessen in einem gerichtlichen Verfahren zu erfolgen.**

*(Nicht amtliche Leitsätze)*

### Aus den Gründen:

Der Kläger hat gegen die Beklagte keinen Anspruch auf Unterlassung der Anzeige der von ihm beanstandeten Suchergebnisse aus Art. 17 Abs. 1 DS-GVO. [...]

a) Wie das Amtsgericht zutreffend ausgeführt hat, kommt als Anspruchsgrundlage für das Begehren des Klägers ausschließlich Art. 17 Abs. 1 DS-GVO in Betracht. Danach hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der sodann unter Buchst. a) bis f) genannten Gründe vorliegt. Dies gilt gemäß Art. 17 Abs. 3 DS-GVO nicht, wenn die Verarbeitung zu einem der dort genannten Zwecke erforderlich ist, insbesondere gemäß Buchst. a) zur Ausübung des Rechts auf freie Information. Im zeitlichen, örtlichen und sachlichen Anwendungsbereich der DS-GVO können Abwehransprüche nicht mehr auf Vorschriften des nationalen Rechts, insbesondere nicht auf §§ 823 Abs. 1, 1004 Abs. 1 BGB, gestützt werden (BGH, Urt. v. 03.05.2022 – VI ZR 832/20 – NJW 2022, 2476, 2477). Der Anwendungsbereich der DS-GVO ist hier eröffnet. Sie gilt zeitlich seit dem 15.05.2018, örtlich werden die beanstandeten Suchergebnisse im Gebiet der Europäischen Union angezeigt und sachlich ist ein auf dauerhafte Auslistung gerichtetes Rechtsschutzbegehren von Art. 17 Abs. 1 DS-GVO erfasst (vgl. BGH, aaO).

b) Entgegen der Ansicht des Amtsgerichts hält die Kammer die Beklagte allerdings für passivlegitimiert. Die Beklagte ist Verantwortliche im Sinne des Art. 17 Abs. 1 DS-GVO. [...] Die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, ist als „Verarbeitung personenbezogener Daten“ einzustufen und der Betreiber dieser Suchmaschine ist als für diese Verarbeitung „Verantwortlicher“ anzusehen (EuGH, Urt. v. 13.05.2014 – C 131/12 – Google Spain – juris Tz. 41). Hier sind sowohl Google LLC als auch die Beklagte als Verantwortliche zu betrachten. Art. 26 DS-GVO setzt voraus, dass es mehrere Verantwortliche geben kann, wobei gemäß Art. 26 Abs. 3 DS-GVO bei einer Aufteilung von Verantwortlichkeiten die betroffene Person unabhängig von dieser Aufteilung ihre Rechte gegenüber jedem einzelnen Verantwortlichen geltend machen kann. Die Tätigkeiten einer Suchmaschine, die der EuGH aufzählt und als Verarbeitung personenbezogener Daten einstuft, sind zwischen Google LLC und der Beklagten aufgeteilt. Google LLC findet, indexiert und speichert Daten und legt eine Rangfolge fest, die Beklagte stellt nach den Google-Nutzungsbe-

dingungen die Informationen den Nutzern im Bereich des Europäischen Wirtschaftsraums und der Schweiz zur Verfügung. Nach dem weiten Verarbeitungsbegriff des Art. 4 Nr. 2 DS-GVO stellt bereits die Anzeige einer Seite mit Suchergebnissen eine Verarbeitung von Daten dar (EuGH, Urt. v. 13.05.2014 – C 131/12 – Google Spain – juris Tz. 57), über deren Zweck und Mittel im Europäischen Wirtschaftsraum und der Schweiz die Beklagte als Diensteanbieterin entscheidet. Sie ist daher als Mitbetreiberin der Suchmaschine und (Mit-)Verantwortliche im Sinne des Art. 17 Abs. 1 DS-GVO anzusehen (so auch LG Köln, Beschl. v. 04.07.2022 – 28 O 168/22 – ZD 2022, 564).

c) Die inhaltlichen Voraussetzungen des Art. 17 DS-GVO für die Löschung von Ergebnislinks einer Suchmaschine liegen jedoch nicht vor. Dazu hat der Europäische Gerichtshof folgende Grundsätze aufgestellt (EuGH, Urt. v. 08.12.2022 – C 460/20 – juris):

aa) Das Recht auf Schutz personenbezogener Daten ist kein uneingeschränktes Recht, sondern muss, wie im vierten Erwägungsgrund der DS-GVO ausgeführt, im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden (EuGH, a.a.O. – juris Tz. 56; so auch BGH, Urt. v. 03.05.2022 – VI ZR 832/20 – NJW 2022, 2476, Tz. 16). [...] Die DS-GVO und insbesondere Art. 17 Abs. 3 Buchst. a) verlangen somit ausdrücklich eine Abwägung zwischen den in Artt. 7 und 8 der Charta verankerten Grundrechten auf Achtung des Privatlebens und auf Schutz personenbezogener Daten und dem durch Art. 11 der Charta gewährleisteten Grundrecht auf freie Information (EuGH, a.a.O., Tz. 57, 58). [...] Danach sind für die Zwecke der Abwägung zwischen dem Recht auf Achtung des Privatlebens und dem Recht auf freie Meinungsäußerung und Information eine Reihe relevanter Kriterien zu berücksichtigen, wie der Beitrag zu einer Debatte von allgemeinem Interesse, der Bekanntheitsgrad der betroffenen Person, der Gegenstand der Berichterstattung, das vorangegangene Verhalten der betroffenen Person, Inhalt, Form und Auswirkungen der Veröffentlichung, die Art und Weise sowie die Umstände, unter denen die Informationen erlangt worden sind, und deren Richtigkeit. [...] Die Frage der Richtigkeit des aufgelisteten Inhalts ist auch ein relevanter Gesichtspunkt bei der Prüfung der Anwendungsvoraussetzungen von Art. 17 Abs. 3 Buchst. a) der DS-GVO im Hinblick auf die Beurteilung der Frage, ob das Recht der Internetnutzer auf Information und die Meinungsäußerungsfreiheit des Inhaltanbieters Vorrang vor den Rechten desjenigen haben können, der eine Auslistung begehrt. Unter diesem Aspekt kann das Recht auf freie Meinungsäußerung und Information zwar unter bestimmten Umständen Vorrang vor den Rechten auf Schutz der Privatsphäre und auf Schutz personenbezogener Daten haben, insbesondere wenn die betroffene Person im öffentlichen Leben eine Rolle spielt, doch kehrt sich dieses Verhältnis jedenfalls dann um, wenn zumindest ein für den gesamten Inhalt nicht unbedeutender Teil der Informationen, um die es in dem Auslistungsantrag geht, unrichtig ist. [...]

bb) Ein Suchmaschinenbetreiber, der selbst nicht für die von ihm gelisteten Inhalte verantwortlich ist, aber durch die Verbreitung von Ergebnislisten dazu beiträgt, dass Nutzer ein mehr oder weniger detailliertes Profil einer Person erstellen können, ist seinerseits verpflichtet, einem Auslistungsantrag stattzugeben, wenn die betroffene Person Nachweise vorlegt, aus denen sich offensichtlich ergibt, dass die in dem

aufgelisteten Inhalt enthaltenen Informationen unrichtig sind oder zumindest ein für diesen gesamten Inhalt nicht unbedeutender Teil dieser Informationen offensichtlich unrichtig ist. [...]

(1) Die Kammer geht davon aus, dass in einem Fall wie diesem, in dem vorgerichtlich vom Kläger keine Nachweise für die offensichtliche Unrichtigkeit der von ihm beanstandeten Inhalte vorgelegt wurden, eine Abwägung der widerstreitenden Interessen in einem gerichtlichen Verfahren zu erfolgen hat. Das Gericht prüft nicht nur, ob vorgerichtlich derartige Nachweise vorgelegt wurden, sondern nimmt aufgrund der beiderseitigen Parteivorträge und einer eventuellen Beweisaufnahme eine umfassende Abwägung vor. Dieser gerichtlichen Abwägung misst der EuGH besondere Bedeutung zu (vgl. EuGH, a.a.O., Tz. 75). [...]

(d) Weiter ist zu berücksichtigen, dass der Kläger auch im gerichtlichen Verfahren nicht bewiesen hat, dass der gegen ihn erhobene Vorwurf, sich am Telefon mit „Heil Hitler“ gemeldet zu haben, unzutreffend ist. Der insoweit nach der oben dargestellten Rechtsprechung des EuGH darlegungs- und beweispflichtige Kläger hat weder schlüssig dargelegt, dass er sich nicht mit „Heil Hitler“ am Telefon gemeldet haben könne, noch haben die von ihm benannten Beweismittel zu einem solchen Ergebnis geführt. [...]

(e) Ebenfalls in die Abwägung einzustellen ist in diesem Zusammenhang, dass der Kläger mangels Greifbarkeit des Inhaltanbieters gegen diese nicht gerichtlich vorgehen kann. Dass dem Kläger insoweit Verteidigungsmittel abgeschnitten sind, kann zwar in der Abwägung nicht unberücksichtigt bleiben. Der Kläger sieht sich aber andererseits keiner völlig aus der Luft gegriffenen Behauptung ausgesetzt, für deren Wahrheit keinerlei Anhaltspunkte bestehen. Der Zeuge M. hat sich öffentlich zu dem behaupteten Vorfall geäußert und der Kläger kannte die damals burschenschaftsintern erhobenen Vorwürfe und kann selbst zur Aufklärung beitragen. Er ist daher nicht jeglicher Möglichkeiten beraubt, sondern kann in angemessenem Umfang vortragen und Beweismittel beibringen. [...]

## Einwand unzulässiger Rechtsausübung kann Auskunftersuchen entgegenstehen

(VG Gelsenkirchen, Beschluss vom 8. Februar 2023 – 15 K 3678/22 –)

1. Wenn ein Auskunftersuchen nach dem IFG offensichtlich verfahrensfremden Zwecken dient, steht der Rechtsausübung der Einwand der Unzulässigkeit.
2. Dieser Einwand kann auch der Geltendmachung von Betroffenenrechten nach der DS-GVO entgegenstehen, wenn die Zwecke ihrer Ausübung außerhalb ihres Schutzbereichs liegen.

*(Nicht amtliche Leitsätze)*

### Aus den Gründen:

Wenn ein Rechtsschutzersuchen erkennbar nicht mehr der Wahrnehmung prozessualer Rechte, sondern ausschließlich verfahrensfremden Zwecken dient, bedarf es keiner förm-

lichen Abweisung oder Verwerfung durch Prozessurteil. Das Ersuchen ist dann von vornherein unbeachtlich; wurde es anfangs unzutreffender Weise als förmlicher Rechtsbehelf behandelt, so ist das Verfahren einzustellen. [...]

2. Das vermeintliche Rechtsschutzersuchen im vorliegenden Einzelfall stellt einen Extremfall unzulässiger Rechtsausübung dar.

Dem „Kläger“ steht für Auskunftersuchen wie dem vorliegenden kein schützenswertes Interesse zur Seite. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hat zu Auskunftersuchen des „Klägers“ nach dem Informationsfreiheitsgesetz ausgeführt, unter Berücksichtigung aller relevanten Aspekte, insbesondere der Vielzahl der Informationsbegehren des Klägers, sei davon auszugehen, dass ein (unterstellter) Anspruch wegen unzulässiger Rechtsausübung ausgeschlossen sei. „Denn der Kläger nutzt seine diesbezüglichen Anträge jedenfalls im Wesentlichen dazu, im Zuge eines privat motivierten Vergeltungsfeldzugs die Justiz und Justizverwaltung zu schikanieren und zu belästigen.“ OVG NRW, Urt. v. 06.10.2022 – 15 A 760/20 – juris Rn. 86.

Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hat mit dem Oberlandesgericht Hamm festgestellt, der „Kläger“ sei von einem Vergeltungsdrang gegenüber der Justiz mit Blick auf erfolglose Gerichtsverfahren in einer familienrechtlichen Angelegenheit getragen (OVG NRW, Urt. v. 6. Oktober 2022 – 15 A 760/20 –, juris Rn. 86; OLG Hamm, Beschl. v. 08.05.2018 – I-15 VA 12/18 –, juris Rn. 59).

Den hierzu getroffenen Feststellungen des Oberverwaltungsgerichts für das Land Nordrhein-Westfalen: „Dieser Beweggrund wird ferner durch die seitens des Beklagten im hiesigen Verfahren wie auch im Verfahren 15 A 593/20 dokumentierte Anzahl an Gesuchen des Klägers gegenüber den Gerichtsverwaltungen belegt. So hat der Kläger mit Stand 30.08.2021 seit dem dritten Quartal 2017 rund 350 Eingaben im Zusammenhang mit Geschäftsverteilungsplänen allein bei der ordentlichen Gerichtsbarkeit des Landes Nordrhein-Westfalen eingereicht, die im Schriftsatz des Beklagten vom 27.09.2021 wie auch im Schriftsatz des Beklagten vom 05.10.2021 im Verfahren 15 A 593/20 im Einzelnen aufgelistet werden. Hinzu treten Einsichtnahmegesuche auch in anderen Gerichtsbarkeiten, namentlich bei den Verwaltungsgerichten, wie dem Senat aufgrund derzeit anhängiger Beschwerden des Klägers in verschiedenen einschlägigen Prozesskostenhilfverfahren bekannt ist. [...]

Bereits die Anzahl der gestellten Anträge zeigt, dass der Kläger den ihm u.a. durch das Informationsfreiheitsgesetz NRW zur Verfügung gestellten Informationsanspruch nutzt, um die Justizbehörden möglichst umfänglich zu beschäftigen. Zusätzlich erhöht er den Arbeitsaufwand der betroffenen Behörden dadurch, dass er gestaffelte Anträge stellt und seine Begehren sukzessive erweitert (so OLG Hamm, Beschl. v. 08.05.2018 – I-15 VA 12/18 –, juris Rn. 59).

Der aus diesem Vorgehen gezogenen Schlussfolgerung, dass diese Staffelung ersichtlich dazu dient, bei den vom Kläger angefragten Behörden zusätzlichen Aufwand zu verursachen, tritt der Senat bei. Mangels eines erkennbaren sonstigen Interesses an einer solchen Vielzahl von Anträgen und angesichts des hiermit auch auf Seiten des Klägers verbundenen Aufwands erscheint zudem der Schluss berechtigt, dass der Kläger seine Gesuche maßgeblich aus der von ihm selbst bezeichneten, privaten Vergeltungsmotivation heraus stellt.

Dies wird auch durch den Schwerpunkt der von ihm adressierten Justizbehörden deutlich, der sich nach Maßgabe der Anzahl der Eingaben vor allem auf das Amtsgericht D. (knapp 250 Anträge) und das diesem übergeordnete Oberlandesgericht Z. (ca. 380 Anträge) bezieht, bei denen der in M. wohnhafte Kläger nach Mitteilung des Beklagten im Verfahren 15 A 593/20 die Mehrzahl seiner familiengerichtlichen Streitigkeiten betrieben hat bzw. derzeit noch betreibt. [...]

Diese Gesamtschau seiner – sicherlich immer noch nicht vollständig erfassten – Auskunftersuchen in der Gerichtsbarkeit des Landes Nordrhein-Westfalen trägt die Überzeugungsbildung, dass dem vorliegenden Verfahren ebenso der Einwand unzulässiger Rechtsausübung entgegensteht. [...]

Für den auf Art. 15 Abs. 3 S. 1 der VO (EU) 2016/679 [...] – nachfolgend DS-GVO – gestützten Antrag zu a) gilt nichts anderes. Das Oberverwaltungsgericht für das Land Nordrhein-Westfalen hat den Einwand unzulässiger Rechtsausübung aus dem Grundsatz von Treu und Glauben abgeleitet (vgl. OVG NRW, Urt. v. 06.10.2022- 15 A 760/20 –, juris Rn. 78).

Dieser allgemeine Rechtsgrundsatz unzulässiger Rechtsausübung kann auch der Geltendmachung eines Betroffenenrechts der DS-GVO entgegenstehen. Nach der Rechtsprechung des Europäischen Gerichtshofs dürfen nationale Gerichte eine innerstaatliche Rechtsvorschrift über die gegen Treu und Glauben verstoßende missbräuchliche Rechtsausübung anwenden, um zu beurteilen, ob ein sich aus einer Gemeinschaftsbestimmung ergebendes Recht missbräuchlich ausgeübt wird (EuGH, Urt. v. 12.05.1998 – C-367/96, ECLI:EU:C:1998:222 = EuZW 1999, 56 Rn. 20f.; Lembke, NJW 2020, 1841 (1845)).

Wenn die rechtsmissbräuchliche Berufung auf Unionsrecht anhand einzelner nationaler Rechtsvorschriften zum Schutz von Treu und Glauben festgestellt werden kann, gilt dies erst recht für den demselben Schutz dienenden allgemeinen, die gesamte Rechtsordnung durchziehenden Rechtsgedanken. Nach der vom Europäischen Gerichtshof hierfür gezogenen Grenze darf hierbei die volle Wirksamkeit und die einheitliche Anwendung des Gemeinschaftsrechts in den Mitgliedstaaten nicht beeinträchtigt werden, insbesondere dürfen die Tragweite einer Gemeinschaftsbestimmung, aus der sich das der Missbrauchskontrolle unterzogene Recht ergibt, nicht verändert oder die mit ihr verfolgten Zwecke nicht vereitelt werden (EuGH, Urt. v. 12.05.1998 – C-367/96, ECLI:EU:C:1998:222 = EuZW 1999, 56 Rn. 22).

Letztlich ist der Anspruch aus Art. 15 DS-GVO von derselben Motivation getragen, die den Einwand unzulässiger Rechtsausübung sonstiger Ansprüche auf Informationszugang, -auskunft und -kopie begründen. Eine andere Würdigung eröffnete die Möglichkeit, den Einwand, der den nationalen Ansprüchen entgegensteht, zu umgehen. Deshalb steht dem vom Kläger geltend gemachten Anspruch aus Art. 15 DS-GVO hier auch der Grundsatz von Treu und Glauben entgegen.

Die Einordnung des vorliegenden Begehrens als gegen den Grundsatz von Treu und Glauben verstoßend wahrt die dargestellten Anforderungen des Unionsrechts. In dem gegebenen Extremfall wird weder die Tragweite der Grundsätze des Datenschutzes und der Betroffenenrechte nach Art. 15 ff. DS-GVO verändert noch die mit ihnen verfolgten Zwecke vereitelt. Datenschutzfremde Zwecke und eine Belästigungsabsicht gegenüber der Gerichtsbarkeit sind nicht vom Schutzzweck der Betroffenenrechte (Transparenz und Rechtmäßigkeitskontrolle, vgl. Erwägungsgrund 63 S. 1 zur DS-GVO) erfasst. [...]

## Kein Anspruch auf Löschung der Daten eines Geschäftsführers aus dem Handelsregister

(OLG Celle, Beschluss vom 24. Februar 2023 – 9 W 16/23 –)

**Der Geschäftsführer einer GmbH hat keinen Anspruch auf Löschung seines in das Registerblatt des Handelsregisters eingetragenen Geburtsdatums sowie Wohnortes.**

*(Nicht amtlicher Leitsatz)*

### Aus den Gründen:

1. Für das Begehren des Antragstellers fehlt es an einer Rechtsgrundlage.

a) Soweit der Antragsteller sich auf Artt. 17, 18 und 21 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, im Folgenden: DS-GVO) zu stützen sucht (vgl. Beschwerdebegründung vom 7. Februar 2023, dort S. 2, Bl. 59R d.A.), vermag er damit nicht durchzudringen.

aa) Ein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO steht dem Antragsteller gemäß § 10a Abs. 3 HGB nicht zu. Dementsprechend ist auch Art. 18 Abs. 1 lit. d DS-GVO nicht einschlägig, weil diese Bestimmung das Bestehen eines Widerspruchsrechts nach Art. 21 Abs. 1 DS-GVO voraussetzt.

bb) Des Weiteren ergibt sich auch aus Art. 17 Abs. 1, Abs. 2 DS-GVO kein Löschananspruch zugunsten des Antragstellers, weil diese Bestimmungen gemäß Art. 17 Abs. 3 lit. b DS-GVO nicht gelten, soweit die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, erfordert, notwendig ist. Eben eine solche rechtliche Verpflichtung ist hier mit Blick auf § 387 Abs. 2 FamFG i.V.m. § 43 Nr. 4b HRV gegeben.

b) Auch auf § 395 FamFG vermag sich der Antragsteller nicht zu stützen. Denn die Aufnahme seines Geburtsdatums und seines Wohnorts in das Handelsregister war mit Blick auf § 387 Abs. 2 FamFG i.V.m. § 43 Nr. 4b HRV nicht unzulässig im Sinne dieser Bestimmung.

2. Zweifel an der Vereinbarkeit der dem Begehren des Antragstellers entgegenstehenden Bestimmung des § 10a Abs. 3 HGB mit Verfassungs- bzw. Europarecht hat der Senat weder generell noch bezogen auf den Streitfall.

a) Die in § 10a Abs. 3 HGB vorgenommene Einschränkung der Rechte aus § 21 DS-GVO ist von Art. 23 Abs. 1 lit. e DS-GVO gedeckt, wonach die Pflichten und Rechte gemäß den Artt. 12 – 22 DS-GVO zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates beschränkt werden können (vgl. Röhrich/Graf von Westphalen/Haas/Ries, HGB, 5. Aufl. 2019, § 10a Rn. 2; Staub/Koch/Harnos, HGB, 6. Aufl. 2023, § 10a Rn. 5 f.). Dazu zählen funktionsfähige und verlässliche öffentliche Register, die für die Sicherheit und Leichtigkeit des Rechtsverkehrs unerlässlich sind (vgl. BT-Drs. 18/12611, S. 67). Vor diesem Hintergrund ist die Regelung des § 10a Abs. 3

HGB nach einhelliger Auffassung im Schrifttum, der sich der Senat anschließt, nicht zu beanstanden. Sie dient der Gewährleistung der Sicherheit und Leichtigkeit des Registerverkehrs (vgl. Krafka, Registerrecht, 11. Aufl. 2019, Rn. 74a); ein Widerspruch gegen die Datenverarbeitung wäre mit den Publizitätsanforderungen des öffentlichen Registers nicht in Einklang zu bringen (vgl. MünchKomm/Krafka, HGB, 5. Aufl. 2021, § 10a Rn. 12; BeckOK/Müther, HGB, 39. Edition, Stand: 15. Januar 2023, § 10a Rn. 4; Oetker/Preuß, HGB, 7. Aufl. 2021, § 10a Rn. 7).

b) Dass das öffentliche Interesse an der Führung des Handelsregisters im Streitfall durch das Interesse des Antragstellers an einer Geheimhaltung seines Geburtsdatums und seines Wohnorts überwogen würde, ist weder hinreichend vorgetragen noch sonst ersichtlich. [...]

bb) Des Weiteren ist, eine tatsächliche Gefährdung des Antragstellers – die er über allgemeine Angaben hinaus nicht konkretisiert hat – zu dessen Gunsten unterstellt, auch weder vorgetragen noch ersichtlich, in welcher Weise eine solche Gefährdung durch die Einsehbarkeit von Geburtsdatum und Wohnort im Handelsregister verursacht oder erhöht werden soll. Soweit es die Nennung des Wohnorts betrifft, ist insbesondere zu berücksichtigen, dass eine genaue Adressangabe nicht erfolgt und ein Ansatzpunkt zum Auffinden des Antragstellers auch bereits mit der Nennung der Geschäftsanschrift der betroffenen Gesellschaft gegeben ist, deren Löschung der Antragsteller indes nicht begehrt.

3. Vermag der Antragsteller sein Begehren nach alldem schon mangels einer dies tragenden Rechtsgrundlage im Registerverfahren nicht durchzusetzen, hat der Senat mit Blick auf den Verweis des Antragstellers auf die mit dem Gesetz zur Umsetzung der Digitalisierungsrichtlinie vom 5. Juli 2021 (DiRUG) jedermann eröffnete Möglichkeit zur kostenfreien Einsichtnahme in das Handelsregister erwogen, inwieweit ein aus Rechtsnormen außerhalb des Registerverfahrens und datenschutzrechtlicher Bestimmungen, beispielsweise §§ 823, 839 BGB oder § 1004 BGB (analog), folgender Anspruch wegen Verfehlung datenschutzrechtlicher Vorgaben durch das DiRUG bestehen könnte.

a) Insoweit ist der Senat jedoch der Auffassung, dass die Prüfung eines etwaigen solchen Anspruchs nicht im Registerverfahren zu erfolgen hat. Das formalisierte Registerverfahren dient der korrekten Führung des Handelsregisters, zielt aber weder auf die inzidente Prüfung der dafür bestehenden Vorgaben noch gar auf die Behebung von dem Gesetzgeber etwa unterlaufenen Auslassungen beispielsweise im Hinblick auf datenschutzrechtliche Belange. Dies hat umso mehr zu gelten, als die Registergerichte nicht ihrerseits durch (Teil-) Löschungen von Einträgen in Einzelfällen womögliche, aus gesetzlichen Vorgaben resultierende generelle Probleme zu lösen in der Lage wären.

b) Im Übrigen bleibt der die Einschränkung datenschutzrechtlicher Ansprüche rechtfertigende Zweck des § 10a Abs. 3 HGB, der als solcher nicht zu beanstanden ist (s.o.), durch das DiRUG unangetastet. Dass allein die Möglichkeit zur kostenfreien Einsichtnahme in das Handelsregister eine Höherbewertung des Interesses am Schutz persönlicher Daten gebieten und einer Beschränkung der Rechte aus § 21 DS-GVO durch § 10a Abs. 3 HGB entgegenstehen würde, vermag der Senat nicht zu erkennen.

## Voraussetzungen einer freiwilligen Einwilligung und Anforderungen an eine Übermittlung von IP-Adressen in die USA

(LG Köln, Urteil vom 12. Januar 2023 – 33 O 376/22 –)

- Datenschutzhinweisen, die sich im Rahmen der Informationspflichten nach Artt. 13 und 14 DS-GVO halten, kommt kein eigener Regelungsgehalt zu, weshalb sie nicht als Allgemeine Geschäftsbedingungen zu qualifizieren sind und damit keiner AGB-Kontrolle unterliegen (Antrag 1.b.).**
- Eine freiwillige Einwilligung setzt voraus, dass der Verbraucher bei der Abgabe der Einwilligung eine echte Wahlmöglichkeit hat und nicht durch die Ausgestaltung des Cookie-Banners einseitig in Richtung einer Einwilligung gelenkt wird. Eine „der Einwilligungserklärung in Form, Funktion und Farbgebung gleichwertige, gleichrangige und gleich einfach zu bedienende Ablehnungsoption“ ist erforderlich es hingegen nicht (Antrag 1.c.).**
- Eine Übermittlung von IP-Adressen in die USA kann weder auf einen Angemessenheitsbeschluss der Kommission noch auf etwaige Standarddatenschutzklauseln gestützt werden. Eine mögliche Einwilligung in die Übermittlung personenbezogener Daten in die USA nach Art. 49 Abs. 1 S. 1 lit. a DS-GVO setzt zudem eine besondere Informiertheit des Einwilligenden voraus. An sie sind höhere Anforderungen als an sonstige Einwilligungen zu stellen. (Antrag 1.d.).**

*(Nicht amtliche Leitsätze)*

### Aus den Gründen:

#### Zu Antrag 1.b.:

Die Klausel unterliegt [...] nicht der AGB-Kontrolle, sodass § 1 UKlaG nicht anwendbar ist. [...]

Eine ausdrückliche Regelung hinsichtlich des Verhältnisses von Datenschutzrecht und AGB-Recht findet sich weder im Unions- noch im nationalen Recht (von Lewinski/Herrmann, PinG 2017, 165 (171)).

Gemäß § 305 Abs. 1 S. 1 BGB sind Allgemeine Geschäftsbedingungen alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt.

Bei den Informationspflichten handelt es sich aber um für die Parteien der Datenverarbeitung (Verantwortliche und betroffene Person) nicht-dispositives Recht (Paal/Henneemann, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO Art. 13 Rn. 7). Es handelt sich bei den Datenschutzhinweisen um Informationen, die der Verantwortliche zwingend bereitzustellen hat, ohne dass es auf seinen Willen ankäme. Aus diesem Grund kann ein Rechtsbindungswille hinsichtlich des Inhalts der Datenschutzhinweise regelmäßig fernliegen. Spiegelbildlich dürften betroffene Personen – zu Recht – regelmäßig nicht davon ausgehen, dass Verantwortliche ihnen mittels der Datenschutzhinweise einen Vertrag antragen. Eine Bindungswirkung von Datenschutzhinweisen scheidet dann bereits an der Hürde der §§ 133, 157 BGB.

Soweit sich Datenschutzhinweise i.R.d. Informationspflichten nach Artt. 13 und 14 DS-GVO halten, unterliegen sie nicht der AGB-rechtlichen Klauselkontrolle, da ihnen insoweit kein eigener Regelungsgehalt zukommt (OLG Hamburg, MMR 2015, 740 m. Anm. Hansen/Struwe; KG, MMR 2020, 239 m. Anm. Heldt, Ls. N01; Hacker, ZfPW 2019, 148 (184); Moos, in: Moos/Schefzig/Arning, Praxishdb. DS-GVO, 2. Aufl., Kap. 2 Rn. 27; Wendehorst/Graf v. Westphalen, NJW 2016, 3745 (3748)). [...]

#### Zu Antrag 1.c.:

Nach Art. 4 Nr. 11 der VO (EU) 2016/679 ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Das setzt voraus, dass der Verbraucher bei der Abgabe der Einwilligung eine echte Wahlmöglichkeit hat und nicht durch die Ausgestaltung des Cookie-Banners einseitig in Richtung einer Einwilligung gelenkt wird.

Eben dies war bei dem streitgegenständlichen Cookie-Banner indessen der Fall. Denn während im Falle des Buttons „Alle akzeptieren“ eine Ein-Klick-Lösung in Größe, Farbe und Layout als Blickfang deutlich gestaltet war, war das Weitersurfen „nur mit den notwendigen Cookies“ im Fließtext versteckt und damit in Größe, Form und Gestaltung nicht ausreichend, um als tatsächliche und gleichwertige Wahlmöglichkeit angesehen zu werden.

Auch die Wahlmöglichkeit „Einstellungen ändern“, führt ebenso wenig zur Wirksamkeit der Einwilligung, da der Button – wie der Landesbeauftragte für Datenschutz und Informationsfreiheit in seiner Stellungnahme vom 27.02.2023 zutreffend umschrieben hat – keine für den Verbraucher erkennbare zu dem Button „Alle akzeptieren“ im Alternativverhältnis stehende Wahlmöglichkeit in Form einer Willenserklärung oder eines Hinweises darauf enthält. So ist in der Formulierung „Einstellungen ändern“ kein unmissverständlicher Hinweis auf eine – wenn auch auf zweiter Ebene – alternative Ablehnungsmöglichkeit der technisch nicht notwendigen Cookies enthalten. Sieht sich der Verbraucher also einer Willenserklärung („Alles akzeptieren“) und daneben einer unspezifischen Konfigurationsmöglichkeit gegenüber, die die mögliche folgende Willenserklärung „Nicht alles akzeptieren/Alles abwählen“ etc.) und damit die Wahlmöglichkeit nicht zu erkennen gibt, wird durch das Klicken des Buttons „Alles akzeptieren“ keine freie Wahl zwischen zwei Willenserklärungen getroffen.

Der Antrag des Klägers ist indessen zu weit gefasst und enthält durch die Formulierung „ohne im Cookie-Banner eine der Einwilligungserklärung in Form, Funktion und Farbgebung gleichwertige, gleichrangige und gleich einfach zu bedienende Ablehnungsoption bereitzustellen“ ausdrücklich eine Verpflichtung zu einer bestimmten Form der Bannergestaltung. Letzteres ergibt sich aber weder aus den Vorschritten der DS-GVO noch aus den Erwägungsgründen. [...]

#### Zu Antrag 1.d.:

Die klägerseits vorgetragene Übermittlung von IP-Adressen sowie Browser- und Geräteinformationen an Google LLC als

Betreiberin von Google Analyse- und Marketingdiensten mit Sitz in den USA ist als unstreitig zu behandeln und ist nicht von den Rechtfertigungstatbeständen der DS-GVO gedeckt. [...]

Die übermittelten IP-Adressen stellen sowohl für die Beklagte als auch Google LLC als Verantwortliche der Datenübermittlung personenbezogene Daten dar.

Dynamische IP-Adressen stellen dann personenbezogene Daten dar, wenn dem Verantwortlichen rechtliche Mittel zur Verfügung stehen, die er vernünftigerweise einsetzen könnte, um mit Hilfe Dritter (z.B. der zuständigen Behörde und des Internetanbieters) die betroffene Person anhand der gespeicherten IP-Adresse bestimmen zu lassen (BGH ZD 2017, 424 = MMR 2017, 605).

Dies ist sowohl hinsichtlich der Beklagten als auch hinsichtlich Google LLC der Fall. Beiden stehen die rechtlichen Mittel zur Verfügung, über Zusatzinformationen von der IP-Adresse einen Rückschluss auf die natürliche Person zu ziehen.

Als Telekommunikationsanbieterin und Websitebetreiberin kann die Beklagte, soweit es sich bei den Besuchern um ihre Kunden handelt, ohne großen Aufwand Internet-Nutzer identifizieren, denen sie eine IP-Adresse zugewiesen hat, da sie in der Regel in Dateien systematisch Datum, Zeitpunkt, Dauer und die dem Internet-Nutzer zugeteilte dynamische IP-Adresse zusammenführen kann. In Kombination können die eingehenden Informationen dazu benutzt werden, um Profile der natürlichen Personen zu erstellen und sie (sogar ohne Heranziehung Dritter) zu identifizieren (vgl. BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 20).

Gleiches gilt für Google LLC, die als Anbieterin von Online-Mediendiensten ebenso über die Mittel verfügt, Personenprofile zu erstellen und diese auszuwerten. Dabei kann gerade die IP-Adresse als personenspezifisches Merkmal dienen (vgl. LG W. I, Urt. v. 20.01.2022 – 3 O 17493/20) und etwa in der Kombination mit der Nutzung anderer Onlinedienste zur Identifizierung herangezogen werden (Feldmann, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Kapitel 4. Datenschutzkonformer Einsatz von Suchmaschinen im Unternehmen, Rn. 12). [...]

In den USA ist kein angemessenes Datenschutzniveau gewährleistet (vgl. EuGH Urt. v. 16.07.2020 – C-311/18 – Facebook Ireland u. Schrems, im Folgenden: Schrems II).

Der EuGH hat ausgesprochen, dass der EU-US Angemessenheitsbeschluss („Privacy Shield“) – ohne Aufrechterhaltung seiner Wirkung – ungültig ist. Die gegenständliche Datenübermittlung findet daher keine Deckung in Art. 45 DS-GVO.

Auch etwaige Standarddatenschutzklauseln vermögen die Datenübermittlung in die USA nicht zu rechtfertigen, da sie nicht geeignet sind ein der DS-GVO entsprechendes Datenschutzniveau zu gewährleisten, insbesondere da solche Verträge nicht vor einem behördlichen Zugriff in den USA schützen. [...]

In Schrems II hat der EuGH zwar ausgeführt, dass Standarddatenschutzklauseln als Instrument für den Internationalen Datenverkehr dem Grunde nach nicht zu beanstanden sind, allerdings hat der EuGH auch darauf hingewiesen, dass Standarddatenschutzklauseln ihrer Natur nach ein Vertrag sind und demnach Behörden aus einem Drittstaat nicht binden können: [...]

Wenn sogar der EU-US Angemessenheitsbeschluss aufgrund der Rechtslage in den USA für ungültig erklärt wurde, so kann erst recht nicht davon ausgegangen werden, dass vertragliche Bindungen zwischen privaten Rechtssubjekten

ein angemessenes Schutzniveau nach Art. 44 DS-GVO für die gegenständliche Datenübermittlung in die USA gewährleisten können. Denn diese können schon ihrer Natur nach ausländische Behörden nicht in ihrer Handlungsmacht beschränken. [...]

Dies entspricht auch der Wertung des EuGH:

„Da diese Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen, kann es je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten.“

Solche Maßnahmen müssten geeignet sein, die im Rahmen des Schrems II Urteils des EuGH aufgezeigten Rechtsschutzlücken – also die Zugriffs- und Überwachungsmöglichkeiten von US-Nachrichtendiensten – zu schließen. Dies ist hier nicht gegeben.

Die Beklagte kann sich auch nicht mit Erfolg auf eine Einwilligung i.S.d. Art. 49 Abs. 1 lit. a) DS-GVO berufen. [...]

Nach Art. 4 Nr. 11 DS-GVO ist eine Einwilligung eine unmissverständlich abgegebene Willensbekundung in der Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung. Für die nach Art. 49 Abs. 1 lit. a) DS-GVO erforderliche Einwilligung ist es schon dem Wortlaut nach darüber hinaus erforderlich, dass die Erklärung „ausdrücklich“ abgegeben wird. Angesichts dieser unterschiedlichen Wortwahl sind an die Einwilligung zu Übermittlungen in Drittländer höhere Anforderungen als an sonstige Einwilligungen zu stellen. Insbesondere setzt Art. 49 Abs. 1 lit. a) DS-GVO schon dem Wortlaut nach eine besondere Informiertheit voraus.

Der Einwilligende muss u.a. darüber informiert worden sein, an welche Drittländer und an welche Empfänger seine Daten übermittelt werden (BeckOK DatenschutzR/Lange/Filip DS-GVO Art. 49 Rn. 7; Klein/Pieper, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, Art. 49 Ausnahmen für bestimmte Fälle Rn. 6).

Hier sind die Website-Besucher aber keineswegs über eine Datenübermittlung an Google LLC unterrichtet worden. In den ehemaligen Datenschutzhinweisen wurde lediglich über eine Übermittlung von Daten an Xandr und Heap informiert, was ersichtlich nicht den Empfänger Google LLC erfasst.

## Presseveröffentlichungen:

### Verwaltungsgericht Köln verpflichtet Bundesgesundheitsministerium zur Herausgabe von Unterlagen zur Maskenbeschaffung

(VG Köln, Urteil vom 19. Januar 2023 – 13 K 2382/21 und 13 K 3485/21 –)

Das Bundesgesundheitsministerium ist zur Herausgabe von Informationen über die Beschaffung von FFP-2-Masken im Zuge der Corona-Pandemie verpflichtet. Dies hat das Verwaltungsgericht Köln mit zwei Urteilen vom 19.01.2023 entschieden. Herausgegeben sind Gutachten und anderweitige

Stellungnahmen einer Beratungsgesellschaft und einer Anwaltskanzlei sowie dem Grunde nach auch E-Mail-Korrespondenz zwischen dem damaligen Gesundheitsminister Jens Spahn und der Unternehmerin Andrea Tandler.

Das Ministerium schrieb im März 2020 in einem so genannten Open-House-Verfahren die Beschaffung von Schutzmasken aus. Bei einem solchen Verfahren hat jedes Unternehmen, das die vorgegebenen Vertragsbedingungen und Preise akzeptiert, einen Anspruch auf Vertragsschluss. Dabei bot der Bund jedem Lieferanten einen Festpreis von 4,50 Euro pro FFP-2-Maske. Zur Unterstützung bei der Abwicklung der Beschaffungsverfahren beauftragte das Ministerium eine Wirtschaftsprüfungsgesellschaft und eine Anwaltskanzlei. Geliefert wurden mehr als eine Milliarde Masken.

Ob Maskenlieferanten ihre vertraglichen Verpflichtungen erfüllt haben, ist Gegenstand zahlreicher zivilgerichtlicher Verfahren, die vor dem Landgericht Bonn anhängig waren und sind. Einer der dort klagenden Unternehmer beantragte auf der Grundlage des Informationsfreiheitsgesetzes beim Bundesgesundheitsministerium im Dezember 2020, ihm Zugang zu allen Gutachten und anderweitigen Stellungnahmen der vom Ministerium beauftragten Beratungsgesellschaft und der Kanzlei zu gewähren. Eine andere Person beantragte im Januar 2021 unter Bezugnahme auf einen Artikel in der Zeitschrift „Der Spiegel“ mit dem Titel „Spahns Schutzmasken-Fiasko“, ihm sämtlichen Schriftverkehr zwischen Jens Spahn und Andrea Tandler in den Jahren 2020 und 2021 zu übersenden. Das Ministerium lehnte die Anträge ab. Dagegen erhoben die Antragsteller jeweils Klage.

Die Klagen hatten weitestgehend Erfolg. Zur Begründung hat das Gericht ausgeführt: Die vom Ministerium angeführten Versagungsgründe stehen der Erteilung der begehrten

Informationen nicht entgegen. Die pauschale Behauptung, eine Informationserteilung bedeute angesichts von mehreren zehntausend zu sichtenden Seiten einen unverhältnismäßigen Verwaltungsaufwand, greift im Hinblick auf die Größe des Ministeriums nicht durch. Auch würden Beratungen der Behörde nicht beeinträchtigt. Die Entscheidung über die Maskenbeschaffung ist abgeschlossen. Ein im Anschluss daran fortlaufender Beratungsprozess lässt sich auch nicht mit dem Argument des Ministeriums konstruieren, die begehrten Informationen betreffen auch die laufenden zivilgerichtlichen Verfahren. Die Informationserteilung hat auch keine nachteiligen Auswirkungen auf die Durchführung eines laufenden Gerichtsverfahrens. Der entsprechende gesetzliche Ausschlussgrund dient dem ordnungsgemäßen Ablauf eines gerichtlichen Verfahrens. Er schützt hingegen nicht die Erfolgsaussichten der öffentlichen Hand vor Gericht. Zudem hat das Ministerium nicht hinreichend dargelegt, welche nachteiligen Auswirkungen die Herausgabe der Informationen auf die zivilgerichtlichen Verfahren haben soll. Dafür, dass die Herausgabe der E-Mail-Korrespondenz zwischen Minister Spahn und Frau Tandler nachteilige Auswirkungen auf die Durchführung strafrechtlicher Ermittlungen haben könnte, hat das Ministerium nichts Hinreichendes vorgebracht. Die mit einem der Urteile ausgesprochene Pflicht zur Herausgabe der E-Mails erstreckt sich allerdings nicht auf solche Teile, die Geschäftsgeheimnisse enthalten. Inwieweit dieser Vorbehalt greift, ist durch das Ministerium zu prüfen.

Gegen die Urteile können die Beteiligten jeweils einen Antrag auf Zulassung der Berufung stellen, über den das Oberverwaltungsgericht in Münster entscheiden würde.

*(Pressemitteilung des VG Köln vom 20.01.2023)*

## BERICHTE, INFOS, SONSTIGES

### Das Forschungsdatengesetz

Das Bundesministerium für Bildung und Forschung (BMBF) führte bis einschließlich den 11.04.2023 eine öffentliche Konsultation zum geplanten Forschungsdatengesetz durch. Wie bereits im Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschland (SPD), Bündnis 90/DIE GRÜNEN und den Freien Demokraten (FDP) vorgesehen, soll mithilfe eines neuen Forschungsdatengesetzes der Zugang zu Forschungsdaten für die öffentliche und private Forschung verbessert sowie vereinfacht werden.<sup>1</sup> Die Einführung neuer Forschungsklauseln soll hierbei für ein wissenschaftsfreundlicheres Umfeld sorgen.

Dieses Vorhaben ist besonders aus Sicht staatlich geförderter Forschungsprojekte wie das Krisenresilienz Projekt CoyPu<sup>2</sup>, welches im Rahmen der Entwicklung einer Krisenresilienzplattform auf die Akquisition hochwertiger Datensätze angewiesen ist, begrüßenswert. Derartige Forschungsprojekte begegnen des Öfteren im Rahmen ihrer Forschungsarbeit rechtlichen Hindernissen, die den Zugang zu und die

<sup>1</sup> Koalitionsvertrag 2021-2025 zwischen der SPD, BÜNDNIS 90/DIE GRÜNEN und FDP, S. 21, Zeile 613-615.

<sup>2</sup> Das Projekt Cognitive Economy Intelligence Plattform für die Resilienz wirtschaftlicher Ökosysteme (CoyPu) (mehr unter: <https://coypu.org>) adressiert die komplexen (wirtschaftlichen) Herausforderungen in Krisensituationen mit einer intelligenten Plattform und wird gefördert durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK).

Verarbeitung von geeigneter Daten erheblich erschweren können. Es bleibt abzuwarten, ob die inhaltliche Ausgestaltung des Forschungsdatengesetzes für eine umfassende und den Anforderungen gerecht werdende Rechtssicherheit sorgen könnte. Auch die potenzielle Nutzung etwaiger Verhaltensregeln gemäß des Art. 40 DS-GVO könnte hierbei von Bedeutung werden.

Sowohl die Erfahrungen der Praxis als auch das Bestreben der Koalition, ein solches Gesetz zu schaffen, zeigen, dass es besonders für den Forschungssektor vorteilhaft sein könnte, die derzeitige Forschungsdateninfrastruktur sowohl auf nationaler als auch auf europäischer Ebene weiterzuentwickeln und voranzutreiben. Hierbei wird allerdings thematisch nicht nur die Frage der datenschutzrechtlichen Anforderungen an die Weitergabe vollständig anonymisierter Daten betroffen sein. Auch die Frage der Anforderungen an einen sog. Datenraum, welcher ein wesentlicher Bestandteil der zu schaffenden Dateninfrastruktur darstellt, wird mit hoher Wahrscheinlichkeit eine wichtige Rolle in der Erarbeitung des Forschungsdatengesetzes sein.

Der SRIW wird im Rahmen des Forschungsprojekts CoyPu die Entwicklung beobachten und mögliche Bedarfe, Konflikte aber auch positive Chancen des Gesetzesvorhabens veröffentlichen.

*Sakyi Mannah*

## Prof. Dr. Tobias Keber neuer Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Der Landtag von Baden-Württemberg hat Herrn Prof. Dr. Tobias Keber mit großer Mehrheit zum Landesbeauftragten für den Datenschutz und die Informationsfreiheit gewählt. Er hat sein Amt zum 1. Juli 2023 angetreten. Prof. Dr. Keber ist seit 2012 Inhaber einer Professur für Medienrecht und Medienpolitik an der Hochschule der Medien in Stuttgart sowie Dozent im Masterstudiengang Medienrecht des Mainzer Medieninstituts für internationales Medien- und Datenschutzrecht.

Prof. Dr. Keber ist der GDD langjährig als Vorsitzender ihres Wissenschaftlichen Beirates verbunden. Zu den Aufgaben des Wissenschaftlichen Beirates gehört die Beratung des Vorstandes der GDD in Grundsatzfragen des Datenschutzes sowie die Ermittlung der Preisträger des jährlich vergebenen GDD-Wissenschaftspreises. Zudem ist Prof. Keber Mitglied des Praxisbeirates der von der GDD mitherausgegebenen Fachzeitschrift RDV.

Mit Herrn Prof. Dr. Keber hat das Land Baden-Württemberg als neuen Landesbeauftragten einen hervorragenden Experten im Datenschutz, der basierend auf seine Forschungstätigkeit auch die aktuellen und rasanten Entwicklungen beim Einsatz von Künstlicher Intelligenz (KI) kompetent begleiten kann.

*RDV-Redaktion*

# BERICHT AUS BRÜSSEL

## Endspurt in der EU-Digitalpolitik

**Kai Zenner\***

Mitte Mai 2023 hat der Rat der Europäischen Union entschieden: die nächste Europawahl findet in weniger als zwölf Monaten vom 6. bis zum 9. Juni 2024 statt. Ungeachtet dessen befinden sich noch 28 Digitalgesetze in den politischen Verhandlungen in Brüssel. Die Europäische Kommission plant darüber hinaus die Präsentation von 9 weiteren Vorschlägen bis Ende des Jahres. Ist es realistisch, dass alle 37 Gesetzesvorhaben bis zur Europawahl offiziell Inkrafttreten? Grundsätzlich ist diese Frage mit 'nein' zu beantworten. Evidenzbasierte Politik, welche die Entscheidungsträger zwingt, den Vorschlag ausführlich zu analysieren und die verschiedenen Interessen miteinander auszubalancieren, benötigt je nach Gesetz wohl mindestens 12 Monate intensiver Verhandlungen. Selbst nach einer Einigung zwischen Vertretern des Europäischen Parlaments und der EU-Mitgliedstaaten stehen noch die Abstimmungen im Plenum und der Fachminister vor. Auch die sprachliche und rechtliche Überprüfung durch Spezialisten, das Übersetzen des Textes in die 24 EU-

Amtssprachen sowie die Veröffentlichung des finalen Gesetzes im offiziellen EU-Amtsblatt dauert mehrere Wochen. Damit eine der 37 Initiativen noch vor der Wahl zum Gesetz werden kann, müssten die jeweiligen politischen Verhandlungen bis spätestens Ende Januar 2024 abgeschlossen sein. In den meisten Fällen dürfte nicht genügend Zeit zur Verfügung stehen.

Das von diesen etablierten Erfahrungswerten aber aufgrund von massivem politischen Druck immer mehr abgewichen wird, zeigte zuletzt der Data Act. Der Vorschlag gilt als eines der wichtigsten aber auch kompliziertesten Digitalgesetze dieser Legislaturperiode. Der Plan der Kommission: das Aufbrechen der existierenden Datensilos damit gerade die kleinen und mittleren EU-Marktakeure die ungenutzten Datenschätze verwerten können. Während dieses Vorhaben grundsätzlich sehr sinnvoll erscheint, wurden die konkreten Vorschläge der EU allerdings von fast allen Akteuren, von US-Technologiekonzernen über europäische KMUs bis hin zur Zivilgesellschaft, kritisiert. Auch der

Bericht des Europäischen Parlaments und die generelle Ausrichtung des Rates halfen wenig dabei der großen Skepsis entgegenzuwirken. Letztendlich schlossen die EU-Gesetzgeber die Trilogverhandlungen in rekordverdächtigen drei Monaten ab. Es schien am Ende wichtiger zu sein den Data Act öffentlich als Gesetz zu verkünden als sicherzustellen, dass die Details stimmen und man mit ihm die anvisierten Ziele überhaupt erreichen kann. Ähnliches passierte schon 2022 beim Digital Services Act. Die Französische Regierung wollte die politische Einigung unbedingt während ihrer Ratspräsidentschaft erzielen und die Erfolgsmeldung noch vor den eigenen nationalen Wahlen verkünden. Dies klappte zwar äußerst knapp, viele Details mussten aber auf technischer Ebene wochenlang nachverhandelt werden. Beide Beispiele stehen für einen grundsätzlichen Trend in Brüssel, welcher den Prinzipien zur besseren Rechtsetzung konträr entgegensteht.

Keine guten Aussichten für die nächsten 6 Monate. Stand die Zeit vor der Europawahl traditionell in Brüssel schon immer für große Emotionen, könnte die faktische Nichtbeachtung der besseren Rechtsetzungsagenda nun dazu führen, dass viele Initiativen noch schnell beschlossen werden, um politische Akzente im Wahlkampf zu setzen. Zumindest aus rechtlicher Sicht ein höchst problematisches Vorgehen. Wie so häufig in meinem 'Bericht aus Brüssel' ein kurzer Blick zur KI-Verordnung, wo man bisher einen anderen Weg gegangen ist. Nach 43 technischen Sitzungen und 12 Treffen auf politischer Ebene in knapp einem Jahr konnte sich das Europäische Parlament im Juni 2023 über die insgesamt 89 Erwägungsgründe, 85 Artikel und 9 Annexe final einigen. In mühsamer Kleinstarbeit ist es dem EU-Ko-Gesetzgeber zum Beispiel gelungen, die vielen Überschneidungen und

Widersprüche zu anderen Digitalgesetzen wie der DS-GVO aufzuheben. Zudem wurden wichtige systematische Änderungen vorgenommen, so dass die KI-Verordnung nun mehr auf den Kontext, in welchem ein hochriskantes KI-System genutzt wird, eingeht und auch dem rasanten technologischen Fortschritt mit mehr Flexibilität entgegentritt. Die EU ist daher auf einem guten Weg die KI-Technologien zukunftssicher zu regulieren. Dennoch hört man seit einigen Wochen mehr und mehr Abgeordnete, Vertreter der Mitgliedstaaten und der Kommission davon sprechen, dass in den gestarteten Trilogverhandlungen Geschwindigkeit wichtiger sei als Qualität. Doch was ist mit innovationsfördernden Maßnahmen? Wie soll die KI-Verordnung national umgesetzt werden? Welche Rolle spielen Kommission und AI Office gegen Fragmentierung? Wie verhindert man, dass die neuen Regeln wieder zu einer Marktkonzentration führen, da sich vor allem KMUs mit der Gesetzeseinhaltung schwer tun? Mit viel Glück und Geschick ist es möglich diese Fragen bis Januar 2024 aufzulösen. Falls es aber nicht gelingt, ist im Falle der KI-Verordnung, wie auch bei allen anderen 36 verbleibenden Initiativen, zu hoffen, dass Qualität immer im Vordergrund steht. Sollten bis Juni 2024 wirklich alle Vorhaben verabschiedet worden sein, hätte die EU insgesamt 104 Digitalgesetze. Viele davon widersprüchlich und überlappend zueinander. Weder der Wirtschaft, Wissenschaft noch der Zivilgesellschaft wäre damit geholfen. Am wenigsten aber der EU, welche sich noch mehr Kritik ausgesetzt sehen würde.

\* Kai Zenner ist Büroleiter und Digitalreferent für MdEP Axel Voss und als Experte des AI Netzwerks der OECD tätig. Der Beitrag gibt die persönliche Auffassung des Autors und nicht die des Europäischen Parlaments wieder.

## BUCHBESPRECHUNG

Ebers (Hrsg.), **Stichwort-Kommentar Legal Tech – Recht | Geschäftsmodelle | Technik**, Nomos Verlag, Baden-Baden, 2023, 1418 S., 149,- €<sup>1</sup>

„Metaverse“, „KI“, „ChatGPT“... – Schlagworte über Schlagworte. Selbst Beethovens 10. Symphonie soll nunmehr durch Künstliche Intelligenz zu Ende komponiert worden sein.<sup>2</sup> Auch der letzte Skeptiker wird also mit dieser fortschreitenden Digitalisierung irgendwann in Kontakt kommen. Für den juristischen Bereich ist es Legal Tech – also das Thema, das der hier rezensierte Stichwort-Kommentar zum Gegenstand hat. Denn die IT-basierte Optimierung rechtlicher Handlungsfelder ist Gegenwart und Zukunft der (juristischen) Berufe, gleich ob gerichtlich oder außergerichtlich. Was das aber nun konkret für die eigene Beratungs- und Entscheidungssituation bedeutet, beleuchtet dieser hervorragende Kommentar. Und zwar in 96 Abschnitten; von Algorithmus, Geschäftsmodellen, Blockchain, Cloudcomputing, natürlich dem Datenschutz, der Dokumentenanalyse, E-Justice und

E-Government, Haftung, Paytech, vorhandene Techniken und sehr vielem mehr. Die entscheidenden rechtlichen Aspekte des Einsatzes von Legal Tech-Anwendungen werden unter Einbeziehung aller betroffenen, auch angrenzenden Rechtsgebiete wie Landesrecht pp. verständlich und fallbezogen dargestellt. Insbesondere die alphabetische Gliederung des Stichwort-Kommentars erleichtert auch dem Neuling im Bereich Legal Tech den Einstieg. Er bietet zudem auch die Möglichkeit eines vertieften Durchdringens der Materie auf hohem, insbesondere praxisrelevantem Kommentarniveau. Mit dem von Ebers herausgegebenen, handlichen und auch optisch ansprechenden Stichwort-Kommentar ist man bis auf Weiteres im Bereich Legal Tech bestens bedient.

<sup>1</sup> Rezensiert von RA/FA InsR/Testamentsvollstrecker (AGT) Christian Weiß, Wellensiek Rechtsanwälte Köln.

<sup>2</sup> So <https://www.dw.com/de/beethoven-10-sinfonie-unvollendete-ki-k%C3%BCnstliche-intelligenz/a-59378632>, abgerufen 07.05.2023.



## Kollege ChatGPT - Generative Künstliche Intelligenz ist in Unternehmen angekommen



Chat-Bots sind in Unternehmen angekommen. Sie werden in Callcentern unter Verarbeitung von Kundendaten eingesetzt. Das geschieht teilweise unter Auswertung der Stimmung von Kunden und ruft Verbraucher- und Datenschützer auf den Plan. Virulent ist auch KI im Arbeitsleben. Die Bundesregierung plant kurzfristig ein Gesetz für den Beschäftigtendatenschutz anzustoßen. Es wird dort auch um KI gehen. Ohne spezifische Regelungen dazu kann die Situation entgleiten, denn es droht großes Streitpotenzial nicht nur mit Betriebsräten und Datenschützern. Schließlich ist es möglich, dass etwa ChatGPT Vorschläge zur Zusammenarbeit von Beschäftigten macht, aber auch zur Vorauswahl von Bewerbern. Formulierungen von Bewerberabsagen

oder die Abfassung einer Kündigung oder einer Klage kann der Bot auch übernehmen. Auch die Haftungsfrage bei Fehlern und Rechtsverletzungen ist offen. Sie stellt sich für Anwender und Nutzer generativer KI. Haftet der Arbeitgeber, der (nicht) autorisiert den Bot nutzende Arbeitnehmer, der Anbieter der Datenbasis oder etwa Microsoft oder SAP, die die Software einbinden oder Anbieter des Datenpools auf den der Bot zugreift? Welche Rechte hat der Betriebsrat und können Kunden oder Beschäftigte den Einsatz von solchen Anwendungen ablehnen? Bevor man die neue Technik einsetzt, sollten diese Fragen geklärt sein. Anderenfalls kann man vor Gericht wegen des nicht verantwortbaren Einsatzes Schiffbruch erleiden.

# DSGVO

CHANCE FÜR ENTLASTUNGEN?

2024

5. SEPT 2023, 15–18 UHR  
#DSGVO2024

PRÄSENZ (BERLIN) UND  
LIVESTREAM

Eine Kooperation von



## DSGVO 2024 – CHANCE FÜR ENTLASTUNGEN?

Seit dem 25. Mai 2018 ist die Datenschutzgrundverordnung (DSGVO) in allen EU- und EWR-Mitgliedsstaaten verbindliches Recht. Ein wichtiger und richtiger Schritt! Datenschutz steht für Vertrauen und wird für viele Unternehmen zum Wettbewerbsvorteil. So verwundert es nicht, dass die DSGVO sich mittlerweile zum Exportschlager entwickelt hat und vielerorts auf der Welt als Blaupause für neue Datenschutzregeln dient.

Doch natürlich gibt es Optimierungspotenzial. Insbesondere kleine und mittlere Unternehmen klagen über die büro-

kratische Belastung durch die DSGVO, auch im Kontext der zunehmenden Digitalisierung. Der Gesetzgeber hat mitgedacht und im Text der DSGVO festgelegt, dass diese erstmals 2020 und dann alle vier Jahre einer Evaluation unterzogen wird. Gemeinsam mit Expertinnen und Experten aus Politik, Verbänden und Unternehmen möchten wir schon jetzt die Diskussion zur DSGVO-Evaluation 2024 eröffnen. Unser Fokus dabei lautet: Wie lässt sich die Wirtschaft besser unterstützen, um datenschutzrechtliche Anforderungen zu erfüllen?

### PROGRAMM

- › Die DSGVO als nachhaltiges Recht
- › Die Sicht der Praxis – wo der Schuh drückt
- › Potentiale und Ergänzungsbedarf der DSGVO
- › Zum Potential der Begleitgesetzgebung und zur Evaluation des BDSG
- › Diskussion der Expertinnen und Experten

### WO?

ALTE MÜNZE BERLIN  
Molkenmarkt 2, 10179 Berlin

### UNTER ANDEREM MIT

- › Dr. Viviane **Reding** (EU-Kommissarin a.D.)
- › Andrea **Backer-Heuvel** (ds<sup>2</sup> Unternehmensberatung)
- › Anna **Kassautzki**, MdB (SPD)
- › Misbah **Khan**, MdB (Bündnis 90/Die Grünen)
- › Mag. Judith **Leschanz** (A1 Telekom)
- › Dr. Simon **Menke** (Otto)
- › Prof. Dr. Boris **Paal** (Universität Leipzig)
- › Dr. Markus **Peifer** (ZDH)
- › Frederick **Richter** (Stiftung Datenschutz)
- › Stefan **Sobotta** (BMI)
- › Thomas **Spaeing** (BvD)
- › und weitere

▶ **Anmeldung und alle Infos auf [www.dsgvo-2024.org](http://www.dsgvo-2024.org)**

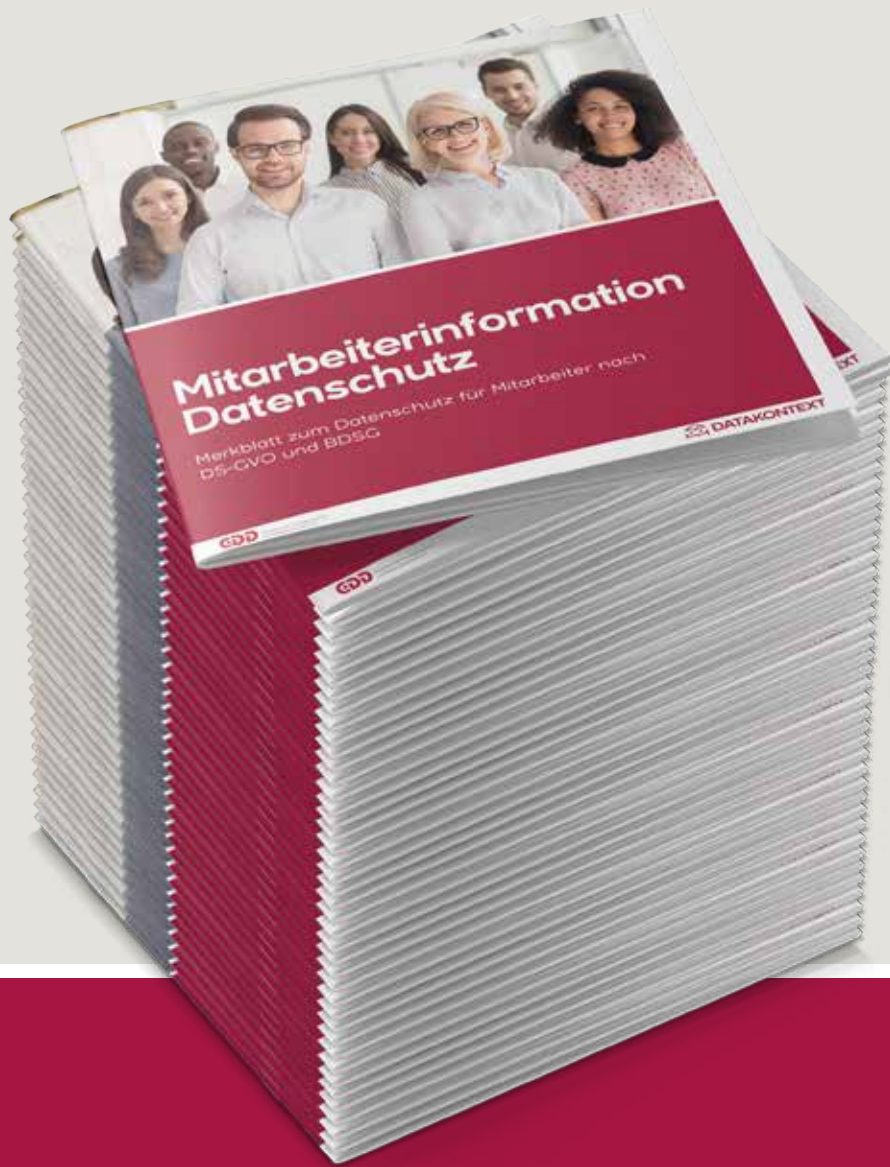


Bundesministerium  
der Justiz

Die Arbeit der Stiftung Datenschutz wird aus dem Bundeshaushalt gefördert (Einzelplan des BMJ)

Medienpartner





**Bestseller**  
millionenfach  
verkauft

# Mitarbeiterinformation Datenschutz

Mitarbeiter einfach und rechtssicher sensibilisieren

- ideal für alle Mitarbeiter
- leicht verständlich
- anschaulich illustriert
- firmenindividuell gestaltbar
- in 5 Sprachen verfügbar

Jetzt bestellen: [datakontext.com/mitarbeiterinformation](https://datakontext.com/mitarbeiterinformation)