

# 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  
Dr. 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/THÜSING:** Die Benennung und Abberufung des Datenschutzbeauftragten

**SIMWINGA:** SRB Rechtssache C-413/23P: Der Begriff „personenbezogene Daten“ und das Risiko der Identifizierung

**KEBER:** Reform der Datenschutzaufsicht –  
Föderale Konzentration statt ineffiziente Zentralisierung

## KURZBEITRÄGE

**SRINIVASAN:** End-user responsibilities on a Generative AI conversation

**KÖHLER:** Zur Maßgeblichkeit automatisierter Entscheidungsvorbereitungen

**REIF:** Praxisfälle zum Datenschutzrecht XXXV: Einschaltung von Dienstleistern –  
Besser am Anfang schon ans Ende denken

## RECHTSPRECHUNG

**EUGH:** Anspruch auf Erläuterung der automatisierten Entscheidung

**BGH:** Verbraucherschutzverbände können Datenschutzverstöße wettbewerbsrechtlich verfolgen

**BGH:** BGH bestätigt Schadenersatz bei Kontrollverlust

**OLG:** Löschungspflicht von Einträgen über erledigte Zahlungsstörungen bei Kreditauskunfteien

**LG:** Maßgeblichkeit des Scorings für die Entscheidung im Rahmen von Art. 22 Abs. 1 DS-GVO

**ArbG:** Datenschutzwidrige Mitteilung zum Krankenstand eines Arbeitnehmers

**OVG:** Kein Anspruch auf Ende-zu-Ende-Verschlüsselung





**Hybrid:  
Online &  
in Köln**

# 49. DAFTA

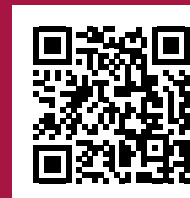
13.-14. November 2025

# 44. RDV-Forum

12. November 2025

Datenschutz trifft Innovation –  
KI verantwortungsvoll gestalten

Jetzt anmelden: [www.datakontext.com/dafta-2025](http://www.datakontext.com/dafta-2025)



<b>EDITORIAL</b>	<b>171</b>	<b>RECHTSPRECHUNG</b>	
		HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ	
<b>VERANSTALTUNGEN</b>	<b>172</b>	<b>Anspruch auf Erläuterung der automatisierten Entscheidung</b> (EuGH, Urt. v. 27.02.2025)	<b>194</b>
<b>AUFSÄTZE</b>		<b>Verbraucherschutzverbände können Daten- schutzverstöße wettbewerbsrechtlich verfolgen</b> (BGH, Urt. v. 27.03.2025)	<b>198</b>
Prof. Peter GOLA/Prof. Dr. Gregor THÜSING, LL.M. <b>Die Benennung und Abberufung des Datenschutzbeauftragten</b>	<b>173</b>	<b>WICHTIGES AUS DER RECHTSPRECHUNG</b> <b>BGH bestätigt Schadenersatz bei Kontrollverlust</b> (BGH, Urt. v. 11.02.2025)	<b>203</b>
Henry SIMWINGA, LL.M. <b>SRB Rechtssache C-413/23P: Der Begriff „personenbezogene Daten“ und das Risiko der Identifizierung</b>	<b>179</b>	<b>Löschungspflicht von Einträgen über erledigte Zahlungsstörungen bei Kreditauskunfteien</b> (OLG Köln, Urt. v. 11.04.2025)	<b>203</b>
Prof. Dr. iur. Tobias KEBER <b>Reform der Datenschutzaufsicht – Föderale Konzentration statt ineffiziente Zentralisierung</b>	<b>184</b>	<b>Maßgeblichkeit des Scorings für die Entscheidung im Rahmen von Art. 22 Abs. 1 DS-GVO</b> (LG Bamberg, Urt. v. 26.03.2025)	<b>206</b>
<b>KURZBEITRÄGE</b>		<b>Datenschutzwidrige Mitteilung zum Krankenstand eines Arbeitnehmers</b> (ArbG Duisburg, Urt. v. 26.09.2024)	<b>208</b>
Ganesh SRINIVASAN <b>End-user responsibilities on a Generative AI conversation</b>	<b>186</b>	<b>Kein Anspruch auf Ende-zu-Ende-Verschlüsselung</b> (OVG NRW, Beschl. v. 20.02.2025)	<b>209</b>
Moritz KÖHLER <b>Zur Maßgeblichkeit automatisierter Entscheidungsvorbereitungen</b>	<b>188</b>	<b>BERICHT AUS BRÜSSEL</b> <b>Vorgaben für GPAI-Modelle</b>	<b>214</b>
RAin Yvette REIF, LL.M. <b>Praxisfälle zum Datenschutzrecht XXXV: Einschaltung von Dienstleistern – Besser am Anfang schon ans Ende denken</b>	<b>190</b>	<b>SCHWAKURAI'S SCHLEPPNETZ</b>	<b>216</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, ada Learning GmbH, Düsseldorf

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 a.D., Bonn

Dr. Martin Kessen, Richter am Bundesgerichtshof, Karlsruhe

Dr. Kevin Leibold, LL.M., Rechtsanwalt, Köln

Thomas Muthlein, DMC Datenschutz Management & Consulting, Frechen

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

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, Referatsleiter bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn

Maria Christina Rost, Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Prof. Dr. Frauke Rostalski, Universität zu Köln

Prof. Dr. Prof. h.c. Jürgen Taeger †, Universität Oldenburg

Rebekka Weiß, LL.M., Microsoft GmbH, 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**

Christina Kopp | Serena Roller  
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 € 185,-  
Einzelheft € 32,-  
MwSt. im Preis enthalten, jeweils inkl. Versandkosten

**Vertrieb/Produktsicherheit**

Torid Kehmeier | Tel.: +49 2234 98949-78  
Torid.kehmeier@datakontext.com  
www.datakontext.com produktsicherheitsverordnung

**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/Hersteller**

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 Verlags. Der Verlag gestattet in der Regel die Herstellung von Fotokopien zu innerbetrieblichen Zwecken, wenn dafür eine Gebühr an die VG Wort, Abteilung Wissenschaft, Goethestr. 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.

**Beilagenhinweis:**

Verlag C.H. Beck, Themenprospekt "Recht Digital 2025"; DATAKONTEXT GmbH, Flyer "Handbuch Beschäftigtendatenschutz"

# VVT im Omnibus - bitte vorsichtig fahren!

Die EU-Kommission plant in sogenannten Omnibus-Paketen EU-Rechtsvorschriften zu vereinfachen und zu harmonisieren. Im Omnibus Pakt IV soll die neue Unternehmenskategorie: „Small Mid-Caps“ (SMC) eingeführt werden, die SMC Unternehmen erfassen, die weniger als 750 Mitarbeiter beschäftigen und entweder einen Jahresumsatz von weniger als 150 Millionen Euro erzielen oder eine Bilanzsumme von weniger als 129 Millionen Euro aufweisen.

Die bestehende Ausnahme von der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten (VVT) gem. Art. 30 DS-GVO, die derzeit für Unternehmen mit weniger als 250 Mitarbeitern gilt, soll auf Unternehmen mit weniger als 750 Mitarbeitern ausgeweitet werden, sofern die Verarbeitung kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Damit würde selbst für größere mittelständische Unternehmen die Basis der Datenschutzorganisation entzogen werden.

Das VVT stellt die Grundlage für die Rechenschaftspflicht gem. Art. 5 Abs. 2 und für das Datenschutzmanagement gem. Art. 24 DS-GVO dar. Im VVT beinhaltet die datenschutzrelevanten Aspekte der Geschäftsprozesse. Es dokumentiert die Rechtmäßigkeit der Datenverarbeitungen und die Angemessenheit der technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO. Zudem erleichtert es die Bearbeitung von Betroffenenrechten wie Auskunftsersuchen und die Klärung von Datenpannen. Für eine Entbürokratisierung ist die geplante Regelung damit sogar kontraproduktiv.

Das VVT wird dann bürokratisch und unproduktiv, wenn es in den Geschäftsprozessen zu kleinteilig angelegt ist und ausgehend von der einzelnen Verarbeitung jede IT-Anwendung erfasst. Der Wortlaut des Art. 30 Abs. 2 DS-GVO könnte hier in der Sache irreführend sein, in dem er auf einzelne „Verarbeitungen“ abstellt. Der Vorgänger der DS-GVO, die EU-Datenschutzrichtlinie (95/46/EG), forderte in Art. 19 eine Meldepflicht für eine Vielzahl von Verarbeitungen, die zur Realisierung eines oder mehrerer verbundener Zweckbestimmungen dienen. Die Umsetzung in § 4d BDSG a.F. sah konsequenterweise eine Meldepflicht von „Verfahren automatisierter Verarbeitungen“ vor.

Eine Entlastung der Unternehmen könnte dadurch erreicht werden, dass im VVT wieder auf eine Bündelung von Verarbeitungen zu verbundenen Zwecken im Sinne von „Verfahren“ abgestellt wird. Diese Begriffsbestimmung nähert sich damit auch der betriebswirtschaftlichen Definition des Geschäftsprozesses an.

Die europäische Dachorganisation CEDPO, deren Vorsitz z.Z. die GDD hat, wird diesen Vorschlag der EU-Kommission unterbreiten als praxisnaher Beitrag zum Bürokratieabbau ohne in die Substanz der Datenschutzorganisation einzugreifen.



**Andreas Jaspers**  
ist Rechtsanwalt und Geschäftsführer  
der Gesellschaft für Datenschutz  
und Datensicherheit (GDD) e.V.

Termine	Thema	Ort	Kontakt
02.09.2025	Datenschutz und Betriebsrat unter der DS-GVO	Online	GDD e.V./DATAKONTEXT
03.09.2025	Websites datenschutzkonform gestalten	Online	GDD e.V./DATAKONTEXT
04.09.2025	Videoüberwachung nach BDSG und DS-GVO	Online	GDD e.V./DATAKONTEXT
08. – 12.09.2025	Einführung in den Datenschutz für die Privatwirtschaft - Teil 1	Köln	GDD e.V./DATAKONTEXT
10.09.2025	KI-Datenschutz im Konzern	Online	GDD e.V./DATAKONTEXT
25.09.2025	Datenschutz Aktuell	Online	GDD e.V./DATAKONTEXT
30.09. – 01.10.2025	Ausbildung zum/zur Datenschutzkoordinator/in	Köln	GDD e.V./DATAKONTEXT
06. – 08.10.2025	Einführung in den technisch-organisatorischen Datenschutz - Teil 2	Hamburg	GDD e.V./DATAKONTEXT
10.10.2025	Kollege ChatGPT	Online	GDD e.V./DATAKONTEXT
14. – 16.10.2025	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
16.10.2025	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
14.10.2025	Konzerndatenschutz	Online	GDD e.V./DATAKONTEXT
15.10.2025	Datenschutz im Home Office und mobilen Arbeiten – Risiken minimieren, Sicherheit maximieren	Online	GDD e.V./DATAKONTEXT
28.10.2025	Datenschutz und IT-Sicherheit in der Cloud	Online	GDD e.V./DATAKONTEXT
29.10.2025	Kennzahlen und KPIs als Mittel zur Überwachung des Datenschutzes	Online	GDD e.V./DATAKONTEXT
30.10.2025	Datenschutz in medizinischen Einrichtungen	Online	GDD e.V./DATAKONTEXT
04.11.2025	Datenschutz im Internet	Online	GDD e.V./DATAKONTEXT
05. – 06.11.2025	Datenschutz-Management nach der DS-GVO - Teil 3	Online	GDD e.V./DATAKONTEXT
12. – 14.11.2025	44. RDV-Forum und 49. Datenschutzfachtagung (DAFTA)	Köln / Online	GDD e.V./DATAKONTEXT
17. – 19.11.2025	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
19.11.2025	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
20.11.2025	Unbegrenzte Mobilität – Cloud, Apps & KI datenschutzkonform einsetzbar?	Online	GDD e.V./DATAKONTEXT



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

## AUFSÄTZE

Prof. Peter Gola/Prof. Dr. Gregor Thüsing, LL.M. (Harvard)

# Die Benennung und Abberufung des Datenschutzbeauftragten<sup>1</sup>

Der folgende Beitrag widmet sich den rechtlichen Grundlagen der Benennung sowie der Abberufung des betrieblichen/behördlichen Datenschutzbeauftragten (DSB). Ausgehend von einem Überblick zu den maßgeblichen Vorschriften der DS-GVO und dem BDSG werden die verschiedenen Möglichkeiten der Einbindung des DSB aufgezeigt. Schließlich wird auf die Form und Befristung der Benennung sowie auf den Abberufungs- und Benachteiligungsschutz des DSB eingegangen.

## I. Allgemeines

Abgesehen von den Voraussetzungen der Pflicht zur Bestellung des DSB und seiner Verschwiegenheit, die der nationale Gesetzgeber – z.T. von der Verordnung abweichend bzw. sie ergänzend – im BDSG geregelt hat, bestimmt sich die Tätigkeit des betrieblichen bzw. behördlichen Datenschutzbeauftragten nach der DS-GVO. Der nationale Gesetzgeber hat in den behördlichen Datenschutzbeauftragten des Bundes betreffenden Regelungen des BDSG (§§ 5–7) Bestimmungen der Verordnung wiederholt und ergänzt. Wiederholungen erfolgten, um auch Behörden, die nicht von der DS-GVO betroffen sind, zu einer DSB-Bestellung gem. der Verordnung zu verpflichten. Zum Teil wird auf diese Normen auch für betriebliche DSB in § 38 Abs. 2 BDSG verwiesen, die für den privaten Bereich die Bestellpflicht über den von der DS-GVO gesetzten Rahmen ausdehnen, aber für kleinere „Einheiten“ noch Ausnahmen zulassen. Aufgabe des DSB ist es, eine unabhängige und „geschützte“ interne Kontroll- und Beratungsfunktion des die Datenschutzverantwortung tragenden „Verantwortlichen“ wahrzunehmen.<sup>2</sup>

## II. Pflicht zur Benennung

### 1. Die DS-GVO

Behörden sind grundsätzlich zur Benennung eines Datenschutzbeauftragten verpflichtet. Für private datenverarbeitende Stellen sieht Art. 37 Abs. 1 DS-GVO eine Bestellpflicht nur unter bestimmten Voraussetzungen vor, nämlich wenn deren Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, welche eine regelmäßige und systematische Beobachtung von betroffenen Personen in großem Umfang erforderlich machen, die Verarbeitung besonderer Kategorien von Daten gem. Art. 9 Abs. 1 DS-GVO in großem Umfang oder von Daten zu strafrechtlichen Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO zum Gegenstand haben.

### 2. Das BDSG

Die §§ 5 bis 7 BDSG regeln Näheres zur Bestellung und den Aufgaben von Datenschutzbeauftragten aller öffentlichen Stellen des Bundes. Dies geschieht weitgehend in Übereinstimmung mit der DS-GVO, um eine einheitliche Regelung auch für nicht in den Anwendungsbereich der DS-GVO fallende Behörden zu schaffen.

Der deutsche Gesetzgeber weicht hinsichtlich der Bestellpflicht nicht öffentlicher Verantwortlicher und Auftragnehmer von Voraussetzungen der DS-GVO ab und hält in § 38 BDSG für die Bestellpflicht betrieblicher Datenschutzbeauftragter im Wesentlichen an den Bestimmungen des § 4 f Abs. 1 BDSG a.F. fest.

Die Befugnis zur nationalen Regelung enthält Art. 37 Abs. 4 DS-GVO. Die Bestellpflicht besteht bei Verantwortlichen und Auftragsverarbeitern, soweit sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Im Falle einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegenden Datenverarbeitung sowie der geschäftsmäßigen Datenverarbeitung zwecks Übermittlung, anonymisierter Übermittlung oder für Zwecke der Markt- oder Meinungsforschung ist sogar unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein Datenschutzbeauftragter zu benennen. Solange im Bereich der automatisierten Datenverarbeitung weniger als zwanzig Mitarbeiter beschäftigt sind, bedarf es – abgesehen von dem Fall der in Art. 37 Abs. 1 DS-GVO bzw. § 38 Abs. 1 BDSG benannten besonderen Risikobereichen – keines betrieblichen Beauftragten.

Die Öffnungsklausel in Art. 37 Abs. 4 DS-GVO bezieht sich ausschließlich auf die Voraussetzungen, unter denen ein Datenschutzbeauftragter zu bestellen ist. Aufgaben und Rechtsstellung des Datenschutzbeauftragten können vom nationalen Gesetzgeber nicht in Abweichung der DS-GVO geregelt werden.

## III. Das Beschäftigungsverhältnis/ Bestelloptionen

### 1. Allgemeines

Die DS-GVO räumt den Verantwortlichen und den Auftragsverarbeitern in Art. 37 Abs. 2 bis 4 DS-GVO eine gewisse Flexibilität hinsichtlich der Art der DSB-Bestellung ein. Der Datenschutzbeauftragte kann Beschäftigter des Bestellpflichtigen oder dessen freier Mitarbeiter sein. Er kann die Aufgabe ne-

<sup>1</sup> Dieser Beitrag ist ein gekürztes Kapitel aus dem von denselben Autoren verfassten Handbuch Beschäftigtendatenschutz, 9. Aufl. 2025.

<sup>2</sup> Baumgartner/Hansch, ZD 2019, 92; Franck, DSB 2019, 181; Franck/Reif, ZD 2015, 405; Gola, PinG 2020, 84; Gola, RDV 2019, 157; Greiner/Senk, NZA 2020, 201; Heberlein, Juris 1/2019, 19; Jaspers/Reif, RDV 2016, 61; Marschall/Müller, ZD 2016, 415; Niklas/Faas, NZA 2017, 1091.

ben anderen Aufgaben wahrnehmen und insoweit auch Datenschutzbeauftragter anderer Unternehmen oder Behörden sein. So kann er von einer Unternehmensgruppe bestellt sein und dann Dienstleistungen in den beteiligten Unternehmen erbringen. Gleiches gilt hinsichtlich der Bestellung für mehrere Behörden. Dabei ist immer zwischen dem Bestellvorgang und dem Beschäftigungs-/Vertragsverhältnis zu unterscheiden, aus dem sich die arbeits-/dienstrechtlichen Rechte und Pflichten ergeben.

Die Benennung erfolgt durch einseitige empfangsbedürftige Erklärung der Leitung der benennenden Stelle. Da die Rechtsfolgen der Erklärung nicht der Privatautonomie unterliegen, sondern sich unmittelbar aus den Art. 38 f. DS-GVO und §§ 38, 6 BDSG ergeben, handelt es sich nicht um eine Willenserklärung, sondern um eine sog. rechtsgeschäftsähnliche Handlung. Die praktischen Konsequenzen der Unterscheidung sind allerdings gering, weil die Regelungen über Rechtsgeschäfte auf rechtsgeschäftsähnliche Handlungen vielfach entsprechend angewendet werden können, so etwa die Anfechtungs- (§§ 119 ff. BGB) oder Stellvertretungsregeln. Die Anfechtungsregeln werden nicht dadurch verdrängt, dass dem DSB Abberufungsschutz gewährt wird (Art. 38 Abs. 3 S. 2 DS-GVO; § 38 Abs. 3 i.V.m. § 6 Abs. 3 S. 3 BDSG).

## 2. Gemeinsame Datenschutzbeauftragte

### a) Gemeinsame Datenschutzbeauftragte in Unternehmensgruppen

Art. 37 Abs. 2 DS-GVO sieht die Möglichkeit der Bestellung von gemeinsamen Datenschutzbeauftragten in Unternehmensgruppen vor. Damit ist auf EU-Ebene die Klarstellung erfolgt, dass auch sog. Konzerndatenschutzbeauftragte in einem Akt bestellt werden können. Diese ist intern zulässig, wenn das Unternehmen, das die Unternehmensgruppe steuert (also beispielsweise eine Holding) gesellschaftsrechtlich berechtigt ist, in dieser Form in die Organisation der einzelnen Unternehmen einzugreifen.<sup>3</sup>

Die Unternehmensgruppe ist dabei in Art. 4 Nr. 16 DS-GVO als Gruppe definiert, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Diese Definition entspricht der des Konzerns in § 18 AktG. Die Bestellung wird dann – auch wenn Art. 35 Abs. 1 DS-GVO den für die Verarbeitung Verantwortlichen als „Besteller“ vorsieht – von dem herrschenden Unternehmen zu erfolgen haben. In Betracht kommt aber auch das Unternehmen, mit dem der Beauftragte einen Arbeits- oder Dienstvertrag hat.

Auch bei gemeinsamer Benennung besteht die Pflicht zur Meldung des DSB an die Aufsichtsbehörden weiter – für jedes bestellpflichtige Konzernunternehmen eigenständig.<sup>4</sup> Fraglich ist, wie bei einer einheitlichen Benennung gem. Art. 37 Abs. 2 DS-GVO zu verfahren ist. Ein vereinfachtes Meldeverfahren sieht die DS-GVO jedoch auch hier nicht vor<sup>5</sup> und kann auch nicht aus Art. 56 Abs. 1 DS-GVO abgeleitet werden.<sup>6</sup>

Die Berufung eines Konzerndatenschutzbeauftragten ist an die Bedingung geknüpft, dass er von jeder Niederlassung aus „leicht erreicht werden kann“. Die leichte Erreichbarkeit muss mit Blick auf die Aufgaben des Datenschutzbeauftragten sowohl für die Verantwortlichen der einzelnen Konzernunternehmen als auch für die Beschäftigten als betroffene Personen erfüllt sein. Die leichte Erreichbarkeit impliziert den persönlichen und sprachlichen Zugang. Die Kommuni-

kationsmöglichkeiten und die büromäßige Organisation insbesondere eines externen DSB müssen hierauf ausgerichtet sein. Der ausschließlich französischsprachige Konzerndatenschutzbeauftragte bei der Konzernmutter in Paris mit Töchtern in anderen europäischen Staaten wird diese Voraussetzung wohl nicht erfüllen können.<sup>7</sup> Das Kriterium der leichten Erreichbarkeit verlangt auch nach weiteren Konkretisierungen, beispielsweise hinsichtlich der Zurverfügungstellung von (fremdsprachlichem) Hilfspersonal.<sup>8</sup>

### b) Gemeinsame Datenschutzbeauftragte bei Behörden und öffentlichen Stellen

Die Regelung des Art. 37 Abs. 3 DS-GVO eröffnet für den öffentlichen Bereich eine ähnliche gemeinsame Bestellmöglichkeit wie sie für Unternehmensgruppen besteht, wobei jedoch offenbleibt, wie die bei der Benennung des DSB kooperierenden Behörden verbunden sein müssen. Die Organisationsstruktur und Größe muss jedenfalls so gestaltet sein, dass die Aufgaben hinsichtlich des Zeitumfangs und ihrer datenschutzrechtlichen Komplexität voll erfüllt werden können. Das gilt z.B. auch für Schulen, wenn jede/r betroffene Schulleiter/-in der Beauftragung zustimmt.

Auf die leichte Erreichbarkeit stellt die Norm zwar im Wortlaut nicht ab, sie ist aber unter dem Gesichtspunkt der Organisationsstruktur zu berücksichtigen.<sup>9</sup> Für Behörden gilt zudem, dass diese nicht nur einem Bediensteten einer anderen öffentlichen Stelle, sondern auch einem privaten Dienstleister die DSB-Funktion übertragen können.

## 3. Interne und externe Datenschutzbeauftragte

Die Bestellung von internen Datenschutzbeauftragten, d.h. von Beauftragten, die die Tätigkeit als Beschäftigte des Verantwortlichen oder des Auftragnehmers wahrnehmen, ist nach Art. 37 Abs. 6 DS-GVO ebenso möglich sein wie die Beauftragung externer Dienstleister.

In der Regel wird bei größeren Unternehmen ein „interner DSB“, d.h. ein Angehöriger des Unternehmens bzw. der Dienststelle, der den „Betrieb“ und die in der Datenverarbeitung beschäftigten Personen kennt, sinnvollerweise mit der Wahrnehmung dieser Aufgabe betraut werden. Auch in kleineren Stellen bietet sich diese Lösung an, indem die Aufgabe des DSB einem Mitarbeiter übertragen wird, der diese neben seinen bisher Vollzeit wahrgenommenen Aufgaben zu erledigen hat.

Für nicht öffentliche Stellen ist aber auch die Bestellung völlig Außenstehender, die den Datenschutz hauptberuflich ausüben und u.U. auf diese Weise mehrere Unternehmen betreuen, möglich. Der betriebliche Beauftragte kann seine Funktionen jedoch nur dann voll entfalten, wenn er sich möglichst nahe am Ort des Geschehens befindet und nicht

3 Gola/Heckmann/Gola, DS-GVO – BDSG, 3. Aufl. 2022, § 5 Rn. 12.

4 Ehmman/Selmayr/Heberlein, DS-GVO, 3. Aufl. 2024, Art 37 Rn. 38.

5 Vgl. die ausführliche Begründung bei Sundermann, ZD 2020, 275 (277).

6 Vgl. die ausführliche Begründung bei Sundermann, ZD 2020, 275 (277).

7 Vgl. ausführlich bei Sydow/Helfrich, DS-GVO, 3. Aufl. 2022, Art. 37 Rn. 96 ff.; Jaspers/Reif, RDV 2016, 61.

8 Vgl. hierzu Laue/Nink/Kremer, Das neue Datenschutzrecht der betrieblichen Praxis, 3. Aufl. 2024, § 8 Rn. 14; Franck/Reif, ZD 2016, 405.

9 Vgl. auch Jaksch/van Daacke, DuD 2018, 758.

nur nachträglich kontrolliert, sondern die Verantwortlichen kontinuierlich berät und bereits bei der Planung und Vorbereitung von Datenverarbeitungsvorhaben dadurch mitwirkt, dass dem Datenschutz frühzeitig Rechnung getragen wird. Als Vorteil wird für eine solche Lösung anzuführen sein, dass der ggf. für mehrere Unternehmen tätige „hauptberufliche“ externe DSB – eben weil er sich hauptberuflich mit Datenschutzfragen befasst – regelmäßig auch die erforderliche allgemeine Fachkunde haben wird.

Fraglich ist nach wie vor, ob als externer Datenschutzbeauftragter auch eine juristische Person (z.B. Unternehmensberatungsgesellschaft) bestellt werden kann.<sup>10</sup> Die Aufsichtsbehörden lehnen dies im Hinblick auf die Regelungen des BDSG a.F. zutreffend weitgehend ab.<sup>11</sup> Die BfDI macht gegenüber den Leitlinien der Artikel-29-Datenschutzgruppe, die akzeptieren, dass ein externer Datenschutzbeauftragter auch eine juristische Person sein könne, geltend, dass auch nach der DS-GVO jede (natürliche) Person, die innerhalb dieser Organisation Funktionen des Datenschutzbeauftragten wahrnimmt, sämtliche Voraussetzungen für die Benennung eines Datenschutzbeauftragten erfüllen müsse. Dabei müssen in einem Team klare Verantwortlichkeiten festgelegt werden.

Keine Bedenken sollten danach bestehen, einen qualifizierten Angehörigen einer juristischen Person namentlich und verantwortlich zum betrieblichen Datenschutzbeauftragten zu bestellen. Der entsprechende Geschäftsbesorgungsvertrag wird dann mit dem Beratungsunternehmen etc. abgeschlossen, das den zu bestellenden Mitarbeiter benennt. Dabei muss die erforderliche Weisungsfreiheit des DSB aber auch gegenüber seinem Arbeitgeber gewährleistet sein.

#### 4. Teilzeit-Datenschutzbeauftragte

##### a) Allgemeines

Die Datenschutzbeauftragten können ihren Aufgaben in Voll- oder Teilzeit nachgehen, wobei mit Teilzeit gemeint ist, dass sie gleichzeitig andere Aufgaben in der Behörde oder dem Unternehmen oder auch außerhalb, d.h. bei einer anderen Behörde oder in einem Unternehmen wahrnehmen. Die bei dem anderen Unternehmen wahrgenommene Aufgabe kann ebenfalls die eines Datenschutzbeauftragten sein.

Mit der Regelung soll insbesondere auch den Bedürfnissen von bestellungspflichtigen kleinen und mittleren Unternehmen Rechnung getragen werden. Insbesondere wenn ein Beschäftigter die Funktion als Datenschutzbeauftragter nur in Teilzeit wahrnehmen soll, gilt es allerdings gem. Art. 38 Abs. 6 S. 2 DS-GVO Interessenskonflikte zu vermeiden.

##### b) Interessenkonflikte

Interessenkollisionen spielten im Rahmen des § 4f Abs. 2 S. 1 BDSG a.F. bei der dort geforderten Zuverlässigkeit des DSB die gewichtige Rolle. Die DS-GVO fordert zwar die Zuverlässigkeit der zu bestellenden Person nicht mehr für die Bestellung, dies jedoch wohl nur deshalb, weil sie eine Grundvoraussetzung ist. Herausgestellt wird nunmehr die Vermeidung des Interessenkonflikts, der insoweit auch bislang die maßgebende Rolle gespielt hatte.

Das Problem einer eventuellen Interessenkollision stellt sich primär, wenn ein Beschäftigter nur „nebenamtlich“ mit der Aufgabe des DSB betraut werden soll. Dass das Problem

auch zunehmend in den Fokus der Behörden rückt, zeigt ein Abschlussbericht des EDSA, der im Rahmen einer koordinierten Prüfung festgestellt hat, dass die Abhängigkeit von DSB besonders durch Interessenkollisionen gefährdet wird.<sup>12</sup>

Personen dürfen nicht zum Datenschutzbeauftragten berufen werden, wenn sie aufgrund noch anderweitiger Funktionen in Interessenkonflikte geraten würden, die über das unvermeidliche Maß hinausgehen; dies soll nach Auffassung der Aufsichtsbehörden<sup>13</sup> regelmäßig der Fall sein, wenn z.B. der Leiter der EDV, der Personalleiter oder bei Direktvertrieb der Vertriebsleiter zum Datenschutzbeauftragten bestellt werden soll.<sup>14</sup>

Als empfehlenswerte Kombination verschiedener Tätigkeiten sieht die Aufsichtsbehörde<sup>15</sup> die von Revision oder Sicherheitsbeauftragten und Datenschutzbeauftragten an.<sup>16</sup> Dem Sicherheitsbeauftragten kann die Datenschutzkontrolle aber nur übertragen werden, wenn er nicht auch für Sicherheitsüberprüfungen der Beschäftigten und die Zusammenarbeit mit dem Verfassungsschutz zuständig ist, d.h. er für IT-Sicherheit zuständig ist.<sup>17</sup> Der Leiter oder Mitarbeiter der IT-Abteilung scheiden aber regelmäßig aus.<sup>18</sup> Gleiches gilt sicherlich für einen Mitarbeiter in den Bereichen Organisation oder in der Rechtsabteilung.<sup>19</sup> Auch private Beziehungen, so z.B., wenn der im Betrieb beschäftigte Ehepartner zum Datenschutzbeauftragten ernannt werden soll, können ein Ausschlussgrund sein, wobei dann aber noch weitere Aspekte hinzutreten müssen.<sup>20</sup>

Die unabhängige Tätigkeit des DSB bedingt auch, dass ihm – wird ihm die Aufgabe nebenamtlich zu einer bisher Vollzeit ausgeübten Tätigkeit übertragen – die hierfür erforderliche Arbeitszeit, d.h. Freistellung von seiner bisherigen Tätigkeit gewährt wird. Dies sollte zur Klarstellung in einer Arbeitsplatzbeschreibung festgelegt werden.

Fraglich war lange, ob Interessenkollisionen auftreten, wenn ein Betriebsrats-/Personalratsmitglied zum DSB bestellt werden soll. Nach Auffassung des EuGH liegt eine Interessenkollision dann vor, wenn einem Datenschutzbeauftragten andere Aufgaben oder Pflichten übertragen werden, die die Festlegung der Zwecke und Mittel der Verarbeitung personenbezogener Daten umfasse. Dies folge aus der funktionellen Unabhängigkeit des Datenschutzbeauftragten, der

10 Vgl. Gola/Heckmann/Gola, DS-GVO – BDSG, 3. Aufl. 2022, § 5 Rn. 17.

11 ULD S–H., 36. TB, Ziff. 5.3; BfDI, 26. TB, 2015/2016, Ziff. 1.8.

12 EDSA, 2023 Coordinated Enforcement Action, „Designation and Position of Data Protection Officers“ v. 16.01.2024, S. 24 ff.; s. hierzu auch Piltz/Häntschel, DSB 2023, 43; Heberlein, ZD 2023, 425.

13 Vgl. bereits Aufsichtsbehörde Baden-Württemberg, Hinweis zum BDSG Nr. 2, Staatsanzeiger vom 01.04.1978, Nr. 26, S. 5.

14 Gleiche Bedenken meldet das BAG, Beschl. v. 22.03.1994 – 1 ABR 51/93 = RDV 1994, 182, auch für einen Mitarbeiter der EDV-Abteilung an; ebenso Simitis/Hornung/Spiecker gen. Döhmann/Drewes, DatenschutzR, 1. Aufl. 2019, Art. 38 Rn. 55 für Mitarbeiter der genannten Bereiche.

15 Aufsichtsbehörde Baden-Württemberg, Hinweis zum BDSG Nr. 5, Staatsanzeiger vom 06.01.1979, Nr. 1/2, S. 7; ferner Hinweis Nr. 31, Staatsanzeiger vom 09.01.1993, Nr. 1/2, S. 5/6 = RDV 1993, 54.

16 So auch Simitis/Hornung/Spiecker gen. Döhmann/Drewes, DatenschutzR, 1. Aufl. 2019, Art. 38 DS-GVO Rn. 55.

17 Simitis/Hornung/Spiecker gen. Döhmann/Drewes, Datenschutzrecht, DS-GVO, 1. Aufl. 2019, Art. 38 Rn. 55; Kühling/Buchner/Bergt/Herbort, DS-GVO/BDSG, 4. Aufl. 2024, Art. 38 Rn. 42.

18 Vgl. Gola/Heckmann/Gola, DS-GVO – BDSG, 3. Aufl. 2022, § 7 Rn. 14.

19 Siehe BfDI-Info, Die Datenschutzbeauftragten in Behörde und Betrieb, S. 11; Schaffland/Wiltfang, § 4 f. Rn. 32, 37 f.

20 Vgl. HessDSB, 41. TB (2012), Ziff. 4.6.

u.a. die Einhaltung der datenschutzrechtlichen Vorgaben überwache. Der EuGH betont aber, dass das nationale Gericht einzelfallabhängig prüfen muss, ob tatsächlich ein Interessenkonflikt vorliegt.<sup>21</sup>

Das BAG kam daraufhin zum Ergebnis, dass die Pflichten eines Datenschutzbeauftragten jedenfalls mit denen eines Betriebsratsvorsitzenden nicht zu vereinbaren sind. Er stellt zunächst fest, dass der Betriebsrat selbst darüber entscheidet, unter welchen konkreten Umständen er welche personenbezogenen Daten in Ausübung der ihm durch das BetrVG zugewiesenen Aufgaben erhebt und auf welche Weise er diese anschließend verarbeitet. Dies stehe der Aufgabe eines DSB entgegen, der seine eigenen Tätigkeiten datenschutzrechtlich überprüfen müsste.<sup>22</sup>

Ob auch im Falle einer „einfachen“ Betriebsratsmitgliedschaft eine Interessenkollision mit dem Amt des DSB vorliegt, ließ das BAG in seiner Entscheidung offen. Brinkmann überträgt aber die vom EuGH und dem BAG aufgestellten Grundsätze auch auf das einfache Betriebsratsmitglied, da es sich beim Betriebsrat um ein Kollegialorgan handele und die Stimmen aller Mitglieder gem. § 33 Abs. 1 S. 1 BetrVG dasselbe Gewicht hätten. Demzufolge würden alle Mitglieder im selben Maße über die Verarbeitung der ihnen im Rahmen ihrer Betriebsrats Tätigkeit zur Verfügung gestellten personenbezogenen Daten bestimmen.<sup>23</sup>

Konflikte können auch entstehen, wenn der DSB für mehrere datenverarbeitende Stellen gleichzeitig tätig wird. Dies gilt sowohl für den internen als auch für den externen DSB. Soll der bei der Konzernmutter angestellte DSB gleichzeitig als DSB der Töchter fungieren, so kann dies im Einzelfall nicht unproblematisch sein. Interessenkonflikte können auch auftreten, wenn der DSB insoweit für den Auftraggeber und den Auftragnehmer einer Datenverarbeitung gleichermaßen bestellt ist und sich vor die Frage gestellt sieht, bei der Durchführung des Auftrags festgestellte Unregelmäßigkeiten dem Auftraggeber mitzuteilen. Um hier nicht gegen die Treuepflicht gegenüber dem einen oder anderen „Arbeitgeber“ zu verstoßen, sollte die Problematik in dem Bestellschreiben geklärt werden.

Stellt ein IT-Dienstleistungsunternehmen, das der verantwortlichen Stelle DV-Dienstleistungen erbringt, den externen DSB, so bedarf der eventuelle Interessenkonflikt ebenfalls besonderer Prüfung.

### c) Konsequenzen bestehender Interessenkonflikte

Liegt ein Interessenkonflikt vor, so führt die Gesetzwidrigkeit der Bestellung nicht dazu, dass die Bestellung unwirksam ist. Konsequenz ist vielmehr, dass der Verantwortliche zum unverzüglichen Widerruf der Bestellung verpflichtet ist.<sup>24</sup>

Ein ausdrückliches Recht der Aufsichtsbehörde, die Abberufung eines sich in einer Interessenkollision befindlichen DSB zu verlangen, wie sie § 38 Abs. 5 S. 3 BDSG vorsah, enthält die DS-GVO nicht. Jedoch kann sie unter Nutzung ihrer Abhilfebefugnisse nach Art. 58 Abs. 2 lit. d) DS-GVO die Anweisung erteilen, Verarbeitungsvorgänge in Einklang mit dieser Verordnung vorzunehmen.

Jedoch auch ohne Verlangen der Aufsichtsbehörde kann bzw. muss der Verantwortliche – auch wenn er den Mangel der Bestellung kannte bzw. erkennt – den gesetzwidrigen Zustand beenden. Dies schon deshalb, weil bei den bußgeldbewehrten Artikeln in Art. 83 Abs. 4 lit. a) DS-GVO die Art. 37,

38, 39 DS-GVO insgesamt benannt sind, sodass die Abberufung dadurch erreicht werden kann, dass die mangelhafte Berufung mit einem Bußgeld belegt wird.

Für die Abberufung müssen jedoch die Voraussetzungen des Art. 38 Abs. 3 S. 2 DS-GVO erfüllt sein, was bedeutet, dass ein wichtiger Grund nicht vorliegt, wenn der Interessenkonflikt dadurch beseitigt werden kann, dass die kollidierende Tätigkeit beendet wird.

Eine Kündigung des Beschäftigungsverhältnisses scheidet bei nicht möglicher Beseitigung der Interessenkollision an § 38 Abs. 2 BDSG i.V.m. § 7 Abs. 2 BDSG. Dies gilt regelmäßig auch für den Fall, dass ein anderweitiger Arbeitsplatz für den DSB nicht zur Verfügung steht. Das Gehalt ist ohne Beschäftigung fortzuzahlen, bis der Kündigungsschutz entfällt.<sup>25</sup>

## IV. Form und Befristung der Benennung

### 1. Art und Weise der Benennung

Anders als das BDSG a.F., das für den Bestellvorgang die Wahrung der Schriftform (§ 126 BGB) forderte (§ 4 f Abs. 1 BDSG), stellt die DS-GVO keine bestimmten Anforderungen an die Form der Bestellung des Datenschutzbeauftragten. Zur Gewährleistung von Rechtssicherheit und aus Dokumentationsgründen (Accountability) erscheint eine schriftliche Bestellung jedoch angezeigt. Dabei ist zu beachten, dass das zu übertragende Amt des DSB und das zugrunde liegende Beschäftigungsverhältnis zwar getrennt zu betrachten sind,<sup>26</sup> dass aber die Bestellung durch den Arbeitgeber nur erfolgen kann, wenn dies arbeitsvertraglich bzw. dienstrechtlich eine Basis hat. Zumeist bedeutet die Übernahme des Amts durch einen vorhandenen Mitarbeiter eine Änderung seines Arbeitsvertrags.

Der Benennungsakt ist zu dokumentieren (Rechenschaftspflicht, Art. 5 Abs. 2 DS-GVO). Ausreichend ist insoweit, dass der Verantwortliche ein entsprechendes Benennungsdokument (etwa ein Benennungsschreiben, gegebenenfalls eine Urkunde), bei Rückgriff auf einen externen Datenschutzbeauftragten zudem eine entsprechende vertragliche Vereinbarung vorlegen kann. Einzelne Festlegungen gegenüber dem DSB können auch im Rahmen einer Arbeitsplatzbeschreibung oder einer betrieblichen Datenschutzordnung geschehen.

### 2. Befristung der Benennung

Zur Frage der Befristung der Bestellung macht die DS-GVO ebenfalls keine Aussage. Sie ist „indirekt“ befristet, wenn dies bei dem der Bestellung zugrunde liegenden Arbeits- oder

21 EuGH, Urt. v. 09.02.2023 – C-453/21 mAnm. Zhou/Wybitul, ArbRB 2023, 98.

22 BAG, Urt. v. 06.06.2023 – 9 AZR 383/19 = ZD 2023, 761 Rn. 36: „Ein als Betriebsratsvorsitzender beteiligter Datenschutzbeauftragter, der seine Überwachungsaufgabe im Spannungsfeld seiner funktionalen Interessen und Aufgaben erfüllen muss, besitzt nicht die für eine Gewährleistung des gesetzlichen Datenschutzes erforderliche Unabhängigkeit. Als Beauftragter für den Datenschutz ist der Vorsitzende des Betriebsrats verpflichtet zu prüfen, ob die von ihm nach außen vertretene Beschlusslage des Betriebsrats mit den Bestimmungen des Datenschutzes im Einklang steht.“

23 Brinkmann, BB 2024, 54 (56 f.).

24 Vgl. BAG, Urt. v. 06.06.2023 – 9 AZR 383/19 = ZD 2023, 761.

25 Dies gilt nach dem LAG Düsseldorf, Urt. v. 23.07.2012 – 9 Sa 593/12 = RDV 2013, 207 = ZD 2013, 357 jedenfalls, wenn 27,5 Monate ohne Beschäftigung abzuwarten sind.

26 Zum sog. Trennungsprinzip auch in vergleichbaren Fällen vgl. Ehrlich, NZA 1993, 248; zutreffend einschränkend BAG, Beschl. v. 22.03.1994 – 1 ABR 51/93 DB 1994, 1678 = MDR 1995, 291 = RDV 1994, 182.

Dienstvertrag der Fall ist. Es ist regelmäßig davon auszugehen, dass mit Ende des Beschäftigungsverhältnisses auch die Bestellung nach dem Willen der Parteien beendet sein soll.

Ob die Bestellung des DSB auch – z.B. zum Zweck der Erprobung – befristet oder kommissarisch erfolgen kann, muss im Hinblick auf die an einen wichtigen Grund geknüpfte Abberufung als fraglich erscheinen. Unzulässig wäre es jedenfalls, durch die Befristung den Kündigungsschutz des DSB unterlaufen zu wollen. Eine Befristung oder eine auflösende Bedingung kann daher nur dann als zulässig angesehen werden, wenn auch hierfür bereits ein wichtiger Grund (z.B. die Rückkehr des auf unbestimmte Zeit erkrankten bisherigen Amtsinhabers, die ohnehin geplante Versetzung auf einen anderen Arbeitsplatz) vorliegt.<sup>27</sup> Keinesfalls darf die kommissarische oder befristete Bestellung des DSB dazu dienen, den DSB daran zu hindern, seine Befugnisse voll auszuschöpfen.<sup>28</sup>

## V. Der Abberufung- und Benachteiligungsschutz

### 1. Der Abberufungsschutz

Art. 38 Abs. 3 S. 2 DS-GVO untersagt dem Verantwortlichen, den Beauftragten wegen Erfüllung seiner Aufgaben abzuberufen. Dabei kann es nicht nur darum gehen, dass er zu engagiert vorgeht, sondern auch darum, dass er sich nicht den Problemen zuwendet, die aus Sicht des Verantwortlichen Vorrang haben oder in seinen Auffassungen nicht mit denen der Anwender im Betrieb übereinstimmt.<sup>29</sup>

Jedoch sind dem Abberufungsschutz Grenzen gesetzt, wie § 6 Abs. 4 und § 38 Abs. 2 BDSG deutlich machen.<sup>30</sup> Liegt ein wichtiger Grund nach § 626 BGB vor, der sich auch aus der Art und Weise der Aufgabenwahrnehmung (z.B. Wahrnehmung unerlaubter Tätigkeit während der Arbeitszeit) ergeben kann, ist die Abberufung möglich.

Der EuGH hat hierzu klargestellt, dass es den Mitgliedstaaten freistehe, in Ausübung ihrer Zuständigkeit strengere Vorschriften für die Abberufung eines Datenschutzbeauftragten als nach EU-Recht zu erlassen. Eine nationale Vorschrift wie § 6 Abs. 4 BDSG, wonach ein Datenschutzbeauftragter nur aus wichtigem Grund abberufen werden könne, stehe Art. 38 Abs. 2 S. 3 DS-GVO nicht entgegen. Dabei komme es nicht darauf an, ob die Abberufung mit der Erfüllung seiner Aufgaben zusammenhänge. Voraussetzung sei nur, dass die nationale Regelung des jeweiligen Mitgliedstaats die Verwirklichung der Ziele der DS-GVO nicht beeinträchtige.<sup>31</sup>

Der für den Widerruf der Bestellung im Übrigen durch den Hinweis auf § 626 BGB geforderte wichtige Grund liegt vor, wenn Tatsachen oder Umstände gegeben sind, die unter Berücksichtigung der Gegebenheiten des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung der Beschäftigung unzumutbar machen. Als wichtiger Grund kommen daher sowohl Aspekte in Betracht, die die weitere Beschäftigung als Datenschutzbeauftragter betreffen, aber auch solche, die das Arbeitsverhältnis allgemein betreffen.

Bereits daraus folgt, dass der Widerruf der Bestellung regelmäßig arbeitsrechtlich einer Änderung bzw. der Kündigung des der Beschäftigung zugrunde liegenden Arbeitsverhältnisses bedarf.<sup>32</sup> Als einseitige, das zugrunde liegende Arbeitsverhältnis nicht berührende Maßnahme des Arbeitgebers ist der Widerruf der Bestellung dann zu verstehen, wenn der Arbeitgeber ausnahmsweise im Rahmen des Di-

rektionsrechts dem Arbeitnehmer zur Konkretisierung seiner Arbeitspflicht bestimmte Tätigkeiten zuweisen und auch wieder entziehen kann. Hier ist sein Direktionsrecht nunmehr gesetzlichen Restriktionen unterworfen, indem die Voraussetzungen des § 626 BGB vorliegen müssen.

Die DS-GVO äußert sich zu Form, Inhalt und Frist der Abberufungserklärung nicht. Es gilt daher Formfreiheit. Damit kann die Abberufung auch konkludent erfolgen und wird jedenfalls mit der Beendigung des Arbeitsverhältnisses verbunden sein, die jedoch, wenn sie per Kündigung erfolgt, gem. § 623 BGB immer der Schriftform bedarf. Hinsichtlich der Frist für die „Ausnutzung“ des wichtigen Grundes für die Abberufung gilt wegen der entsprechenden Anwendung die Zwei-Wochen-Frist des § 626 BGB.

Endet die Bestellpflicht durch Reduzierung der bei dem Verantwortlichen Beschäftigten oder z.B. durch Änderung der Geschäftstätigkeit oder Betriebsstilllegung, verliert der DSB sein „gesetzliches“ Amt. Eines ausdrücklichen Widerrufs der Bestellung bedarf es nicht.<sup>33</sup> Der DSB kann aber ggf. als „freiwilliger“ DSB seine Aufgaben weiter wahrnehmen. In derartigen Fällen ist zur Klarstellung ein „vorsorglicher“ Widerruf und eine Zuweisung einer neuen Tätigkeit geboten, da anderenfalls eine konkludente Weiterbeschäftigung als „freiwillig“ bestellter DSB die Folge sein könnte. Sollen auf diesen die Regelungen der DS-GVO bzw. des BDSG intern weiter Anwendung finden, bedarf auch das einer Vereinbarung.

Eine besondere Problematik ergibt sich bei der Fusion von Firmen, wobei sich die Frage stellt, ob der DSB der eingegliederten Firma bzw. bei Neugründung jeder der bisherigen DSB<sup>34</sup> sein Amt wegen des Wegfalls der ihn bestellenden verantwortlichen Stelle und des Umstands, dass das Gesetz nur einen DSB vorschreibt, automatisch verliert. Für den Fall, dass die DSB-Tätigkeit arbeitsvertraglich vereinbart ist, verfügt jedoch andererseits § 613a BGB, dass der neue Arbeitgeber in den bestehenden Arbeitsvertrag eintritt.

Das BAG<sup>35</sup> hat jedoch für den Fall der Fusion zweier Krankenkassen das Amt des DSB infolge des Wegfalls des ihn bestellenden Arbeitgebers als erloschen bewertet.<sup>36</sup> Im Falle der Insolvenz erlischt die Pflicht des Unternehmens zur Bestellung eines Datenschutzbeauftragten erst dann, wenn – nach Abschluss des Insolvenzverfahrens – der Betrieb eingestellt wird bzw. im Rahmen der Abwicklung des Unternehmens die Mitarbeiterzahl unter die gesetzliche Bestellgrenze fällt.<sup>37</sup> Der Eintritt der Insolvenz ist jedoch kein wichtiger Grund, der

27 Nach Marschall/Müller, ZD 2016, 415 (416) soll jedoch nicht nur die Bestellung des externen, sondern auch die des internen DSB die Möglichkeit der unbefristeten Befristung haben.

28 Insoweit mag eine Befristung auf fünf Jahre akzeptabel sein, so Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 615.

29 Vgl. bei Kühling/Buchner/Bergt/Herbort, DS-GVO/BDSG, 4. Aufl. 2024, Art. 37 Rn. 46 f.

30 A.A. Piltz, BDSG, Praxiskommentar für die Wirtschaft, 1. Aufl. 2018, § 38 Rn. 23, wonach die Abberufung keinen Einfluss auf das Arbeitsverhältnis haben und aus betrieblichen Gründen jederzeit möglich sein soll.

31 EuGH, Ur. v. 09.02.2023 – C-453/21 mAnm. Zhou/Wybitul, ArbRB 2023, 98.

32 Vgl. BAG, Ur. v. 13.03.2007 – 9 AZR 612/05 = RDV 2007, 138.

33 Zum Abberufungsschutz vgl. bei v.d. Plath/Bussche/Raguse, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, § 6 Rn. 13 ff.

34 Vgl. SächsDSG, 14. TB (2009), S. 16.

35 BAG, Ur. v. 29.09.2010 – 10 AZR 588/09 = RDV 2011, 882.

36 Ebenso ArbG Cottbus, Ur. v. 14.02.2013 – 3 Ca 1043/12 = RDV 2013, 207.

37 Lfd Baden-Württemberg, 31. TB (2012/2013), Ziff. 10.1.

zum Widerruf oder zur Kündigung berechtigt. Ggf. geht der DSB somit als Letzter.

## 2. Das Benachteiligungsverbot

Das Verbot der Benachteiligung des Beauftragten für den Datenschutz ist eine Konsequenz aus seiner Unabhängigkeit. Ein Arbeitgeber/Dienstherr hat vielseitige Möglichkeiten, einen ihm missliebigen Beauftragten zu „bestrafen“. Sie reichen von der Übergehung bei der Beförderung bis hin zur Entlassung. Vor einer ihn benachteiligenden Entlassung ist der betriebliche DSB nunmehr speziell durch den nur bei wichtigem Grund zulässigen Widerruf seiner Bestellung geschützt. Aber auch mit anderen Benachteiligungen muss ein DSB, der seine Aufgaben sorgfältig erfüllt, rechnen. Werden sie offenkundig, kann er ihnen unter Berufung auf das Benachteiligungsverbot entgegenreten. Im Konfliktfalle, namentlich bei einer nachhaltigen Störung des Vertrauensverhältnisses, werden indes die Grenzen seiner Wirkungsmöglichkeiten erkennbar. Hier wird die Aufsichtsbehörde unterstützend eingreifen müssen. Auch die Mitarbeitervertretung wird, wenn die Benachteiligung sich in einer mitbestimmungspflichtigen Personalmaßnahme niederschlägt bzw. der DSB bei solchen Maßnahmen übergangen wird, für den DSB aktiv werden müssen. Das Benachteiligungsverbot dauert auch nach der Abberufung des DSB an, soweit Vorgänge aus der DSB-Zeit noch bei Personalentscheidungen relevant werden.

## VI. Der Kündigungsschutz des DSB (§ 6 Abs. 4 S. 2 und § 38 Abs. 2 BDSG)

Die DS-GVO enthält keine Regelungen zu einem Kündigungsschutz des DSB. Auch ohne diesbezügliche Öffnungsklausel ist der nationale Gesetzgeber jedoch befugt, diesen für die arbeitsrechtliche Situation des DSB spezifisch zu regeln. Dies hat er getan, indem er die bisher in § 4 f Abs. BDSG a.F. enthaltene Regelung in § 6 Abs. 4 S. 2 und 3 und in der Verweisregelung des § 38 Abs. 2 BDSG fortgeführt hat.

Der mit einem als Arbeitnehmer beschäftigten DSB bestehende Arbeitsvertrag kann nur einseitig vom Arbeitgeber beendet werden, wenn ein Grund vorliegt, der ihn zur Kündigung ohne Einhaltung einer Kündigungsfrist berechtigt.

Dass der externe DSB den Kündigungsschutz nicht genießt, mag für Unternehmen zu der Überlegung führen, von einem DSB im Anstellungsverhältnis abzusehen. Derartige oder sonstige wirtschaftliche Überlegungen können jedoch nicht als wichtiger Grund für die Kündigung des angestellten DSB dienen.<sup>38</sup>

Ist die Tätigkeit des Datenschutzbeauftragten Gegenstand einer arbeitsvertraglichen Vereinbarung – und das muss nicht nur bei einem hauptamtlich, d.h. ausschließlich mit Aufgaben des DSB betrauten Arbeitnehmer der Fall sein –, so kann sich eine Abberufung zudem nur in Form der gleichzeitigen Kündigung dieser arbeitsvertraglichen Abre-

de vollziehen, wobei sich die Kündigung je nachdem, ob das Arbeitsverhältnis beendet oder unter Wahrnehmung anderer Aufgaben fortgesetzt werden soll, als Beendigungs- oder Änderungskündigung darstellt. Nach Auffassung des BAG<sup>39</sup> kommt sogar eine im Arbeitsverhältnis die Ausnahme bildende Teilkündigung in Betracht, die das alte Arbeitsverhältnis eines Teilzeit-DSB im früheren Umfang weiter bestehen lässt. Das setzt aber wohl voraus, dass der Mitarbeiter vor der Übertragung der zusätzlichen DSB-Tätigkeit mit der Haupttätigkeit volltags beschäftigt war. In einer nachfolgenden Entscheidung hat das BAG<sup>40</sup> aber festgestellt, dass im Regelfall auch mit dem Widerruf der Bestellung eines nebenamtlichen DSB diese ohne Teilkündigung endet.

## VII. Fazit

Es hat sich gezeigt, dass bei der Benennung und Abberufung des DSB nicht nur das Datenschutzrecht, sondern bei internen DSB vor allem auch das Arbeitsrecht eine sehr wichtige Rolle spielt. Für die Praxis folgt daraus, dass Sachverhalte zwingend ganzheitlich zu betrachten sind. Der Beschäftigtendatenschutz gewinnt zunehmend an Bedeutung – auch ohne eigenständiges Beschäftigtendatengesetz.<sup>41</sup>



### Prof. Peter Gola

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



### Prof. Dr. Gregor Thüsing, LL.M.

ist Direktor des Instituts für Arbeitsrecht und Recht der sozialen Sicherheit der Universität Bonn und Vorstandsmitglied der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

38 Vgl. BAG, Urte. v. 29.09.2010 – 10 AZR 588/09 = RDV 2011, 237.

39 BAG, Urte. v. 13.03.2007 – 9 AZR 612/05 = RDV 2007, 128.

40 EuGH, Urte. v. 23.03.2011 – 10 AZR 562/09 = RDV 2011, 237.

41 S. hierzu Thüsing, DB 2024, 2830.

Henry Simwinga, LL.M.

# SRB Rechtssache C-413/23P: Der Begriff „personenbezogene Daten“ und das Risiko der Identifizierung

In der sich ständig weiterentwickelnden digitalen Landschaft haben innovative Technologien die Geschäftspraktiken verändert und den Datenaustausch innerhalb der europäischen Digitalwirtschaft vereinfacht. Diese Fortschritte haben jedoch auch wichtige Fragen zum Thema personenbezogene Daten aufgeworfen. Die Datenschutz-Grundverordnung (DS-GVO) spielt eine entscheidende Rolle bei der Bewältigung dieser Probleme, da sie personenbezogene Daten während und nach der Verarbeitung schützt und sicherstellt, dass die Rechte der betroffenen Personen gewahrt werden.

Der Begriff „personenbezogene Daten“ ist ein weit gefasster Begriff, der potenziell alle Arten von Informationen umfassen kann. In der letzten Zeit gibt es eine Reihe von Rechtsprechungen zu diesem Thema, die versuchen, diesen Begriff klar zu definieren, um Rechtssicherheit zu schaffen. Wie der Fall Single Resolution Board (SRB) zeigt, gibt es jedoch noch viele Fragen, mit denen sich die Gerichte befassen müssen.

In diesem Aufsatz werden wir zunächst den Begriff „personenbezogene Daten“ anhand der Rechtsprechung untersuchen. Anschließend werden wir uns mit den Schlussanträgen des Generalanwalts Spielmann (GA) im Fall SRB befassen und abschließend die Auswirkungen der Schlussanträge des GA für den Fall betrachten, dass der Gerichtshof der Europäischen Union (EuGH) diese nicht aufhebt. Zunächst geben wir jedoch einen kurzen Überblick über den Fall zwischen SRB und dem Europäischen Datenschutzbeauftragten (EDSB).

## I. Zusammenfassung des Falls

Im Anschluss an seinen Beschluss über einen Abwicklungsplan hat der SRB die Anteilseigner und Gläubiger aufgefordert, im Rahmen des Anhörungsverfahrens Stellung zu nehmen. Das Verfahren wurde in zwei Phasen durchgeführt, nämlich der Registrierungsphase und der Konsultationsphase.

Im Rahmen der Registrierungsphase wurden die betroffenen Anteilseigner und Gläubiger aufgefordert, ihre Interessen unter Ausübung ihres Anhörungsrechts geltend zu machen. Während dieser Phase wurden die betroffenen Anteilseigner und Gläubiger einer weiteren Prüfung unterzogen, um festzustellen, wer tatsächlich betroffen war, damit sie in die zweite Phase überführt werden konnten.

In der zweiten Phase (Konsultationsphase) konnten die betroffenen Anteilseigner und Gläubiger, deren Status vom SRB überprüft worden war, ihre Stellungnahmen zur vorläufigen Entscheidung abgeben.

Daraufhin beauftragte der SRB einen unabhängigen externen Gutachter, namentlich Deloitte, mit der Bewertung der relevanten Stellungnahmen der betroffenen Anteilseigner und Gläubiger. Der SRB übermittelte die Stellungnahmen über einen virtuellen Server an Deloitte, auf den nur eine ausgewählte Gruppe von Deloitte-Mitarbeitern Zugriff hatte. Die Stellungnahmen wurden pseudonymisiert und mit einem alphanumerischen Code gekennzeichnet. Deloitte hatte keinen Zugriff auf die Registrierungsdatenbank, um die natürlichen Personen zu identifizieren, die am Anhörungsverfahren teilgenommen hatten.

Der EDSB erhielt Beschwerden von Gläubigern und Aktionären, die im Rahmen der Anhörungsinitiative der SRB Stellungnahmen abgegeben hatten. Sie machten geltend, dass die SRB sie nicht darüber informiert habe, dass ihre Stellungnahmen an einen Dritten weitergeleitet würden. In der Folge gab der EDSB den Beschwerdeführern in dem

Sinne recht, dass die SRB gegen Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725<sup>1</sup> verstoßen habe, da er den Beschwerdeführern nicht mitgeteilt habe, dass ihre Stellungnahmen an einen Dritten weitergegeben würden. Der SRB legte beim Gericht Rechtsmittel ein und machte geltend, dass die pseudonymisierten Daten aus Sicht des Dritten (des Empfängers) keine personenbezogenen Daten seien und daher die Verpflichtungen aus Art. 15 Abs. 1 lit. d) nicht gelten würden.

Seit jeher hat das Gericht entschieden, dass pseudonymisierte Daten, die an einen Datenempfänger übermittelt werden, nicht als personenbezogene Daten gelten, wenn der Empfänger nicht über die Möglichkeit verfügt, die Daten natürlichen Personen zuzuordnen.<sup>2</sup>

Nach der Entscheidung des Gerichts legte der EDSB Berufung ein. Zum Zeitpunkt der Veröffentlichung dieses Artikels hatte der EuGH noch nicht über die Angelegenheit entschieden. Der Generalanwalt hat jedoch seine Schlussanträge<sup>3</sup> veröffentlicht, in denen er das Urteil des Gerichts bestätigt, wenngleich er feststellt, dass der SRB die Beschwerdeführer über seine Absicht, ihre Stellungnahmen an einen Dritten weiterzuleiten, hätte informieren müssen, da dies eine Verpflichtung des für die Verarbeitung Verantwortlichen ist, wenn er personenbezogene Daten erhebt und daher der Pseudonymisierung vorausgeht.

1 Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

2 In der Rechtssache T-557/20 Single Resolution Board gegen den Europäischen Datenschutzbeauftragten [2023] ECLI:EU:T:2023:219.

3 Schlussanträge des Generalanwalts Spielmann in der Rechtssache C-413/23P Europäischer Datenschutzbeauftragter gegen Single Resolution Board [2025] ECLI:EU:C:2025:59.

## II. Der Begriff der personenbezogenen Daten

### 1. Rechtsgrundlage

Bevor wir uns mit dem geltenden Recht befassen, möchte ich an Folgendes erinnern. Der SRB-Fall stützt sich auf den Begriff der personenbezogenen Daten in Art. 3 Abs. 1 der Verordnung 2018/1725, der sich an die Organe, Einrichtungen, Ämter und Agenturen der Union richtet. Es ist jedoch von entscheidender Bedeutung, von nun an im Auge zu behalten, dass Art. 3 der Verordnung 2018/1725 identisch ist mit Art. 4 Abs. 1 der DS-GVO<sup>4</sup>. Aus den obigen Ausführungen geht hervor, dass der Gesetzgeber einen einheitlichen Ansatz für den Schutz personenbezogener Daten innerhalb der Europäischen Union anstrebte. Folglich ist Art. 3 Abs. 1 der Verordnung 2018/1725 und Art. 4 Abs. 1 DS-GVO identisch auszulegen.

Das Konzept der personenbezogenen Daten basiert auf der Definition in Art. 4 Abs. 1 DS-GVO, in dem es unter anderem heißt: „Personenbezogene Daten sind alle Informationen die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt bestimmt werden kann, insbesondere durch Zuordnung zu einer Kennung [...] identifiziert werden kann“. In Erwägungsgrund (ErwG) 26 der DS-GVO heißt es in S. 3 und 4: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“

Im Wesentlichen müssen, wie oben dargelegt, zwei Voraussetzungen erfüllt sein, um festzustellen, ob es sich bei den verarbeiteten Informationen um personenbezogene Daten handelt. Es handelt sich um die Kriterien „Bezug zu“ und „Identifizierbarkeit“, die kumulativ erfüllt sein müssen.

Im Rahmen des „relate to“-Tests („Bezug zu“-Test) soll festgestellt werden, ob eine Verbindung bzw. ein Bezug zwischen den fraglichen Informationen und einer natürlichen Person besteht. Im Einklang damit hat die Artikel-29-Datenschutzgruppe (WP) teilweise erklärt, dass [...] „ein „Inhaltselement“ oder ein „Zweckelement“ oder ein „Ergebniselement“ vorhanden sein sollte, damit die Daten als „personenbezogen“ angesehen werden.<sup>5</sup> In der Praxis wird dies fast immer festgestellt, wenn man bedenkt, dass in einem digitalen Raum menschliche Interaktionen oder Kennzeichnungen mit Informationen bis zu einem gewissen Grad unvermeidlich sind. Darüber hinaus stellt die Arbeitsgruppe fest, [...] „bei Vorhandensein des inhaltlichen Elements brauchen die anderen Elemente nicht vorhanden zu sein, damit die Daten als personenbezogen angesehen werden können.“<sup>6</sup>

Wenn also klar ist, dass der Inhalt der verarbeiteten Informationen eine Person betrifft, erübrigt sich die Bewertung von Zweck und Ergebnis. Vermutlich liegt dem die Überlegung zugrunde, dass in Fällen, in denen nicht klar ist, ob der

Inhalt selbst unbestreitbar mit einer Person verknüpft ist, die Validierung des Konzepts der personenbezogenen Daten durch die Bewertung der Auswirkungen des „Zwecks“ oder „Ergebnisses“ der Verarbeitung ausgeweitet werden würde.<sup>7</sup>

Darüber hinaus stellt der EDSA in seinen Leitlinien fest, dass “[...] vernetzte Fahrzeuge immer größere Datenmengen [generieren], von denen die meisten als personenbezogene Daten betrachtet werden können, da sie sich auf Fahrer oder Insassen beziehen. Auch wenn die von einem vernetzten Fahrzeug erhobenen Daten nicht direkt mit einem Namen, sondern mit technischen Aspekten und Merkmalen des Fahrzeugs verknüpft sind, betreffen sie den Fahrer oder die Insassen des Fahrzeugs.“<sup>8</sup> Daraus ergibt sich, dass die meisten Daten im Zusammenhang mit vernetzten Fahrzeugen personenbezogene Daten sind, soweit sie sich auf natürliche Personen beziehen können, und daher wahrscheinlich in den Geltungsbereich der Datenschutz-Grundverordnung fallen.<sup>9</sup>

Die zweite der beiden zu prüfenden Komponenten ist, ob sich die Informationen auf eine identifizierbare Person beziehen. In der Praxis wird der „relate to“-Test fast immer nachgewiesen, aber gleichzeitig sollte nicht immer davon ausgegangen werden, dass sich die Informationen immer auf eine Person beziehen, ohne dass ein gründlicher Test durchgeführt wird, um zu beweisen, dass eine Verbindung besteht. In der Praxis liegt der Schwerpunkt jedoch logischerweise auf der Identifizierbarkeitsprüfung (sog. „identifiable“-Test/„Identifizierbarkeitstest“), ohne die nicht festgestellt werden kann, dass die Informationen mit einer identifizierbaren betroffenen Person verknüpft sind. ErwG 26 der DS-GVO unterstreicht dies, indem er unter anderem feststellt: „Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.“ Dabei sind alle Mittel zu berücksichtigen, die der für die Verarbeitung Verantwortliche oder eine andere Person nach vernünftigem Ermessen einsetzen kann. Schließlich hat der EuGH seit langem festgestellt, dass der Begriff der personenbezogenen Daten ein weites Konzept ist, das potenziell alle Arten von Informationen umfasst.<sup>10</sup>

### 2. Rechtsprechung

Die Rechtsprechung hat gezeigt, wie wichtig die Prüfung der Identifizierbarkeit ist, die ein entscheidender Faktor bei der Feststellung ist, ob sich die fraglichen Informationen auf eine bestimmte Person beziehen.

4 Siehe Art. 98 DS-GVO und die Erwägungsgründe 4 und 5 der Verordnung 2018/1725.

5 Artikel-29-Datenschutzgruppe, „Stellungnahme 4/2007 zum Begriff der personenbezogenen Daten“, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), S. 11, Zugriff am 20.03.2025.

6 Ebd. S. 13 f.

7 Beispiele für solche Situationen finden sich auf Seite 13 der Stellungnahme WP 4/2007.

8 EDSA-Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, [https://www.edpb.europa.eu/system/files/2021-03/edpb\\_guidelines\\_202001\\_connected\\_vehicles\\_v2.0\\_adopted\\_en.pdf](https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf), Rn. 3, Zugriff am 10.04.2025.

9 Ebd. S. 62.

10 Ebd. Nr. 2 Abs. 29.

In der Rechtssache Breyer<sup>11</sup> wurden die Informationen über eine dynamische IP-Adresse als personenbezogene Daten eingestuft, obwohl eine dynamische IP-Adresse im Gegensatz zu einer statischen IP-Adresse keine Verbindung zwischen einem Computer und dem physischen Anschluss an das vom Internetdiensteanbieter verwendete Netz ermöglicht. Dies bedeutet jedoch nicht, dass eine dynamische IP-Adresse keine Informationen über eine identifizierbare natürliche Person enthält.

Das Gericht stellte fest, dass der Anbieter des Online-Mediendienstes, in diesem Fall die Bundesrepublik Deutschland, in der Lage war, die Nutzer zu identifizieren, selbst wenn die Informationen, die für die Zuordnung verwendet werden könnten, bei den Internetdiensteanbietern vorhanden waren. Das Gericht führte jedoch weiter aus, dass es von entscheidender Bedeutung ist, zu verstehen, dass wir, selbst wenn Zuordnungsinformationen vorhanden sind, kritisch bewerten müssen, ob die Kombination einer dynamischen IP-Adresse mit den zusätzlichen Daten, über die der Internetdiensteanbieter verfügt, ein vernünftiges Mittel zur Identifizierung der betroffenen Person darstellt.

Es war vernünftig zu behaupten, dass der Anbieter des Mediendienstes (die Bundesrepublik Deutschland) im Rahmen seiner Befugnisse wahrscheinlich und vernünftigerweise die zur Identifizierung der betroffenen Person erforderlichen Informationen von dem Internetzugangsanbieter erhalten konnte.<sup>12</sup> Dies zeigt, dass bei der Durchführung einer „Identifizierungsprüfung“ unbedingt zu bewerten ist, ob die gesamte Übung ein Mittel darstellt, das vernünftigerweise zur Identifizierung einer betroffenen Person verwendet werden kann.<sup>13</sup>

In ähnlicher Weise stellte Generalanwalt Sánchez-Bordona in seinen Schlussanträgen in der Rechtssache C-319/22 fest, dass „dass die FIN personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO sind, sofern derjenige, der Zugang zu ihnen hat, über Mittel verfügen kann, die es ihm bei vernünftiger Betrachtung ermöglichen, sie zur Identifizierung des Eigentümers des jeweiligen Fahrzeugs zu nutzen“.<sup>14</sup> Wie aus dem obigen Beispiel von Breyer hervorgeht, ist es von wesentlicher Bedeutung, die entsprechenden Daten mit einer identifizierbaren Person zu verknüpfen. Dieses Bewertungsmuster setzt sich in Novak<sup>15</sup> fort, wo im Wesentlichen entschieden wurde, dass ein Prüfungsskript, das einem Prüfungskandidaten zugeordnet werden kann, personenbezogene Daten darstellt<sup>16</sup>. Diese Argumentation folgt auch einem gemeinsamen Thema, nämlich dem Risiko der Re-Identifizierung durch Mittel, die vernünftigerweise zur Identifizierung einer betroffenen Person verwendet werden können.

Darüber hinaus hat der EuGH in der Rechtssache OLAF entschieden, dass das Risiko der Identifizierung der betroffenen Person durch eine Pressemitteilung nicht als unbedeutend angesehen werden kann, selbst wenn ein durchschnittlicher Leser diese Informationen nicht der betroffenen Person zuordnen könnte, sondern unter der Voraussetzung, dass Leser, die in demselben wissenschaftlichen Bereich arbeiten und mit dem beruflichen Hintergrund dieser Person vertraut sind, diese Informationen dieser Person zuordnen würden.<sup>17</sup> Informationen können sich also auf eine betroffene Person beziehen, auch wenn diese Informationen als unbedeutend angesehen werden. Wichtig ist, dass eine gründliche Identifizierbarkeitsprüfung durchgeführt wird, bei der jede Mög-

lichkeit in Frage gestellt werden kann, die wahrscheinlich und vernünftigerweise zur Identifizierung der betroffenen Person verwendet werden kann.

Im Zusammenhang mit den Informationen in den vorangegangenen Abschnitten kommen wir nun zum Thema dieses Artikels, nämlich den Schlussanträgen des Generalanwalts in der Rechtssache SRB.

### III. Schlussanträge von GA Spielmann in der SRB-Rechtssache C-413/223

Es ist möglich, dass der EuGH zu dem Zeitpunkt, an dem Sie diesen Aufsatz lesen, bereits ein Urteil in dieser Angelegenheit gefällt hat. Es genügt zu sagen, dass es trotzdem eine interessante Lektüre ist, weil sie Ihr Verständnis für die Argumentation hinter der Entscheidung des EuGH erweitern und mit der Schlussanträge von GA Spielmann vergleichen oder kontrastieren würden.

In seinen Schlussanträgen vom 06.02.2025 stellt GA Spielmann die Rechtssache als eine Gelegenheit für den Gerichtshof dar, „im Zusammenhang mit pseudonymisierten Daten den Begriff „personenbezogene Daten“ und die sich daraus ergebenden Verpflichtungen im Hinblick auf die Einhaltung der Verpflichtung zu einer fairen und transparenten Datenverarbeitung zu klären“.<sup>18</sup>

Wie wir in der obigen Rechtsprechung gesehen haben, ist die Identifizierbarkeit der betroffenen Personen von zentraler Bedeutung, um festzustellen, ob es sich bei den fraglichen Informationen um personenbezogene oder rechtlich gesehen um nicht personenbezogene Daten handelt, wobei letztere nicht in den Anwendungsbereich der Datenschutz-Grundverordnung fallen.

Wir werden nun den „relate to“-Test und den „identifiable“-Test im Zusammenhang mit den pseudonymisierten Daten anwenden, die im Mittelpunkt des SRB-Streits stehen.

#### 1. Der „relate to“-Test

In Randnummer 30 folgert der GA, dass „Informationen sich auf eine bestimmte oder bestimmbar natürliche Person beziehen, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Wirkung mit einer bestimmten Person ‚verknüpft‘ sind“. Er behauptet weiter, dass die Kommentare, die an DeLoitte übermittelt wurden, obwohl sie gefiltert, kategorisiert und aggregiert wurden, sich auf bestimmte oder bestimmbar natürliche Personen beziehen, da sie sich auf ihre Verfasser beziehen.<sup>19</sup> Dies ist vergleichbar mit dem Test, der in der Rechtssache Nowak angewandt wurde, in der die Verbin-

11 In der Rechtssache C-582/14, Patrick Breyer gegen Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.

12 Ebd. Rn. 47.

13 Ebd. Rn. 45.

14 Schlussanträge des Generalanwalts Campos Sánchez-Bordona, Gesamtverband Autoteile-Handel e.V. gegen Scania CV AB, Rn. 42.

15 Rechtssache C-479/22 P, OC gegen Europäische Kommission [2024] ECLI:EU:C:2024:215, Rn. 61.

16 Ebd. Rn. 35.

17 Rechtssache C-479/22 P, OC gegen Europäische Kommission [2024] ECLI:EU:C:2024:215, Rn. 61.

18 Übersetzung des Verfassers: Ebd. Nr. 2 Abs. 2.

19 Übersetzung des Verfassers: Ebd. Nr. 2 Abs. 39.

dung auf der Grundlage der Tatsache hergestellt wurde, dass die in einem Prüfungsskript enthaltenen Informationen mit dem Verfasser in Verbindung standen.<sup>20</sup>

## 2. Der „identifiable“-Test

Bevor wir den Identifizierungstest anwenden, lohnt es sich, den Kontext der SRB-Sache in Erinnerung zu rufen, denn im Vergleich zur oben zitierten Rechtsprechung geht es in der SRB-Sache bis zu einem gewissen Grad um die Einstufung von pseudonymisierten Informationen.

Bei der Verarbeitung personenbezogener Daten müssen die für die Verarbeitung Verantwortlichen Techniken zum Schutz der Privatsphäre (PETS) einsetzen, um die Sicherheit der Verarbeitung zu gewährleisten. Es gibt verschiedene Arten von Technologien zum Schutz der Privatsphäre, zu denen auch die Pseudonymisierung gehört. Bei der Pseudonymisierung werden personenbezogene Daten als eine einzige Eingabe verwendet. Sie führt zu zwei getrennten Ergebnissen: pseudonymisierte Daten und eine Vergleichstabelle, die wir als Zusatzinformationen bezeichnen. Um die Sicherheit zu maximieren, werden diese beiden Informationsgruppen durch wirksame technische und organisatorische Maßnahmen strikt voneinander getrennt, um die Integrität der pseudonymisierten Daten zu gewährleisten. Dieser Dual-Output-Ansatz stärkt nicht nur die Privatsphäre, sondern schützt auch sensible Informationen vor unbefugtem Zugriff. In Bezug auf die betroffenen Personen ist daher jeder der beiden Outputs nur in Kombination mit dem anderen sinnvoll oder wirkungsvoll.

Daher lautet die Legaldefinition der Pseudonymisierung in Art. 4 Abs. 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.“

Wie aus der obigen Definition und dem Standpunkt der Kommission in Ziffer 48 der Schlussanträge der GA hervorgeht, bezieht sich die Definition in Art. 4 Abs. 5 der DS-GVO auf die Pseudonymisierung als Prozess und nicht auf das Konzept der pseudonymisierten Daten.

Darüber hinaus heißt es in ErwG 26 S. 2 der DS-GVO: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.“ Aus der Konstruktion dieses Satzes lässt sich ableiten, dass der Prozess der Pseudonymisierung dazu führen kann, dass die betroffenen Personen nicht mehr identifizierbar sind. Wie der GA in seinen Schlussanträgen feststellte, wäre S. 2 dieses Erwägungsgrundes andernfalls sinnlos.

Spielmann wies darauf hin, dass „wenn es unmöglich ist, diese betroffenen Personen zu identifizieren, sie daher rechtlich gesehen durch den Pseudonymisierungsprozess ausreichend geschützt sind, ungeachtet der Tatsache, dass die zusätzlichen Identifikationsdaten nicht vollständig gelöscht wurden.“<sup>21</sup> Es kann nicht genug betont werden, dass es nicht

darum geht, pseudonymisierte Daten automatisch aus dem Anwendungsbereich der DS-GVO auszuschließen, sondern dass solche Daten (pseudonymisierte Daten) unter bestimmten Bedingungen nicht unter den Begriff der personenbezogenen Daten fallen.

Mit Blick auf den Wortlaut von ErwG 26 S. 2 erinnert uns der GA daran, dass Daten nur dann rechtlich nicht als personenbezogene Daten eingestuft werden können, wenn die Gefahr einer Identifizierung nicht besteht oder unbedeutend ist.<sup>22</sup> Es genügt zu sagen, dass es wichtig ist, sich vor Augen zu halten, dass die Fähigkeit des SRB zur Re-Identifizierung der betroffenen Personen nicht automatisch dazu führt, dass die übermittelten Daten für den Empfänger als personenbezogene Daten eingestuft werden. Diese Unterscheidung ist wesentlich.

Die obige Betonung der GA steht im Einklang mit der Argumentation in der Rechtssache Breyer, in der das Gericht im Wesentlichen feststellte, dass Informationen, die sich auf eine betroffene Person in einer IP-Adresse beziehen, nicht in den Anwendungsbereich der DS-GVO fallen, „wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene“.<sup>23</sup>

Im Rahmen eines alternativen zweiten Rechtsmittelgrundes wies der GA darauf hin, dass „[...] es dem EDSB obliegt, nachzuweisen, aus welchem Grund, sei es rechtlich oder technisch, das vom SRB im vorliegenden Fall durchgeführte Pseudonymisierungsverfahren nicht ausreichend war und zu dem Schluss hätte führen müssen, dass Deloitte personenbezogene Daten verarbeitet“.<sup>24</sup> Im Wesentlichen stimmt der GA mit dem Gericht überein, indem er feststellt, dass der EDSB die Beweislast für den Gegenbeweis tragen sollte, dass die an Deloitte übermittelten pseudonymisierten Daten nicht robust genug waren, um rechtlich einer Einstufung als personenbezogene Daten zu entgehen.

Wie das Gericht feststellte, konnte der EDSB natürlich nicht zwingend nachweisen, dass es sich bei den von SRB an Deloitte übermittelten pseudonymisierten Daten um personenbezogene Daten handelt. Die Behauptung des EDSB, dass die Informationen, die Deloitte von SRB erhalten hat, als personenbezogene Daten eingestuft werden sollten, war daher anmaßend.

## IV. Auswirkungen

Erstens ist es von entscheidender Bedeutung zu erkennen, dass der GA in seinen Schlussanträgen in der Rechtssache SRB an dem von Breyer aufgestellten strengen Standard für die Identifizierung von Informationen als nicht personenbezogene Daten festgehalten hat. Der Kontext, in dem diese Schlussanträge angewandt werden, ist nicht nur wichtig, sondern entscheidend für das Verständnis ihrer Auswirkungen. Die

<sup>20</sup> Ebd. Nr. 15 Abs. 41.

<sup>21</sup> Übersetzung des Verfassers: Ebd. Nr. 2 Abs. 51.

<sup>22</sup> Ebd. Nr. 2 Abs. 57.

<sup>23</sup> Ebd. Nr. 11 Abs. 46.

<sup>24</sup> Übersetzung des Verfassers: Ebd. Nr. 2 Abs. 96.

Schlussfolgerung hierzu ergibt sich aus der Aussage des GA, als er in Randnummer 57 feststellte, dass „dies nur dann der Fall sein kann, wenn das Risiko der Identifizierung nicht vorhanden oder so gering ist, dass die Daten rechtlich nicht als personenbezogene Daten eingestuft werden können“.

Zweitens wird sich die Entscheidung des EuGH als letzte Instanz in gewisser Weise auf die gemeinsame Nutzung von Daten im Rahmen des Data Act im Zusammenhang mit dem Internet der Dinge (IoT) auswirken. Wie wir bereits gesehen haben, heißt es beispielsweise in den EDSA-Leitlinien zu vernetzten Fahrzeugen: „[...] vernetzte Fahrzeuge immer größere Datenmengen [generieren], von denen die meisten als personenbezogene Daten betrachtet werden können, da sie sich auf Fahrer oder Insassen beziehen. Auch wenn die von einem vernetzten Fahrzeug erhobenen Daten nicht direkt mit einem Namen, sondern mit technischen Aspekten und Merkmalen des Fahrzeugs verknüpft sind, betreffen sie den Fahrer oder die Insassen des Fahrzeugs [...]. Solche technischen Daten werden von einer natürlichen Person erzeugt und ermöglichen ihre direkte oder indirekte Identifizierung durch die Person, die für die Verarbeitung der Daten verantwortlich ist (im Folgenden „Verantwortlicher“), oder durch eine andere Person“.<sup>25</sup>

Drittens werden sich die Schlussanträge des GA, wenn sie Bestand haben, positiv auf Auftragsverarbeiter in ähnlichen Situationen auswirken, denn wie der GA unter Randnummer 58 seiner Schlussanträge erwähnt, stellt er fest, dass es „[...] unverhältnismäßig ist, einem Unternehmen, das die betroffenen Personen nicht angemessen identifizieren kann, Verpflichtungen aus der Verordnung 2018/1725 aufzuerlegen, die dieses Unternehmen theoretisch nicht erfüllen könnte oder die es speziell dazu verpflichten würden, die betroffenen Personen zu identifizieren“.

Schließlich liegt die Beweislast bei den Aufsichtsbehörden, zu prüfen, ob die pseudonymisierten Daten robust genug sind, um als rechtlich nicht personenbezogene Daten zu gelten. Auf den ersten Blick mag dies den Anschein erwecken, dass die Verantwortung vom für die Verarbeitung Verantwortlichen auf die Aufsichtsbehörden verlagert wird. Meiner Ansicht nach und vor allem in der Praxis wäre diese Behauptung weit von der Realität entfernt. Wenn wir uns an ein ähnliches Beispiel erinnern, so stellte der GA fest, dass die Informationspflicht des für die Verarbeitung Verantwortlichen der Pseudonymisierung vorausgeht und der für die Verarbeitung Verantwortliche daher unabhängig von der Sichtweise des Empfängers die Beschwerdeführer darüber hätte informieren müssen, dass die Kommentare an Deloitte weitergelei-

tet werden würden. Das bedeutet, dass die Grundsätze für die Verarbeitung personenbezogener Daten dem Prozess der Pseudonymisierung vorausgehen. Im Übrigen dient Art. 30 der DS-GVO genau diesem Zweck, und dankenswerterweise hebt der SRB-Fall dieses entscheidende Element hervor, indem er den Aufsichtsbehörden die Möglichkeit gibt, das von dem für die Verarbeitung Verantwortlichen geführte Verzeichnis der Verarbeitungstätigkeiten anzufordern, um ihre Beweislast zu beseitigen.

## V. Schlussfolgerung

Wie wir gesehen haben, wurde in der Rechtssache SRB sowohl vor dem Gericht als auch in den Schlussanträgen des GA eines der beiden Schlüsselemente des Begriffs der personenbezogenen Daten nicht erfüllt. Der GA stellte fest, dass sich die an Deloitte übermittelten Informationen auf die Verfasser dieser Kommentare beziehen; da der EDSB jedoch keine Beweise für das Gegenteil vorlegte, dass es sich bei den übermittelten Daten rechtlich gesehen um nicht personenbezogene Daten handelte, wie von SRB behauptet, konnte nicht festgestellt werden, dass die übermittelten Daten mit den Verfassern der besagten Kommentare identifiziert werden konnten.

Im Zusammenhang mit dem SRB-Fall ist es von entscheidender Bedeutung, die Identifizierbarkeitsprüfung aus der Sicht des Empfängers, insbesondere von Deloitte, zu bewerten. Es stellt sich eine dringende Frage: Wäre es gerechtfertigt, einer Einrichtung, die nicht in der Lage ist, die betroffenen Personen vernünftig zu identifizieren, Datenschutzpflichten aufzuerlegen?



### Henry Simwinga, LL.M.

ist Referent für Datenschutz und Datensicherheit und Beauftragter für EU-Beziehungen/Internationale Angelegenheiten bei der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. in Bonn.

<sup>25</sup> Ebd. Nr. 8 S.4.

Prof. Dr. iur. Tobias Keber

# Reform der Datenschutzaufsicht – Föderale Konzentration statt ineffiziente Zentralisierung<sup>1</sup>

Spätestens seit dem Draghi-Report vom Herbst 2024<sup>2</sup> und der Europawahl im Juni 2024 sind die Europäischen Institutionen um die Wettbewerbsfähigkeit der EU besorgt. Auf nationaler Ebene beklagte die „Initiative für einen handlungsfähigen Staat“<sup>3</sup> öffentlichkeitswirksam einen „bisweilen überzogenen“ Datenschutz. Weniger Regelungsdichte, Abbau von Pflichten und Obliegenheiten sowie weniger Kontrollen wünscht man sich. Weniger Grundrechtsschutz forderte man immerhin nicht explizit. Zu den Datenschutzaufsichtsbehörden liest man im Zwischenbericht der Initiative, „die Aufsicht über den nicht öffentlichen Bereich (Unternehmen), die heute durch die Datenschutzaufsichtsbehörden der Länder ausgeübt wird, (...) solle bei der Bundesbeauftragten erfolgen, um eine uneinheitliche Rechtsauslegung zu vermeiden, die Effizienz zu steigern und eine Spezialisierung zu ermöglichen.“

Freilich bleibt die These zur angeblich uneinheitlichen Rechtsauslegung dabei ebenso unbelegt, wie eine Begründung erfolgt, weshalb eine inhaltliche Spezialisierung ausgerechnet nur bei einer Behörde des Bundes möglich sein soll. Dessen ungeachtet scheinen einige Aspekte Eingang in den Koalitionsvertrag von CDU, CSU und SPD für die 21. Legislaturperiode gefunden zu haben. Zu lesen ist dort: „Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an.“<sup>4</sup>

Was hat es mit dem gegenüber einer vorbehaltlosen Absicht deutlich zurückhaltender formuliertem Streben nach „Bündelung“ auf sich? Offensichtlich ist etwas anderes gemeint als „Zentralisierung“, also dem Begriff, der die Debatte bisweilen historisch auch schon begleitet hat. Die projektierte Bündelung soll „im Interesse der Wirtschaft“ bestehen. „Die Wirtschaft“ gibt es allerdings nicht. Es gibt Weltkonzerne, kleine und mittlere Unternehmen, StartUps, freie Berufe, Handwerker und den Bäcker um die Ecke. Die nicht abschließend Aufgezählten haben jedoch höchst unterschiedliche Interessen.

## I. Föderale Konzentration statt Zentralisierung

Was also könnte die im Koalitionsvertrag erwähnte Bündelung verständigerweise bedeuten? Bei einer Reform der Zuständigkeiten im Bereich der Wirtschaft sind verschiedene Varianten denkbar. In dem gerade vorgelegten Rechtsgutachten „Verfassungsrechtliche Möglichkeiten der Aufgabenbündelung im Föderalstaat“ von David Roth-Isigkeit für den Normenkontrollrat wird das systematisiert.<sup>5</sup> Für die hier anzustellende Diskussion wertvoll sind die Argumente, die dort jeweils für und gegen das Modell einer vertikalen Hochzonung von Vollzugsaufgaben von den Ländern auf den Bund einerseits, bzw. einer Stärkung der horizontalen Länderkooperation andererseits, verarbeitet werden.

Vorteile einer Hochzonung sollen einheitliche Standards im gesamten Bundesgebiet sein, Skalierungs- und Digitalisierungsvorteile sollen durch zentrale Portale gehoben und parallele Strukturen vermieden werden. Bei der Analyse potenzieller Nachteile dieses Ansatzes wird die Gefahr einer Verschiebung der verfassungsrechtlichen Grundentscheidung für den dezentralen Vollzug gesehen, die Abweichungen nur in den Grenzen des Art. 87 Abs. 3 S. 1 GG erlaubt. Auch der Verlust von Bürgernähe und lokaler Expertise in diesem Modell wird problematisiert.

Die zweite Variante beschreibt eine Bündelung durch verstärkte Länderkooperation. Diese errichten eine gemeinsame Trägerorganisation, die für alle oder mehrere Länder Verwaltungsaufgaben erfüllt. Hier können einheitliche Standards über Ländergrenzen hinweg gesichert und die Bündelung von Fachwissen ermöglicht werden, ohne die vertikale Kompetenzordnung im Grundsatz zu verschieben. Insgesamt wirbt das Gutachten für eine ausgeglichene Balance zwischen

den verfassungsrechtlich gesteckten Zielen der Leistungsfähigkeit der Verwaltung einerseits und föderalen Grundprinzipien andererseits. Für die Einordnung des Rechtsgutachtens relevant ist schließlich, dass mögliche Effizienzgewinne bei der Verwaltung im Allgemeinen betrachtet werden, nicht aber die spezifische Situation der Datenschutzaufsicht. Beleuchtet man diese näher, zeigt sich folgender Befund.

### 1. Ein Systemwechsel wäre teuer

Eine vertikale Hochzonung von Vollzugsaufgaben der Länder auf Bund wäre erstens teuer. Die Datenschutzaufsichtsbehörden der Länder beschäftigen derzeit etwa 450 Mitarbeiterinnen und Mitarbeiter für den nicht öffentlichen Bereich, die jährlich rund 70.000 Vorgänge bearbeiten.<sup>6</sup> In Baden-Würt-

1 Der Beitrag geht auf einen Impuls des Verfassers am 05.05.2025 im Rahmen des 27. Wiesbadener Forums Datenschutz im Hessischen Landtag zurück. Der Impuls in voller Länge wird im Tagungsband zur Veranstaltung im Nomos Verlag erscheinen. Eindrücke und Programm der Veranstaltung sind abrufbar unter: <https://hessischer-landtag.de/termine/27-wiesbadener-forum-datenschutz>.

2 The Draghi report on EU competitiveness (2024), abrufbar unter: [https://commission.europa.eu/topics/eu-competitiveness/draghi-report\\_en](https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en).

3 Zwischenbericht der Initiative für einen handlungsfähigen Staat (2025), abrufbar unter: [ghst.de/fileadmin/images/01\\_Bilddatenbank\\_Website/Demokratie\\_staerken/Initiative\\_für\\_einen\\_handlungsfähigen\\_Staat/20250311\\_Zwischenbericht\\_interaktiv.pdf](https://ghst.de/fileadmin/images/01_Bilddatenbank_Website/Demokratie_staerken/Initiative_für_einen_handlungsfähigen_Staat/20250311_Zwischenbericht_interaktiv.pdf).

4 Verantwortung für Deutschland, Koalitionsvertrag von CDU, CSU und SPD, 21. Legislaturperiode, Rn. 2106, abrufbar unter: <https://www.koalitionsvertrag2025.de/>.

5 Roth-Isigkeit (2025): Rechtsgutachten: Verfassungsrechtliche Möglichkeiten der Aufgabenbündelung im Föderalstaat. abrufbar unter: [https://www.normenkontrollrat.bund.de/Webs/NKR/DE/veroeffentlichungen/gutachten/\\_documents/2025-04-15-nkr-folgegutachten-buendelung-foederalstaat-gaap.html](https://www.normenkontrollrat.bund.de/Webs/NKR/DE/veroeffentlichungen/gutachten/_documents/2025-04-15-nkr-folgegutachten-buendelung-foederalstaat-gaap.html).

6 Siehe hierzu auch: Wünschelbaum (2025): Alle Macht nach Bonn? In Legal Tribune Online (LTO), abrufbar unter: <https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn>.

temberg beispielsweise wurden im Jahr 2024 insgesamt 4.037 Beschwerden bearbeitet. Allein im Zuständigkeitsbereich des LfDI BW erfolgten im gleichen Jahr 1360 Beratungen, dazu kommen 4470 Anmeldungen zu Schulungen im hauseigenen Schulungs- und Beratungszentrum.<sup>7</sup> Die Erfahrung insoweit zeigt: Beratungsleistungen vor Ort sind nicht skalierbar, da die Unternehmen ganz unterschiedliche, spezifische Fragen zu konkreten Problemen haben. Die Zahlen zeigen auch, wie herausfordernd ein Systemwechsel wäre, denn es würde einen ganz erheblichen Personalaufbau bei der BfDI nötig machen, da eine unmittelbare Verschiebung der Personalressourcen von Ländern zum Bund nicht möglich ist. Der Bundeshaushalt würde geschätzt mit einem hohen zweistelligen Millionenbetrag zusätzlich belastet. Dies stünde in direktem Widerspruch zur expliziten Vorgabe im Koalitionsvertrag, die Konsolidierung des Bundeshaushalts durch den Abbau von mindestens acht Prozent aller Stellen in der Bundesverwaltung voranzutreiben.

## 2. Erhebliche Effizienzverluste in der Transformationsphase

Zweitens wäre ein zentralisierender Ansatz unionsrechtlich hoch problematisch. Abseits der Frage, ob und wie weit eine partielle Zuständigkeitsübertragung mit der strukturell geschuldeten völligen Unabhängigkeit der Landesdatenschutzbeauftragten aus Art. 8 Abs. 3 GRCh bzw. Art. 52 DS-GVO überhaupt vereinbar wäre, wären die mit dem Systemwechsel in der Übergangsphase sicher entstehenden Effizienzverluste mit der Rechtsprechung des EuGH zu Arbeitsfähigkeit und Handlungspflichten der Aufsichtsbehörden<sup>8</sup> schwerlich vereinbar. Der EuGH stellt immer wieder klar: Beschwerden müssen bearbeitet und Verstöße verfolgt werden. Karenzzeiten für aufwendige behördliche Transformationsprozesse sind nicht vorgesehen.

## 3. Kein Nutzen und erhebliche Nachteile für KMU

Drittens würde ein invasiver Systemwechsel neue Abgrenzungsfragen aufwerfen und in der Umstrukturierungsphase erhebliche Rechtsunsicherheit auslösen, denn die Zuständigkeit für laufende Verfahren, die Bindungswirkung bestehender Bescheide sowie die Verfahrensführung in der Übergangszeit wäre unklar. Vor allem kleine und mittelständische Unternehmen würden mit dieser Rechtsunsicherheit belastet. Zudem trifft der Verlust der Beratung vor Ort ebenfalls hauptsächlich kleinere Marktteilnehmer, die somit gleich doppelt belastet würden. Dieses Ergebnis stünde diametral dem erklärten Ziel im Koalitionsvertrag entgegen, vor allem die Stakeholder zu entlasten. Nach dem Bundesamt für Statistik sind das übrigens über 99% der Unternehmen in Deutschland.

Die Transaktionskosten für einen invasiven Systemwechsel wären demnach hoch, ein Mehrwert, der allenfalls für große, länderübergreifend tätige Unternehmen entstehen könnte, bildet nur einen überschaubaren Begünstigtenkreis ab. Die Mehrheit der kleinen und mittelständigen Unternehmen würde einen Ansprechpartner und Beratung vor Ort verlieren. Erhebliches Gewicht bei einem invasiven Systemwechsel hätte auch das Abrücken vom Grundsatz des dezentralen Verwaltungsvollzugs, der jedenfalls in der Gesamtschau der Durchführungsprojekte zu den europäischen zunehmend systemisch zu werden droht.

Vorzugswürdig ist also ein Modell, dass mit dem Koalitionsvertrag, der explizit die Stärkung der DSK fordert, ebenso machbar ist: durch föderale Konzentration und stärkere An-

wendung des Einer-für-Alle-Prinzips einerseits lokale Beratungsstrukturen zu erhalten und darüber hinaus eine einheitliche Rechtsanwendung institutionell sicherzustellen.

## II. Vorschlag der Datenschutzaufsichtsbehörden der Länder vom 26.03.2025

Vor diesem Hintergrund ist dann auch der Vorschlag der Datenschutzaufsichtsbehörden der Länder vom 26. März 2025 zu sehen, den diese einstimmig vorgelegt haben.<sup>8</sup> Die vorgeschlagenen Strukturmaßnahmen erfassen drei zentrale Gesichtspunkte.

1. Zentrale Zuständigkeit einer Aufsichtsbehörde bei länderübergreifenden Sachverhalten, z.B. bei Forschungsprojekten oder bei Konzernen mit mehreren Standorten.
2. Effiziente Arbeitsteilung durch Ausweitung des Einer-für-Alle-Prinzips (EfA) auf die Datenschutzbehörden. Das Ergebnis der Prüfung von länderübergreifend oder bundesweit eingesetzten Verfahren durch eine Landesbehörde bindet dann die anderen Behörden.
3. Institutionalisierung der DSK mit einer Geschäftsstelle und Formung zum gemeinsamen Entscheidungsgremium von Bund und Ländern. So würde Rechtssicherheit durch verbindliche Mehrheitsentscheidungen in der DSK geschaffen.

Der Vorschlag vermeidet die gewichtigen Nachteile, die mit einem teuren, ineffizienten und für die meisten Wirtschaftsakteure nachteiligen Systemwechsel verbunden wären. Der Vorschlag vermeidet auch, was in der Debatte um die Belange (nur) der Wirtschaft zunehmend in den Hintergrund zu treten scheint: Die Sicht auf Bürgerinnen und Bürger. Bisher erhalten diese wie die Unternehmen auch, Beratung zum Datenschutz aus einer Hand und vor Ort. Das geschieht unabhängig davon, ob ihre Daten von öffentlichen oder privaten Stellen verwendet werden. Diese Ausrichtung ist richtig, denn Bürgerinnen und Bürger differenzieren nicht nach Zuständigkeiten. Menschenzentrierte Gestaltung von Verfahren denkt vom Menschen aus und nicht von der Annahme her, zentral ließen sich bestimmte Vorgänge möglicherweise effizienter abarbeiten. Wenn Bürgerinnen und Bürger mit einer Entscheidung ihrer Aufsichtsbehörde nicht einverstanden sind, können sie klagen. Vor Ort. Weite Wege zur Wahrnehmung eines Gerichtstermins schwächen effektiven Rechtsschutz. Auch kleine und mittelständische Unternehmen sowie Startups wünschen sich Beratung dort, wo ihr Geschäftsmodell entsteht und wo sich der Sitz des Unternehmens befindet.



**Prof. Dr. iur. Tobias Keber**

ist Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg.

© Stefan Zeitz

<sup>7</sup> 40. Tätigkeitsbericht des LfDI BW, S. 160, abrufbar unter: <https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/>.

<sup>8</sup> Eckpunkte für eine freiheitliche und grundrechtsorientierte Digitale Zukunft. Abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/en/Entschliessung\\_Datenschutzpolitisches\\_Eckpunktepapier.pdf](https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutzpolitisches_Eckpunktepapier.pdf).

# KURZBEITRÄGE

## End-user responsibilities on a Generative AI conversation

Ganesh Srinivasan\*

Redaktionelle Vorbemerkung: Der nachfolgende Beitrag stammt von Ganesh Srinivasan, General Manager für Informationssicherheit bei Icertis, einem amerikanischen Anbieter von Vertragsmanagementsoftware. Er wird hier in der englischen Originalfassung veröffentlicht. Der Beitrag behandelt die Verantwortlichkeiten des Endnutzers eines KI-Systems mit allgemeinem Verwendungszweck (engl.: general purpose AI, kurz: GPAl) aus einer technisch-ethischen Perspektive. Im Zentrum der Überlegungen stehen technische und ethische Anforderungen an den Nutzer, der ein GPAl-System für Zwecke verwenden möchte, die nach der KI-VO als hochriskant klassifiziert sind. Ob und unter welchen Voraussetzungen ein solcher Nutzer zudem gem. Art. 25 Abs. 1 lit. c) KI-VO als Anbieter eines Hochrisiko-KI-Systems gilt und daher unter anderem sicherzustellen hat, dass das GPAl-System die besonderen Anforderungen der KI-VO an Hochrisiko-KI-Systeme erfüllt, ist eine komplexe Frage, die bislang nicht abschließend beantwortet ist.<sup>1</sup>

An important actor in the lifecycle of general-purpose AI (GPAl) systems is the end-user, that requires a dedicated and special mention. To give this some context, let us first look at the responsibilities of the various players in this association.<sup>2</sup>

Model provider	AIML engineer	AI App developers	End-user
Choice of data to train the model	Focus on fine-tuning model output to specific industries, business requirements	Primary focus is on a targeted solution boundary (banking, insurance, legal, etc.) with guardrails tailored to the specific nature of the app in context	Focus of this document – the end-user brings an “outside-in” perspective to the GPAl system.
Primary responsibility on bias, fairness, safety & harmful content	Consequent focus on accuracy of output, protection against	An additional layer of semantic filtering for profanity, relevance, protection against misinformation, prompt injections etc.	User is expected to demonstrate ‘responsible’ use, for the intended scope and functionality
Ethical, moral boundaries, legal constructs & Privacy	Provides an additional layer of filter over the base model response for bias, fairness, stereotypes, handling sensitive data		

Provides the base constructs for allowed categories, protection from hallucinations, extensibility through APIs			
---	--	--	--

The control over the various layers involved in this orchestration now has the end user as well in perspective.

Category	Model provider	AIML Engineer	AI App developer	End-user
Infrastructure	HIGH	MEDIUM	LOW	NA
Data	HIGH	MEDIUM	LOW	NA
Application	LOW	MEDIUM	HIGH	MEDIUM
Prompt	MEDIUM	MEDIUM	HIGH	HIGH

The semantic nature of a generative AI medium places a lot of significance on the extent of control, wielded by the end-

\* Ganesh Srinivasan ist General Manager für Informationssicherheit bei Icertis, einem amerikanischen Anbieter für Vertragsmanagement Software.

1 Dazu Schwartzmann/Zenner EuDIR 2025, 3 (8 f.).

2 Dazu ausführlich Srinivasan EuDIR 2025, 51 (Hinweis der Redaktion).

user, at the application layer and most importantly with the PROMPT itself. Compared with a traditional web-application that protects any input field against typical web application attacks, the LLM powered generative AI app is now open to the 'free-will' of the end-user who has the control to discuss a wide array of topics, the relevance of which needs to be validated through this entire process flow across the application layer and beyond.

**Focus on the end-user provided input**

If we are to take ONLY the high-risk use of the GPAI system as defined by the EU AI Act, the following matrix of responsibilities lies on the end-user through the access they have via the prompt or information they make available to the AI system through data uploads or otherwise.

High-Risk AI Category	End-User Responsibilities	Justification
<b>Biometric identification and categorization</b>	Ensure accurate and authorized use of the system; avoid manipulation of inputs.	Misuse or manipulation could lead to privacy breaches and wrongful identification.
<b>Critical infrastructure management</b>	Provide accurate data and follow protocols strictly; report anomalies promptly.	Incorrect data or malicious inputs can jeopardize public safety and disrupt critical services.
<b>Education and vocational training</b>	Submit truthful information; use the system ethically for assessments.	Manipulated inputs can lead to unfair assessments and affect educational outcomes.
<b>Employment, workers management, and self-employment</b>	Submit accurate information during recruitment processes; adhere to ethical standards in monitoring.	False information can lead to unfair hiring or termination; unethical monitoring can infringe on privacy.
<b>Access to essential private and public services</b>	Provide accurate data for eligibility assessments; avoid fraudulent submissions.	Manipulated data can lead to unfair access to benefits, impacting those in genuine need.
<b>Law enforcement</b>	Ensure legitimate use of the system; report suspicious activities or misuse.	Manipulation can result in wrongful profiling and criminal predictions, affecting justice and public trust.

<b>Migration, asylum, and border control management</b>	Provide authentic documentation; avoid misrepresentation.	False information can affect asylum decisions and border control measures, impacting individuals' lives.
Administration of justice and democratic processes	Engage ethically with the system; avoid influencing the system with biased data or inputs.	Manipulation can undermine the fairness of judicial decisions and democratic integrity.

This emphasizes the need for a clear **Consent Notice** – to the end-user, that calls out the following.

- **Purpose of Use:** Clearly state the intended purposes of the AI system and the specific tasks it is designed to perform.
- **User Responsibilities:** Outline the responsibilities of the end-user, including the need to provide accurate information, avoid manipulative inputs, and use the system ethically.
- **Data Integrity:** Emphasize the importance of submitting truthful and authentic data to ensure the system's reliability and fairness.
- **Ethical Use:** Highlight the expectation for users to engage with the system ethically, avoiding misuse or manipulation.
- **Potential Consequences:** Inform users of the potential consequences of misuse, including impacts on fairness, safety, and societal trust.
- **Privacy and Security:** Provide information on how the system ensures data privacy and security, and the user's role in maintaining these standards.
- **Reporting Mechanisms:** Offer clear instructions on how users can report any anomalies, unethical use, or system malfunctions.
- **Acknowledgment and Agreement:** Include a section where users acknowledge their understanding of the consent notice and agree to comply with the outlined responsibilities.

**Conclusion**

The focus on end-user input also means additional guard-rails for the application developers and the GPAI system owners that go through a semantic classification on high, medium, low risk – in the context of the purpose intended by a given system. We could possibly segue into that topic in the following edition.

# Zur Maßgeblichkeit automatisierter Entscheidungsvorbereitungen

Zugleich eine Anmerkung zu LG Bamberg Urteil vom 26.03.2025 – 41 O 749/24 KOIN

Moritz Köhler\*

„And so it begins“: Seit der EuGH im Dezember 2023 zur grundsätzlichen Anwendbarkeit des in Art. 22 Abs. 1 DS-GVO normierten Verbots der automatisierten Entscheidung im Einzelfall auf die Erstellung von Bonitätsscores geurteilt hat, wird die Auslegung des nun zentralen Begriffs der Maßgeblichkeit durch die nationalen Gerichte mit Spannung erwartet. Der Generalanwalt hatte auf diese Entwicklung bereits in seinen Schlussanträgen zum betreffenden Verfahren hingewiesen und sie begrüßt.<sup>1</sup> Mit Blick auf ein aktuelles Urteil des LG Bamberg,<sup>2</sup> in dem ein nationales Gericht soweit ersichtlich erstmals über die Maßgeblichkeit des Scorings für die Kreditvergabe zu befinden hatte, wäre allerdings eine Orientierungshilfe zur Konkretisierung des Merkmals seitens des EuGH wünschenswert gewesen.

## I. Entscheidungsvorbereitungen i.R.v. Art. 22 Abs. 1 DS-GVO

Art. 22 Abs. 1 DS-GVO verbietet<sup>3</sup> es dem Verantwortlichen, eine betroffene Person einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung zu unterwerfen, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Anders als insbesondere in der deutschen Literatur bis zum wegweisenden Urteil des EuGH überwiegend angenommen wurde, umfasst der Begriff der Entscheidung i.S.v. Art. 22 Abs. 1 DS-GVO nicht lediglich die Letztentscheidung eines Kreditinstituts über den Abschluss eines Darlehensvertrags, sondern bereits „das Ergebnis der Berechnung der Fähigkeit einer Person zur Erfüllung künftiger Zahlungsverpflichtungen in Form eines Wahrscheinlichkeitswerts“.<sup>4</sup> Die weite Auslegung des Entscheidungsbegriffs dürfte nicht lediglich auf die klassische SCHUFA-Konstellation anwendbar sein, sondern auch auf Zwei-Personen-Konstellationen, andere Score-Werte und sogar andere Formen der automatisierten Entscheidungsvorbereitung. Jedenfalls lassen sich der Begründung des EuGH zur weiten Auslegung des Entscheidungsbegriffs keine Argumente entnehmen, die nicht auch in Zwei-Personen-Konstellationen oder etwa für natürlichsprachliche Entscheidungsvorschläge Geltung beanspruchen.<sup>5</sup>

## II. Das Merkmal der Maßgeblichkeit

Eine qualifizierte Wirkung sollen Entscheidung(svorbereitungen) entfalten, wenn sie ein Handeln mit entsprechender Wirkung „maßgeblich leiten“.<sup>6</sup> Dass hierdurch eine Umgehung des Merkmals der „Ausschließlichkeit“ droht, sei nur am Rande erwähnt.<sup>7</sup> Schließlich obliegt es den nationalen Gerichten, im Einzelfall festzustellen, ob ein SCHUFA-Score die Entscheidung eines Kreditinstituts im Einzelfall maßgeblich geleitet hat. Im Verfahren vor dem EuGH nahmen die Richter eine solche maßgebliche Leitung an, da „ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen dazu [führt], dass die Bank die Gewährung des beantragten Kredits ablehnt.“ Feststehen dürfte außerdem, dass ein lediglich „formales Abnicken“ der Ent-

scheidungsansätze durch einen menschlichen Sachbearbeiter aus einer automatisierten keine menschliche Entscheidung macht.<sup>8</sup>

Ob grundsätzlich eine inhaltliche Auseinandersetzung zumindest in Form einer Plausibilitätsprüfung im Einzelfall erforderlich ist, um den Anwendungsbereich des Art. 22 Abs. 1 DS-GVO unberührt zu lassen, oder ob sogar die bloße Überwachung des Systembetriebs durch einen Menschen genügt, muss hier nicht diskutiert werden, obwohl jedenfalls die Eigenschaft der Vorschrift als individuelles Betroffenenrecht für die erstgenannte Auffassung spricht. Was das LG Bamberg noch unter einer maßgeblichen Leitung und damit vom Verbot des Art. 22 Abs. 1 DS-GVO erfasst sieht, strapaziert allerdings Wortlaut und Telos der Norm. Konkret stützt das Gericht die Maßgeblichkeit des „Sch.“-Scores für die Entscheidung über die Vergabe eines Kredits auf die Bezahlung eines Entgelts durch das Kreditinstitut. Es führt aus, dass im Geschäftsverkehr keine kostenpflichtigen Auskünfte eingeholt werden, wenn deren Inhalte für den Anfragenden keine Rolle spielen.<sup>9</sup> Art. 22 Abs. 1 DS-GVO verbietet aber nicht, dass eine automatisierte Entschei-

\* Moritz Köhler ist wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und Doktorand bei Prof. Dr. Gregor Thüsing und Prof. Dr. Rolf Schwartmann.

1 Generalanwalt Pikamäe, Schlussanträge v. 16.03.2023 – C-634/21, ECLI:EU:C:2023:220 Rn. 45 – SCHUFA Holding AG.

2 LG Bamberg, Urte. v. 26.03.2025 – 41 O 749/24 KOIN, RDV 2025, 203, in dieser Ausgabe.

3 EuGH, Urte. v. 07.12.2023 – C-634/21, ECLI:EU:C:2023:957 Rn. 52 – SCHUFA Holding AG.

4 EuGH, Urte. v. 07.12.2023 – C-634/21, ECLI:EU:C:2023:957 Rn. 46 – SCHUFA Holding AG.

5 So auch HmbBfDI, Pressemitteilung v. 07.12.2023, [https://datenschutz-hamburg.de/fileadmin/user\\_upload/HmbBfDI/Pressemitteilungen/2023/2023-12-07-PM\\_EuGH\\_Urteil\\_Schufa\\_Auswirkungen\\_auf\\_KI.pdf](https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2023/2023-12-07-PM_EuGH_Urteil_Schufa_Auswirkungen_auf_KI.pdf) (Stand: 15.7.2024).

6 EuGH, Urte. v. 07.12.2023 – C-634/21, ECLI:EU:C:2023:957 Rn. 46 – SCHUFA Holding AG.

7 Dazu Schwartmann/Köhler/Zenner/Schwartmann/Benedikt/Köhler, KI-VO, 2. Teil 3. Kap. Rn. 41.

8 Paal/Schulz ZfDR 2025, 89 (101).

9 LG Bamberg, Urte. v. 26.03.2025 – 41 O 749/24 KOIN, RDV 2025, 203 (204), in dieser Ausgabe.

dung für ein Handeln mit qualifizierter Wirkung „eine Rolle spielt“. Die Vorschrift verbietet nach der Rechtsprechung des EuGH lediglich die maßgebliche Leitung des Handelns durch die automatisierte Entscheidung.

### III. Berücksichtigung der Ligue-des-droits-humains-Rechtsprechung

Darüber hinaus weist das Gericht selbst darauf hin, dass das Kreditinstitut im vorliegenden Fall neben dem SCHUFA-Score weitere Faktoren, namentlich Einkommen und Vermögen, zur Entscheidungsfindung herangezogen hat. Der Score war also nur einer unter mehreren Parametern, die von einem menschlichen Sachbearbeiter in der Entscheidungsfindung berücksichtigt wurden. Dass das LG Bamberg trotzdem ohne weitere Begründung von einer verbotenen Entscheidung ausgehen will, ist unter Berücksichtigung der Rechtsprechung des EuGH im Urteil Ligue des droits humains ebenfalls kritisch zu betrachten. Demnach ist eine individuelle Überprüfung automatisch generierter Ergebnisse durch einen Menschen nicht mit dem Recht auf einen wirksamen Rechtsbehelf aus Art. 47 GRCh vereinbar, wenn dieses Recht auf hohem Schutzniveau zu gewährleisten ist und „selbstlernende Systeme“ zum Einsatz kommen.<sup>10</sup> Erkennt der EuGH damit aber die individuelle Überprüfung algorithmisch generierter Ergebnisse durch einen Menschen als Regelfall an, verbleibt für besonders risikoreiche Entscheidungssituationen lediglich die Eingliederung des automatisiert erstellten Entscheidungsvorschlags in eine Reihe von Parametern, die von einem Menschen angemessen gewichtet werden.<sup>11</sup>

So ist auch die Gewährleistung des Rechts auf einen wirksamen Rechtsbehelf sichergestellt. Würde man mit dem LG Bamberg dagegen auch diese Konstellation als vom Verbot des Art. 22 Abs. 1 DS-GVO erfasst erachten, stellt sich die Frage, welcher Raum nicht nur für das Scoring, sondern für eine große Zahl automatisierter Entscheidungsvorbereitungen verbleibt.<sup>12</sup> Die Erwartung ist berechtigt, dass das entscheidende Gericht bei Zugrundelegung mehrerer Entscheidungsfaktoren gesondert begründet, warum das Ergebnis der automatisierten Entscheidung in unangemessenem Verhältnis berücksichtigt wurde.

### IV. Ergebnis

Es ist zu hoffen, dass die nationalen Gerichte bei der weiteren Konkretisierung des Merkmals der Maßgeblichkeit Fingerspitzengefühl beweisen. Dabei sollte die Rechtsprechung des EuGH nicht nur teilweise berücksichtigt werden: Eine automatisierte Entscheidung fällt unter Art. 22 Abs. 1 DS-GVO, wenn sie eine Handlung mit qualifizierter Wirkung „maßgeblich leitet“, nicht bereits, wenn sie für diese maßgeblich ist.

<sup>10</sup> EuGH, Urt. v. 21.06.2022 – C-817/19, ECLI:EU:C:2022:491 Rn. 195 – Ligue des droits humains.

<sup>11</sup> Dazu Köhler EuDIR 2025, 16 (20 Rn. 20 f.).

<sup>12</sup> Thüsing LTO vom 10.12.2023, <https://www.lto.de/recht/meinung/m/eugh-c63421-schufa-scoring-folgen-ki-automatisierte-verarbeitung-kreditauskunft> (Stand: 15.07.2025).

**Sichern Sie  
sich Ihren  
fachlichen  
Vorsprung!**

## Ausbildung zum/zur Datenschutzkoordinator/in

### Grundlagenwissen mit Zertifizierungsmöglichkeit

30.09.–01.10.2025 | Köln

Referent: Thomas Mühtlein

#### Schwerpunkte:

##### Grundlagen

- ✓ Rollen und Aufgaben in der Datenschutz-Organisation
- ✓ Stellung und Aufgabe als Datenschutzkoordinator/in

##### Wichtige Datenschutz-Prozesse

- ✓ Bearbeitung von Betroffenenrechten
- ✓ Reaktionen bei Datenpannen
- ✓ Zusammenarbeit mit Dienstleistern

Jetzt anmelden: [www.datakontext.com](http://www.datakontext.com)



# Praxisfälle zum Datenschutzrecht XXXV: Einschaltung von Dienstleistern – Besser am Anfang schon ans Ende denken

RAin Yvette Reif, LL.M.\*

## I. Sachverhalt

Die als GmbH organisierte Anwaltskanzlei K benutzt bereits seit 10 Jahren dieselbe Anwaltssoftware für die Mandatsbearbeitung und Kommunikation mit ihren Mandanten. Betrieben wird die Software auf Servern in einem Rechenzentrum des Anbieters A der Anwaltssoftware. Auf den Servern des Rechenzentrums sind auch die konkreten Mandantendatensätze gespeichert, welche von der Kanzlei mittels der Software erzeugt werden. Mit Blick auf die von A erbrachten Leistungen wurde zwischen K und A seinerzeit ein Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO geschlossen.

Der Anbieter der Software hat allerdings nunmehr angekündigt, dass er die Software bis zum Ende des laufenden Jahres einstellen wird. Die Kanzlei hat sich daher nach einer neuen entsprechenden Software umgesehen ist und ist auch fündig geworden. Nun geht es darum, dass die Daten, die in dem alten Programm verarbeitet wurden, sprich alle Informationen mit Blick auf die Beratungen und Prozesse der letzten zehn Jahre, in das neue Programm überführt werden sollen, damit diese Informationen im Rahmen des täglichen Kanzleigeschäfts auch weiterhin zur Verfügung stehen. Dazu ist es erforderlich, dass der bisherige Anbieter die über das Programm verarbeiteten Daten in einem marktüblichen gängigen Format zur Verfügung stellt, welches den Import im Rahmen der neu eingesetzten Software ermöglicht. Hierzu ist A nur gegen Bezahlung des zusätzlichen Aufwandes bereit, welcher ihm entsteht. A bietet jedoch an, die gespeicherten Daten nach Beendigung der Vertragsbeziehung zu löschen und die Löschung entsprechend zu bestätigen, ohne dass hierfür zusätzliche Kosten anfallen.

Die Kanzlei K fragt sich daher, inwiefern die Möglichkeit besteht, auf datenschutzrechtlichem Weg ohne Zusatzzahlung an die Daten zu kommen. Es könne doch nicht sein, dass der Anbieter die Herausgabe von Informationen blockieren könne, obwohl es sich datenschutzrechtlich um Informationen handele, welche ihr selbst als Verantwortlichem im Sinne der DS-GVO zustünden.

Der Auftragsverarbeitungsvertrag besagt nichts Konkretes zur Art und Weise der Abwicklung der Beendigung des Vertragsverhältnisses bzw. Kosten der Beendigung, die ggf. entstehen, wenn der Auftraggeber die im Auftrag verarbeiteten Daten in einem marktüblichen Format zur Verfügung gestellt bekommen möchte. Mit Blick auf eine Beendigung des Auftragsverhältnisses werden lediglich die Vorgaben nach Art. 28 Abs. 3 lit. g) DS-GVO wiederholt.

Muss K in den sauren Apfel beißen und den hohen Betrag bezahlen oder besteht die Möglichkeit, die gewünschten Informationen über die DS-GVO vom Dienstleister zu erhalten?

## II. Musterlösung

### 1. Anspruch auf Herausgabe der Daten im marktüblichen Format auf Basis der Auftragsverarbeitung?

A könnte auf Basis der DS-GVO-Bestimmungen zur Auftragsverarbeitung zur Herausgabe der verarbeiteten Mandantendatensätze an K verpflichtet sein.

Dazu müsste es sich bei der von A erbrachten Dienstleistung um eine Auftragsverarbeitung handeln und A müsste zudem als Auftragsverarbeiter (Art. 28 DS-GVO) rechtlich verpflichtet sein, K die begehrten Daten in einem marktüblichen Format herauszugeben.

#### a) Vorliegen einer Auftragsverarbeitung

Maßgebliches Kriterium für die Unterscheidung zwischen einem – ggf. auch gemeinsam<sup>1</sup> – datenschutzrechtlich Verantwortlichen (Art. 4 Nr. 7 DS-GVO) und einem Auftragsverarbeiter (Art. 28 DS-GVO) ist die Weisungsgebundenheit des Auftragsverarbeiters im Verhältnis zum Auftraggeber. Während datenschutzrechtlich Verantwortliche steuernden Einfluss auf die Zwecke und wesentlichen Mittel der personenbezogenen Datenverarbeitung haben, unterwirft sich der Auftragsverarbeiter diesbezüglich den Vorgaben des Auftraggebers und wird nur als dessen „verlängerter Arm“ tätig.

Die Bereitstellung von Speicherplatz und Ressourcen auf einem Server (sog. Hosting) stellt einen klassischen Anwendungsfall der Auftragsverarbeitung dar. Insbesondere haben entsprechende Dienstleister über die Erbringung des Services hinaus kein Interesse an den verarbeiteten Informationen, d.h., sie verfolgen mit den Informationen keine eigenen Zwecke, sondern werden typischerweise rein weisungsgebunden tätig. Ausgelagert wird nur eine technische Unterstützungs-/Hilfsfunktion bezogen auf einen konkreten Teilaspekt (Datenspeicherung) des Gesamtprozesses „Mandantenbetreuung“.<sup>2</sup>

A ist also mit Blick auf die Verarbeitung der Mandantendatensätze als Auftragsverarbeiter i.S.v. Art. 28 DS-GVO anzusehen.

\* 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.

<sup>1</sup> Vgl. Art. 26 DS-GVO.

<sup>2</sup> Für Kriterien zur Abgrenzung der Auftragsverarbeitung zur (alleinigen bzw. gemeinsamen) datenschutzrechtlichen Verantwortlichkeit vgl. GDD, Praxishilfe DS-GVO Joint Controllership, Vers. 1.0 (Dez. 2019), Abschn. 9.1.

## b) Verpflichtung des Auftragsverarbeiters, die verarbeiteten Daten nach Vertragsende in einem gängigen Format zur Verfügung zu stellen?

Fraglich ist allerdings, ob aus der Stellung von A als Auftragsverarbeiter des K auch eine Verpflichtung resultiert, K die verarbeiteten Daten nach Vertragsende in einem gängigen Format zur Verfügung zu stellen. Dies könnte insofern naheliegen, als es sich datenschutzrechtlich um Informationen handelt, die K als Verantwortlichem im Sinne der DS-GVO zuzuordnen sind, und A mit Bezug auf die im Auftrag verarbeiteten Informationen keine eigenständige Verarbeitungsbeugnis zukommt.

Nach der DS-GVO gibt es gem. Art. 28 Abs. 3 S. 2 lit. g) allerdings zwei Alternativen, wie ein Auftragsverhältnis datenschutzkonform beendet werden kann, nämlich erstens die Löschung der im Auftrag verarbeiteten Daten durch den Dienstleister und zweitens die Rückgabe der Daten an den Auftraggeber unter gleichzeitiger Löschung der vorhandenen Kopien. Jedenfalls die erste Alternative bietet der Dienstleister hier ohne zusätzliche Kosten an, wodurch dem Datenschutz genüge getan sein dürfte.

Zwar stellt nach dem ausdrücklichen Wortlaut von Art. 28 Abs. 3 S. 2 lit. g) die DS-GVO auf die „Wahl des Verantwortlichen“ ab hinsichtlich der Frage, ob im Auftrag verarbeitete Daten zurückgegeben werden sollen oder aber nur<sup>3</sup> gelöscht. Der Dienstleister lässt dem Auftraggeber vorliegend aber durchaus diese Wahl, er verlangt nur im Fall einer bestimmten Entscheidung des Auftraggebers eine zusätzliche Vergütung. Fragen der Vergütung im Zusammenhang von Dienstleistungen sind aber grundsätzlich auf zivilrechtlicher Ebene zu beantworten. Ob bzw. welche Vergütung für eine Leistung gefordert wird, ist im Ausgangspunkt Frage der Privatautonomie. Etwas anderes mag im Einzelfall gelten, wenn aufgrund unangemessener finanzieller Forderungen des Dienstleisters die Gefahr besteht, dass datenschutzrechtliche Pflichten vernachlässigt werden könnten. Dies kann etwa relevant werden, wenn ein Auftragsverarbeiter ein gesondertes Entgelt für die gesetzlich angelegten Kontrollen (Art. 28 Abs. 3 S. 2 lit. h) DS-GVO) des Verantwortlichen mit Blick auf die Auftragsverarbeitung vorsieht.<sup>4</sup> Dafür bestehen mit Blick auf den hier zu beurteilenden Sachverhalt keine Ansatzpunkte.

A ist damit nicht auf Basis der DS-GVO-Bestimmungen zur Auftragsverarbeitung zur Herausgabe der verarbeiteten Mandantendatensätze an K verpflichtet.

## 2. Anspruch auf Basis von Art. 20 DS-GVO (Datenportabilität)

In ihrem Art. 20 sieht die DS-GVO explizit die Möglichkeit vor, personenbezogene Daten „in einem strukturierten, gängigen und maschinenlesbaren Format“ zu erhalten und damit in der Form, die der Kanzlei A im vorliegenden Fall weiterhelfen würde.

Mit diesem sog. Recht auf Datenportabilität, das mit Inkrafttreten der DS-GVO neu eingeführt wurde, dessen praktische Bedeutung allerdings im Ergebnis gering geblieben ist, sollte v.a. Internetnutzern ermöglicht werden, „ihre“ Daten, die sie im Rahmen der Nutzung von Online-Diensten (etwa sozialen Netzwerken) bereitgestellt haben, zu anderen Online-Diensten mitzunehmen.<sup>5</sup>

Im Detail gewährt Art. 20 DS-GVO unter den dort im Einzelnen geregelten Voraussetzungen zwei verschiedenartige Rechte: Zum einen kann die betroffene Person verlangen, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (Recht auf Erhalt<sup>6</sup>). Zum anderen kann die betroffene Person die direkte Übermittlung der einem (ersten) Verantwortlichen bereitgestellten personenbezogenen Daten an einen anderen (zweiten) Verantwortlichen erwirken (Recht auf Erwirkung der direkten Übermittlung<sup>7</sup>). Mit Blick auf die Weiterverwendbarkeit der Informationen, die auf den Antrag hin zur Verfügung zu stellen sind, ist der Anspruch nach Art. 20 DS-GVO insoweit weiter als derjenige auf Auskunft aus Art. 15 DS-GVO und ergänzt diesen.

Die vorstehenden Ausführungen zeigen bereits, dass Art. 20 DS-GVO der Anwaltskanzlei hier nicht weiterhelfen kann: Bei dem Recht aus Art. 20 DS-GVO handelt es sich um einen Anspruch der „betroffenen Person“, d.h. derjenigen natürlichen Person, deren personenbezogene Daten verarbeitet werden (vgl. Art. 4 Nr. 1 DS-GVO), gegen den Verantwortlichen. Als betroffene Personen anzusehen sind hier primär die Mandanten der Kanzlei, über welche Informationen in den bei A gespeicherten Datensätzen enthalten sind, ggf. zudem die jeweils sachbearbeitenden Rechtsanwälte. Die Anwaltskanzlei selbst kann als juristische Person nicht betroffene Person im Sinne der DS-GVO sein und damit auch nicht Antragstellerin im Rahmen von Art. 20 DS-GVO. Im Übrigen ist der Anspruch aus Art. 20 DS-GVO, wie bereits ausgeführt, gegen den Verantwortlichen (Art. 4 Nr. 7 DS-GVO) gerichtet. Vorliegend geht es aber um ein Begehren des Verantwortlichen selbst gegen seinen Auftragsverarbeiter.

Ein Anspruch der Kanzlei gegen ihren bisherigen Dienstleister auf Herausgabe der Mandantendatensätze auf Basis von Art. 20 DS-GVO scheidet damit aus.

## III. Ergänzende Praxisinformationen

### 1. Zivilrechtliche Beurteilung mit Blick auf die Herausgabe der Daten

Wie dargestellt, ist die Frage, ob K für die Bereitstellung der Daten in einem gängigen Format zusätzlich zahlen muss, eine solche, die auf zivilrechtlicher Ebene zu klären ist. Datenschutzrechtlich hat K keinen Anspruch auf entsprechende Bereitstellung der durch A verarbeiteten Informationen.

Entscheidend wird zivilrechtlich insbesondere die Auslegung des zwischen den Parteien geschlossenen Dienstleistungsvertrages sein und in diesem Zusammenhang konkret die Natur der erbrachten Dienstleistung. Die Vertragsaus-

<sup>3</sup> Im Fall der „Rückgabe“ der Daten muss der Auftragnehmer bei ihm verbleibende Daten im Nachgang ebenfalls löschen.

<sup>4</sup> EDSA, Leitlinien 7/2020 (Vers. 2.0 v. 07.07.2021) Rn. 145; zum Ganzen auch BayLfD, Aktuelle Kurz-Information 6: Entgeltspflicht für Kontrollen bei der Auftragsverarbeitung?, 15.11.2021.

<sup>5</sup> Brandt/Grewe, MMR 2023, 928 (929).

<sup>6</sup> Schwartmann/Jaspers/Thüsing/Kugelman/Rudolph, DS-GVO/BDSG, 3. Aufl. (2024), DS-GVO Art. 20 Rn. 13.

<sup>7</sup> Schwartmann/Jaspers/Thüsing/Kugelman/Rudolph, DS-GVO/BDSG, 3. Aufl. (2024), DS-GVO Art. 20 Rn. 13.

legung (§§ 133, 157 Bürgerliches Gesetzbuch – BGB)<sup>8</sup> ist ein Verfahren, um den Inhalt eines Vertrags zu ermitteln, wenn dieser nicht eindeutig ist oder eine Lücke im Vertrag besteht. Bei der Vertragsauslegung ist der wirkliche Wille der Vertragsparteien zu erforschen.

Hier ist die vertragliche Vereinbarung zwischen K und A insofern nicht eindeutig, als zwar klar ist, dass K als Auftraggeber bei Vertragsende mit Blick auf die im Auftrag verarbeiteten Daten ein Wahlrecht hat, nämlich dahingehend, ob vom Auftragnehmer eine „Rückgabe“ der Informationen oder lediglich Löschung verlangt wird, fraglich ist aber bereits, ob die getroffene Vereinbarung auch auf die Bereitstellung der Daten in einem marktüblichen Format gerichtet oder es bereits ausreichend ist, wenn der Auftragnehmer die Daten in dem Format bereitstellt, in welchem sie bei ihm vorliegen. Unklar ist des Weiteren, ob der Auftragnehmer für eine „Rückgabe“ der Daten eine extra Vergütung verlangen kann oder ob dies als Service anzusehen ist, welcher durch die erbrachten regelmäßigen Zahlungen des Auftraggebers als mitabgedeckt anzusehen ist.

Als Argument im Rahmen der Auslegung ließe sich anführen, dass, obwohl im Vertrag wie auch in der DS-GVO beide Optionen (Löschung oder „Rückgabe“) vorgesehen sind, aufgrund der Natur der Dienstleistung – insbes. der weiteren Angewiesenheit auf die Informationen für das laufende Geschäft bzw. die Wahrung bestehender Aufbewahrungspflichten – im konkreten Fall nur die Rückgabe der Daten gemeint sein konnte und diese insofern auch mit den bisherigen regelmäßigen Zahlungen an den Dienstleister abgegolten ist. Zu beachten ist allerdings, dass, soweit ersichtlich, keine einschlägige Literatur bzw. Rechtsprechung zu dieser praxisrelevanten Frage besteht und es kaum prognostizierbar ist, ob ein Gericht der dargestellten Argumentation folgen würde.

Jedenfalls, dass auch die Umwandlung der Daten in ein anderes Format ohne Zusatzzahlung geschuldet ist, kann angesichts der bei der Auslegung von Verträgen zu beachtenden Wortlautgrenze mit guten Gründen bezweifelt werden. Die Wortlautgrenze ist ein entscheidendes Kriterium bei der Bestimmung, ob noch Auslegung oder bereits – unzulässige – Rechtsfortbildung betrieben wird.

Fazit: Der vorliegende Fall zeigt deutlich, wie wichtig es in der Praxis ist, bei der Vergabe von Dienstleistungen bereits am Anfang an das Ende zu denken. Es sollte nicht nur die pauschale Regelung aus Art. 28 Abs. 3 S. 2 lit. g) DS-GVO

übernommen werden in den Vertrag, sondern konkrete Vereinbarungen insbes. dazu getroffen werden, in welchem Format die verarbeiteten Informationen nach Vertragsende bereitzustellen sind und ob hierfür eine zusätzliche Vergütung gezahlt werden soll.

## 2. Anforderungen an einen Anspruch auf Datenportabilität (Art. 20 DS-GVO)

Wie ausgeführt, scheidet ein Anspruch auf Datenportabilität aus Art. 20 DS-GVO vorliegend bereits daran, dass es sich um einen Anspruch der betroffenen Person gegen den Verantwortlichen handelt, hier der Anspruch aber weder von einer betroffenen Person noch gegen den Verantwortlichen geltend gemacht wird.<sup>9</sup>

Anders als bei dem verwandten Anspruch auf Auskunft aus Art. 15 DS-GVO, der voraussetzungslos geltend gemacht werden kann, müssten mit Blick auf den Anspruch auf Datenportabilität im Übrigen gleich mehrere Voraussetzungen kumulativ erfüllt sein, damit ein Verantwortlicher entsprechend verpflichtet ist. Im Einzelnen stellt Art. 20 DS-GVO folgende Anforderungen, damit ein Anspruch nach der Norm gegeben ist, d.h. wahlweise ein Recht auf Erhalt der Daten bzw. eines auf Erwirkung der direkten Übermittlung derselben<sup>10</sup>:

- Es muss um solche personenbezogenen Daten gehen, welche die betroffene Person dem Verantwortlichen i.S.v. Art. 20 DS-GVO „bereitgestellt“ hat (Beispiel: Angaben zu Kontaktdaten, Alter etc.). Durch Verantwortliche selbst generierte Daten mit Bezug auf die betroffene Person sind nicht Gegenstand des Anspruchs.<sup>11</sup>
- Gegenstand des Anspruchs sind nur Daten, deren Verarbeitung aufgrund einer Einwilligung oder eines Vertrages erfolgt.
- Der Anspruch bezieht sich schließlich nur auf Daten, die mithilfe automatisierter Verfahren verarbeitet werden.

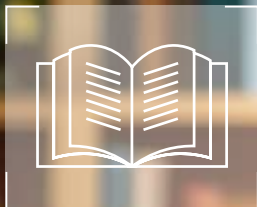
8 § 133 BGB: „Bei der Auslegung einer Willenserklärung ist der wirkliche Wille zu erforschen und nicht an dem buchstäblichen Sinne des Ausdrucks zu haften.“ § 157 BGB: „Verträge sind so auszulegen, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern.“

9 Vgl. oben unter II.2.

10 Vgl. auch oben II.2.

11 Schwartmann/Jaspers/Thüsing/Kugelmann/Rudolph, DS-GVO/BDSG, 3. Aufl. (2024), DS-GVO Art. 20 Rn. 58.

**VIDEO-  
LEARNING**



Shutterstock - stock.adobe.com



**KI-KOMPETENZ**

# KI-Kompetenz aufbauen und nachweisen

- ✓ Art. 4 der KI-VO einfach erfüllen!
- ✓ KI-Fachwissen verständlich & praxisnah
- ✓ Abschlusstest & Zertifikat zur Dokumentation
- ✓ Flexibel abrufbar - ideal für alle Beschäftigten
- ✓ Inklusive 20-seitigem Merkblatt für nachhaltige Wissensvermittlung

**70 Minuten  
Video-Learning  
mit 3 GDD-  
Experten**



Jetzt bestellen: [www.datakontext.com/Video-KI-Kompetenz](http://www.datakontext.com/Video-KI-Kompetenz)

# RECHTSPRECHUNG

## HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

### Anspruch auf Erläuterung der automatisierten Entscheidung

(EuGH, Urteil vom 27. Februar 2025 – C-203/22 –)

#### Relevanz für die Praxis

Der EuGH bezieht in der vorliegenden Entscheidung Stellung zur umstrittenen Frage, ob sich aus Art. 15 Abs. 1 lit. h) DS-GVO ein Recht auf Erläuterung der konkreten automatisierten Entscheidung ergibt. Er legt das Merkmal der aussagekräftigen Information über die involvierte Logik weit aus. Demnach muss sich der Inhalt der geschuldeten Erklärung auf ein bestimmtes bzw. konkretes Ergebnis beziehen. Die Offenlegung des Algorithmus genügt den Anforderungen der DS-GVO demnach nicht. Vielmehr muss der Verantwortliche Informationen über die konkrete Entscheidung erteilen. Eine mögliche Maßnahme liegt daher in der Information darüber, in welchem Maße eine Abweichung bei den berücksichtigten personenbezogenen Daten zu einem anderen Ergebnis geführt hätte. Sofern sich der Verantwortliche darauf beruft, dass eine solche Auskunft geschützte Informationen enthält, darf er deren Erteilung nicht pauschal verweigern. Vielmehr muss er die Auskunft der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht übermitteln, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des in Art. 15 DS-GVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln.

1. **Art. 15 Abs. 1 lit. h) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist dahin auszulegen, dass bei automatisierten Entscheidungsfindungen (einschließlich Profilings) im Sinne von Art. 22 Abs. 1 DS-GVO die betroffene Person vom Verantwortlichen im Rahmen des Anspruchs auf Erteilung „aussagekräftiger Informationen über die involvierte Logik“ verlangen kann, ihr anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form die Verfahren und Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – beispielsweise eines Bonitätsprofils – konkret angewandt wurden.**
2. **Art. 15 Abs. 1 lit. h) der Verordnung 2016/679 ist dahin auszulegen, dass in Fällen, in denen nach Ansicht des**

**Verantwortlichen die Informationen, die der betroffenen Person gem. dieser Bestimmung zu übermitteln sind, von der DS-GVO geschützte Daten Dritter oder Geschäftsgeheimnisse im Sinne von Art. 2 Nr. 1 der Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 08.06.2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung umfassen, der Verantwortliche diese angeblich geschützten Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht zu übermitteln hat, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des in Art. 15 DS-GVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln.**

#### Zu den Vorlagefragen:

#### Zur ersten und zur zweiten Vorlagefrage sowie zur Vorlagefrage 3.a)

Mit der ersten und der zweiten Vorlagefrage sowie mit der Vorlagefrage 3.a), die gemeinsam zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 1 lit. h) DS-GVO dahin auszulegen ist, dass bei automatisierten Entscheidungsfindungen (einschließlich Profilings) im Sinne von Art. 22 Abs. 1 DS-GVO die betroffene Person vom Verantwortlichen im Rahmen des Anspruchs auf Erteilung „aussagekräftiger Informationen über die involvierte Logik“ verlangen kann, umfassend die Verfahren und die Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – beispielsweise eines Bonitätsprofils – konkret angewandt wurden.

Nach ständiger Rechtsprechung des Gerichtshofs sind bei der Auslegung einer Bestimmung des Unionsrechts nicht nur ihr Wortlaut, sondern auch ihr Kontext und die Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, zu berücksichtigen (Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 19 sowie die dort angeführte Rechtsprechung).

Was zunächst den Wortlaut von Art. 15 Abs. 1 lit. h) DS-GVO betrifft, ist darauf hinzuweisen, dass zum einen die Bedeutungen des Ausdrucks „aussagekräftige Informationen“ im Sinne dieser Bestimmung in ihren verschiedenen Sprachfassungen auseinandergehen – in einigen Fassungen wird, wie in der französischen, auf die Funktionalität („nuttige“ in der niederländischen, „úteis“ in der portugiesischen) oder die Relevanz („pertinente“ in der rumänischen) der zu übermittelnden Informationen abgestellt, während das Augenmerk in anderen Fassungen eher auf der Bedeutung dieser Informationen liegt („significativa“ in der spanischen und „istotne“ in der polnischen Fassung). Schließlich können die in der deutschen und in der englischen Fassung dieser Bestimmung

verwendeten Begriffe („aussagekräftig“ bzw. „meaningful“) jeweils sowohl dahin verstanden werden, dass auf die gute Verständlichkeit der Informationen abgestellt wird, als auch dahin, dass es um eine gewisse Qualität der Informationen geht.

Die Vielfalt der Bedeutungen in den verschiedenen Sprachfassungen ist im Sinne einer Komplementarität der in der vorstehenden Randnummer wiedergegebenen Bedeutungen zu verstehen, was bei der Auslegung des Ausdrucks „aussagekräftige Informationen über die involvierte Logik“ im Sinne von Art. 15 Abs. 1 lit. h) DS-GVO zu berücksichtigen ist, wie im Wesentlichen vom Generalanwalt in Nr. 65 der Schlussanträge ausgeführt.

Zum anderen kann, angesichts der allgemein gehaltenen Formulierung, der Verweis auf diese Bestimmung bzw. auf die „involvierte Logik“ einer automatisierten Entscheidungsfindung, die Gegenstand der „aussagekräftigen Informationen“ ist, ein breites Spektrum an „Logiken“ umfassen, die zur Anwendung kommen, wenn personenbezogene Daten oder andere Daten verarbeitet werden, um automationsunterstützt zu einem bestimmten Ergebnis zu gelangen. Diese Auslegung wird durch bestimmte Sprachfassungen der Bestimmung gestützt, in denen Begriffe verwendet werden, die verschiedene Aspekte der gewöhnlichen Bedeutung des Begriffs „Logik“ in sich vereinen. Dies gilt zum Beispiel für die tschechische und die polnische Sprachfassung mit den Begriffen „postupu“ bzw. „zasady“, die mit „Verfahren“ und „Grundsätze“ übersetzt werden können.

Unter den Wortlaut von Art. 15 Abs. 1 lit. h) DS-GVO sind daher alle Informationen zu subsumieren, die für das Verfahren und die Grundsätze der automatisierten Verarbeitung personenbezogener Daten zum Erreichen eines bestimmten Ergebnisses auf der Grundlage dieser Daten maßgeblich sind.

Zum Kontext, in den sich der in Art. 15 Abs. 1 lit. h) DS-GVO enthaltene Ausdruck „aussagekräftige Informationen über die involvierte Logik“ einfügt, ist erstens darauf hinzuweisen, dass diese Informationen nur einen Teil der Informationen darstellen, die unter das in dieser Bestimmung vorgesehene Auskunftsrecht fallen, da dieses auch die Informationen zur Tragweite und zu den angestrebten Auswirkungen der in Rede stehenden Verarbeitung für die betroffene Person umfasst.

Zwar sind diese Informationen, für die gem. den Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, angenommen am 3. Oktober 2017 von der durch Art. 29 der Richtlinie 95/46 eingesetzten Datenschutzgruppe, in der überarbeiteten und am 6. Februar 2018 angenommenen Fassung, „echte, greifbare Beispiele“ anzuführen sind, um sie aussagekräftig und verständlich zu machen, nicht Gegenstand der Fragen des vorlegenden Gerichts, jedoch sind sie als Teil des Kontexts zu berücksichtigen, zu dem der Ausdruck „aussagekräftige Informationen über die involvierte Logik“ gehört.

Zweitens hat der Gerichtshof zum Umstand, dass der Ausdruck „aussagekräftige Informationen über die involvierte Logik“ auch in Art. 13 Abs. 2 lit. f) und in Art. 14 Abs. 2 lit. g) DS-GVO vorkommt, bereits festgestellt, dass im Fall einer automatisierten Entscheidungsfindung im Sinne von Art. 22 Abs. 1 DS-GVO das in Art. 15 Abs. 1 lit. h) DS-GVO verankerte, diese Informationen betreffende Auskunftsrecht und

die zusätzlichen Informationspflichten des Verantwortlichen gem. Art. 13 Abs. 2 lit. f) und Art. 14 Abs. 2 lit. g) DS-GVO eine Einheit bilden (vgl. in diesem Sinne Urt. v. 07.12.2023, SCHUFA Holding u.a. [Scoring], C 634/21, EU:C:2023:957, Rn. 56).

Drittens ist, wie im Wesentlichen vom Generalanwalt in den Nr. 58 bis 60 der Schlussanträge ausgeführt, im Rahmen der kontextuellen Auslegung der für den Fall einer automatisierten Entscheidungsfindung vorgesehenen Auskunftsrechte die Rechtsprechung des Gerichtshofs zu den Anforderungen zu berücksichtigen, die der Verantwortliche gem. Art. 15 Abs. 3 DS-GVO erfüllen muss.

So ist insbesondere dem Umstand Rechnung zu tragen, dass das in Art. 12 Abs. 1 DS-GVO vorgesehene Erfordernis der Transparenz der übermittelten Informationen für sämtliche Daten und Informationen gem. Art. 15 gilt, einschließlich derjenigen, die automatisierte Entscheidungsfindungen betreffen.

Um zu gewährleisten, dass die betroffene Person in die Lage versetzt wird, die ihr vom Verantwortlichen übermittelten Informationen in vollem Umfang zu verstehen, verpflichtet Art. 12 Abs. 1 DS-GVO den Verantwortlichen, geeignete Maßnahmen zu treffen, um insbesondere der betroffenen Person diese Daten und Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (vgl. i.S.d. Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 38).

Die Prüfung des Kontexts von Art. 15 Abs. 1 lit. h) DS-GVO bestätigt somit die Auslegung, die sich aus der Analyse der in dieser Bestimmung verwendeten Ausdrücke ergibt, wonach „aussagekräftige Informationen über die involvierte Logik“ einer automatisierten Entscheidungsfindung im Sinne dieser Bestimmung alle maßgeblichen Informationen zum Verfahren und zu den Grundsätzen der automatisierten Verarbeitung personenbezogener Daten zwecks Erreichen eines bestimmten Ergebnisses umfassen und diese Informationen aufgrund des Transparenzerfordernisses außerdem in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln sind.

Zum Zweck der DS-GVO ist schließlich darauf hinzuweisen, dass ihr Ziel insbesondere darin besteht, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen zu gewährleisten, und zwar insbesondere ihres in Art. 16 AEUV gewährleisteten Rechts auf Schutz der personenbezogenen Daten, das in Art. 8 der Charta als Grundrecht verankert ist und das in Art. 7 der Charta verankerte Recht auf ein Privatleben ergänzt (vgl. i.S.d. Urt. v. 04.10.2024, Schrems [Mitteilung von Daten an die breite Öffentlichkeit], C 446/21, EU:C:2024:834, Rn. 45 und die dort angeführte Rechtsprechung).

Die DS-GVO hat also, wie sich aus ihrem elften Erwägungsgrund ergibt, den Zweck, die Rechte der betroffenen Personen zu stärken und präzise festzulegen (Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 33 und die dort angeführte Rechtsprechung).

Was konkret das in Art. 15 DS-GVO vorgesehene Auskunftsrecht betrifft, muss es der betroffenen Person nach der Rechtsprechung des Gerichtshofs ermöglichen, zu überprüfen, ob sie betreffende Daten richtig sind und ob sie in zulässiger Weise verarbeitet werden (Urt. v. 04.05.2023, Österreichi-

sche Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 34, und v. 26.10.2023, FT [Kopien der Patientenakte], C 307/22, EU:C:2023:811, Rn. 73).

Dieses Auskunftsrecht ist 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 Art. 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 ihre in den Art. 79 und 82 DS-GVO vorgesehenen Rechte auf Einlegung eines gerichtlichen Rechtsbehelfs bzw. auf Schadenersatz auszuüben (vgl. i.S.d. Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 35).

Insbesondere im speziellen Kontext des Erlasses einer Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung beruht, bezweckt das Recht der betroffenen Person, die in Art. 15 Abs. 1 lit. h) DS-GVO genannten Informationen zu erhalten, hauptsächlich, ihr die wirksame Ausübung der ihr nach Art. 22 Abs. 3 DS-GVO zustehenden Rechte zu ermöglichen, nämlich des Rechts auf Darlegung ihres eigenen Standpunkts und des Rechts auf Anfechtung der Entscheidung.

Wenn von einer automatisierten Entscheidung – einschließlich Profiling – betroffene Personen nicht in der Lage wären, vor der Darlegung ihres Standpunkts oder der Anfechtung der Entscheidung die Gründe für diese Entscheidung nachzuvollziehen, würden diese Rechte ihren Zweck, diese Personen gegen die besonderen Risiken für ihre Rechte und Freiheiten zu schützen, die mit der automatisierten Verarbeitung personenbezogener Daten verbunden sind, nicht in vollem Umfang erfüllen (vgl. i.S.d. Urt. v. 07.12.2023, SCHUFA Holding u.a. [Scoring], C 634/21, EU:C:2023:957, Rn. 57).

Gemäß dem 71. ErwG der DS-GVO muss die betroffene Person, wenn sie einer Entscheidung unterworfen wird, die ausschließlich auf einer automatisierten Verarbeitung beruht und die sie erheblich beeinträchtigt, das Recht auf Erläuterung dieser Entscheidung haben. Wie vom Generalanwalt in Nr. 67 seiner Schlussanträge ausgeführt, bietet Art. 15 Abs. 1 lit. h) DS-GVO der betroffenen Person also ein echtes Recht auf Erläuterung der Funktionsweise des Mechanismus der automatisierten Entscheidungsfindung, der diese Person unterworfen worden ist, und des Ergebnisses, zu dem diese Entscheidung geführt hat.

Aus der Prüfung der Ziele der DS-GVO und insbesondere von Art. 15 Abs. 1 lit. h) DS-GVO ergibt sich, dass das Recht auf „aussagekräftige Informationen über die involvierte Logik“ bei einer automatisierten Entscheidungsfindung im Sinne dieser Bestimmung als ein Recht auf Erläuterung des Verfahrens und der Grundsätze zu verstehen ist, die bei der automatisierten Verarbeitung der personenbezogenen Daten der betroffenen Person zur Anwendung kamen, um auf der Grundlage dieser Daten zu einem bestimmten Ergebnis – etwa einem Bonitätsprofil – zu gelangen. Damit die betroffene Person die ihr durch die DS-GVO und insbesondere deren Art. 22 Abs. 3 gewährten Rechte wirksam ausüben kann, müssen im Rahmen dieser Erläuterung die relevanten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form übermittelt werden.

Weder die bloße Übermittlung einer komplexen mathematischen Formel (etwa eines Algorithmus), noch die detaillierte Beschreibung jedes Schritts einer automatisierten Entscheidungsfindung genügen diesen Anforderungen, da beides keine ausreichend präzise und verständliche Erläuterung darstellt.

Wie sich aus S. 28 der in Rn. 45 des vorliegenden Urteils genannten Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679 ergibt, sollte nämlich zum einen der Verantwortliche einfache Möglichkeiten finden, die betroffene Person über die der Entscheidungsfindung zugrunde liegenden Überlegungen bzw. Kriterien zu informieren. Zum anderen verpflichtet die DS-GVO den Verantwortlichen zur Übermittlung aussagekräftiger Informationen über die involvierte Logik, „nicht unbedingt zu einer ausführlichen Erläuterung der verwendeten Algorithmen oder zur Offenlegung des gesamten Algorithmus“.

Die „aussagekräftigen Informationen über die involvierte Logik“ einer automatisierten Entscheidungsfindung im Sinne von Art. 15 Abs. 1 lit. h) DS-GVO müssen also das Verfahren und die Grundsätze, die konkret zur Anwendung kommen, so beschreiben, dass die betroffene Person nachvollziehen kann, welche ihrer personenbezogenen Daten im Rahmen der in Rede stehenden automatisierten Entscheidungsfindung auf welche Art verwendet wurden, ohne dass die Komplexität der im Rahmen einer automatisierten Entscheidungsfindung vorzunehmenden Arbeitsschritte den Verantwortlichen von seiner Erläuterungspflicht entbinden könnte.

Was konkret ein Profiling wie das im Ausgangsverfahren in Rede stehende betrifft, könnte das vorliegende Gericht es insbesondere als ausreichend transparent und nachvollziehbar erachten, die betroffene Person zu informieren, in welchem Maße eine Abweichung bei den berücksichtigten personenbezogenen Daten zu einem anderen Ergebnis geführt hätte.

Ferner ist zur Frage, ob die übermittelten Informationen der betroffenen Person eine Überprüfung der Richtigkeit der sie betreffenden, der automatisierten Entscheidungsfindung zugrunde liegenden personenbezogenen Daten ermöglichen müssen, darauf hinzuweisen, dass das Recht auf Auskunft über diese Daten nicht durch Art. 15 Abs. 1 lit. h) DS-GVO begründet wird, sondern durch den einleitenden Satz von Art. 15 Abs. 1 DS-GVO, der der betroffenen Person das Recht gewährleistet, die Richtigkeit dieser Daten zu überprüfen; dies ergibt sich aus der in Rn. 53 des vorliegenden Urteils wiedergegebenen Rechtsprechung.

Schließlich ist zur Feststellung des vorliegenden Gerichts, wonach die CK von D & B gem. Art. 15 Abs. 1 lit. h) DS-GVO übermittelten Informationen tatsachenwidrig seien, da CK gem. dem „tatsächlichen“ Profiling als nicht zahlungskräftig anzusehen sei, obwohl die genannten Informationen das Gegenteil nahelegten, darauf hinzuweisen, dass zwar dem vorliegenden Gericht zufolge die so festgestellte Nichtübereinstimmung darauf zurückzuführen ist, dass D & B CK nicht über das ihre Person betreffende Profiling informiert habe, das für den Mobilfunkanbieter erstellt worden sei und auf dessen Grundlage CK der Abschluss bzw. die Verlängerung eines Vertrags verweigert worden sei, dies aber im Wege des Rechts auf Auskunft über das so erstellte Bonitätsprofil zu beheben wäre. Hierzu ergibt sich aus der Rechtspre-

chung des Gerichtshofs, dass die vom Verantwortlichen selbst erzeugten personenbezogenen Daten unter Art. 14 DS-GVO fallen (vgl. i.S.d. Urt. v. 28.11.2024, *Másdi*, C 169/23, EU:C:2024:988, Rn. 48).

Eine Erläuterung der Unterschiede zwischen dem Ergebnis eines solchen „tatsächlichen“ Profilings – seine Durchführung unterstellt – und dem CK von D & B mitgeteilten Ergebnis, das D & B zufolge mittels „gleichwertiger Gewichtung“ der CK betreffenden Daten zustande kam, fällt hingegen sehr wohl unter „aussagekräftige Informationen über die involvierte Logik“ des so erstellten Profilings. Im Einklang mit den Ausführungen in Rn. 58 des vorliegenden Urteils müsste D & B also in präziser, transparenter, verständlicher und leicht zugänglicher Form das Verfahren und die Grundsätze erläutern, anhand derer das „tatsächliche“ Profiling erstellt wurde.

Gemäß den vorstehenden Ausführungen ist auf die erste und die zweite Vorlagefrage sowie die Vorlagefrage 3.a) zu antworten, dass Art. 15 Abs. 1 lit. h) DS-GVO dahin auszulegen ist, dass bei automatisierten Entscheidungsfindungen (einschließlich Profilings) im Sinne von Art. 22 Abs. 1 DS-GVO die betroffene Person vom Verantwortlichen im Rahmen des Anspruchs auf Erteilung „aussagekräftiger Informationen über die involvierte Logik“ verlangen kann, ihr anhand der maßgeblichen Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form das Verfahren und die Grundsätze zu erläutern, die bei der automatisierten Verarbeitung ihrer personenbezogenen Daten zur Gewinnung eines bestimmten Ergebnisses – beispielsweise eines Bonitätsprofils – konkret angewandt wurden.

#### **Zu den Vorlagefragen 3.b), 3.c), 4.a) und 4.b) sowie zur fünften und zur sechsten Vorlagefrage**

Mit den Vorlagefragen 3.b), 3.c), 4.a) und 4.b) sowie der fünften und der sechsten Vorlagefrage, die gemeinsam zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 15 Abs. 1 lit. h) DS-GVO dahin auszulegen ist, dass in Fällen, in denen nach Ansicht des Verantwortlichen die Informationen, die der betroffenen Person gem. dieser Bestimmung zu übermitteln sind, von der DS-GVO geschützte Daten Dritter oder Geschäftsgeheimnisse im Sinne von Art. 2 Nr. 1 der Richtlinie 2016/943 umfassen, der Verantwortliche diese angeblich geschützten Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht zu übermitteln hat, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des in Art. 15 DS-GVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln.

Nach dem 4. ErwG der DS-GVO ist das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht und muss unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. Somit steht die DS-GVO im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der Charta anerkannt wurden und in den Verträgen verankert sind (Urt. v. 26.10.2023, FT [Kopien der Patientenakte], C 307/22, EU:C:2023:811, Rn. 59 und die dort angeführte Rechtsprechung).

Außerdem sollte gem. dem 63. ErwG dieser Verordnung das Auskunftsrecht der betroffenen Person hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen.

Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Art. 23 Abs. 1 lit. i) DS-GVO sieht hierzu im Wesentlichen vor, dass eine Beschränkung des Umfangs der u.a. in Art. 15 DS-GVO vorgesehenen Pflichten und Rechte nur möglich ist, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die den Schutz der Rechte und Freiheiten anderer Personen sicherstellt.

Zum verwandten, in Art. 15 Abs. 4 DS-GVO verankerten Recht auf Erhalt einer Kopie hat der Gerichtshof bereits festgestellt, dass dessen Ausübung die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen sollte (vgl. i.S.d. Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 43).

In diesem Zusammenhang hat der Gerichtshof entschieden, dass 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 sind. 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. ErwG der DS-GVO ergibt (Urt. v. 04.05.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 44).

Zur Frage, wie das Auskunftsrecht gem. Art. 15 Abs. 1 lit. h) DS-GVO so umgesetzt werden kann, dass die Rechte und Freiheiten anderer Personen gewahrt werden, ist darauf hinzuweisen, dass ein nationales Gericht nach der Rechtsprechung der Ansicht sein kann, dass ihm personenbezogene Daten von Parteien oder Dritten übermittelt werden müssen, damit es in voller Kenntnis der Sachlage und unter Beachtung des Grundsatzes der Verhältnismäßigkeit die betroffenen Interessen abwägen kann. Diese Beurteilung kann es gegebenenfalls dazu veranlassen, die vollständige oder teilweise Offenlegung der ihm so übermittelten personenbezogenen Daten gegenüber der Gegenpartei zuzulassen, wenn es der Auffassung ist, dass eine solche Offenlegung nicht über das hinausgeht, was erforderlich ist, um die effektive Wahrnehmung der Rechte zu gewährleisten, die den Rechtsuchenden aus Art. 47 der Charta erwachsen (Urt. v. 02.03.2023, Norra Stockholm Bygg, C 268/21, EU:C:2023:145, Rn. 58).

Wie vom Generalanwalt in Nr. 94 seiner Schlussanträge ausgeführt, kann diese Rechtsprechung uneingeschränkt auf den Fall übertragen werden, dass die Informationen, die der betroffenen Person im Rahmen des durch Art. 15 Abs. 1 lit. h) DS-GVO garantierten Auskunftsrechts zur Verfügung gestellt werden müssen, geeignet sind, zu einer Beeinträchtigung der Rechte und Freiheiten anderer Personen zu führen, insbesondere, da sie durch die DS-GVO geschützte personenbezogene Daten Dritter oder ein Geschäftsgeheimnis im Sinne von Art. 2 Nr. 1 der Richtlinie 2016/943 enthalten. Auch in diesem Fall sind diese Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht zu übermitteln, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des Rechts der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten zu ermitteln.

Hinsichtlich der Notwendigkeit, dies von Fall zu Fall zu ermitteln, steht Art. 15 Abs. 1 lit. h) DS-GVO insbesondere der Anwendung einer Bestimmung wie § 4 Abs. 6 DSG entgegen, die das in Art. 15 DS-GVO vorgesehene Auskunftsrecht der betroffenen Person grundsätzlich ausschließt, wenn die Auskunft ein Geschäfts- oder Betriebsgeheimnis des Verantwortlichen oder eines Dritten gefährden würde. Ein Mitgliedstaat kann das Ergebnis einer durch das Unionsrecht vorgegebenen, auf Einzelfallbasis durchzuführenden Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben (vgl. i.d.S. Urt. v. 07.12.2023, SCHUFA Holding u.a. [Scoring], C 634/21, EU:C:2023:957, Rn. 70 und die dort angeführte Rechtsprechung).

Angesichts der vorstehenden Ausführungen ist auf die Vorlagefragen 3.b), 3.c), 4.a) und 4.b) sowie auf die fünfte und die sechste Vorlagefrage zu antworten, dass Art. 15 Abs. 1 lit. h) DS-GVO dahin auszulegen ist, dass in Fällen, in denen nach Ansicht des Verantwortlichen die Informationen, die der betroffenen Person gem. dieser Bestimmung zu übermitteln sind, von der DS-GVO geschützte Daten Dritter oder Geschäftsgeheimnisse im Sinne von Art. 2 Nr. 1 der Richtlinie 2016/943 umfassen, der Verantwortliche diese angeblich geschützten Informationen der zuständigen Aufsichtsbehörde oder dem zuständigen Gericht zu übermitteln hat, die die einander gegenüberstehenden Rechte und Interessen abwägen müssen, um den Umfang des in Art. 15 DS-GVO vorgesehenen Auskunftsrechts der betroffenen Person zu ermitteln. [...]

### Zur Vertiefung

[Urteil] *Besondere datenschutzrechtliche Herausforderungen des SCHUFA-Scorings* = RDV 1/2024

[Urteil] *Reichweite des Rechts auf Kopie aus Art. 15 Abs. 3 S. 1 DS-GVO* = RDV 4/2023

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

## Verbraucherschutzverbände können Datenschutzverstöße wettbewerbsrechtlich verfolgen

(BGH, Urteil vom 27. März 2025 – I ZR 186/17 –)

### Relevanz für die Praxis

Der BGH hat in seinem Urteil bestätigt, dass Verbraucherschutzverbände wie Mitbewerber berechtigt sind, wettbewerbsrechtlich gegen Datenschutzverstöße vorzugehen. Er betont zudem, dass es einen Auftrag einer konkreten Person hierfür nicht bedarf. Es genügt vielmehr, wenn der Verband eine Kategorie oder Gruppe von identifizierbaren natürlichen Personen benennt und sich darauf beruft, dass deren Rechte verletzt seien. Damit stärkt der BGH den Verbraucherschutz v.a. im digitalen Raum. Neben Datenschutzverbänden und einzelnen Verbrauchern tritt damit ein weiterer Akteur auf, um gegen Datenschutzverstöße größeren Ausmaßes vorzugehen.

1. **Qualifizierten Einrichtungen steht gem. § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 S. 1 Nr. 1 UKlaG die Befugnis zu, wegen Verstößen gegen Informationspflichten gem. Art. 12 Abs. 1 S. 1 DS-GVO in Verbindung mit Art. 13 Abs. 1 lit. c) und e) DS-GVO unabhängig von der konkreten Verletzung von Rechten einzelner betroffener Personen und ohne Auftrag einer betroffenen Person wegen Verstößen gegen das Gesetz gegen den unlauteren Wettbewerb, ein Verbraucherschutzgesetz im Sinne von § 2 Abs. 2 Nr. 13 UKlaG, und der Verwendung einer unwirksamen Allgemeinen Geschäftsbedingung gem. § 1 UKlaG im Wege einer Klage vor den Zivilgerichten vorzugehen.**
2. **In dem Verstoß gegen die datenschutzrechtlichen Informationspflichten gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO liegt zugleich ein Verstoß gegen Lauterkeitsrecht unter dem Gesichtspunkt des Vorenthaltens einer wesentlichen Information gem. § 5a Abs. 1 UWG vor.**
3. **Ausgehend von der wirtschaftlichen Bedeutung der Verarbeitung von personenbezogenen Daten für internetbasierte Geschäftsmodelle, deren Nutzung der Verbraucher mit der Preisgabe personenbezogener Daten vergütet, kommt den Unterrichtungspflichten gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO zentrale Bedeutung zu, um sicherzustellen, dass der Verbraucher bei seiner mit einer Nachfrageentscheidung verknüpften Einwilligung in die Verarbeitung personenbezogener Daten über Umfang und Tragweite dieser Einwilligungserklärung möglichst umfassend ins Bild gesetzt wird, um eine informierte Entscheidung treffen zu können.**

### Aus den Gründen:

I. Die Klage ist zulässig.

[...] 2. Die [...] prozessuale Klagebefugnis (vgl. BGH, GRUR 2020, 896 [juris Rn. 32] – App-Zentrum I, m.w.N.) liegt [...] vor.

a) Der Kläger war vor Inkrafttreten der Datenschutz-Grundverordnung gem. § 8 Abs. 3 Nr. 3 UWG sowie aus § 3 Abs. 1 S. 1 Nr. 1 UKlaG befugt, die Klageanträge im Wege der Klage vor den Zivilgerichten zu verfolgen (vgl. BGH, GRUR 2020, 896 [juris Rn. 24 bis 28] – App-Zentrum I).

b) Diese ursprünglich bestehende prozessuale Klagebefugnis (vgl. BGH, GRUR 2020, 896 [juris Rn. 32] – App-Zentrum I, m.w.N.) ist nicht mit Geltung der Datenschutz-Grundverordnung ab dem 25. Mai 2018 (Art. 99 Abs. 2 DS-GVO) entfallen.

aa) Ausgehend vom Klagebegehren des Klägers, der als Verbraucherverband die Verletzung einer die Beklagte betreffenden Informationspflicht über Zweck und Umfang einer Einwilligung des Nutzers in die Verarbeitung seiner personenbezogenen Daten geltend macht (vgl. BGH, GRUR 2020, 896 [juris Rn. 19] – App-Zentrum I), hängt im Streitfall die Zulässigkeit der Klage davon ab, ob qualifizierten Einrichtungen nach Inkrafttreten der Datenschutz-Grundverordnung gem. § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 S. 1 Nr. 1 UKlaG die Befugnis zusteht, wegen Verstößen gegen diese Verordnung unabhängig von der konkreten Verletzung von Rechten einzelner betroffener Personen und ohne Auftrag einer betroffenen Person wegen Verstößen gegen das Gesetz gegen den unlauteren Wettbewerb, ein Verbraucherschutzgesetz im Sinne von § 2 Abs. 2 Nr. 13 UKlaG und der Verwendung einer unwirksamen Allgemeinen Geschäftsbedingung gem. § 1 UKlaG im Wege einer Klage vor den Zivilgerichten vorzugehen (BGH, GRUR 2020, 896 [juris Rn. 17 und Rn. 55 bis 62] – App-Zentrum I; GRUR 2023, 193 [juris Rn. 11] – App-Zentrum II). Dies bestimmt sich danach, ob die maßgeblichen Bestimmungen des deutschen Rechts über die Klagebefugnis gem. § 8 Abs. 3 Nr. 3 UWG und gem. § 3 Abs. 1 S. 1 Nr. 1 UKlaG mit den in Art. 80 Abs. 2 DS-GVO geregelten Voraussetzungen vereinbar sind (vgl. EuGH, GRUR 2022, 920 [juris Rn. 49 und 62] – Meta Platforms Ireland; BGH, GRUR 2023, 193 [juris Rn. 10] – App-Zentrum II).

bb) Der Gerichtshof der Europäischen Union hat entschieden, dass Art. 80 Abs. 2 DS-GVO eine geeignete Grundlage für die Verfolgung von Verstößen gegen die Datenschutz-Grundverordnung durch Verbände nach dem Gesetz gegen den unlauteren Wettbewerb und dem Unterlassungsklagengesetz bilden kann (vgl. EuGH, GRUR 2022, 920 [juris Rn. 79] – Meta Platforms Ireland).

(1) Nach Art. 80 Abs. 2 DS-GVO können die Mitgliedstaaten vorsehen, dass jede der in Abs. 1 dieses Artikels genannten Einrichtungen, Organisationen oder Vereinigungen unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der gem. Art. 77 DS-GVO zuständigen Aufsichtsbehörde eine Beschwerde einzulegen und die in den Art. 78 und 79 DS-GVO aufgeführten Rechte (hier: das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter nach Art. 79 DS-GVO) in Anspruch zu nehmen, wenn ihres Erachtens die Rechte einer betroffenen Person gem. der Verordnung infolge einer Verarbeitung verletzt worden sind.

(2) Durch die Bestimmung des Art. 80 Abs. 2 DS-GVO ist den Mitgliedstaaten ein Ermessensspielraum hinsichtlich ihrer Umsetzung eröffnet worden. Damit die in Art. 80 Abs. 2 DS-GVO vorgesehene Verbandsklage erhoben werden kann, müssen die Mitgliedstaaten von der ihnen durch diese Be-

stimmung eingeräumten Möglichkeit Gebrauch machen, diese Art der Vertretung betroffener Personen in ihrem nationalen Recht vorzusehen (vgl. EuGH, GRUR 2022, 920 [juris Rn. 59] – Meta Platforms Ireland). Danach ist maßgeblich, ob sich die im Streitfall in Rede stehenden Bestimmungen zur Klagebefugnis von Verbänden gem. § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 S. 1 Nr. 1 UKlaG in den Rahmen des jedem Mitgliedstaat durch Art. 80 Abs. 2 DS-GVO eingeräumten Ermessensspielraums einfügen. Dieser Spielraum ist im Wege der Auslegung unter Berücksichtigung des Wortlauts des Art. 80 Abs. 2 DS-GVO sowie der Systematik und der Ziele der Datenschutz-Grundverordnung zu ermitteln (vgl. EuGH, GRUR 2022, 920 [juris Rn. 62] – Meta Platforms Ireland). Dabei ist zu berücksichtigen, dass die in Art. 80 Abs. 2 DS-GVO den Mitgliedstaaten eröffnete Möglichkeit, ein Verfahren einer Verbandsklage gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten vorzusehen, an eine Reihe von Anforderungen an den persönlichen und sachlichen Anwendungsbereich geknüpft ist (EuGH, GRUR 2022, 920 [juris Rn. 63] – Meta Platforms Ireland).

cc) Vorliegend sind sowohl die Anforderungen an den persönlichen Anwendungsbereich als auch die den sachlichen Anwendungsbereich des Art. 80 Abs. 2 DS-GVO betreffenden Voraussetzungen erfüllt.

(1) Die dem Kläger durch § 8 Abs. 3 Nr. 3 UWG und § 3 Abs. 1 S. 1 Nr. 1 UKlaG eingeräumte Klagebefugnis fällt in den persönlichen Anwendungsbereich von Art. 80 Abs. 2 DS-GVO. Der Kläger erfüllt als Verband zur Wahrung von Verbraucherinteressen die in Art. 80 Abs. 1 DS-GVO an die Klagebefugnis einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht zu stellenden Anforderungen (vgl. EuGH, GRUR 2022, 920 [juris Rn. 65 f. und 79] – Meta Platforms Ireland; GRUR 2024, 1357 [juris Rn. 41] – Meta Platforms Ireland [Verbandsklage]; BGH, GRUR 2023, 193 [juris Rn. 16] – App-Zentrum II).

(2) Mit der Klage wird außerdem die Verletzung von Datenschutzrechten einer betroffenen Person im Sinne des Art. 80 Abs. 2 DS-GVO geltend gemacht. Insoweit ist unschädlich, dass der Kläger seine Klage unabhängig von der konkreten Verletzung von Datenschutzrechten einer betroffenen Person und ohne Auftrag einer solchen Person erhoben hat (vgl. BGH, GRUR 2020, 896 [juris Rn. 7] – App-Zentrum I; GRUR 2023, 193 [juris Rn. 18] – App-Zentrum II; EuGH, GRUR 2022, 920 [juris Rn. 36] – Meta Platforms Ireland), sondern Gegenstand des Klagebegehrens allein die abstrakte Überprüfung der Präsentation des App-Zentrums durch die Beklagte am objektivrechtlichen Maßstab des Datenschutzrechts ist.

(a) Der Gerichtshof der Europäischen Union hat entschieden, dass von einer Einrichtung im Sinne von Art. 80 Abs. 2 DS-GVO nicht verlangt werden kann, dass sie diejenige Person im Voraus individuell ermittelt, die von einer Verarbeitung von Daten, die mutmaßlich gegen die Bestimmungen der Datenschutz-Grundverordnung verstößt, konkret betroffen ist. Der Begriff "betroffene Person" im Sinne von Art. 4 Nr. 1 DS-GVO umfasst nicht nur eine "identifizierte natürliche Person", sondern auch eine "identifizierbare natürliche Person", also eine natürliche Person, die direkt oder indirekt, mittels Zuordnung zu einer Kennung wie insbesondere einem Namen, einer Kennnummer, Standortdaten oder einer Online-Kennung identifiziert werden kann. Unter diesen Umständen kann die Benennung einer Kategorie oder Gruppe von Per-

sonen, die von einer solchen Verarbeitung betroffen sind, für die Erhebung einer solchen Verbandsklage ausreichen (vgl. EuGH, GRUR 2022, 920 [juris Rn. 68 f.] – Meta Platforms Ireland; BGH, GRUR 2023, 193 [juris Rn. 18] – App-Zentrum II).

(b) Die von der Gestaltung des App-Zentrums angesprochenen Nutzer der Internetplattform Facebook, die an der Durchführung eines dort angebotenen Spiels interessiert waren und deshalb potenziell durch Betätigung des Buttons "Sofort spielen" ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten erklären konnten, sind identifizierbare natürliche Personen im vorstehenden Sinne (BGH, GRUR 2023, 193 [juris Rn. 18] – App-Zentrum II).

(3) Der Kläger macht mit den Klageanträgen zudem geltend, dass im Sinne von Art. 80 Abs. 2 DS-GVO seines Erachtens Rechte einer betroffenen Person gem. der Datenschutz-Grundverordnung "infolge einer Verarbeitung" verletzt worden sind.

(a) Nach der Rechtsprechung des Gerichtshofs der Europäischen Union ist diese Voraussetzung erfüllt, wenn sich die Einrichtung darauf beruft, dass die Verletzung der Rechte dieser Person anlässlich einer Verarbeitung personenbezogener Daten geschieht und auf einer Missachtung der Pflicht beruht, die dem Verantwortlichen gem. Art. 12 Abs. 1 S. 1 und Art. 13 Abs. 1 lit. c) und e) der Verordnung obliegt, der betroffenen Person spätestens bei dieser Datenerhebung Informationen über den Zweck der Datenverarbeitung und die Empfänger der Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (EuGH, GRUR 2024, 1357 [juris Rn. 65] – Meta Platforms Ireland [Verbandsklage]).

(b) Diese Voraussetzungen sind im Streitfall erfüllt. Gegenstand der Klageanträge ist der Vorwurf des Klägers, die Beklagte habe mit der beanstandeten Gestaltung ihres App-Zentrums die sich aus Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO ergebenden Verpflichtung verletzt, der betroffenen Person die Informationen über den Zweck der Datenverarbeitung und den Empfänger personenbezogener Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (vgl. BGH, GRUR 2020, 896 [juris Rn. 30] – App-Zentrum I; GRUR 2023, 193 [juris Rn. 27] – App-Zentrum II).

(c) Die Revision rügt ohne Erfolg, der Kläger habe nicht im Einklang mit den vom Gerichtshof der Europäischen Union zur Auslegung von Art. 80 Abs. 2 DS-GVO aufgestellten Grundsätzen dargelegt, dass die Rechte einer betroffenen Person gem. der Datenschutz-Grundverordnung infolge einer Verarbeitung verletzt worden seien.

Der Gerichtshof der Europäischen Union hat unter Bezugnahme auf die Ausführungen des Generalanwalts ausgeführt, dass die Datenverarbeitung, von der die Einrichtung meint, dass sie gegen die Bestimmungen der Datenschutz-Grundverordnung verstoße, existieren muss und somit nicht rein hypothetischer Natur sein darf (EuGH, GRUR 2024, 1357 [juris Rn. 44] – Meta Platforms Ireland [Verbandsklage] in Verbindung mit Rn. 48 der Schlussanträge des Generalanwalts in der Rechtssache C-757/22 v. 25.01.2024). Im Streitfall kann nicht davon ausgegangen werden, dass der Kläger mit der Klage nicht existierende und somit rein hypothetische Verstöße gegen die Verletzung der sich aus den Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO ergebenden Informa-

tionspflichten geltend macht. Der konkrete Inhalt der im App-Zentrum gemachten Angaben ist unstrittig. Es wird außerdem weder von der Revision geltend gemacht noch ist sonst ersichtlich, dass Nutzer der Internetplattform Facebook das von der Beklagten dort präsentierte App-Zentrum tatsächlich nicht genutzt, insbesondere den Button "Sofort spielen" nicht betätigt und damit auch keine Datenverarbeitung ausgelöst haben.

dd) Einer Klagebefugnis nach Maßgabe von Art. 80 Abs. 2 DS-GVO steht außerdem nicht entgegen, dass der Kläger mit einem Verstoß gegen die Vorschriften zum Schutz der personenbezogenen Daten der Verbraucher zugleich einen Verstoß gegen andere Vorschriften zum Schutz der Verbraucher und zur Bekämpfung unlauterer Geschäftspraktiken beanstandet (vgl. EuGH, GRUR 2022, 920 [juris Rn. 66 und Rn. 77 bis 82] – Meta Platforms Ireland; BGH, GRUR 2023, 193 [juris Rn. 19] – App-Zentrum II).

II. Das Berufungsgericht hat die Klageanträge rechtsfehlerfrei für begründet erachtet.

1. Das mit dem Unterlassungsantrag zu 1 angegriffene Verhalten verstößt gegen Vorschriften zum Schutz der personenbezogenen Daten der Verbraucher und stellt deshalb zugleich eine unlautere geschäftliche Handlung gem. § 3 Abs. 1 UWG dar, die die Beklagte unter dem Gesichtspunkt der Wiederholungsgefahr zur Unterlassung verpflichtet (§ 8 Abs. 1 S. 1 UWG).

a) Der auf Wiederholungsgefahr gestützte Unterlassungsanspruch ist nur begründet, wenn das beanstandete Verhalten sowohl nach dem zum Zeitpunkt seiner Vornahme geltenden Recht wettbewerbswidrig war als auch nach dem zur Zeit der Revisionsentscheidung geltenden Recht wettbewerbswidrig ist (st. Rspr.; vgl. nur BGH, Urt. v. 13.07.2023 – I ZR 60/22, GRUR 2023, 1710 [juris Rn. 18] = WRP 2024, 72 – Eigenlaborgewinn, m.w.N.). So liegt es im Streitfall. Die mit dem Unterlassungsantrag zu 1 angegriffene Präsentation von Spielen im App-Zentrum der Beklagten verstößt sowohl gegen die zum Zeitpunkt der Verletzungshandlung maßgeblichen datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG als auch gegen die nunmehr geltenden Bestimmungen gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO (dazu B II 1 b). Darin liegt zugleich ein Verstoß gegen Lauterkeitsrecht unter dem Gesichtspunkt des Vorenthaltes einer wesentlichen Information gem. § 5a Abs. 2 UWG in der zum Zeitpunkt der Verletzungshandlung am 26.11.2012 geltenden Fassung (a.F.) und § 5a Abs. 1 UWG in der derzeit geltenden Fassung (n.F.) (dazu B II 1 c). Außerdem liegt die für den geltend gemachten Unterlassungsanspruch gem. § 8 Abs. 1 S. 1 UWG erforderliche Wiederholungsgefahr vor (dazu B II 1 d).

b) Die Präsentation des App-Zentrums verstieß gegen die zum Zeitpunkt seiner Vornahme geltenden datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG (dazu B II 1 b aa) und stellt außerdem einen Verstoß gegen die nunmehr geltenden Vorschriften gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO dar (dazu B II 1 b bb).

[...]

bb) Die beanstandete Präsentation des App-Zentrums verstößt auch gegen die nunmehr geltenden Informationspflichten gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO.

(1) Gemäß Art. 12 Abs. 1 S. 1 DS-GVO hat der Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen gem. Art. 13 und 14 DS-GVO und alle Mitteilungen gem. den Art. 15 bis 22 und Art. 34 DS-GVO, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Nach Art. 13 Abs. 1 DS-GVO hat der Verantwortliche für den Fall, dass personenbezogene Daten bei der betroffenen Person erhoben werden, der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (lit. c) sowie gegebenenfalls die Empfänger oder Kategorien von Empfängern der persönlichen Daten (lit. e)) mitzuteilen.

(2) Aus den bereits dargelegten rechtsfehlerfreien Feststellungen des Berufungsgerichts ergibt sich, dass die angegriffene Präsentation der Spiele im App-Zentrum der Beklagten auch den Anforderungen der Unterrichtungspflichten nach Art. 13 Abs. 1 DS-GVO nicht genügt.

c) In dem Verstoß gegen die datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG und Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO liegt zugleich ein Verstoß gegen Lauterkeitsrecht unter dem Gesichtspunkt des Vorenthaltens einer wesentlichen Information gem. § 5a Abs. 2 UWG a.F. beziehungsweise § 5a Abs. 1 UWG n.F.

aa) Allerdings hat der Senat in seinen Vorabentscheidungsersuchen einen Verstoß gegen das Lauterkeitsrecht unter dem Gesichtspunkt des Rechtsbruchs gem. § 3a UWG angenommen. Daran hält er nicht fest. In den Fällen des Vorenthaltens einer für die geschäftliche Entscheidung eines Verbrauchers wesentliche Information ist die Unlauterkeit einer geschäftlichen Handlung nach der neueren Rechtsprechung des Senats allein nach § 5a Abs. 2 UWG a.F. beziehungsweise § 5a Abs. 1 UWG n.F. zu beurteilen (vgl. BGH, Urt. v. 11.07.2024 – I ZR 164/23, GRUR 2024, 1449 [juris Rn. 21] = WRP 2024, 1345 – nikotinhaltige Liquids, m.w.N.).

bb) Gemäß § 5a Abs. 2 UWG a.F. handelt unlauter, wer die Entscheidungsfähigkeit von Verbrauchern dadurch beeinflusst, dass er eine Information vorenthält, die im konkreten Fall unter Berücksichtigung aller Umstände einschließlich der Beschränkungen des Kommunikationsmittels wesentlich ist. Nach § 5a Abs. 1 UWG n.F. handelt unlauter, wer einen Verbraucher oder sonstigen Marktteilnehmer irreführt, indem er ihm eine wesentliche Information vorenthält, (Nr. 1) die der Verbraucher oder der sonstige Marktteilnehmer nach den jeweiligen Umständen benötigt, um eine informierte geschäftliche Entscheidung zu treffen, und (Nr. 2) deren Vorenthalten dazu geeignet ist, den Verbraucher oder den sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Gemäß § 5a Abs. 2 Nr. 3 UWG n.F. gilt die nicht rechtzeitige Bereitstellung wesentlicher Informationen als Vorenthalten.

cc) Die Beklagte hat im Sinne dieser Bestimmungen den Nutzern des App-Zentrums wesentliche Informationen vorenthalten.

(1) Indem die Beklagte bei der Präsentation des App-Zentrums die datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG sowie Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO nicht erfüllt hat, hat sie ihren Nutzern

Informationen im Sinne von § 5a Abs. 2 UWG a.F. beziehungsweise § 5a Abs. 1 und 2 Nr. 3 UWG n.F. vorenthalten.

(2) Diese Informationen sind wesentlich im Sinne dieser Bestimmungen.

(a) Ob sich die Wesentlichkeit bereits aus den Vermutungsregelungen gem. § 5a Abs. 4 UWG a.F. und § 5b Abs. 4 UWG n.F. ergibt, ist im Streitfall allerdings zweifelhaft. [...]

(b) Diese Fragen können im Streitfall jedoch dahinstehen. Die in Rede stehenden datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG sowie Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO sind unbeschadet des Eingreifens der Vermutungsregelung gem. § 5a Abs. 4 UWG a.F. und § 5b Abs. 4 UWG n.F. in der im Streitfall zu beurteilenden Konstellation nach den allgemeinen Grundsätzen als wesentlich im Sinne von § 5a Abs. 2 UWG a.F. und § 5a Abs. 1 UWG n.F. anzusehen.

Danach ist eine Information nicht schon allein deshalb wesentlich im Sinne des § 5a UWG, weil sie für die geschäftliche Entscheidung des Verbrauchers von Bedeutung sein kann, sondern nur dann, wenn ihre Angabe unter Berücksichtigung der beiderseitigen Interessen vom Unternehmer erwartet werden kann und ihr für die geschäftliche Entscheidung des Verbrauchers zudem ein erhebliches Gewicht zukommt. Zwar ergeben sich aus § 5a UWG Informationspflichten, die über das hinausreichen, was notwendig ist, um Fehlvorstellungen zu vermeiden, die sich andernfalls einstellen würden. Den Unternehmer trifft aber keine allgemeine Aufklärungspflicht über Tatsachen, die für die geschäftliche Entscheidung des angesprochenen Verkehrs möglicherweise von Bedeutung sind. Ob eine Information für die geschäftliche Entscheidung des Verbrauchers von besonderem Gewicht ist, richtet sich nach dem Erwartungs- und Verständnishorizont des Durchschnittsverbrauchers. Die Beurteilung, ob eine Information im Einzelfall unter Berücksichtigung aller Umstände als wesentlich anzusehen ist, ist Sache der Gerichte der Mitgliedstaaten (BGH, Urt. v. 25.07.2024 – I ZR 143/23, GRUR 2024, 1345 [juris Rn. 13 f.] = WRP 2024, 1056 – durchschnittliche Sternebewertung, m.w.N.).

Nach diesen Maßstäben kommt der Erfüllung der datenschutzrechtlichen Informationspflichten gem. § 13 Abs. 1 S. 1 Hs. 1 TMG sowie Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO erhebliches Gewicht für die geschäftliche Entscheidung des Nutzers der Internetplattform Facebook zu, ob er im App-Zentrum der Plattform den Button "Sofort spielen" betätigen soll.

Eine geschäftliche Entscheidung ist nach § 2 Abs. 1 Nr. 1 UWG jede Entscheidung eines Verbrauchers darüber, ob, wie und unter welchen Bedingungen er ein Geschäft abschließen, eine Zahlung leisten, eine Ware oder Dienstleistung behalten oder abgeben oder ein vertragliches Recht im Zusammenhang mit einer Ware oder Dienstleistung ausüben will, unabhängig davon, ob der Verbraucher sich entschließt, tätig zu werden. Hierzu gehören nicht nur die Entscheidung über den Erwerb oder Nichterwerb eines Produkts, sondern auch damit unmittelbar zusammenhängende Entscheidungen wie das Betreten eines Geschäfts, das Aufsuchen eines Verkaufsportals im Internet oder der Aufruf der Internetseite eines Unternehmens, um sich näher mit dem Unternehmen oder seinem Produktangebot zu befassen (BGH, Urt. v. 29.05.2024 – I ZR 43/23, GRUR 2024, 1041 [juris Rn. 64] = WRP 2024, 933

– Hydra Energy, mwN). Der Begriff "geschäftlich" grenzt rein privates von nicht erwerbswirtschaftlich bestimmtem Handeln ab (vgl. Keller in Harte-Bavendamm/Henning-Bodewig, UWG, 5. Aufl., § 2 Rn. 222 i.V.m. Rn. 22). Es ist nicht erforderlich, dass es sich um ein entgeltliches Geschäft handelt oder dass der Verbraucher durch seine Entscheidung unmittelbar einen finanziellen Nachteil erleidet, so dass auch die Inanspruchnahme unentgeltlicher Dienstleistungen im Internet eine geschäftliche Entscheidung darstellen kann (vgl. Omsels WRP 2016, 553 Rn. 43 bis 45; Sosnitza, in: Ohly/Sosnitza, UWG, 8. Aufl., § 2 Rn. 4).

Nach diesen Maßstäben handelt es sich bei der Entscheidung der Betätigung des Buttons "Sofort spielen" im App-Zentrum der Internetplattform Facebook und die damit verbundene Einwilligung in die Verarbeitung personenbezogener Daten nicht lediglich um eine rein private, sondern um eine geschäftliche Entscheidung. Die in § 13 Abs. 1 S. 1 Hs. 1 TMG geregelte Pflicht zur Information über Zweck und Umfang der Einwilligungserklärung dient nicht allein dem Schutz des Persönlichkeitsrechts, sondern zumindest auch dem Schutz der geschäftlichen Interessen der Verbraucher. Die Bestimmung setzt Art. 10 der Richtlinie 95/46/EG in nationales Recht um (vgl. OLG Hamburg, WRP 2013, 1203 Rn. 40; OLG Köln, WRP 2016, 885 Rn. 24; Schmitz, in: Spindler/Schmitz, TMG, 2. Aufl., § 13 Rn. 127) und ist daher richtlinienkonform auszulegen. Insoweit ist zu berücksichtigen, dass die Richtlinie 95/46/EG insgesamt nicht nur dem Schutz des durch Datenverarbeitung betroffenen Persönlichkeitsrechts (Art. 1 Abs. 1 sowie Erwägungsgrund 10 der Richtlinie) dient. Aus Erwägungsgründen 2 ("Entwicklung des Handels"), 6 (Erleichterung des "grenzüberschreitenden Verkehrs personenbezogener Daten") und vor allem aus den Erwägungsgründen 3, 7, 8 und 9 ergibt sich, dass der Unionsgesetzgeber auch das Spannungsfeld zwischen dem Schutz des Persönlichkeitsrechts und dem freien Datenverkehr innerhalb der Union als Wirtschaftsfaktor im Blick hatte. Zweck der Richtlinie ist auch eine Angleichung der nationalen Datenschutzvorschriften zum Zwecke des innergemeinschaftlichen Handels mit Daten unter Aufrechterhaltung des Schutzes der Grundrechte der Betroffenen. Dementsprechend ist gem. Art. 1 der Richtlinie 95/46/EG nicht nur bestimmt, dass die Mitgliedstaaten den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleisten (Abs. 1), sondern auch, dass die Mitgliedstaaten den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten aus den in Abs. 1 der Bestimmung geschützten Rechten nicht beschränken und untersagen (Abs. 2). Die Wahrung der Grundrechte der Betroffenen wird mithin nicht isoliert betrachtet, sondern mit Blick auf das Funktionieren des Binnenmarktes (vgl. OLG Köln, WRP 2016, 885 Rn. 26). Der Richtlinie 95/46/EG liegt damit ersichtlich die Annahme zugrunde, dass personenbezogene Daten Grundlage oder sogar Gegenstand unionsweit erbrachter Dienstleistungen oder Waren-geschäfte sein können. Ausgehend von der wirtschaftlichen Bedeutung der Verarbeitung von personenbezogenen Daten für internetbasierte Geschäftsmodelle, bei deren Nutzung sich für den Verbraucher nach der Lebenserfahrung nicht selten die Frage stellt, erwünschte Dienstleistungen nicht durch Zahlung eines Entgelts, sondern mit der Preisgabe personen-

bezogener Daten zu vergüten, kommt den Informationspflichten gem. Art. 10 der Richtlinie 95/46/EG und gem. § 13 Abs. 1 TMG zentrale Bedeutung zu, um sicherzustellen, dass der Verbraucher bei seiner mit einer Nachfrageentscheidung verknüpften Einwilligung in die Verarbeitung personenbezogener Daten über Umfang und Tragweite dieser Einwilligungserklärung möglichst umfassend ins Bild gesetzt wird, um eine informierte Entscheidung treffen zu können.

Nichts anderes gilt für die Unterrichtungspflichten gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO. Diese dienen ebenfalls auch dem Verbraucherschutz. Die Datenschutz-Grundverordnung bezweckt zum einen den Schutz der Grundrechte und Grundfreiheiten (Art. 1 Abs. 1 DS-GVO), trifft daneben aber auch Bestimmungen zum freien Verkehr personenbezogener Daten (Art. 1 Abs. 1 DS-GVO). Gemäß Art. 1 Abs. 3 DS-GVO darf zudem der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden. Die technologische Entwicklung und Globalisierung ist in Erwägungsgrund 6 ausdrücklich angesprochen, der unionsweite Verkehr personenbezogener Daten als Wirtschaftsfaktor in den Erwägungsgründen 2, 3, 5, 6, 7 und vor allem 9 und 10. Vor diesem Hintergrund sollen die Unterrichtungspflichten gem. Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO auch sicherstellen, dass der Verbraucher bei einer Einwilligung in die Verarbeitung personenbezogener Daten, die mit einer auf Waren oder Dienstleistungen bezogenen Nachfrageentscheidung verknüpft ist, über Umfang und Tragweite dieser Einwilligungserklärung umfassend informiert wird.

Die in § 13 Abs. 1 S. 1 Hs. 1 TMG sowie Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und e) DS-GVO gesetzlich bestimmten datenschutzrechtlichen Informationspflichten sind danach auch wesentlich im Sinne von § 5a Abs. 2 UWG a.F. und § 5a Abs. 1 UWG n.F. Sie sollen – wie dargelegt – sicherstellen, dass der Verbraucher bei seiner mit einer Nachfrageentscheidung verknüpften Einwilligung in die Verarbeitung personenbezogener Daten über Umfang und Tragweite dieser Einwilligungserklärung möglichst umfassend ins Bild gesetzt wird, um eine informierte Entscheidung treffen zu können (§ 5a Abs. 1 Nr. 1 UWG n.F.). Die Erfüllung dieser Informationspflichten kann unter Berücksichtigung der beiderseitigen Interessen vom Unternehmer erwartet werden, ihnen kommt für die vom Verbraucher im Hinblick auf die Betätigung des Buttons "Sofort spielen" zu treffende informierte Entscheidung ein erhebliches Gewicht zu.

Da die in Rede stehenden datenschutzrechtlichen Unterrichtungspflichten gerade dazu dienen, dem Verbraucher diejenigen Informationen mitzuteilen, die für seine Abwägung der Vor- und Nachteile einer die Datenverarbeitung rechtfertigende Einwilligung relevant sind, ist ein Verstoß schließlich auch geeignet, den Verbraucher zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte (§ 5a Abs. 1 Nr. 2 UWG n.F.).

d) Das Berufungsgericht ist mit Recht vom Bestehen der für den geltend gemachten Unterlassungsanspruch gem. § 8 Abs. 1 S. 1 UWG erforderlichen Wiederholungsgefahr ausgegangen. [...]

2. Das Berufungsgericht hat ferner mit Recht angenommen, dass der auf das Verbot der Verwendung der Angabe

"Diese Anwendung darf Statusmeldungen, Fotos und mehr in deinem Namen posten" gerichtete Unterlassungsantrag zu 2 begründet ist. Diese Angabe stellt eine wegen des Verstoßes gegen die im Streitfall maßgebenden datenschutzrechtlichen Informationspflichten unangemessen benachteiligende und daher unwirksame Allgemeine Geschäftsbedingung dar (vgl. bereits BGH, GRUR 2020, 896 [juris Rn. 23] – App-Zentrum I).

## WICHTIGES AUS DER RECHTSPRECHUNG

### BGH bestätigt Schadenersatz bei Kontrollverlust

(BGH, Urteil vom 11. Februar 2025 – VI ZR 365/22 –)

**Zum Anspruch auf Schadenersatz nach Art. 82 Abs. 1 DS-GVO bei der Verwaltung von Personalakten durch hierzu nicht befugte Dritte.**

#### Aus den Gründen:

2. Der geltend gemachte Feststellungsanspruch ist auch begründet, Art. 82 Abs. 1 DS-GVO. [...]

a) Ein Verstoß gegen die Datenschutz-Grundverordnung liegt nach den getroffenen Feststellungen vor. Das Berufungsgericht hat die von der Beklagten bis zum Erlass der Organisationsverfügung vom 22. August 2019 geübte Praxis, die Verwaltung der Personalakten von Bundesbeamten wie der Klägerin durch Bedienstete des Landes Niedersachsen vornehmen zu lassen, als von § 111a BBG a.F. i.V.m. § 26 BDSG i.V.m. Art. 88 DS-GVO nicht gedeckte Verarbeitung personenbezogener Daten durch Dritte und damit als Verstoß gegen die Datenschutz-Grundverordnung (der Sache nach: gegen Art. 5 Abs. 1 lit. a), Art. 28 DS-GVO) gewertet. Die Beklagte sei selbst von der offensichtlichen Rechtswidrigkeit dieser Praxis ausgegangen und habe weder näher zu den Einzelheiten der geübten Personalaktenverwaltung vorgetragen noch eine vorherige Zustimmung der obersten Dienstbehörde behauptet. Hiergegen wendet die Beklagte auch mit der Revisionserwiderung nichts ein; Rechtsfehler sind insoweit auf der Grundlage der vom Berufungsgericht getroffenen und nicht mit Gegenrügen angegriffenen Feststellungen im Übrigen nicht ersichtlich.

b) Zu Unrecht hat das Berufungsgericht einen durch diesen Verstoß gegen die Datenschutz-Grundverordnung verursachten Schaden der Klägerin verneint. Der Schaden liegt hier bereits in dem durch die Überlassung ihrer Personalakte an Bedienstete des Landes verursachten vorübergehenden Verlust der Kontrolle der Klägerin über ihre in ihrer Personalakte enthaltenen personenbezogenen Daten.

aa) Schon der bloße Kontrollverlust kann, wie der Senat in Umsetzung der jüngeren Rechtsprechung des Gerichtshofs (Urt. v. 04.10.2024 – C-200/23, juris Rn. 145, 156 i.V.m. 137- Agentsia po vpisvanijata; v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 33 – PS GbR; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 42 – juris; vgl. zuvor bereits EuGH, Urt. v. 25.01.2024 – C-687/21, NJW 2024, 2009 Rn. 66 – MediaMarktSaturn; v.

14.12.2023 – C-456/22, NZA 2024, 56 Rn. 17-23 – Gemeinde Ummendorf sowie – C-340/21, NJW 2024, 1091 Rn. 82 – Nacionalna agentsia za prihodite) entschieden hat, einen ersatzfähigen immateriellen Schaden i.S.d. Art. 82 Abs. 1 DS-GVO darstellen (Senat, Urt. v. 18.11.2024 – VI ZR 10/24, WM 2024, 2301 Rn. 30 m.w.N.). Anders als das Berufungsgericht meint, muss der Verpflichtung zum Ausgleich keine über diesen Kontrollverlust hinausgehende "benennbare und insoweit tatsächliche Persönlichkeitsrechtsverletzung gegenüberstehen"; auch muss der Beeinträchtigung des Betroffenen kein besonderes "Gewicht" zukommen, das "über eine individuell empfundene Unannehmlichkeit hinausgeht oder das Selbstbild oder Ansehen ernsthaft beeinträchtigt" (vgl. Senat, a.a.O. Rn. 29 m.w.N.).

bb) Nach diesen Grundsätzen liegt der Schaden hier ohne Weiteres darin, dass die Beklagte auch nach dem 25.05.2018 die personenbezogenen, in deren Personalakte enthaltenen Daten der Klägerin hierzu nicht berechtigten Dritten, nämlich Bediensteten des Landes Niedersachsen, zur Bearbeitung überlassen und diese Praxis erst mit Organisationsverfügung vom 22.08.2019 beendet hat. Der vom Berufungsgericht in diesem Zusammenhang angeführte Umstand, dass auch die mit Personalangelegenheiten betrauten Bediensteten des Landes Niedersachsen zur Verschwiegenheit verpflichtet waren, steht der Annahme eines Schadens insoweit dem Grunde nach nicht entgegen, sondern wird erst bei Bemessung der Höhe des zu leistenden Schadenersatzes (§ 287 ZPO) zu berücksichtigen sein (S. zu den Bemessungskriterien weiterführend Senat, a.a.O. Rn. 92 ff., insb. 99).

### Löschungspflicht von Einträgen über erledigte Zahlungstörungen bei Kreditauskunfteien

(OLG Köln, Urteil vom 11. April 2025 – 15 U 294/24 –)

**Entsprechend der gesetzlichen Wertung des § 882e Abs. 3 Nr. 1 ZPO dürfen Wirtschaftsauskunfteien Informationen über Zahlungstörungen, die auch in das Schuldnerverzeichnis nach § 882b ZPO eingetragen sind oder dort eingetragen werden könnten, nicht länger speichern, wenn die vollständige Befriedigung des Gläubigers gemeldet worden ist.**

#### Aus den Gründen:

Die [...] Schadenersatzansprüche sind entgegen der Auffassung des Landgerichts gem. Art. 82 Abs. 1 DS-GVO in dem aus dem Tenor ersichtlichen Umfang gerechtfertigt.

1. Die Beklagte hat gegen die Datenschutz-Grundverordnung verstoßen, indem sie die in den ursprünglichen Klageanträgen genannten Einträge über Zahlungstörungen des Klägers auch nach dem Ausgleich der Forderungen am 02.12.2020, am 04.11.2021 beziehungsweise im Dezember 2022 für drei beziehungsweise gut zwei Jahre weiterhin gespeichert und für ihre Kunden zum Abruf bereitgehalten hat. Nach der Erfüllung der Forderungen war die fortdauernde Speicherung der – nunmehr zusätzlich mit einem Erledigungsvermerk versehenen – Einträge betreffend die zuvor

aufgetretenen Zahlungstörungen rechtswidrig, weil die in Art. 6 Abs. 1 DS-GVO genannten Bedingungen nicht länger erfüllt waren.

a) Dies gilt insbesondere für die in Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO genannte Bedingung. Die von dieser Vorschrift geforderte Beurteilung der Frage, ob die berechtigten Interessen der Beklagten vernünftigerweise nicht durch eine kürzere Dauer der Datenspeicherung erreicht werden können, erfordert eine Abwägung der einander gegenüberstehenden Rechte und Interessen (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 92). Bei dieser Abwägung ist vorliegend in Ermangelung einer gesetzlichen Regelung der für Wirtschaftsauskunfteien maßgeblichen Speicherfristen (vgl. BT-Drs. 20/10859 S. 34 ff. [Buchstabe f nebst Begründung]) die gesetzliche Wertung des § 882e Abs. 3 Nr. 1 ZPO maßgeblich zu berücksichtigen. Danach wird eine Eintragung im Schuldnerverzeichnis auf Anordnung des zentralen Vollstreckungsgerichts gelöscht, wenn diesem die vollständige Befriedigung des Gläubigers nachgewiesen worden ist. Unter Berücksichtigung dieser Wertung hätte die Beklagte die fraglichen Einträge über Zahlungstörungen des Klägers löschen müssen, nachdem ihr die vollständige Befriedigung der Gläubiger durch entsprechende Meldungen der Gläubiger nachgewiesen worden war.

aa) Der Europäische Gerichtshof hat entschieden, dass Art. 5 Abs. 1 lit. a) und Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO einer Praxis privater Wirtschaftsauskunfteien entgegenstehen, die darin besteht, in ihren eigenen Datenbanken aus einem öffentlichen Register stammende Informationen über die Erteilung einer Restschuldbefreiung zugunsten natürlicher Personen zum Zweck der Lieferung von Auskünften über die Kreditwürdigkeit dieser Personen für einen Zeitraum zu speichern, der über die Speicherdauer der Daten im öffentlichen Register hinausgeht (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166). Die anderslautende Entscheidung des Senats vom 27.01.2022 – 15 U 153/21 – (ZD 2022, 233), die nach Rücknahme der dagegen eingelegten Revision rechtskräftig geworden ist, ist damit ebenso überholt wie die vom Landgericht angeführten Entscheidungen der Oberlandesgerichte Stuttgart (Urt. v. 10.08.2022 – 9 U 24/22, ZD 2022, 691) und Oldenburg (Urt. v. 23.11.2021 – 13 U 63/21, ZD 2022, 103, ausdrücklich aufgegeben im Beschl. v. 13.03.2024 – 13 W 9/24, Anlage zur Berufungsreplik) sowie des Kammergerichts (Urt. v. 15.02.2022 – 27 U 51/21, ZD 2022, 335).

bb) Zwar bezieht sich die Entscheidung des Europäischen Gerichtshofs nur auf in einem Insolvenzregister veröffentlichte Informationen über die Erteilung einer Restschuldbefreiung. Für Eintragungen im Schuldnerverzeichnis gem. § 882b ZPO kann aber nichts Anderes gelten (vgl. BeckOK-Datenschutzrecht/Krämer, § 31 BDSG Rn. 77 [Stand: 01.11.2024]), denn zwischen dem Insolvenzregister und dem Schuldnerverzeichnis bestehen keine Unterschiede, die für die vorzunehmende Interessenabwägung von wesentlicher Bedeutung wären. Es ist der Beklagten deshalb verwehrt, aus dem öffentlichen Schuldnerverzeichnis stammende Informationen zum Zweck der Lieferung von Auskünften über die Kreditwürdigkeit der eingetragenen Schuldner für einen Zeitraum zu speichern, der über die Speicherdauer der Daten im öffentlichen Register hinausgeht (vgl. OLG Oldenburg, Beschl. v. 13.03.2024 – 13 W 9/24, Anlage zur Berufungsreplik;

LG München, Urt. v. 19.07.2024 – 47 O 16029/23, Anlage zur Berufungsbegründung).

Der Europäische Gerichtshof hat bei seiner Entscheidung berücksichtigt, dass die Analyse einer Wirtschaftsauskunftei insoweit, als sie eine objektive und zuverlässige Bewertung der Kreditwürdigkeit der potenziellen Kunden der Vertragspartner der Wirtschaftsauskunftei ermöglicht, Informationsunterschiede ausgleichen und damit Betrugsrisiken und andere Unsicherheiten verringern kann. Andererseits stelle die Verarbeitung von Daten über die Erteilung der Restschuldbefreiung einen schweren Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte der betroffenen Person dar, weil solche Daten als negativer Faktor bei der Beurteilung der Kreditwürdigkeit der betroffenen Person dienen; die Weitergabe solcher Daten sei geeignet, die Ausübung ihrer Freiheit erheblich zu erschweren, insbesondere wenn es darum gehe, Grundbedürfnisse zu decken. Zudem seien die Folgen für die betroffene Person umso größer und die Anforderungen an die Rechtmäßigkeit der Speicherung dieser Informationen umso höher, je länger die fraglichen Daten gespeichert würden (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 93 bis 95). Diese Erwägungen lassen sich ohne Weiteres auf Eintragungen im Schuldnerverzeichnis gem. § 882b ZPO übertragen.

Der Europäische Gerichtshof hat bei seiner Entscheidung ferner das Ziel eines öffentlichen Insolvenzregisters berücksichtigt, eine bessere Information der betroffenen Gläubiger und Gerichte zu gewährleisten (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 96). Das Schuldnerverzeichnis gem. § 882b ZPO dient ersichtlich demselben Zweck. Soweit der Europäische Gerichtshof ferner darauf abgestellt hat, dass das Ziel der Erteilung einer Restschuldbefreiung, dem Begünstigten eine erneute Beteiligung am Wirtschaftsleben zu ermöglichen, gefährdet wäre, wenn Wirtschaftsauskunfteien Daten über eine Restschuldbefreiung auch nach einer Löschung aus dem öffentlichen Insolvenzregister speichern und verwenden könnten (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 98), steht auch diese Erwägung einer Übertragung der Rechtsprechung auf Eintragungen im Schuldnerverzeichnis nicht entgegen. Es ist kein Grund ersichtlich, warum das Interesse eines im Schuldnerverzeichnis eingetragenen Schuldners, sich nach Befriedigung seiner Gläubiger und nach einer Löschung des Eintrags im Schuldnerverzeichnis am Wirtschaftsleben zu beteiligen, geringeres Gewicht haben sollte, als das Interesse eines Insolvenzschuldners nach Erteilung der Restschuldbefreiung und nach Löschung des entsprechenden Eintrags im Insolvenzregister. Ebenso wie im Falle des Insolvenzregisters müssen deshalb auch beim Schuldnerverzeichnis die vom deutschen Gesetzgeber (vgl. EuGH, Urt. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 97) geregelten zeitlichen Beschränkungen für die Datenspeicherung im öffentlichen Register auch für die Speicherung entsprechender Einträge durch die Beklagte maßgeblich sein.

cc) Zwar wird in der obergerichtlichen Rechtsprechung angenommen, bei einer Speicherung und Verarbeitung von Daten durch die Beklagte sei eine dem Schuldnerverzeichnis vergleichbare Situation nicht gegeben (vgl. OLG Frankfurt, Urt. v. 18.01.2023 – 7 U 100/22, ZD 2023, 217 Rn. 37 f.; OLG Bremen, Urt. v. 03.07.2023 – 1 U 8/22, ZD 2023, 748 Rn. 15; OLG München, Beschl. v. 30.01.2025 – 37 U 3936/24, Anlage BB 6; v.

20.02.2025 – 37 U 4148/24, Anlage BB 7; OLG Koblenz, Beschl. v. 05.03.2025 – 5 U 1018/24, Anlage BB 9; vom 10. März 2025 – 5 U 1026/24, Anlage BB 10; OLG Stuttgart, Beschl. v. 04.04.2025 – 9 U 141/24, Anlage zum Schriftsatz v. 10.03.2025). Diese Erwägungen, denen sich das Landgericht angeschlossen hat, überzeugen aber nicht.

Warum der Kreis an potenziell gegenüber der Beklagten Auskunftsberechtigten deutlich geringer sein soll als der Personenkreis, der zu einer Einsicht in das Schuldnerverzeichnis befugt ist, und warum eine Auskunftserteilung durch die Beklagte von höheren Voraussetzungen abhängig sein soll als eine – ebenfalls kostenpflichtige (Nummer 2.3 der Anlage zu § 124 JustG NRW) – Einsicht in das Schuldnerverzeichnis, erschließt sich mit Blick auf § 882f Abs. 1 ZPO nicht (vgl. OLG Stuttgart, Urte. v. 10.08.2022 – 9 U 24/22, ZD 2022, 691 Rn. 49; OLG Oldenburg, Beschl. v. 13.03.2024 – 13 W 9/24, Anlage zur Berufungsreplik).

Vor allem aber kann es darauf nach der Entscheidung des Europäischen Gerichtshofs nicht mehr ankommen. Denn das Insolvenzregister, auf das sich die Entscheidung des Gerichtshofs bezieht, kann – anders als das Schuldnerverzeichnis – sogar von beliebigen Dritten ohne große Schwierigkeiten und ohne Darlegung eines berechtigten Interesses eingesehen werden. Unter anderem deshalb hatte der Senat die Regelung des § 3 InsoBekV in Bezug auf die Speicherung von Daten durch die Beklagte für nicht maßgeblich erachtet (vgl. Senatsurt. v. 27.01.2022 – 15 U 153/21, ZD 2022, 233 Rn. 38), woran nach der Entscheidung des Gerichtshofs nicht festgehalten werden kann.

dd) Zur Vermeidung von Wertungswidersprüchen darf die Beklagte Informationen über Zahlungsstörungen, die in das Schuldnerverzeichnis nach § 882b ZPO eingetragen sind oder dort eingetragen werden könnten, auch dann nicht länger speichern als für das Schuldnerverzeichnis vorgesehen, wenn die Beklagte die Informationen nicht durch Einsicht in das Schuldnerverzeichnis, sondern aus anderen Quellen erhalten hat (vgl. OLG Oldenburg, Beschl. v. 13.03.2024 – 13 W 9/24, Anlage zur Berufungsreplik). Solche aus anderen Quellen stammenden Informationen über Zahlungsstörungen, die auch in das Schuldnerverzeichnis eingetragen werden könnten, muss die Beklagte deshalb nach der gesetzlichen Wertung des § 883e Abs. 3 Nr. 1 ZPO löschen, wenn ihr die vollständige Befriedigung des Gläubigers nachgewiesen wird.

Aus den Gesetzesmaterialien zu dieser Vorschrift ergibt sich, dass ihr die Erwägung zugrunde liegt, dass durch eine vollständige Befriedigung des Gläubigers das Informationsinteresse des Geschäftsverkehrs beseitigt wird (BT-Drucks. 16/10069 S. 40). Diese Wertung des deutschen Gesetzgebers muss ausgehend von der Entscheidung des Europäischen Gerichtshofs auch dann maßgeblich sein, wenn Wirtschaftsauskunfteien wie die Beklagte Informationen über Zahlungsstörungen speichern, die auch in das Schuldnerverzeichnis eingetragen werden könnten (vgl. LG Duisburg, Urte. i. Verfahren 4 O 423/23, Anlage zur Berufungsbeurteilung; LG Berlin II, Urte. v. 24.03.2025 – 61 O 385/24, Anlage zum Schriftsatz des Klägers v. 27.03.2025; für § 882e Abs. 1 ZPO ebenso OLG Stuttgart, Urte. v. 10.08.2022 – 9 U 24/22, ZD 2022, 691 Rn. 49). Denn Wirtschaftsauskunfteien verfolgen mit ihren Datenbanken keine anderen Zwecke als das Schuldnerverzeichnis (vgl. OLG Oldenburg, Beschl. v. 13.03.2024 –

13 W 9/24, Anlage zur Berufungsreplik). Auch dieses soll nach dem Willen des Gesetzgebers und entgegen den Ausführungen der Beklagten nicht nur die Vollstreckung von Forderungen ermöglichen, sondern es hat weitergehend die Funktion eines Auskunftsregisters über die Kreditwürdigkeit einer Person (vgl. BT-Drs. 16/10069 S. 37). Keinem anderen Zweck dient die Datenbank der Beklagten. Auf die von ihr vorgenommenen statistischen Untersuchungen kann es deshalb nicht ankommen; die Ergebnisse dieser Untersuchungen ändern nichts an der Maßgeblichkeit der gesetzlichen Wertung.

Dass die Eintragung in das Schuldnerverzeichnis nach § 882c ZPO eine Anordnung des Gerichtsvollziehers voraussetzt, während die Datenverarbeitung der Beklagten in der Regel auf einer Meldung des Gläubigers beruht, ist ebenfalls unerheblich. Es ist kein Grund ersichtlich, warum an der Speicherung einer von einem privaten Gläubiger gemeldeten Zahlungsstörung ein größeres Interesse bestehen sollte als an der Speicherung einer vom Gerichtsvollzieher im Rahmen eines Zwangsvollstreckungsverfahrens angeordneten Eintragung. Ferner kann es auch nicht darauf ankommen, dass eine Löschung nach § 882e Abs. 3 Nr. 1 ZPO verfahrensmäßig von einer Anordnung des zentralen Vollstreckungsgerichts abhängt.

ee) Allerdings ist bezüglich der drei Forderungen, die gegen den Kläger gerichtet waren, eine Eintragung in das Schuldnerverzeichnis nicht erfolgt und hätte offenbar auch nicht erfolgen dürfen, weil die Voraussetzungen des § 882c Abs. 1 S. 1 ZPO nicht vorlagen. Auch dies ändert aber nichts daran, dass die Beklagte die Forderungen löschen musste, nachdem ihr durch entsprechende Meldungen der Gläubiger deren vollständige Befriedigung nachgewiesen worden war. Denn wenn in den in § 882c Abs. 1 S. 1 ZPO genannten Fällen, in denen (sogar) Vollstreckungsmaßnahmen (Antrag auf Erteilung einer Vermögensauskunft) zunächst nicht zu einer Befriedigung geführt haben, entsprechende Einträge nach der späteren Befriedigung des Gläubigers gelöscht werden müssen, muss dies auch und erst recht gelten, wenn der Schuldner – wie im Streitfall offenbar der Kläger – den Gläubiger einer titulierten beziehungsweise mehrfach angemahnten unstreitigen Forderung ohne den Druck von Vollstreckungsmaßnahmen befriedigt (zutreffend LG München, Urte. v. 19.07.2024 – 47 O 16029/23, Anlage zur Berufungsbeurteilung).

b) Dass nach Ziffer IV. 1 lit. b) der vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit genehmigten Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien v. 25.05.2024 auch personenbezogene Daten über ausgeglichene Forderungen für bestimmte Zeiträume gespeichert werden dürfen, ist unerheblich. Denn Verhaltensregeln i.S.d. Art. 40 DS-GVO, die zu einer anderen Beurteilung führen würden als derjenigen, die sich nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO ergibt, können bei der Abwägung nach dieser Bestimmung nicht berücksichtigt werden (vgl. EuGH, Urte. v. 07.12.2023 – C-26/22, ZD 2024, 166 Rn. 105). Davon geht die Beklagte auch selbst aus.

2. Entgegen der Auffassung des Landgerichts ist dem Kläger wegen des Verstoßes gegen die Datenschutz-Grundverordnung ein immaterieller Schaden entstanden. Dabei kann es dahinstehen, ob ein Kontrollverlust vorliegt (vgl. OLG Schleswig, Urte. v. 22.11.2024 – 17 U 2/24, juris Rn. 133). Denn jedenfalls hat der Kläger eine Rufschädigung erlitten (vgl. ErwG

85 DS-GVO). Ob eine Rufschädigung allein daraus folgt, dass die Beklagte die Daten über die Zahlungsstörungen auch nach der Erfüllung der einzelnen Forderungen weiterhin gespeichert hat, kann offenbleiben. Denn jedenfalls hat die Beklagte ausweislich der Einblendung auf Seite 2 der erstinstanzlichen Treplik im Jahr 2023 – also nach der Erfüllung der letzten Forderung – mehreren Banken, einem Energieversorgungsunternehmen und einem Telekommunikationsunternehmen Scorewerte und Erfüllungswahrscheinlichkeiten mitgeteilt, die sie unter Berücksichtigung der Zahlungsstörungen ermittelt hatte. Die fortdauernde Speicherung der Zahlungsstörungen ist somit dafür ursächlich geworden, dass die Beklagte ihren genannten Vertragspartnern gegenüber die Kreditwürdigkeit des Klägers in Zweifel gezogen hat, was sich abträglich auf dessen sozialen Geltungsanspruch ausgewirkt hat (vgl. BGH, Urt. v. 28.01.2025 – VI ZR 183/22, NJW 2025, 1059 Rn. 12; Senatsurteile v. 25.04.2024 – 15 U 204/22; v. 13.02.2025 – 15 U 35/24). Dass die genannten Übermittlungen keine weiteren nachteiligen Folgen für den Kläger hatten, steht der Annahme eines immateriellen Schadens in Gestalt einer Rufschädigung nicht entgegen (vgl. OLG Hamburg, Urt. v. 30.08.2023 – 13 U 71/21, juris Rn. 7).

3. Die Haftung der Beklagten ist nicht nach Art. 82 Abs. 3 DS-GVO ausgeschlossen. Die Beklagte hat nicht nachgewiesen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Der Umstand, dass sie sich genehmigten Verhaltensregeln unterworfen hat, schließt ihre Haftung nicht aus (vgl. Bergt, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl., Art. 82 DS-GVO Rn. 50; Bergt/Pesch, ebd., Art. 40 DS-GVO Rn. 43; vgl. auch Art. 42 Abs. 4 DS-GVO bei einer Zertifizierung). Denn da die Genehmigung der Verhaltensregeln keine Erlaubniswirkung hat, durfte die Beklagte nicht auf die Richtigkeit der der Genehmigung zugrunde liegenden Rechtsauffassung vertrauen, sondern musste damit rechnen, dass die in den Verhaltensregeln vorgesehenen Speicherfristen im Fall einer gerichtlichen Überprüfung als zu lang angesehen werden. Insbesondere musste sie damit rechnen, dass die für öffentliche Register geltenden Speicherfristen als auch für sie maßgeblich angesehen werden, was in der obergerichtlichen Rechtsprechung bereits lange vor Klageerhebung im November 2023 vertreten worden war (vgl. OLG Schleswig, Urt. v. 02.07.2021 – 17 U 15/21, ZD 2021, 584). Die Beklagte kann sich daher nicht mit Erfolg auf einen unvermeidbaren Rechtsirrtum berufen, unabhängig von der Frage, ob ein Rechtsirrtum den Schädiger im Rahmen von Art. 82 Abs. 3 DS-GVO überhaupt entlasten kann.

4. Der Höhe nach bemisst der Senat den immateriellen Schaden mit einem Betrag von 500 € (vgl. BGH, Urt. v. 28.01.2025 – VI ZR 183/22, NJW 2025, 1059 Rn. 13).

Nach der neueren Rechtsprechung des Europäischen Gerichtshofs erfüllt der in Art. 82 Abs. 1 DS-GVO vorgesehene Schadenersatzanspruch ausschließlich eine Ausgleichsfunktion, jedoch keine Abschreckungs- oder Straffunktion. Daraus folgt, dass sich die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung nicht auf die Höhe des Schadenersatzes auswirken kann (vgl. EuGH, Urt. v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 59 f.; v. 20.06.2024 – C-590/22, ZD 2024, 519 Rn. 41; BGH, Urt. v. 18.11.2024 – VI ZR 10/24, NJW 2025, 298 Rn. 25; v. 28.01.2025 – VI ZR 183/22, NJW 2025, 1059 Rn. 10 f.).

Ausgehend von diesen Grundsätzen erscheint im Streitfall ein Betrag von 500 € erforderlich, aber auch ausreichend, um den vom Kläger erlittenen immateriellen Schaden auszugleichen. Dabei ist zu berücksichtigen, dass die rechtswidrige Datenspeicherung über einen Zeitraum von mehreren Jahren andauert und – wie unter Ziffer 2 ausgeführt – zu mehreren Übermittlungen von negativen Scorewerten an Vertragspartner der Beklagten geführt hat. Dass diese Übermittlungen weitere negative Folgen für den Kläger hatten, lässt sich allerdings nicht feststellen. Soweit der Kläger behauptet hat, ihm seien wegen seiner Eintragung bei der Beklagten der Abschluss eines Mobilfunk- und eines Energielieferungsvertrags verwehrt worden, hat das Landgericht diesen Vortrag als nicht erwiesen angesehen. Dies greift die Berufung nicht an. Soweit der Kläger sich auf Probleme im Zusammenhang mit einem Umzug und mit einer diesbezüglichen Kreditaufnahme berufen hat, lässt sich nicht feststellen, dass diese Probleme kausal auf einen Verstoß der Beklagten gegen die Datenschutz-Grundverordnung zurückzuführen sind. Denn die Probleme sollen nach dem Vortrag des Klägers bereits im Jahr 2021 und/oder im Oktober 2022 aufgetreten sein. Zu diesem Zeitpunkt war die dritte Forderung noch nicht erledigt und die Beklagte war noch berechtigt, diese Zahlungsstörung zu speichern und bei der Berechnung des Scorewertes zu berücksichtigen. Entsprechendes gilt, soweit der Kläger behauptet hat, er habe eine Stelle nicht erhalten. Der Kläger hat bei seiner persönlichen Anhörung erklärt, dies sei im Frühjahr 2021 oder 2022 gewesen (Seite 1 der Sitzungsniederschrift des Landgerichts vom 31.05.2024). Des Weiteren wird die Schwere der Rufschädigung dadurch relativiert, dass die von der Beklagten gespeicherten Zahlungsstörungen tatsächlich aufgetreten waren und die Beklagte der Ermittlung des Scorewertes keinen falschen Sachverhalt zugrunde gelegt hat.

5. Der Zinsanspruch folgt aus den §§ 291, 288 Abs. 1 S. 2 BGB.

6. Als weiterer materieller Schaden sind die dem Kläger durch das Anwaltsschreiben vom 03.08.2023 entstandenen Kosten ersatzfähig. Ausgehend davon, dass der immaterielle Schaden nur mit 500 € zu bemessen ist, sind die ersatzfähigen Kosten allerdings nicht nach einem Gegenstandswert von 5.500 €, sondern nur nach einem Wert von bis zu 5.000 € zu bemessen. Es errechnet sich ein Betrag von 540,50 € (1,3 Geschäftsgebühren zuzüglich Auslagenpauschale und Umsatzsteuer).

## Maßgeblichkeit des Scorings für die Entscheidung im Rahmen von Art. 22 Abs. 1 DS-GVO

(LG Bamberg, Urteil vom 26. März 2025 – 41 O 749/24 KOIN –)

**1. Berechnung und Weitergabe eines Bonitätsscores sind gem. Art. 22 Abs. 1 DS-GVO verboten, wenn sie das Handeln der kreditgebenden Banken maßgeblich leiten. Davon ist sogar dann auszugehen, wenn die Banken zur Entscheidung über die Kreditvergabe weitere Faktoren wie Einkommen und Vermögen berücksichtigen.**

## 2. Die bloße Mitteilung von entgegen Art. 22 Abs. 1 DS-GVO automatisiert berechneten Bonitätsscores an potenziell kreditgebende Banken begründet einen Kontrollverlust, der einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO darstellt.

(Nicht amtliche Leitsätze)

### Aus den Gründen:

Die Klage ist im tenorierten Umfang begründet.

#### 1. Anträge Ziff. II, III

Der Kläger hat gegen die Beklagte einen Anspruch auf Unterlassen einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Erstellung des Bonitätsscores sowie auf Unterlassen von deren Mitteilung. Dieser ergibt sich aus §§ 1004, 823 Abs. 2 BGB i.V.m. Art. 22 Abs. 1 DS-GVO. [...]

#### c) Verstoß gegen Art. 22 Abs. 1 DS-GVO

Durch die automatisierte Erstellung der den Kläger betreffenden Bonitätsscores und deren Weitergabe hat die Beklagte gegen Art. 22 Abs. 1 DS-GVO verstoßen. Art. 22 Abs. 2 DS-GVO verbietet eine Entscheidung, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht und gegenüber der betroffenen Person rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (vgl. EuGH, Ur. v. 07.12.2023, C-634/21, NJW 2024, 413, Rn. 43). Diese Voraussetzungen liegen hier vor.

aa) Der in Art. 22 Abs. 1 DS-GVO enthaltene Begriff der Entscheidung ist in der DS-GVO nicht definiert. Wie der EuGH (EuGH, Ur. v. 07.12.2023, C-634/21, NJW 2024, 413, Rn. 44 ff.) festgestellt hat, ist, auch unter Zugrundelegung des 71. ErwG der DS-GVO, der Begriff so weit auszulegen, dass das Ergebnis der Berechnung der Fähigkeit einer Person zur Erfüllung künftiger Zahlungsverpflichtungen in Form eines Wahrscheinlichkeitswerts erfasst wird.

bb) Unstreitig erfolgt die Berechnung der Bonitätsscores durch die Beklagte vollständig automatisiert.

cc) Die Berechnung der Bonitätsscores durch die Beklagte beeinträchtigt den Kläger auch in ähnlicher Weise wie eine sich entfaltende rechtliche Wirkung. Nach Überzeugung des Gerichts wird das Handeln Dritter – insbesondere kreditgebender Banken – maßgeblich von dem von der Beklagten mitgeteilten Wahrscheinlichkeitswert geleitet. Hierfür spricht schon, dass die abfragenden Vertragspartner der Beklagten für die Abfragen unstreitig ein Entgelt zu leisten haben. Dass für eine Auskunft bezahlt wird, die für die Entscheidung irrelevant ist, ist nicht anzunehmen. Der EuGH verlangt in seiner Entscheidung EuGH vom 07.12.2023 (C-634/21, NJW 2024, 413) auch nicht, dass der von der Beklagten berechnete Bonitätsscore der einzige für die Entscheidung der Banken ausschlaggebende Grund ist. Die Ausführungen der Beklagten, es sei dem Geschäftsverkehr immanent, dass die Beklagte ihre Leistung Vertragspartnern nicht kostenfrei zur Verfügung stellt, erscheint dabei durchaus nachvollziehbar. Es ist dem Geschäftsverkehr aber ebenso immanent, dass keine kostenpflichtigen Auskünfte eingeholt werden, wenn deren Inhalte für den Anfragenden keine Rolle spielen. Dass Einkommen und Vermögen, wie von der Beklagten vorgebracht, ebenfalls von Relevanz sein dürften, ist naheliegend, ändert aber nichts daran, dass auch der von der Beklagten

mitgeteilte Bonitätsscore ein offensichtlich maßgebliches Entscheidungskriterium darstellt. Dies bestätigen auch die vom Kläger vorgelegten Schreiben diverser Banken, insb. Anl. K10, K12b, K13. Auch wenn diese nur teilweise den hiesigen Kläger betreffen, ergibt sich aus ihnen die grundsätzliche Bedeutung eines entsprechenden Scores für die Teilnahme am Wirtschaftsleben, insb. im Hinblick auf kreditrelevante Geschäfte.

dd) Ein Fall des Art. 22 Abs. 2 DS-GVO, wonach die automatisierte Entscheidung entgegen Art. 22 Abs. 1 DS-GVO zulässig wäre, liegt nicht vor.

(1) Anders als die Beklagte meint, ist die automatisierte Entscheidung nicht nach Art. 22 Abs. 2 lit. a) DS-GVO zulässig. Die Beklagte ist schon nicht Vertragspartnerin der betroffenen Person – hier des Klägers –, sondern eines Dritten. Soweit die Beklagte meint, es sei eine weite Auslegung erforderlich, die das Dreiecksverhältnis zwischen Kunden, potenziellem Vertragspartner und Auskunftgeber berücksichtigt, wird dem nicht beigetreten. Diese Argumentation übersieht, dass Art. 22 DS-GVO eine Schutzvorschrift zugunsten des Verbrauchers ist. Insoweit verbietet sich eine erweiternde Auslegung der Ausnahmetatbestände (LG Leipzig, 07 O 2658/23). Sie entspricht auch nicht dem Sinn und Zweck der Vorschrift, da der von ihr vorgesehene Verbraucherschutz durch die Konstruktion eines entsprechenden Dreiecksverhältnisses ausgehebelt werden würde.

(2) Die automatisierte Berechnung der Bonitätsscores durch die Beklagte ist nicht aufgrund von nationalen Rechtsvorschriften, denen der Verantwortliche unterliegt und die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen enthalten, zulässig, Art. 22 Abs. 2 lit. b) DS-GVO. In der einzig in Betracht kommenden Vorschrift des § 31 BDSG ist ausschließlich die „Verwendung“ eines Wahrscheinlichkeitswerts genannt, nicht aber die Berechnung eines solchen. Da § 31 BDSG als Ausnahmeregelung zur Schutzvorschrift des Art. 22 Abs. 1 DS-GVO formuliert ist, verbietet sich eine gegen den Wortlaut gerichtete erweiterte Auslegung des Begriffs „Verwendung“ (LG Leipzig, 07 O 2658/23).

d) Die für einen Anspruch aus § 1004 BGB erforderliche Wiederholungsgefahr ist vor dem Hintergrund, dass die Beklagte schon nach eigenen Angaben der Auffassung ist, das Scoring nur automatisiert vornehmen zu können (vgl. Klagerwiderrung, S. 4, Bl. 61 d.A.), gegeben. [...]

#### 2. Antrag Ziff. V (Schadenersatz)

a) Es liegt ein Verstoß gegen Art. 22 DS-GVO vor, s.o.

b) Auch der von Art. 82 Abs. 1 DS-GVO vorausgesetzte Schaden bei dem Kläger liegt vor. Der Begriff des „immateriellen Schadens“ ist in Ermangelung eines Verweises in Art. 82 I DS-GVO auf das innerstaatliche Recht der Mitgliedsstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren. Dabei soll nach ErwG 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadenersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforder-

derlich (BGH, Urt. v. 18.11.2024, VI ZR 10/14, GRUR 2024, 1910 Rn. 28). Dabei kann bereits ein kurzzeitiger Kontrollverlust einen immateriellen Schaden darstellen, ohne dass der Nachweis zusätzlicher spürbarer negativer Folgen erforderlich ist (vgl. ebd.). Dies zugrunde gelegt, ist hier vom Vorliegen eines Schadens auszugehen. Wie sich aus der von der Beklagten an den Kläger erteilten Auskunft (Anl. K1/B1) ergibt, teilte die Beklagte auf verschiedene Anfragen hin Scores hinsichtlich des Klägers an diverse Banken mit, die eine vergleichsweise geringe Erfüllungswahrscheinlichkeit auswiesen. Die bloße Mitteilung von entgegen Art. 22 Abs. 1 DS-GVO automatisiert berechneten Bonitätsscores an potenzielle Vertragspartner des Klägers stellt einen beachtlich größeren Eingriff in die Rechtsposition des Klägers dar als dies in der vom BGH (Urt. v. 18.11.2024, VI ZR 10/14, GRUR 2024, 1910) entschiedenen Konstellation der Fall war. Denn dort handelte es sich um den Kontrollverlust an selbst in einem sozialen Netzwerk angelegten Daten, während die vorliegend weitergegebenen Daten nicht vom Kläger selbst mitgeteilt, sondern durch die Beklagte auf rechtswidrige Weise berechnet wurden und zugleich auch unmittelbar die Teilnahme des Klägers am Wirtschaftsleben betreffen.

c) Der Verstoß gegen Art. 22 DS-GVO war für den eingetretenen Schaden auch kausal, da gerade die auf automatisierter Berechnung beruhenden Scores den anfragenden Banken mitgeteilt wurden, wodurch der immaterielle Schaden eintrat.

d) Die DS-GVO enthält keine Bestimmung über die Bemessung des aus Art. 82 Abs. 1 DS-GVO geschuldeten Schadenersatzes. Insbesondere können aufgrund des unterschiedlichen Zwecks der Vorschriften nicht die in Art. 83 DS-GVO genannten Kriterien herangezogen werden. Die Bemessung richtet sich vielmehr entsprechend dem Grundsatz der Verfahrensautonomie nach den innerstaatlichen Vorschriften über den Umfang der finanziellen Entschädigung. In Deutschland ist somit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden (BGH Urt. v. 18.11.2024 – VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 93 m.w.N.). Dabei dürfen die Modalitäten der Schadensermittlung bei einem – wie im Streitfall – unter das Unionsrecht fallenden Sachverhalt nicht ungünstiger sein als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz). Auch dürfen sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz) (BGH Urt. v. 18.11.2024 – VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 95 m.w.N.). In Anbetracht der Ausgleichsfunktion des in Art. 82 DS-GVO vorgesehenen Schadenersatzanspruchs, wie sie in ErwG 146 S. 6 DS-GVO zum Ausdruck kommt, ist eine auf Art. 82 DS-GVO gestützte Entschädigung in Geld als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DS-GVO dagegen nicht erfüllen. Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen hat (BGH Urt. v. 18.11.2024 – VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 96

m.w.N.). Vor dem Hintergrund dieser Erwägungen erscheint im vorliegenden Fall ein Schadenersatz in Höhe von 1.000 € angemessen. [...]

## Datenschutzwidrige Mitteilung zum Krankenstand eines Arbeitnehmers

(ArbG Duisburg, Urteil vom 26. September 2024 – 3 Ca 77/24 –)

**Auch die bloße Mitteilung darüber, dass sich ein Arbeitnehmer „im Krankenstand“ befindet, stellt die Verarbeitung eines Gesundheitsdatums im Sinne des Art. 9 DS-GVO dar.**

*(Nicht amtlicher Leitsatz)*

Der Kläger hat gegen die Beklagte einen Anspruch auf Entschädigung nach Art. 82 Abs. 1 DS-GVO in ausgerichteter Höhe.

a) Der Kläger ist für den geltend gemachten Anspruch aktivlegitimiert. Denn anspruchsberechtigt ist nach Art. 82 Abs. 1 DS-GVO jede Person, der wegen eines Verstoßes gegen die DS-GVO ein Schaden entstanden ist.

b) Die Beklagte ist als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO passivlegitimiert im Sinne von Art. 82 Abs. 1 DS-GVO.

c) Es liegt auch ein Verstoß gegen die DS-GVO im Sinne von Art. 82 Abs. 1 DS-GVO vor. Als Verstoß kommen materielle und formelle Verstöße in Betracht. Nach Wortlaut und Zielrichtung der Norm muss kein Verstoß gegen in der DS-GVO geregelte Datenschutzbestimmungen vorliegen; es genügt vielmehr ein Verstoß gegen die Verordnung selbst (Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Edition, Stand 01.08.2022, Art. 82 DS-GVO Rn. 14). Im Hinblick auf Erwägungsgrund 146 S. 1 zur DS-GVO muss allerdings bei einer Verarbeitung gegen die DS-GVO verstoßen worden sein (Nemitz, in: Ehmman/Selmayr, DS-GVO, 2. Auflage 2018, Art. 82 Rn. 8). Die Beweislast für einen solchen Verstoß obliegt grundsätzlich dem Anspruchsteller, wobei die allgemeine Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO zu Erleichterungen führen kann (Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Edition, Stand 01.08.2022, Art. 82 DS-GVO Rn. 16).

aa) Es liegt ein Verstoß gegen Art. 5 Abs. 1 lit. 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 über seinen aktuellen Gesundheitszustand, die in ihrem Versand als E-Mail an deren Empfänger zu erblicken ist (OLG Hamm Urt. v. 20.01.2023 – 11 U 88/22, GRUR-RS 2023, 1263 Rn. 68-73), 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 lit. a) DS-GVO vor, noch war die Verarbeitung in Gestalt der Übermittlung als E-Mail für einen der in Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) DS-GVO genannten Zwecke erforderlich.

Eine Einwilligung des Klägers war insbesondere nicht in seiner eigenen E-Mail vom 11.05.2023 an einen ausgewählten Personenkreis zu sehen. Selbst wenn der vom Kläger gewählte Adressatenkreis in Teilen dem von der Beklagten gewählten Adressatenkreis in ihrem Schreiben vom 11.06.2023 entsprach, lag hierin unter keinen Umständen eine Einwilligung des Klägers gegenüber der Beklagten, Daten über seinen Gesundheitszustand zu versenden, und zwar weder ausdrücklich noch konkludent.

bb) Zudem liegt ein Verstoß gegen Art. 9 Abs. 1 DS-GVO vor. Nach dieser Vorschrift ist die Verarbeitung von Gesundheitsdaten untersagt, sofern nicht eine Ausnahme nach Art. 9 Abs. 2 DS-GVO vorliegt. Gesundheitsdaten sind gem. Art. 4 Nr. 15 DS-GVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Gemäß Erwägungsgrund 35 S. 1 zur DS-GVO sollen hierzu alle Daten gehören, die sich auf den Gesundheitszustand der betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand hervorgehen. Anknüpfungspunkt ist damit der Gesundheitszustand, nicht aber die Krankheit einer Person, weshalb auch die Feststellung, dass eine Person genesen oder überhaupt völlig gesund ist, vom Begriff der Gesundheitsdaten erfasst wird (Weichert, in: Kühling/Buchner, DS-GVO, BDSG, 3. Auflage 2020, Art. 4 Nr. 15 DS-GVO Rn. 1).

Gesundheitsdaten sind hier die Informationen über den Zeitpunkt der andauernden Krankheit des Klägers sowie deren Ursachenzusammenhang in Bezug auf den geschilderten Konflikt mit dem geschäftsführenden Präsidium sowie die mittelbare Schlussfolgerung der Beklagten, dass eine tatsächliche Arbeitsunfähigkeit nicht vorliege.

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 lit. a) DS-GVO vor (siehe oben unter 1., c), aa)), noch war die Verarbeitung in Gestalt der Übermittlung als Anhang zu der E-Mail für einen der in Art. 9 Abs. 2 lit. b) bis j) DS-GVO genannten Zwecke erforderlich.

2. Der Kläger hat auch einen immateriellen Schaden i.S.v. Art. 82 Abs. 1 DS-GVO erlitten.

Der Begriff des immateriellen Schadens im Sinne von Art. 82 Abs. 1 DS-GVO ist – europarechtlich autonom und unter Berücksichtigung der in den Erwägungsgründen zur DS-GVO niedergelegten Zielsetzungen – weit auszulegen (OLG Koblenz, Ur. v. 18.05.2022 – 5 U 2141/21). Der immaterielle Schaden braucht keine Erheblichkeitsgrenze zu erreichen (EuGH (Dritte Kammer) Ur. v. 14.12.2023 – C-456/22 (VX, AT/Gemeinde Ummendorf), es muss jedoch ein über die Verletzung eines Rechts aus der DS-GVO vorliegender Schaden immaterieller Art dargelegt werden, der auf der Rechtsverletzung beruht (EuGH (Dritte Kammer) Ur. v. 14.12.2023 – C-456/22 (VX, AT/Gemeinde Ummendorf; OLG Koblenz, Ur. v. 18.05.2022 – 5 U 2141/21, juris Rn. 74; OLG Frankfurt, Ur. v. 02.03.2022 – 13 U 206/20, juris Rn. 70 f.; OLG Bremen, Beschl. v. 16.07.2021 – 1 W 18/21, juris Rn. 2; Buchner/Wessels, in: ZD 2022, 251 (254 f.)). Auch ein immaterieller Schaden muss daher konkret dargelegt werden (OLG Brandenburg, Beschl. v. 11.08.2021 – 1 U 69/20, juris Rn. 3; OLG Bremen, Beschl. v. 16.07.2021 –

1 W 18/21, juris Rn. 2; LG Hamburg, Ur. v. 04.09.2020 – 324 S 9/19, juris Rn. 34; Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Edition, Stand 01.08.2022, Art. 82 DS-GVO Rn. 23a).

Vorliegend liegt der immaterielle Schaden des Klägers darin begründet, dass sämtliche knapp 10.000 Mitglieder des X. e.V. von seiner Erkrankung, der Dauer seiner Erkrankung sowie des vermeintlichen Vortäuschens seiner Erkrankung Ende 2022 Kenntnis erlangt haben und ihn sogar in seiner Freizeit auf die Vorgänge ansprechen. Dadurch wurde seine Reputation beschädigt, sein Ruf geschwächt.

3. Zum Ersatz dieses immateriellen Schadens hält die Kammer einen Betrag in Höhe von 10.000 Euro für geboten:

Art. 82 I DS-GVO ist nach Auffassung des EuGH unter Anwendung der geltenden Auslegungsgrundsätze dahin auszulegen, dass der in dieser Bestimmung vorgesehene Schadenersatzanspruch eine Ausgleichsfunktion hat, die eine auf diese Bestimmung gestützte Entschädigung in Geld ermöglichen soll, den konkret aufgrund des Verstoßes gegen diese Verordnung erlittenen Schaden vollständig auszugleichen, und keine abschreckende oder Straffunktion erfüllt (EuGH (Dritte Kammer) Ur. v. 14.12.2023 – C-456/22 (VX, AT/Gemeinde Ummendorf).

Vor diesem Hintergrund hält die erkennende Kammer eine Entschädigung in Höhe von 10.000 € für angemessen, aber auch ausreichend. Dabei hat die Kammer berücksichtigt, dass der europäische Ordnungsgeber das verletzte Recht als bedeutsam einordnet, was sich an der Zuordnung der Gesundheitsdaten zu den besonders sensiblen Daten in Art. 9 DS-GVO zeigt. Da keine abschreckende Funktion oder Straffunktion zu erfüllen ist, knüpft die Kammer den Betrag an das Ausmaß der Beeinträchtigung, nämlich die Kenntnismahme von knapp 10.000 Vereinsmitgliedern an. Unberücksichtigt hat das Gericht den vorangegangenen Konflikt bzw. die Korrespondenz zwischen dem Kläger und der Beklagten als Präsidentin des X. e.V. gelassen. Denn dieser Umstand spielt für die Frage nach der Höhe des Entschädigungsanspruchs keine Rolle, sondern war bei der Frage relevant, ob der Kläger in die Verbreitung seiner Daten eingewilligt hat (was er nicht hat, siehe oben).

Art. 82 III DS-GVO stellt, so betrachtet, klar, dass der Verantwortliche von der Haftung gem. Abs. 2 befreit wird, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (EuZW 2024, 270 Rn. 93, beck-online). Ein entsprechender Nachweis wurde hier von der Beklagten nicht geführt.

## Kein Anspruch auf Ende-zu-Ende-Verschlüsselung

(OVG NRW, Beschluss vom 20. Februar 2025 – 16 B 288/23 –)

**1. Der in Art. 18 Abs. 1 lit. d) DS-GVO genannte Zeitraum („solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen“) ist nicht gleichbedeutend mit dem Zeitraum zwischen der Stellung eines Antrags auf**

**Gewährung einstweiligen Rechtsschutzes betreffend die Einschränkung einer Datenverarbeitung und einer diesbezüglichen Entscheidung in der Hauptsache.**

- 2. Eine Vorwegnahme der Hauptsache liegt nicht vor, wenn eine einstweilige Maßnahme begehrt wird, die bei entsprechendem Ausgang des Hauptsacheverfahrens für die Zukunft wieder beendet werden kann (wie BVerfG, Beschl. v. 30.09.2024 – 2 BvR 150/24 -).**

**Aus den Gründen:**

II. Der Antragsteller stellt die Annahme des Verwaltungsgerichts, er habe keinen Anordnungsanspruch glaubhaft gemacht, mit seinem Beschwerdevorbringen nicht durchgreifend in Frage.

1. Das Verwaltungsgericht hat zutreffend angenommen, dass Art. 18 Abs. 1 lit. d) DS-GVO keine Anspruchsgrundlage für das Begehren des Antragstellers darstellt. Nach dieser Vorschrift hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die betroffene Person Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DS-GVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Wurde die Verarbeitung gem. Abs. 1 eingeschränkt, so dürfen diese personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden (Art. 18 Abs. 2 DS-GVO). Das Verwaltungsgericht hat dazu ausgeführt, dem Antragsteller gehe es nicht nur um die Einschränkung der Datenverarbeitung für die Dauer des bereits abgeschlossenen Überprüfungsverfahrens, sondern um eine Verpflichtung der Antragsgegnerin, zukünftig eine Ende-zu-Ende-Verschlüsselung bei der Verarbeitung der personenbezogenen Daten des Antragstellers zu verwenden.

Dem setzt der Antragsteller ohne Erfolg den Hinweis entgegen, der Betroffene könne ausdrücklich auf Basis einer Einwilligung die Einschränkung der Verarbeitung teilweise aufheben und damit sei nach Art. 18 Abs. 2 DS-GVO jede Verarbeitung auch solcher Daten zulässig, deren Verarbeitung nach Art. 18 Abs. 1 DS-GVO eingeschränkt worden sei. Dieses Vorbringen versteht der Senat dahingehend, dass der Antragsteller meint, aufgrund seines Widerspruchs gegen die Verarbeitung seiner personenbezogenen Daten durch die Antragsgegnerin sei die Datenverarbeitung mit der in Art. 18 Abs. 2 DS-GVO beschriebenen Rechtsfolge eingeschränkt und er könne diese Einschränkung dadurch wieder teilweise aufheben, dass er in eine Übermittlung unter den in seinem Antrag genannten Voraussetzungen (Ende-zu-Ende-Verschlüsselung bzw. eine dem Stand der Technik und dem Risiko entsprechende Verschlüsselung) einwillige.

Unabhängig vom Stand des in Art. 18 Abs. 1 lit. d) DS-GVO i.V.m. Art. 21 Abs. 1 DS-GVO vorgesehenen Überprüfungsverfahrens bleibt dieses Vorbringen ohne Erfolg. Die Einschränkungen für die Datenverarbeitung unter den in Art. 18 Abs. 1 lit. d) DS-GVO genannten Voraussetzungen gelten nach dem

Wortlaut der Vorschrift in zeitlicher Hinsicht nur, „solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen“. Dem Antragsteller geht es im vorliegenden Verfahren jedoch nicht um den Zeitraum während des Überprüfungsverfahrens nach Art. 21 DS-GVO, sondern um eine von diesem Zeitraum unabhängige Regelung für die Übermittlung seiner personenbezogenen Daten. Dem steht nicht entgegen, dass er seinen Antrag im Verfahren auf Gewährung einstweiligen Rechtsschutzes zeitlich „bis zu einer Entscheidung in der Hauptsache“ begrenzt hat. Diese zeitliche Begrenzung ist lediglich dem Charakter des Verfahrens auf Gewährung einstweiligen Rechtsschutzes geschuldet.

Da der Antragsteller die geltend gemachten Ansprüche nicht aus Art. 18 Abs. 1 lit. d) DS-GVO herleiten kann und es nicht auf das in dieser Vorschrift in Bezug genommene Überprüfungsverfahren gem. Art. 21 Abs. 1 DS-GVO ankommt, musste das Verwaltungsgericht dem Antrag auch nicht deswegen stattgeben, weil nach Ansicht des Antragstellers nicht ersichtlich sei, welche in Art. 21 Abs. 1 S. 2 DS-GVO angeführten zwingenden Gründe hier gegen eine Ende-zu-Ende-Verschlüsselung sprächen.

2. Der Antragsteller stellt weiter die Annahme des Verwaltungsgerichts, er könne einen Anspruch auf Datenübermittlung im Wege einer Ende-zu-Ende-Verschlüsselung oder einer sonstigen Verschlüsselung, die über die von der Antragsgegnerin verwendete hinausgehe, nicht aus Art. 32 DS-GVO herleiten, nicht durchgreifend in Frage.

Das Verwaltungsgericht hat diese Ansicht mit einer Gesamtbetrachtung unter Berücksichtigung der in Art. 32 Abs. 1 DS-GVO genannten Kriterien begründet. Es hat ausgeführt, nach dieser Vorschrift sei die Antragsgegnerin bei der Verarbeitung personenbezogener Daten verpflichtet, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Erforderlich seien eine Risikoeinschätzung und darauf basierend die Feststellung des Schutzbedarfs der Daten. Die in Art. 32 Abs. 1 lit. a) DS-GVO genannte Maßnahme der Verschlüsselung personenbezogener Daten müsse den in Art. 5 Abs. 1 lit. f) DS-GVO genannten Zielsetzungen der Integrität und Vertraulichkeit genügen sowie dem Stand der Technik entsprechen; darüber hinausgehende spezifische Anforderungen für das einzusetzende Verschlüsselungsverfahren ließen sich Art. 32 DS-GVO aber nicht entnehmen. Der Antragsteller habe nicht hinreichend glaubhaft gemacht, dass die Datenverarbeitung der Antragsgegnerin für ihn ein besonderes Risiko darstelle. Seinen Ausführungen lasse sich nicht entnehmen, dass ein erhöhtes Risiko mit Blick auf die Datenverarbeitung der Antragsgegnerin bestehe, diese etwa einem gesteigerten Risiko ausgesetzt sei, Opfer von Hackerangriffen zu werden. Ebenso wenig sei die Antragsgegnerin in der Vergangenheit durch Sicherheitslücken aufgefallen. Vielmehr erfolge die Datenübertragung bei der Antragsgegnerin stets unter TLS-Verschlüsselung und werde im Kommunikationsprozess mit anderen staatlichen Stellen zusätzlich gesichert

(SINA-Box, Client-Zertifikate). Zudem hat das Verwaltungsgericht auf das von der Antragsgegnerin vorgelegte (und bei positivem Abschluss der jährlichen Überwachungsaudits bis zum 17.06.2025 gültige) IT-Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik vom 18.06.2022 Bezug genommen und ausgeführt, es seien keine Anhaltspunkte dafür ersichtlich, dass die Antragsgegnerin ihr IT-Sicherheitskonzept nicht oder nicht hinreichend umsetze.

Die gegen diese Ausführungen gerichteten Einwände des Antragstellers betreffen einzelne Aspekte der Gesamtbetrachtung. Sie führen auch bei gemeinsamer Würdigung nicht zum Erfolg der Beschwerde. Dies liegt insbesondere daran, dass der Antragsteller mit seinem Beschwerdevorbringen die für die Gesamtbetrachtung nach Art. 32 Abs. 1 DS-GVO wesentliche Einschätzung des Verwaltungsgerichts nicht durchgreifend in Zweifel zieht, wonach er das von der Datenverarbeitung der Antragsgegnerin für ihn ausgehende besondere Risiko nicht glaubhaft gemacht habe, und sich die von ihm begehrte Art der Datenübermittlung jedenfalls ohne ein solches erhöhtes Risiko nicht aus Art. 32 Abs. 1 DS-GVO ableiten lasse. Dabei besteht Einigkeit darüber, dass es sich bei den in Rede stehenden Daten des Antragstellers nicht um personenbezogene Daten i.S.v. Art. 9 und 10 DS-GVO handelt.

a) Das Verwaltungsgericht hat zu der behaupteten Gefährdung für Leib, Leben und Freiheit des Antragstellers ausgeführt, dessen Hinweis auf den ihn betreffenden Beschluss des Bundesverwaltungsgerichts vom 10.06.2021 – 3 B 19.20 – genüge nicht, um einen derart erhöhten Schutzbedarf glaubhaft zu machen, der eine Ende-zu-Ende-Verschlüsselung gebiete, weil es sich bei der vom Antragsteller in Bezug genommenen Passage lediglich um eine Wiedergabe der Ausführungen des Berufungsgerichts handle. Die dort wiedergegebene Einschätzung des Berufungsgerichts beruhe auf konkreten und durch Belege gestützten Angaben des Antragstellers im dortigen Verfahren sowie ergänzend auf einer im Zusammenhang mit § 41 Abs. 2 StVG stehenden Gefährdungsbewertung der Polizeidirektion. Vorliegend habe der Antragsteller keine konkreten Angaben oder Belege eingereicht, die ein besonderes Risiko für ihn durch die Datenverarbeitung der Antragsgegnerin belegen könnten. Der Umstand, dass der Antragsteller in einem Verfahren zur Eintragung einer Übermittlungssperre erfolgreich dargelegt habe, dass durch die Übermittlung von in das Fahrzeugregister eingetragenen Daten schutzwürdige Interessen beeinträchtigt würden, reiche nicht aus, um dies auch für eine Datenverarbeitung durch die Antragsgegnerin anzunehmen. Gleiches gelte für den Hinweis des Antragstellers auf die zu seiner Person eingetragene Auskunftssperre nach § 51 BMG.

Der dagegen gerichtete Vorwurf des Antragstellers, das Verwaltungsgericht sei rechtswidrig davon ausgegangen, er müsse den erhöhten Schutzbedarf zweifelsfrei nachweisen, trifft nicht zu. Das Verwaltungsgericht hat ausdrücklich ausgeführt, der Antragsteller müsse seine Gefährdung glaubhaft machen (Seite 8, 11 des Beschlusses), und näher erläutert, aus welchen Gründen dies nicht erfolgt sei.

Die Einwände des Antragstellers, seine Gefährdung sei in anderen Gerichtsverfahren festgestellt worden und ein individuell-konkreterer Vortrag könne nicht verlangt werden, greifen nicht durch. Sie genügen schon nicht den Darlegungsanforderungen des § 146 Abs. 4 S. 3 VwGO. Danach

muss der Beschwerdeführer u.a. die Gründe darlegen, aus denen die Entscheidung abzuändern oder aufzuheben ist, und sich mit der angefochtenen Entscheidung auseinandersetzen. Die – hier erfolgte – bloße Wiederholung des erstinstanzlichen Vorbringens reicht dazu grundsätzlich nicht aus; Entsprechendes gilt für die Bezugnahme auf die bereits erstinstanzlich vorgelegte eidesstattliche Versicherung des Antragstellers vom 29.08.2022, in der der Antragsteller geltend macht – allerdings ohne dafür Nachweise vorzulegen –, aufgrund seines beruflichen Umgangs mit [...] bestehe für ihn die Gefahr, Opfer einer Entführung oder eines Raubes zu werden [...]. Der Antragsteller geht nicht auf die zutreffende Argumentation des Verwaltungsgerichts ein, dass das Bundesverwaltungsgericht in der vom Antragsteller in Bezug genommenen Passage nicht Tatsachen betreffend diesen selbst festgestellt, sondern lediglich Ausführungen der Vorinstanz wiedergegeben hat, und aus welchen Gründen ein Verweis auf Gefährdungseinschätzungen anderer Gerichte oder Behörden in anderen rechtlichen Zusammenhängen (Fahrzeug-, Melderegister) keine belastbaren Rückschlüsse auf die vorliegende Fallkonstellation zulässt. Unabhängig vom Vorstehenden hat der Antragsteller auch im Beschwerdeverfahren keine konkreten Belege für die von ihm geltend gemachte besondere Gefährdung vorgelegt.

b) Aus den vorgenannten Gründen kann der Antragsteller auch nicht mit Erfolg rügen, die Datenverarbeitung der Antragsgegnerin sei im Lichte von Art. 5 DS-GVO formell rechtswidrig, weil diese keine Einzelfallprüfung bezogen auf seine besonders schutzbedürftigen personenbezogenen Daten vorgenommen habe. Daher kommt auch die vom Antragsteller thematisierte Sperrung seiner Daten für eine nicht hinreichend verschlüsselte Übermittlung als „Sanktionswirkung für ein Unterlassen nach Art. 5 DS-GVO“ nicht in Betracht.

c) Die Ausführungen des Verwaltungsgerichts, wonach für die Antragsgegnerin kein gesteigertes Risiko erkennbar sei, Opfer von Hackerangriffen zu werden, und diese in der Vergangenheit auch nicht durch Sicherheitslücken aufgefallen sei, betreffen der Sache nach den Aspekt „Eintrittswahrscheinlichkeit“ in Art. 32 Abs. 1 DS-GVO. Sie werden vom Antragsteller mit seinem Beschwerdevorbringen inhaltlich nicht in Frage gestellt. Das Verwaltungsgericht hat mit diesen Ausführungen nicht vom Antragsteller einen Nachweis für das Gegenteil verlangt.

d) Die Rüge des Antragstellers, die Antragsgegnerin habe keine ausreichende Transportverschlüsselung glaubhaft gemacht, greift nicht durch. Das Verwaltungsgericht hat zur Transportverschlüsselung ausgeführt, die von der Antragsgegnerin verwendete Transportverschlüsselung sei datenschutzrechtlich ausreichend. Zur Begründung hat es sich u.a. auf das von der Antragsgegnerin vorgelegte IT-Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik vom 18. Juni 2022 gestützt. Außerdem hat es die Angaben der Antragsgegnerin angeführt, wonach jede Datenübermittlung verschlüsselt erfolge, etwa durch TLS-Verschlüsselungen, und im Kommunikationsprozess mit anderen staatlichen Stellen zusätzliche Sicherungen beständen (SINA-Box, Client-Zertifikate). Konkrete Anhaltspunkte dafür, dass diese Angaben der Antragsgegnerin nicht zutreffen könnten oder die im IT-Sicherheitszertifikat angeführten Maßnahmen nicht umgesetzt würden, zeigt der Antragsteller nicht auf.

Soweit er die von der Antragsgegnerin verwendete Verschlüsselungstechnik für zu unsicher hält und meint, TLS 1.2 entspreche nicht mehr dem aktuellen Stand der Technik, vielmehr gebe es bereits seit 2018 TLS 1.3, jedenfalls aber sei jede TLS-Verschlüsselung zu unsicher, führt dies nicht zum Erfolg seiner Beschwerde. Denn die Verschlüsselung über TLS stellt, wie vom Verwaltungsgericht ausgeführt, nicht die einzige Sicherheitsmaßnahme der Antragsgegnerin dar. Im Beschwerdeverfahren hat die Antragsgegnerin zudem ergänzt, die Transportverschlüsselung sei so konzipiert, dass sie vom Browser-Client der Anfragenden bis zur Firewall der Antragsgegnerin reiche; es gebe also keine „Zwischenstationen“, auf denen die Inhalte unverschlüsselt abgelegt wären; die Netzkomponenten auf dem Routing-Weg im Internet könnten keinen Einblick in die Kommunikationsinhalte gewinnen. Konkrete Anhaltspunkte dafür, dass diese Angaben wahrheitswidrig sein könnten, sind weder substantiiert vorgetragen noch sonst ersichtlich. Abgesehen davon kann der Antragsteller im Rahmen der nach Art. 32 Abs. 1 DS-GVO erforderlichen Gesamtbetrachtung ohne besondere, in seiner Person liegende Umstände, die hier nicht glaubhaft gemacht sind, nicht von der Antragsgegnerin verlangen, dass die ihn betreffenden personenbezogenen Daten nur unter höheren Sicherheitsanforderungen elektronisch übermittelt werden dürfen, als dies bei personenbezogenen Daten anderer Personen, die bei der Antragsgegnerin gespeichert sind, der Fall ist. Dies gilt auch für etwaige Übermittlungen durch Telefax, E-Mail oder Telefon, die vom Baustein „CON.9 Informationsaustausch“ des IT-Grundschutzes der Antragsgegnerin erfasst werden, der nach seiner Nr. 1.1. unterschiedliche Kommunikationswege wie z.B. persönliche Gespräche, Telefonate, Briefe u.a. in den Blick nimmt.

e) Weiter ohne Erfolg macht der Antragsteller mit seiner Beschwerdebegründung vom 03.04.2023 geltend, den vom Verwaltungsgericht angenommenen Prüfungsmaßstab „sozialadäquat“ kenne die Datenschutz-Grundverordnung nicht. Im Schriftsatz vom 27.05.2023 versteht der Antragsteller diesen Begriff dahingehend, dass damit eine Transportverschlüsselung gemeint sei, die dem üblichen Stand der Technik entspreche. In diese Richtung geht auch die Formulierung des Verwaltungsgerichts, das in Anlehnung an die entsprechende Wortwahl des insoweit zitierten Verwaltungsgerichts Mainz, Urt. v. 17.12.2020 – 1 K 778/19.MZ –, juris, Rn. 40: „Vielmehr ist die Kommunikation mittels (obligatorisch) transportverschlüsselter E-Mails auch im geschäftlichen Verkehr durchaus als sozialadäquat und wohl derzeit noch als (Mindest-) Stand der Technik einzustufen“, die von der Antragsgegnerin verwendete Transportverschlüsselung mit diesem Begriff

bezeichnet hat. Der Sache nach stellen die Ausführungen des Verwaltungsgerichts in diesem Zusammenhang eine zusammenfassende Bewertung unter Berücksichtigung der in Art. 32 Abs. 1 DS-GVO genannten Kriterien dar und ist als solche rechtlich nicht zu beanstanden.

f) Die Ausführungen des Antragstellers dazu, dass Art. 2 Abs. 2 lit. d) DS-GVO den geltend gemachten Anspruch nicht ausschließe, führen nicht zum Erfolg der Beschwerde, weil auch das Verwaltungsgericht von dieser Rechtsauffassung ausgegangen ist.

III. Das Vorbringen des Antragstellers zum Anordnungsgrund stellt den angegriffenen Beschluss nicht in Frage, weil das Verwaltungsgericht diesen nicht mehr geprüft hat, nachdem es den Anordnungsanspruch verneint hat.

Die Kostenentscheidung beruht auf § 154 Abs. 2 VwGO, die Streitwertfestsetzung auf den §§ 47 Abs. 1, 52 Abs. 1 und 2 sowie 53 Abs. 2 Nr. 1 GKG. Der sich danach für das Hauptsacheverfahren ergebende Streitwert von 5.000 Euro ist nach Nr. 1.5 des Streitwertkatalogs für die Verwaltungsgerichtsbarkeit im Verfahren des vorläufigen Rechtsschutzes wegen dessen vorläufigen Charakters zu halbieren. Er ist nicht wegen einer Vorwegnahme der Hauptsache in der Höhe des Hauptsachestreitwerts festzusetzen.

Eine – allein in Ausnahmefällen zulässige – Vorwegnahme der Hauptsache liegt nur dann vor, wenn die begehrte vorläufige Entscheidung faktisch keine vorläufige wäre, sondern einer endgültigen gleichkäme. Dies ist nicht der Fall, wenn eine einstweilige Maßnahme begehrt wird, die bei entsprechendem Ausgang des Hauptsacheverfahrens für die Zukunft wieder beendet werden kann. Die bloße Tatsache, dass eine vorübergehende Maßnahme als solche nach dem Ende des Hauptsacheverfahrens für dessen Dauer nicht mehr rückgängig gemacht werden kann, macht die vorläufige Regelung nicht zu einer faktisch endgültigen.

Vgl. BVerfG, Beschl. v. 30.09.2024 – 2 BvR 150/24 –, juris, Rn. 40, m.w.N.; OVG NRW, Beschl. v. 10.05.2024 – 19 E 289/24 –, juris, Rn. 5 ff., v. 12.01.2023 – 16 E 474/21 – (n. v.), und v. 09.01.2023 – 4 B 415/22 –, juris, Rn. 22.

Ausgehend von diesen Maßstäben würde dem Begehren des Antragstellers bei einem Erfolg des einstweiligen Rechtsschutzverfahrens nicht tatsächlich und rechtlich endgültig, sondern nur zeitlich vorübergehend bis zu einer Entscheidung in der Hauptsache entsprochen. Eine auch für die Zukunft unabänderliche oder zumindest nachwirkend prägende Regelung wäre damit nicht verbunden. Eine zeitlich vorübergehende Datenübermittlung unter den vom Antragsteller begehrten Bedingungen könnte für die Zukunft ohne Weiteres wieder beendet werden. [...]

caralegal verbindet **Datenschutz und KI-Governance** in einer intuitiven Plattform. Mit der Data Responsibility Platform managen Sie Datenschutz und KI-Risiken **effizient und rechtssicher**. Ihre DSGVO- und KI-VO-Compliance ist strukturiert gebündelt an einem Ort.



## Privacy Flow

- Zentrale, einheitliche Dokumentation mit Datenharmonisierung
- Eigenständige Mitarbeit durch alle Fachbereiche
- Automatisierte Prozesse und klare Verantwortlichkeiten
- Strukturierte Steuerung von Risiken und Audits



## AI Flow

- KI-Systeme systematisch erfassen und klassifizieren
- Automatisierte Risikobewertung nach KI-VO
- Fachübergreifende Zusammenarbeit an einem Ort
- Umfangreiches Compliance-Dashboard und Experten-Support



### KI trifft Datenschutz: Die caralegal-Synergie.

Scannen Sie den QR-Code und entdecken Sie, wie Sie mit caralegal das volle Synergiepotenzial von DSGVO und KI-VO ausschöpfen.

# BERICHT AUS BRÜSSEL

Axel Voss/Moritz Köhler\*

Die KI-Verordnung war spätestens seit Beginn der Trilog-Verhandlungen Gegenstand intensiver politischer Diskussionen. Im Mai hat der Diskurs mit der Ankündigung der EU-Kommission, eine Aussetzung des Geltungsbeginns bestimmter Vorgaben der KI-Verordnung zu prüfen,<sup>1</sup> einen neuen Höhepunkt erreicht.

## Vorgaben für GPAI-Modelle

Der aktuelle Streit um Wirkmacht und Innovationsfreundlichkeit der KI-Verordnung ist an den Vorgaben des Gesetzes für KI-Modelle mit allgemeinem Verwendungszweck (engl.: Generalpurpose AI models, kurz: GPAI-Modelle) in den Art. 51 ff. KI-VO entbrannt.

Zu den GPAI-Modellen gehören etwa große KI-Sprachmodelle, wie sie hinter den populären KI-Chatbots stehen. Auch andere generative KI-Systeme wie beispielsweise Bildgeneratoren basieren auf GPAI-Modellen. Vereinfacht lassen sich die Modelle als Murmelbahn beschreiben, in der die Murmel auf den wahrscheinlichsten nächsten Wortteil oder den wahrscheinlichsten nächsten Pixel fällt. Da GPAI-Modelle die Grundlage für eine Reihe von Systemen bilden können, die von nachgelagerten Anbietern bereitgestellt werden, nehmen die Anbieter der GPAI-Modelle entlang der KI-Wertschöpfungskette nach den Erwägungen des europäischen Gesetzgebers eine besondere Rolle und Verantwortung ein.<sup>2</sup>

Unter Berücksichtigung dieser besonderen Rolle und Verantwortung sind die Anbieter der GPAI-Modelle zu besonderer Transparenz verpflichtet.<sup>3</sup> Sie müssen unter anderem eine technische Dokumentation sowie spezifische Informationen für nachgelagerte System-Anbieter erstellen und aktualisieren, eine Strategie zur Einhaltung des Urheberrechts auf den Weg bringen und eine hinreichend detaillierte Zusammenfassung der für das Training des GPAI-Modells verwendeten Inhalte erstellen und veröffentlichen. Von GPAI-Modellen, die über Fähigkeiten mit hohem Wirkungsgrad verfügen, geht nach der Konzeption der KI-Verordnung ein systemisches Risiko aus. Anbieter von GPAI-Modellen mit systemischem Risiko müssen über die Transparenzpflichten hinaus besondere Sicherheitsmaßnahmen ergreifen, um eine Verwirklichung des systemischen Risikos zu minimieren.<sup>4</sup>

## Debatte während der Trilog-Verhandlungen

Die beschriebene Regulierung von GPAI-Modellen ist keinesfalls Produkt einer geradlinigen Entwicklung. Im Kommissionsentwurf<sup>5</sup> war eine Regulierung der Modelle noch gar nicht vorgesehen, da die besondere Regulierungsbedürftigkeit der spezifischen Technologie im Jahr 2021 noch kein Thema war.<sup>6</sup> Die Anbieter der GPAI-Modelle wollten es bei dieser Herangehensweise belassen: Sie beriefen sich darauf, dass die Modelle zu unspezifisch seien, um als Anknüpfungspunkt einer Regulierung zu dienen. Schließlich könnten die Anbieter der GPAI-Modelle nicht vorhersehen, wie nachgelagerte

Anbieter einzelner KI-Systeme die Modelle in ihre Produkte einbinden.<sup>7</sup> Demgegenüber setzte sich insbesondere das Parlament unter Berufung auf die besondere Verantwortung der Modell-Anbieter für deren Regulierung ein.<sup>8</sup> Kurz vor Beginn der letzten Runde der Trilog-Verhandlungen warfen auch Deutschland, Frankreich und Italien ihren Hut in den Ring und veröffentlichten ein Positionspapier, in dem sie eine verpflichtende Selbstregulierung der Anbieter von GPAI-Modellen vorschlugen.<sup>9</sup>

Schließlich konnte sich zwar das Parlament mit seinem Vorschlag einer klassischen Regulierung durchsetzen. Der Pflichtenkatalog in den finalen Art. 51 ff. KI-VO ist allerdings wesentlich kleiner als zunächst vorgesehen.

## Streit um Praxisleitfäden

Perspektivisch sollen sich Anbieter von GPAI-Modellen auf die Einhaltung einer harmonisierten europäischen Norm berufen können, um eine Vermutung der Konformität mit den in der KI-Verordnung statuierten Pflichten zu begründen.<sup>10</sup> Bislang wurde bei der Normungsorganisation CEN-CENELEC allerdings kein spezifischer Normungsauftrag eingereicht.

Bis die harmonisierte europäische Norm für GPAI-Modelle angenommen ist, sollen sich die Anbieter auf die Befolgung von Praxisleitfäden berufen können, die von zahlreichen Experten unter der Federführung des bei der Kommission angesiedelten Büros für Künstliche Intelligenz entwickelt werden. Die Praxisleitfäden sollten eigentlich spätestens am

\* Axel Voss ist Mitglied des Europäischen Parlaments für die EVP. Moritz Köhler ist wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln und beobachtet für die Gesellschaft für Datenschutz und Datensicherheit das politische Geschehen in Brüssel.

1 Bertuzzi, EU Commission eyes pausing AI Act's entry into application, <https://www.mlex.com/mlex/articles/2344845/eu-commission-eyes-pausing-ai-act-s-entry-into-application> (Stand: 14.07.2025).

2 ErwG 101 S. 1 KI-VO.

3 Art. 53 Abs. 1 KI-VO.

4 Art. 55 Abs. 1 KI-VO.

5 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final.

6 Vgl. dazu und zu den daraus resultierenden Herausforderungen der KI-VO bei der Regulierung von GPAI-Anwendungen Schwartmann/Zenner, GPAI-Anwendungen auf dem Prüfstand: Die Regulierung der KI-VO entlang der Wertschöpfungskette, EuDIR 2025, 3.

7 Schwartmann/Köhler, Ausgewählte Probleme des Entwurfs zur KI-Verordnung, RDV 2024, 27 (28).

8 Abänderungen des Europäischen Parlaments vom 14.06.2023 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), [https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236\\_DE.html](https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DE.html) (Stand: 14.07.2025), Abänderung 399.

9 Dazu Rusch, Berlin, Paris und Rom wollen Selbstregulierung für GPT & Co., Tagesspiegel Background v. 20.11.2023, <https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/berlin-paris-und-rom-wollen-selbstregulierung-fuer-gpt-co> (Stand: 14.07.2025).

10 Art. 53 Abs. 4 S. 2 und Art. 55 Abs. 2 S. 2 KI-VO.

02.05.2025 vorliegen, aufgrund anhaltender Diskussionen steckten sie aber lange im dritten Entwurf fest. Schließlich wurden sie am 10.07.2025 veröffentlicht.<sup>11</sup>

Derzeit holt die Kommission Rückmeldungen zu den Leitfäden ein. Es ist allerdings unklar, wann die finale Version angenommen wird.

Bereits kurz nach Veröffentlichung des dritten Entwurfs warnten zahlreiche Mitverhandler der KI-Verordnung davor, dass die Praxisleitfäden die Regelungen verwässern könnten, auf die sich Kommission, Rat und Parlament in mühsamen Trilog-Verhandlungen verständigt hatten.<sup>12</sup> Insbesondere die Vorgaben zur Bestimmung eines systemischen Risikos von GPAI-Modellen blieben hinter den Vorgaben des Art. 51 KI-VO zurück, aber auch Transparenzpflichten, Modellbewertungen und der Schutz von Whistleblowern würden gegenüber den Zielen der Verordnung reduziert.<sup>13</sup>

Auf der anderen Seite hat sich in den Reihen der Modell-Anbieter, insbesondere im Silicon Valley, Widerstand gegen die Praxisleitfäden gebildet. In den U.S.A. sind die Segel weiter auf Deregulierung gesetzt, was auch und gerade für die Technologiebranche gilt. Den europäischen Regulierungsbestrebungen wird vor diesem Hintergrund Technologiefeindlichkeit vorgeworfen.

### Aussetzung des Geltungsbeginns?

Die Situation um die Praxisleitfäden ist also außerordentlich verfahren: Während eine Seite strengere Vorgaben zur Umsetzung der Ziele der KI-Verordnung verlangt, will die andere Seite die Zeit bis vor die Einigung in den Trilog-Verhandlungen zurückdrehen. In dieser Gemengelage hatte die Kommission

im Mai also angekündigt, eine Aussetzung des Geltungsbeginns der Vorgaben zu GPAI-Modellen zu prüfen.<sup>14</sup> Denn die Art. 51 ff. KI-VO gelten seit dem 2. August 2025. Vor diesem Hintergrund wäre eine Aussetzung des Geltungsbeginns in erster Linie ein Sieg für die Industrie gewesen.

Ein Eingriff der Kommission in die Arbeiten an den Praxisleitfäden wäre bedenklich. Die Ergebnisse der politischen Einigung aus den Trilog-Verhandlungen könnten im Nachhinein durch die demokratisch nur mittelbar legitimierte Fassung der Praxisleitfäden verändert werden. Erfreulicherweise ist die Kommission von dem Vorhaben, den Geltungsbeginn der Art. 51 ff. KI-VO auszusetzen, mittlerweile abgerückt.<sup>15</sup>

Es steht daher wieder zu hoffen, dass sich eine europäische Lösung für eine europäische Verordnung findet, die die Ergebnisse der Trilog-Verhandlungen und die Unabhängigkeit der Verfasser der Praxisleitfäden respektiert.

11 Kommission, The General-Purpose AI Code of Practice, <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai> (Stand: 10.7.2025).

12 Brief abrufbar unter <https://fortune.com/2025/03/26/eu-ai-act-code-of-practice-disinformation-election-benifei-trump-appease-tech-lobbying/> (Stand: 10.06.2025). Dazu EU lawmakers warn against 'dangerous' moves to water down AI rules, <https://www.ft.com/content/9051af42-ce3f-4de1-9e68-4e0c1d1de5b5> (Stand: 14.07.2025).

13 Statement von Axel Voss und Kai Zenner, [https://www.linkedin.com/posts/kzenner\\_avossgpai-code-activity-7310548578165231618-hjek?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAD\\_ddDYB8eq6-nvg6laDsUPl6fd\\_VFEIYWA](https://www.linkedin.com/posts/kzenner_avossgpai-code-activity-7310548578165231618-hjek?utm_source=share&utm_medium=member_desktop&rcm=ACoAAD_ddDYB8eq6-nvg6laDsUPl6fd_VFEIYWA) (Stand: 10.07.2025).

14 Bertuzzi, EU Commission eyes pausing AI Act's entry into application, <https://www.mlex.com/mlex/articles/2344845/eu-commission-eyes-pausing-ai-act-s-entry-into-application> (Stand: 14.07.2025).

15 Chee, EU sticks with timeline for AI rules, <https://www.reuters.com/world/europe/artificial-intelligence-rules-go-ahead-no-pause-eu-commission-says-2025-07-04/> (Stand: 14.07.2025).



# Ausbildung zum/zur Datenschutz-auditor/in GDDcert. EU

13.-14.10.2025 | Online  
Referent: Alexander Forssman

## Schwerpunktthemen:

- ✓ Herleitung der Pflicht zur Durchführung eines »Datenschutzaudits«
- ✓ Begriffe, Definitionen, Vorgehensweisen
- ✓ Feststellungen von Konformitäten bzw. Abweichungen
- ✓ Erstellung eines Abschlussberichts
- ✓ Durchführung eines Datenschutzaudits

Jetzt  
anmelden!



[www.datakontext.com](http://www.datakontext.com)



## KI tastend erkunden



KI ist ein autonomes Werkzeug, das sich ohne menschlichen Einfluss verändert. Wie geht man mit autonomen Werkzeugen der Gattung KI um, deren Risiken und Möglichkeiten nicht konkret erkennbar sind? Um KI in ihrer Eigenschaft als mathematische Impulse zu begreifen, deren Gedankensimulationen wir über unsere Köpfe in unsere Welt holen, sollte man auf Bewährtes zurückgreifen. Jeder, der es einmal mit einem Tier zu tun hatte, kann die Möglichkeiten und Risiken, die mit ihm verbunden sind, einschätzen. Jeder normale Mensch hat Respekt und je nach dem auch berechnete Angst vor Tieren. Stellen wir uns KI doch als Tier vor, das uns im November 2022 begegnet ist. Das Geschöpf hat viele Funktionen und Erscheinungsformen. Es ist faszinierend und hat Eigenschaften, die wir von Menschen und Tieren kennen, aber es ist weder Mensch noch Tier, sondern Mathematik. Das wissen wir und dennoch inte-

grieren es viele ungeprüft in ihr Leben. Das Geschöpf hat zwar noch keine eigene Agenda, simuliert aber Gedanken und Geschichten in simulierter Kreativität, die wir in unser Denken und Handeln aufnehmen. Das reicht, um in die Irre geführt zu werden. Es wäre klug und naheliegend, KI interessiert, aber behutsam und bedacht in unser Leben zu lassen. Das versteht sich grundsätzlich. Dennoch nehmen Kinder zuweilen einen kräftigen Schluck aus einer Flasche mit grünem Spülmittel, das aussieht wie Waldmeistersirup. Als Erwachsene sollten wir gewarnt sein, bevor wir in einen unbekanntem Pilz beißen, der lecker aussieht, oder uns einem Schimpansen an den Hals werfen, weil er aussieht wie ein Kuscheltier. So sollten wir es auch mit der KI halten. Deren Möglichkeiten erkennt man sofort. Sie bergen aber Gefahren, die so unsichtbar sind wie die der „Wunderfaser“ Asbest oder wie die von Röntgenstrahlen.

# DatenTag

PRÄSENZ

MIT LIVESTREAM

Change Hub Berlin • 16. September 2025, 10–16 Uhr

Datenschutz – Ein Grundrecht für die Gesellschaft



**Prof. Dr. Louisa Specht-Riemenscheider**  
Bundesbeauftragte für den  
Datenschutz und  
die Informationsfreiheit



**Dr. Stefan Brink**  
wida – wissenschaftliches  
institut für die digitalisierung  
der arbeitswelt



**Markus Beckedahl**  
Zentrum für Digitalrechte  
und Demokratie

Das Grundrecht auf Datenschutz ist von essenzieller Bedeutung. Denn es schützt die Rechte und Freiheiten von Menschen vor Beeinträchtigungen durch öffentliche oder kommerzielle Akteure.

Viele Erwartungen lasten auf dem Datenschutz, doch zugleich hat er in der öffentlichen Wahrnehmung einen schweren Stand: Es geht wenig darum, was der Datenschutz ermöglicht. Debatten drehen sich eher darum, was er ausbremst. Dabei will der Datenschutz die Digitalisierung gar nicht verhindern, sondern in Bahnen lenken, die individuelle und gesellschaftliche Belange respektieren.

Die konkrete Umsetzung des Grundrechtsschutzes nur als Bürokratie wahrzunehmen, greift zu kurz. Dies verkennt die Chancen, die moderner Datenschutz bieten kann. Beim DatenTag wollen wir über Kern und Bedeutung des Datenschutzes in der heutigen Zeit sprechen – mit einem Rückblick auf seine Geschichte und einem Ausblick in seine Zukunft: Wie kommen wir (wieder) zu einer vor allem positiven, konstruktiv wirkenden Wahrnehmung dieses Grundrechts?



Anmeldung und Livestream:  
[sds-links.de/datenschutz-  
grundrecht-gesellschaft](https://sds-links.de/datenschutz-grundrecht-gesellschaft)



# Datenschutz- Awareness stärken

Interaktive E-Learning-Kurse mit  
echtem Menschen als Trainer

## Unsere E-Learning-Kurse:

- ✓ persönlich begleitet – ein echter Mensch führt durch den Kurs
- ✓ interaktiv & motivierend – Micro-Learning mit Quiz am Ende jedes Moduls
- ✓ rechtlich sicher – Teilnahmezertifikat & DS-GVO-konforme Nachweise
- ✓ flexibel einsetzbar – SCORM-Datei oder ISO 27001-zertifiziertes LMS
- ✓ sofort startklar – keine Softwareinstallation, kein IT-Projekt nötig

Jetzt kostenfrei testen:  
[elearning-mit-zertifikat.de](https://elearning-mit-zertifikat.de)

