

**EDITORIAL****VERANSTALTUNGEN****AUFSÄTZE**

Prof. Dr. Gregor THÜSING

**Automatisierte Entscheidung im Einzelfall beim Scoring: Wann wird eine Kreditentscheidung „maßgeblich“ beeinflusst?**

Prof. Dr. Petra GEHRING/Dr. Christian PERSON

**Rechtsformwahl: eine Herausforderung für Datentreuhänder**

Alexander STICHLING

**Künstliche Intelligenz im Automobil – Rechtsrahmen und Implikationen von diskriminierender KI****KURZBEITRÄGE**

Prof. Dr. Rolf SCHWARTMANN/Moritz KÖHLER

**Prüfen in der „KI-Ära“**

Ganesh SRINIVASAN

**Semantic Risk Classification – need for runtime solutions**

RAin Yvette REIF, LL.M. / RA Dr. Johannes ZHOU

**Praxisfälle zum Datenschutzrecht XXXVIII: Auftragsverarbeitung oder (gemeinsame) Verantwortlichkeit?****3 RECHTSPRECHUNG****HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ****4****Neues zum Personenbezug:****Die SRB-Entscheidung des EuGH**

(EuGH, Urt. v. 4.9.2025)

**39****Es bleibt dabei: Kontrollverlust allein ist immaterieller Schaden**

(BGH, Urt. v. 11.11.2025)

**43****5****WICHTIGES AUS DER RECHTSPRECHUNG****Kein Plattformprivileg im Anwendungsbereich der DS-GVO**

(EuGH, Urt. v. 2.12.2025)

**48****15****Rechtfertigung der Übermittlung personenbezogener Positivdaten**

(BGH, Urt. v. 14.10.2025)

**52****22****28****BERICHT AUS BRÜSSEL****Der Fahrplan der Kommission****für den Digitalen Omnibus****57****30****SCHWAKURAI'S SCHLEPPNETZ****60****35****ERRATUM:**

Im Beitrag "Cloud Computing: Zwischen Datenschutz und Abhängigkeit" von Herrn Luca Sawatzki in der Ausgabe 6/25 ab Seite 294 ff. ist es beim Korrekturlauf von Seiten der RDV-Redaktion und des Satzbetriebs in einigen Fußnoten zu Übertragungsfehlern gekommen.

Eine korrigierte Version des Aufsatzes finden Sie in der Onlineversion der RDV.

**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

Prof. Dr. Martin Kessen, LL.M. (University of Texas), Richter am Bundesgerichtshof

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

Thomas Muthlein, DMC Datenschutz Management & Consulting, Köln

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

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, LL.M. (TH Köln), LL.M. (Passau)  
(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

**Bezugspreise**

Jahresabonnement	€ 195,- (Inland)
Jahresabonnement	€ 197,- (Ausland)
Einzelheft	€ 36,-

MwSt. im Preis enthalten, jeweils inkl. Versandkosten

**Vertrieb/Produktsicherheit**

Dieter Schulz | Tel.: +49 2234 98949-78  
dieter.schulz@datakontext.com  
www.datakontext.com produktsicherheitsverordnung

**Abo-Service**

Tel.: +49 89 2183-7110 | Fax: +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  
Tel.: +49 2234 98949-0 | Fax: +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)  
Tel.: +49 2234 98949-60  
wolfgang.scharf@datakontext.com  
www.datakontext.com

**Manuskripte**

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

**Urheber- und Verlagsrechte**

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

Sachregister 2025

## EDITORIAL



## 2025 – Das Jahr der Neuausrichtung

Digital- und datenrechtlich markierte das Jahr 2025 eine Neuausrichtung. Die Zeichen des im April abgeschlossenen Koalitionsvertrags der Regierung Merz stehen auf Digitalisierung und Staatsmodernisierung. Es wurde ein Digitalministerium geschaffen, die Bundesnetzagentur erhält weitreichende Befugnisse in der Datenaufsicht. Die Bundesbeauftragte für Datenschutz und Informationsfreiheit soll künftig auch Datennutzungsbeauftragte werden und Aufgaben von den Landesdatenschutzbehörden übernehmen. Im Mai machte das Oberlandesgericht Köln den Weg dafür frei, dass Meta sein KI-Modell an europäische Verhältnisse anpassen kann. Die Datennutzungsbeauftragte in Spe hat der Bundesregierung in ihrer Funktion als Datenschutzbeauftragte ihre Facebook-Fanpage untersagt. Das Datenschutzrecht steht für die Kölner Verwaltungsrichter der Information der Öffentlichkeit über eine Facebook-Fanpage der Bundesregierung aber nicht entgegen. Die Datenschutzbehörde will die Schlappe nicht hinnehmen und hat den Fall vor das Oberverwaltungsgericht Münster gebracht. Im November entschieden Gerichte in London und München darüber, ob das Urheberrecht auch für KI-Anbieter gilt. In München schlug man sich auf die Seite der Urheber, in London gab man einem KI-Anbieter Recht. Bald muss der Europäische Gerichtshof über einen solchen Fall entscheiden und wird zumindest in der EU für Rechtsklarheit sorgen können. Ebenfalls im November schickte die EU-Kommission einen Gesetzesvorschlag aufs Gleis. Der sog. „Datenomnibus“ soll das Datenschutzrecht mit Blick auf die Bedürfnisse der Digitalwirtschaft liberalisieren. Die DS-GVO soll angepasst werden, um das Datenrecht zu entschlacken und einfacher zu machen. Im Dezember folgte noch ein Paukenschlag aus Deutschland. Der Bundeskanzler hat mit den Ministerpräsidenten einen Beschluss in Sachen Staatsmodernisierung gefasst. Dabei ging es auch um Vereinfachungen im Datenschutzrecht. Danach soll die Datenschutzaufsicht für Unternehmen bis Ende 2027 reformiert werden. Ziel ist die Durchsetzung einer einheitlichen Auslegung des Datenschutzrechts. Offen ist, ob das durch Bündelung der Kompetenzen bei einer Zentralbehörde des Bundes geschieht, oder durch eine Umstrukturierung bei den Landesbehörden umgesetzt werden soll. Zudem soll sich die Bestellpflicht eines betrieblichen Datenschutzbeauftragten nach der DS-GVO richten und der bewährte deutsche Sonderweg einer Bestellpflicht ab 20 Personen, die im Unternehmen mit Datenverarbeitung betraut sind, aufgegeben werden. Dagegen hat sich die GDD am 18.12.2025 auf ihrem Parlamentarischen Abend in Berlin klar positioniert.

**Prof. Dr. Rolf Schwartzmann**

ist Leiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln, ist Mitherausgeber von *Recht der Datenverarbeitung* (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Termine	Thema	Ort	Kontakt
21.4.2026	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
22.4.2026	Hacker-Tools für Profis: Sicherheitslücken erkennen und schließen	Köln	GDD e.V./DATAKONTEXT
22.4.2026	Datenschutz im Homeoffice und mobilen Arbeiten – Risiken minimieren, Sicherheit maximieren	Online	GDD e.V./DATAKONTEXT
23.4.2026	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
28.4.2026	Compliance-Tests und Schwachstellenscannen	Online	GDD e.V./DATAKONTEXT
28.-29.4.2026	Datenschutz-Management nach der DS-GVO – Teil 3	Köln	GDD e.V./DATAKONTEXT
5.5.2026	Künstliche Intelligenz im Konzern: Datenschutz, AI Act und praktische Umsetzung	Online	GDD e.V./DATAKONTEXT
6.5.2026	Datenschutz im Internet	Online	GDD e.V./DATAKONTEXT
7.5.2026	Datenschutz und Betriebsrat unter der DS-GVO	Online	GDD e.V./DATAKONTEXT
12.5.2026	Datenschutz-Folgenabschätzung	Online	GDD e.V./DATAKONTEXT
19.5.2026	Repetitorium GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
19. -20.5.2026	Ausbildung zum Datenschutzauditor GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
20.5.2026	Repetitorium GDDcert. EU	Online	GDD e.V./DATAKONTEXT
27.5.2026	Prüfung zum Datenschutzauditor GDDcert. EU	Online	GDD e.V./DATAKONTEXT
1.6.2026	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Online	GDD e.V./DATAKONTEXT
9.6.2026	Datenschutz und Künstliche Intelligenz	Online	GDD e.V./DATAKONTEXT
10.6.2026	Zertifizierung zum Betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V./DATAKONTEXT
10.-12.6.2026	13. Hamburger Datenschutztage	Hamburg	GDD e.V./DATAKONTEXT
16.6.2026	Ausbildung zum Datenschutzkoordinator GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
23.-25.6.2026	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Online	GDD e.V./DATAKONTEXT
24.6.2026	Prüfung zum Datenschutzkoordinator GDDcert. EU	Online	GDD e.V./DATAKONTEXT
25.6.2026	Aktuelle Prüfpraxis Datenschutzaufsichtsbehörden	Online	GDD e.V./DATAKONTEXT
30.6.2026	ISO 27701 und Datenschutz	Online	GDD e.V./DATAKONTEXT



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

## AUFSÄTZE

Prof. Dr. Gregor Thüsing

# Automatisierte Entscheidung im Einzelfall beim Scoring: Wann wird eine Kreditentscheidung „maßgeblich“ beeinflusst?

Art. 22 DS-GVO rückt das Scoring ins Zentrum datenschutzrechtlicher Diskussionen. Mit seinem Urteil in der Rechtssache C-634/21 hat der EuGH den Begriff der „maßgeblichen“ Beeinflussung geprägt, ohne ihn klar zu konturieren. Dies hat in Praxis und Wissenschaft erhebliche Unsicherheit darüber ausgelöst, wann ein Score bereits eine verbotene automatisierte Entscheidung im Einzelfall darstellt. Vor diesem Hintergrund setzt sich der Beitrag kritisch mit der EuGH-Rechtsprechung auseinander und entwickelt Kriterien, anhand derer die Maßgeblichkeit der Scoreverwendung präziser bestimmt werden kann.

## I. Dunkel spricht der Mund der Pythia

Jüngst titelte Bild: „Ist der SCHUFA-Score am Ende doch rechtswidrig?“. Und erkannte auch, wo der juristische Hase im Pfeffer liegt: „Es geht um das Wort ‚maßgeblich‘“.<sup>1</sup> In der Tat, der EuGH hat in seiner Entscheidung Rs. C-634/21 einen neuen Begriff in das Datenschutzrecht eingeführt, und seitdem ist unklar, was damit gemeint ist. Die Vorgeschichte dieser Entscheidung ist bekannt: Das VG Wiesbaden legte dem EuGH nicht nur die Frage vor, ob Art. 6 Abs. 1 und Art. 22 DS-GVO einer innerstaatlichen Regelung wie § 31 BDSG entgegenstehen, sondern auch, ob die automatisierte Erstellung eines Wahrscheinlichkeitswertes eine unter Art. 22 Abs. 1 DS-GVO fallende, ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung darstellt. Diese erste, gedanklich vorgelagerte Vorlagefrage, um deren rechtliche Beurteilung es in dem hiesigen Beitrag geht, erwies sich als folgenreich:

„1. Ist Art. 22 Abs. 1 der Verordnung (EU) 2016/679 dahingehend auszulegen, dass bereits die automatisierte Erstellung eines Wahrscheinlichkeitswertes über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung darstellt, die der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wenn dieser mittels personenbezogener Daten der betroffenen Person ermittelte Wert von dem Verantwortlichen an einen dritten Verantwortlichen übermittelt wird und jener Dritte diesen Wert seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person maßgeblich zugrunde legt?“<sup>2</sup>

Der Generalanwalt knüpfte in seinen Schlussanträgen daran an und übernahm partiell den Wortlaut der Frage:

„Art. 22 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) ist dahin auszulegen, dass bereits die automatisier-

te Erstellung eines Wahrscheinlichkeitswerts über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung darstellt, die der betroffenen Person gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wenn dieser mittels personenbezogener Daten der betroffenen Person ermittelte Wert von dem Verantwortlichen an einen dritten Verantwortlichen übermittelt wird und jener Dritte nach ständiger Praxis diesen Wert seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person maßgeblich zugrunde legt.“<sup>3</sup>

Der EuGH übernahm das dann wiederum fast wörtlich und antwortete, wie wohl vom VG Wiesbaden erhofft:

„Art. 22 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) ist dahin auszulegen, dass eine „automatisierte Entscheidung im Einzelfall“ im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.“<sup>4</sup>

1 Ochse, BILD-online v. 17.7.2025, abrufbar unter: <https://www.bild.de/leben-wissen/sparfochs/bild-analyse-ist-der-schufa-score-am-ende-doch-rechtswidrig-686e4cc9bfdec31b7cda9784>.

2 EuGH, Urt. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905 Rn. 27; Hervorhebung durch den Verfasser.

3 GA Pikamäe, Schlussantr. v. 16.3.2023 – C-634/21, BeckRS 2023, 4643 Rn. 95; Hervorhebung durch den Verfasser.

4 EuGH, Urt. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905; Hervorhebung durch den Verfasser.

Dreimal „maßgeblich“ – ohne dass dies in der DS-GVO steht. Dunkel spricht der Mund der Pythia. Seitdem rätseln Praxis, Wissenschaft und Gerichte: Wann liegt eine „maßgebliche“ Beeinflussung vor und wann nicht? Das VG Wiesbaden hat diesen Maßstab durch seine Frage in die Welt gesetzt – und der EuGH und sein Generalanwalt haben es übernommen, ohne ihn präzise zu konturieren.

## II. Welche Entscheidung ist gemeint: Das Scoring selbst oder die Kreditvergabe?

Eine gewisse Unsicherheit mag schon dahingehend bestehen, welche Entscheidung gemeint ist. Der EuGH macht deutlich, „dass eine ‚automatisierte Entscheidung im Einzelfall‘ im Sinne dieser Bestimmung vorliegt“, wenn die von ihm genannten Bedingungen erfüllt sind. Aber wer trifft sie: Die Auskunftsei oder der Kreditgeber? Welche Entscheidung ist gemeint: Das Scoring selbst oder die Kreditvergabe? Der EuGH – wie auch schon sein Generalanwalt – knüpft an die Vorstellung des VG Wiesbaden an. Dieses ging klar davon aus, dass es das Scoring selbst ist, das eine Entscheidung im Sinne des Art. 22 DS-GVO darstellt:

„Das Gericht geht jedoch davon aus, dass die Erstellung eines Score-Wertes durch eine Auskunftsei nicht lediglich ein die Entscheidung des dritten Verantwortlichen vorbereitendes Profiling ist, sondern gerade eine selbstständige „Entscheidung“ im Sinne des Art. 22 Abs. 1 DS-GVO.“<sup>5</sup>

### Dem folgte der Generalanwalt:

„Dagegen ist der Aspekt, der mir eine entscheidende Rolle zu spielen scheint, derjenige, der mit der Frage zusammenhängt, ob das Verfahren der Entscheidungsfindung so ausgestaltet ist, dass das von der Auskunftsei durchgeführte Scoring die Entscheidung des Finanzinstituts über die Gewährung oder Ablehnung des Kredits vorbestimmt. Sollte das Scoring ohne irgendein Eingreifen einer Person erfolgen, durch das gegebenenfalls das Scoring-Ergebnis und die Richtigkeit der in Bezug auf den Kreditantragsteller zu treffenden Entscheidung überprüft werden könnten, erscheint es logisch, davon auszugehen, dass es sich bei dem Scoring selbst um die „Entscheidung“ im Sinne von Art. 22 Abs. 1 DS-GVO handelt.“<sup>6</sup>

### Dies ist dann auch der Ansatz des EuGH:

„Daher ist unter Umständen wie jenen des Ausgangsverfahrens, unter denen der von einer Wirtschaftsauskunftsei ermittelte und einer Bank mitgeteilte Wahrscheinlichkeitswert eine maßgebliche Rolle bei der Gewährung eines Kredits spielt, die Ermittlung dieses Wertes als solche als Entscheidung einzustufen, die i.S.v. Art. 22 Abs. 1 DS-GVO gegenüber einer betroffenen Person „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.““<sup>7</sup>

Das Gesagte verwundert und kann nicht richtig sein – und eben das macht sie so sperrig im Kontext des Datenschutzrechts. Denn wenn dem so ist, dann ist im Zeitpunkt der Scoreerstellung dem Verantwortlichen noch gar nicht klar, ob sein Verhalten rechtmäßig ist oder nicht. Wenn der Score erstellt wird, und noch nicht verwendet wurde, dann weiß er nicht, ob und ggf. wann dieser Score gegenüber einer betroffenen Person „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“ – das liegt nicht mehr

in seiner Hand. Er weiß nicht, welche Entscheidung sein Kunde trifft. Um es klar zu sagen: Hier wird der Verantwortliche für etwas verantwortlich, wofür er nicht verantwortlich sein kann, weil er die spätere Entscheidung gar nicht kennt und aus datenschutzrechtlichen Gründen mangels Erforderlichkeit auch regelmäßig wohl nicht kennen darf. Für den Verantwortlichen, der einen Score erstellt, ist es vor der Weitergabe nicht möglich zu beurteilen, ob der Score die spätere Entscheidung maßgeblich beeinflusst oder nicht, sodass der Nachweis der Rechtmäßigkeit der Datenverarbeitung (vgl. Art. 5 Abs. 2 und Art. 24 Abs. 1 S. 1 DS-GVO) zum Zeitpunkt der Scoreerstellung unmöglich ist. Ultra posse nemo obligatur gilt aber auch im Datenschutzrecht.<sup>8</sup> Die Rechtmäßigkeit der Scoreerstellung wird durch die Entscheidung des EuGH von einem nachgelagerten Verhalten eines Dritten abhängig gemacht, auf das der Verantwortliche keinen Einfluss hat. Überzeugender ist es daher in dem übermittelten Score eine Entscheidungshilfe zu sehen und nicht die Entscheidung selbst. Zumindest dann, wenn er bei der Weiterleitung des Scores eine maßgebliche Verwendung im Sinne der Entscheidung des EuGH in der Rs. C-634/21 untersagt, oder sich der Verwender dazu verpflichtet, eine solche Nutzung zu unterlassen, bricht der Zurechnungszusammenhang ab.<sup>9</sup> Das entspricht allgemeinen Haftungsgrundsätzen aus dem Zivil- und Strafrecht, wonach die Kausalkette durchbrochen wird, wenn ein Dritter durch eigenständiges Handeln dazwischentritt:

„Je mehr der Zweite bzw. Dritte das Geschehen beherrscht und prägt, umso weniger ist der durch ihn verursachte Schaden noch dem Erstverantwortlichen zuzurechnen.“<sup>10</sup>

Der Kunde des Verantwortlichen, der den Score verwendet, trifft die Entscheidung, ob das Vertragsverhältnis mit der betroffenen Person zustande kommt oder nicht. Der Scoreersteller kann diese Entscheidung nicht beeinflussen. Der Verwender beherrscht das weitere Geschehen. Handelt der Verwender ggf. entgegen der vertraglichen Vereinbarung, die die maßgebliche Nutzung untersagt, und verwendet den Score dennoch maßgeblich, dann ist es der Verwender, der die betroffene Person der automatisierten Verarbeitung unterwirft und nicht der Verantwortliche, der den Score erstellt hat. In diesem Fall handelt der Verwender des Scores eigenmächtig, sodass er richtigerweise auch für die automatisierte Einzelentscheidung verantwortlich ist. Der Scoreersteller hat durch die vertragliche Vereinbarung der Unterlassung einer maßgeblichen Verwendung des Scores alles in seiner Macht

5 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 21.

6 GA Pikamäe, Schlussantr. v. 16.3.2023 – C-634/21, BeckRS 2023, 4643 Rn. 42; Hervorhebung durch den Verfasser.

7 EuGH, Urt. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905 Rn. 50; Hervorhebung durch den Verfasser.

8 So Heckmann, MMR 2023, 816 (818); Hacker, MMR 2018, 779 (783 f.)

9 Ähnlich schon die Kritik durch Taeger, BKR 2024, 41 (46): „Während es im Tatbestand des Art. 22 DS-GVO heißt, dass eine betroffene Person nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen sein darf, soll die Anwendung des Verbots aus Art. 22 DS-GVO schon auf das externe Scoring nun von dem im Tatbestand nicht vorkommenden Begriff ‚maßgeblich‘ abhängen, der die Verwendung des Scorewertes durch den Kreditgeber im Verhältnis zur Wirtschaftsauskunftsei also einem Dritten beschreibt. Es ist nicht nachvollziehbar, dass nach der „Theorie vom Zusammenwirken“ die Rechtmäßigkeit der externen Wahrscheinlichkeitswertberechnung vom künftigen, nicht vorhersehbaren Verhalten des Empfängers eines Scores abhängen soll.“; Hervorhebung im Original.

10 Pardey/Balke/Link/Pardey, Schadenrecht, 2023, Kausalität und Zurechnung Rn. 24; Hervorhebung durch den Verfasser.

stehende getan, um eine automatisierte Einzelentscheidung abzuwenden.

### III. Maßgebliche Beeinflussung: Versuch einer Deutung

Wenn dem aber nicht der Fall ist, dann stellt sich in der Tat die Frage nach der Maßgeblichkeit. Der Wortsinn hilft hier wohl nicht allzu viel weiter. Will man den EuGH auslegen, dann wird man feststellen, dass die Bedeutungen in den verschiedenen Übersetzungen des Urteils recht weit auseinanderliegen: Die englische Übersetzung verwendet mit „draws strongly on ...“ ebenfalls eine unpräzise Bezeichnung, die französische spricht wiederum von „déterminante“. Letzterer Begriff wird ins Deutsche u.a. mit ausschlaggebend, maßgebend oder bestimmend übersetzt.<sup>11</sup> Ausschlaggebend bedeutet aber etwas anderes als maßgeblich.<sup>12</sup> Am besten, man fokussiert sich auf die Verfahrenssprache Deutsch und nähert sich aus dem Herkommen des Begriffs aus der Entscheidung des VG Wiesbaden.

#### 1. Hinweise des VG Wiesbaden, des Generalanwalts und des EuGH

Das VG Wiesbaden selbst erläutert den Begriff nicht weiter. Es trifft lediglich die faktische Aussage, der „Verantwortliche muss seine Entscheidung zwar nicht allein vom Score-Wert abhängig machen, tut es in aller Regel jedoch maßgeblich.“<sup>13</sup> Das VG Wiesbaden geht davon aus, dass die Entscheidung über das Eingehen einer vertraglichen Beziehung mit der betroffenen Person „praktisch in so erheblichem Maße durch den von Wirtschaftsauskunfteien übermittelten Score-Wert determiniert [wird], dass jener gleichsam durch die Entscheidung des dritten Verantwortlichen durchschlägt.“<sup>14</sup> Laut dem VG Wiesbaden „[entscheidet e]igentlich ... über das Ob und Wie der Vertragseingehung des dritten Verantwortlichen mit der betroffenen Person ... der aufgrund automatisierter Verarbeitung von der Wirtschaftsauskunftei erstellte Score-Wert.“<sup>15</sup> Es ergänzt, dass „[e]ine Kreditvergabe ... trotz eines grundsätzlich ausreichenden Score-Werts (aus anderen Gründen, wie etwa des Fehlens von Sicherheiten oder Zweifeln am Erfolg einer zu finanzierenden Investition) versagt werden [mag], ein nicht ausreichender Score-Wert hingegen ... jedenfalls im Bereich der Verbraucherdarlehen in fast jedem Fall und auch dann zur Versagung eines Kredits führen [wird], wenn etwa eine Investition im Übrigen als lohnend erscheint.“<sup>16</sup> Schließlich weist es darauf hin, dass „Erfahrungen aus der behördlichen Datenschutzaufsicht [zeigen, d]ass Score-Werten bei der Kreditvergabe und der Gestaltung ihrer Bedingungen die entscheidende Rolle zukommt“.<sup>17</sup>

„Fast in jedem Fall“ – „entscheidende Rolle“. Das Gericht suggeriert einen Regelfall der Scoreverwendug, der selber – weil nur der Einzelfall Gegenstand des Verfahrens war – nicht weiter hinterfragt oder belegt wurde. Der Generalanwalt gibt dies dann wieder und versteht dies als eine de facto-Entscheidung, wo der Score dann eben doch das einzige Kriterium zur Kreditablehnung wäre:

„Da erstens Art. 22 Abs. 1 DS-GVO verlangt, dass die fragliche Entscheidung „ausschließlich“ auf einer automatisierten Verarbeitung beruht, und zweitens der Wortlaut einer Bestimmung im Allgemeinen die Grenze für jede Auslegung darstellt,

erscheint es erforderlich, dass die automatisierte Verarbeitung der einzige Aspekt bleibt, der den Ansatz des Finanzinstituts gegenüber dem Kreditantragsteller rechtfertigt. Dies wäre der Fall, wenn im Rahmen des Verfahrens ein Mensch beteiligt wäre, ohne jedoch in der Lage zu sein, den Kausalzusammenhang zwischen der automatisierten Verarbeitung und der endgültigen Entscheidung zu beeinflussen. Die Auskunftsei müsste de facto die endgültige Entscheidung für das Finanzinstitut treffen.“<sup>18</sup>

In Fußnote 19 deutet der Generalanwalt an, dass ggf. sogar ein „nicht unwesentlicher Einfluss“ reichen könnte:

„Ein solcher Ansatz erscheint mir umso notwendiger, als weder SCHUFA noch der HBDI in der mündlichen Verhandlung eine klare Antwort auf die Frage geben konnten, ob die Score-Werte die Entscheidungen der Finanzinstitute vorbestimmen sollen. Der Vertreter von SCHUFA hat jedoch darauf hingewiesen, dass diese die Erfahrung und die Fachkenntnis der Auskunftseien in Anspruch nähmen, um die Zahlungsfähigkeit einer natürlichen Person festzustellen, was grundsätzlich als ein Hinweis auf einen nicht unwesentlichen Einfluss auf den Entscheidungsprozess ausgelegt werden könnte.“

Der Generalanwalt will letzteres aber wohl nicht als seinen Maßstab verstanden wissen – der Widerspruch zum Satz davor wäre offensichtlich – sondern nur als eine Beschreibung der Wirklichkeit. Es kommt also auf die Tatsachen an. Die aber zu ermitteln, ist Aufgabe des nationalen Gerichts:

„Es handelt sich im Wesentlichen um eine Tatsachenfrage, die meines Erachtens am besten von den nationalen Gerichten beurteilt werden kann. Ich schlage daher vor, dem vorlegenden Gericht die Aufgabe zu übertragen, selbst festzustellen, inwieweit unter Berücksichtigung der oben genannten Kriterien das Finanzinstitut im Allgemeinen durch das von einer Auskunftsei wie SCHUFA vorgenommene Scoring gebunden ist.“<sup>19</sup>

#### Der EuGH übernimmt das ohne weitere Hinweise zu geben:

„So führt nach den Sachverhaltsfeststellungen des vorlegenden Gerichts im Fall eines von einem Verbraucher an eine Bank gerichteten Kreditantrags ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen dazu, dass die Bank die Gewährung des beantragten Kredits ablehnt.“<sup>20</sup>

#### 2. Vorschläge des Schrifttums

Schrifttum und nationale Instanzgerichte haben sich an diesen Hinweisen weiter entlanggehängt. Sie lösen sich zuweilen doch recht klar von den Hinweisen des Verfahrensgangs und formulieren echt freihändig eigene Ansätze:

Scholz, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, 2. Auflage 2025, Art. 22 DS-GVO Rn. 27 ff.: „Das Urteil des EuGH überzeugt nicht. Es führt zu einem Bruch mit der in der DS-GVO zum Ausdruck kommenden Wertung, im

11 PONS-Online Wörterbuch, abrufbar unter: <https://de.pons.com/übersetzung-2/französisch-deutsch/déterminante>.

12 S. nachfolgend Gliederungspunkt III. 3.a).

13 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 25.

14 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 25.

15 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 25.

16 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 25.

17 VG Wiesbaden, Beschl. v. 1.10.2021 – 6 K 788/20.WI, BeckRS 2021, 30719 Rn. 25.

18 GA Pikamäe, Schlussantr. v. 16.3.2023 – C-634/21, BeckRS 2023, 4643 Rn. 44.

19 GA Pikamäe, Schlussantr. v. 16.3.2023 – C-634/21, BeckRS 2023, 4643 Rn. 45.

20 EuGH, Ur. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905 Rn. 48.

Rahmen des Tatbestandes des Art. 22 Abs. 1 zwischen dem Profiling in Form des Scorings einerseits und der darauf beruhenden Entscheidung andererseits zu unterscheiden (Rn. 5, 20, 23). Das Fehlen spezifischer und risikoadäquater Zulässigkeitsvoraussetzungen für das Profiling ... kann nicht durch eine allein auf den Fall des Kredit Scorings bezogene Überdehnung des Anwendungsbereichs des Art. 22 Abs. 1 kompensiert werden. Die Einführung des wenig konkreten Kriteriums der „Maßgeblichkeit“ des Scorewertes für die Entscheidung des Kreditinstituts führt zu neuen Abgrenzungsschwierigkeiten und zu einer Vermengung der Verantwortlichkeiten. Denn die Erstellung des Scorewertes durch die Wirtschaftsauskunftei erhält ihre Bedeutung erst durch den im Verantwortungsbereich des Kreditinstituts liegenden Kreditvergabeprozess. Die Wirtschaftsauskunftei hat keinen Einfluss auf das hierfür erforderliche Risikomanagement des Kreditinstituts. Und der externe Score kann sich nur dann in vollem Umfang in der Kreditentscheidung niederschlagen, wenn er für das Kreditinstitut ein „KO-Kriterium“ darstellt. Darüber hinaus ist die vom EuGH vorgenommene Auslegung des Art. 22 Abs. 1 nicht erforderlich, um die von der DS-GVO geforderte Transparenz herzustellen. Vielmehr obliegt es dem Kreditinstitut, dafür Sorge zu tragen, dass es die Vorgaben des Art. 15 Abs. 1 lit. h) erfüllen kann ... Eine Rechtsschutzlücke für die betroffenen Personen ist daher nicht erkennbar ... Bezogen auf das Kredit-Scoring ergibt sich folgende Rechtslage: Die Vorschrift ist nicht nur anwendbar, wenn durch den Scorewert eine Kreditentscheidung vorgegeben wird, sondern auch, wenn der Scorewert maßgeblich in die Entscheidung mit einfließt und damit zu deren wesentlicher Grundlage wird.<sup>125</sup>[Fn.: Erfahrungen aus dem Bereich der Datenschutzaufsicht sprechen dafür, dass dem Scorewert nicht nur eine, sondern die entscheidende Rolle bei der Kreditvergabe und der Gestaltung der Kreditbedingungen zukommt. Dazu Korczak/Wilken, Scoring im Praxistest, S. 19; Abel RDV 2006, 108 (112 f.).] Eine ausschließlich automatisierte Entscheidung liegt danach vor, wenn der Kreditsachbearbeiter einen Kreditantrag allein aufgrund eines negativen Score-Ergebnisses ohne weitere Prüfung anhand zusätzlicher (eigener) Kriterien ablehnt.<sup>126</sup>[Fn.: Vgl. Gola/Heckmann/Schulz Art. 22 DS-GVO Rn. 14; Paal/Pauly/Martini Art. 22 DS-GVO Rn. 24; Kühling/Klar/Sackmann, DatenschutzR, Rn. 493; Horstmann/Dalmer, ZD 2022, 260 (262); zu § 6a BDSG a.F. bereits BGHZ 200, 38 Rn. 34; Möller/Florax, MMR 2002, 809; Plath/Kamlah, § 6a BDSG Rn. 12 f.; Gola/Schomerus, § 6a Rn. 6; Abel, RDV 2006, 108 (112 f.). EG 71 UAbs. 1 S. 1 nennt als Beispiel für eine automatisierte Einzelentscheidung ausdrücklich die „automatische Ablehnung eines Online-Kreditanspruchs.“] Dies ist etwa der Fall, wenn die Kreditvergaberichtlinien eines Instituts die Verweigerung eines Kredits vorsehen, ohne dem zuständigen Sachbearbeiter Beurteilungsspielräume für eine abweichende Entscheidung einzuräumen (z.B. Unterschreitung des sog. Cut-Off-Score<sup>127</sup>[Fn.: Dabei handelt es sich um den Grenz-Scorewert des höchsten Risikos, zu dem der Kreditgeber grds. noch bereit ist, einen Kredit zu vergeben. Der „Cut-off“ stellt in aller Regel dann auch die Arbeitsanweisung für den Sachbearbeiter dar, nicht anders zu entscheiden.]).<sup>128</sup>[Fn.: Vgl. Beckhusen, Der Datenumgang innerhalb des Kreditinformationssystems der SCHUFA, S. 267; BeckOK DatenschutzR/v. Lewinski Art. 22 DS-GVO Rn. 25. Zur vollautomatisierten Impfterminvergabe auf Basis eines Scorewertes Ruschemeier NVwZ 2021, 750 (752).] Dabei ist es unerheblich, ob die Scoreberechnung durch das Kreditinstitut – also die ent-

scheidende Stelle – selbst (internes Scoring) oder durch eine Wirtschaftsauskunftei (externes Scoring) erfolgt.<sup>129</sup>[Fn.: So auch Weichert, DuD 2005, 585; a.A. Taeger, RDV 2017, 3 (6); Paal/Pauly/Martini, Art. 22 DS-GVO Rn. 24. Zur Unterscheidung von internem und externem Scoring vgl. ULD, Scoringssysteme zur Beurteilung der Kreditwürdigkeit, S. 23 ff. m.w.N.] Allerdings geht der EuGH in diesen Fällen davon aus, dass beim externen Scoring bereits die Erstellung des Scorewertes durch die Auskunftei eine Entscheidung i.S.d. Art. 22 Abs. 1 darstellt, da das Handeln des Kreditinstituts maßgeblich von dem übermittelten Scorewert geleitet wird....<sup>130</sup>[Fn.: So EuGH – C 634/21, ECLI:EU:C:2023:957 Rn. 48, der davon ausgeht, dass ein unzureichender Scorewert „in nahezu allen Fällen“ zur Ablehnung des Kredits führt.] Kein Verstoß gegen die Vorschrift liegt hingegen vor, wenn im Falle drohender Ablehnung aufgrund eines schlechten Scorewertes frühzeitig eine oder mehrere weitere Personen durch den Sachbearbeiter hinzugezogen werden, die aufgrund entsprechender Entscheidungskompetenzen und Entscheidungsspielräume befugt und fachlich in der Lage sind, die automatisierte Vorgabe inhaltlich zu überprüfen und zu bewerten.<sup>131</sup>[Fn.: So ULD, Scoringssysteme zur Beurteilung der Kreditwürdigkeit, S. 87; Gola/Heckmann/Schulz, Art. 22 DS-GVO Rn. 15. Dass der Entscheidungsträger seinerseits an gewisse Vorgaben gebunden ist, ist unschädlich, solange diese nicht fest mit der automatisierten Einzelbewertung verknüpft sind.] Die Kompetenz, die automatisierte Entscheidung korrigieren zu dürfen, sollte dokumentiert werden. Maßgeblich ist aber auch hier, dass bei der geforderten individuellen Würdigung der Gesamtumstände im Hinblick auf die Zahlungswilligkeit und -fähigkeit außer dem Scorewert und den Kreditantragsdaten noch weitere Faktoren (z.B. Alter, Einkommen, Kundenhistorie) in die neue Entscheidung einfließen. Dabei ist es unschädlich, wenn diese Faktoren bereits bei der Scoreberechnung selbst berücksichtigt wurden.<sup>132</sup>[Fn.: Zur Diskussion insgesamt Abel, RDV 2006, 112 f.; Weichert, DuD 2006, 402 f.; LDI NW/Wuermeling, Living by Numbers 2005, 108 weist darauf hin, dass in der Praxis des SCHUFA-Verfahrens dem Sachbearbeiter neben dem Score auch der vollständige SCHUFA-Auszug und alle Daten zur Verfügung stehen, die die Bank selbst über den potenziellen Kreditnehmer bereithält. Iraschko-Luscher, DuD 2005, 471 f. betont in diesem Kontext zu Recht das Nachweisproblem und fordert eine gesetzliche Beweislastumkehr zulasten des Kreditunternehmens.] Es ist auch nicht erforderlich, dass alle Einzelheiten der Scorewertberechnung nachvollzogen werden.<sup>133</sup>[Fn.: So auch Sydow/Marsch/Helfrich, Art. 22 DS-GVO Rn. 47; Gola/Heckmann/Schulz, Art. 22 DS-GVO Rn. 15.] Insbes. beim externen Scoring wird dies schon praktisch kaum möglich sein. Der von einer Auskunftei an das Kreditinstitut übermittelte Scorewert wird vielmehr direkt automatisiert in andere Parameter des Kreditinstituts eingearbeitet. Der Sachbearbeiter wird nur noch mit dem Ergebnis „Kreditgewährung ja/nein“ konfrontiert, ohne die einzelnen, zu dem Scorewert führenden Berechnungen zu kennen und zu verstehen.“ (Hervorhebungen durch den Verfasser)

Blasek, ZD 2024, 258 (260): „Somit lässt sich argumentieren, dass ein Scorewert dann maßgeblich für die Entscheidung ist, wenn der Entscheidungsprozess so angelegt ist, dass ein bestimmter Scorewert zwangsläufig zur Ablehnung eines Kredits oder zur Versagung eines Neuvertrags (z.B. Handy-Vertrag) führt.“<sup>27</sup>[Fn.: Ähnl. Rohrmoser: „überbordende Rolle des Scores, die der Mensch nicht kippen kann“, abrufbar unter:

[https://www.lto.de/recht/meinung/m/eugh-schufa-verfahren-kommentar-prozessvertreter-mensch-gefahr-algorithmus/.](https://www.lto.de/recht/meinung/m/eugh-schufa-verfahren-kommentar-prozessvertreter-mensch-gefahr-algorithmus/) Denn in einem so definierten Entscheidungsprozess wäre ein Mensch lediglich formal eingebunden und die Gefahr, vor der Art. 22 DS-GVO schützen will, würde sich trotz menschlicher Beteiligung am Prozess realisieren. b) Maßgeblichkeit je nach Branche Für die Kreditwürdigkeitsprüfung von Verbraucherdarlehensverträgen enthalten §§ 505a, 505b BGB und § 18a KWG Anforderungen. Daraus ergibt sich, dass Grundlage der Prüfung Auskünfte des potenziellen Kreditnehmers und erforderlichenfalls solche von Auskunftgebern sein können. Gleichzeitig ist das Kreditinstitut verpflichtet, die Informationen in angemessener Weise zu überprüfen, was bei einem externen Scorewert kaum zu leisten sein dürfte. § 505b Abs. 1 BGB und § 18a Abs. 3 KWG sprechen zunächst dafür, dass Kreditgeber sich nicht allein auf die Aussagen Dritter verlassen, sondern sich eine breitere Informationsbasis schaffen. Darüber, ob und welche Informationen eine Bank in die Entscheidungsfindung einbezieht und wie die Informationen dann insgesamt gewichtet werden, sagen sie aber erst einmal nichts. Die Praxis der Banken wird hier je nach Qualität der und Vertrauen in die eigene Datenbasis unterschiedlich sein. Anfragen an einige Banken haben ergeben, dass diese in unterschiedlichem Maße SCHUFA-Auskünfte<sup>28</sup>[Fn.: Anfragen der Autorin an: Mittelbrandenburgische Sparkasse: nur Negativdaten; DKB: alles, was die SCHUFA anbietet (Negativ- oder Positivdaten, Scorewerte, Daten über bereits laufende Darlehen)] in ihre Prüfung einbeziehen, die SCHUFA-Scorewerte für die Kreditentscheidung allein aber nicht ausschlaggebend oder determinierend sind. Das heißt aber nicht, dass von Banken für die Entscheidung erforderlich gehaltene externe Scorewerte nicht das Zünglein an der Waage sein können. In anderen Branchen (z.B. Mobilfunk, Versandhandel) wird die Entscheidungsfindung deutlich stärker auf die SCHUFA-Scores zugeschnitten sein. Denn dort gibt es keine den §§ 505a, 505b BGB und § 18a KWG vergleichbaren Vorgaben hinsichtlich der Informations- und Entscheidungsgrundlage. Diese Anbieter treffen regelmäßig binnen Sekunden oder Minuten Entscheidungen basierend auf SCHUFA-Scorewerten, ohne andere Informationen über den potenziellen Kunden zu haben, die ein Urteil über dessen Zahlungsfähigkeit zulassen.“

Günther/Gerigk/Berger, NZA 2024, 234 (236): „Gleichwohl lassen sich aus der Entscheidung des EuGH nur bedingt Schlüsse für den KI-Einsatz im Betrieb ziehen. KI-Anwendungen bringen in der Arbeitswelt keineswegs nur Wahrscheinlichkeitswerte gleich einem SCHUFA-Score hervor. Während der Bankmitarbeiter, der über den Kreditantrag zu entscheiden hat, den antragstellenden Verbraucher oft gar nicht kennt und letztlich nur die eingereichten Unterlagen und den SCHUFA-Score als Entscheidungsgrundlage zur Verfügung hat, ist das Verhältnis zwischen Arbeitnehmer und Vorgesetzten ungleich weniger anonym. Der Vorgesetzte, der sich einer KI zur Genehmigung von Urlaubsanträgen, Beförderungen oder der Erteilung von Arbeitszeugnissen bedient, kennt seine Mitarbeiter in der Regel persönlich. Es ist deshalb weniger wahrscheinlich, dass der Vorgesetzte den KI-Vorschlägen blind vertraut und der KI in nahezu allen Fällen ungeprüft zustimmt. Richtigerweise ist daher in der arbeitsrechtlichen Praxis ein Einsatz von KI-Systemen in einem größeren Umfang möglich als in Fällen der Kreditvergabe. Für die menschliche Letztentscheidung ist ausreichend (aber auch notwendig), dass der Vorgesetzte die KI-generierten Resultate

überprüft, also etwa unplausible Entscheidungsvorschläge der KI herausfiltert und korrigiert.“<sup>25</sup>[Fn.: BeckOK DatenschutzR/v. Lewinski, 46. Ed. 1.11.2023, DS-GVO Art. 22 Rn. 25.1.] Die Kompetenz zu abweichenden Entscheidungen muss im Einzelfall allerdings, wie die Rechtsprechung des EuGH verdeutlicht, auch wahrgenommen werden, um sich nicht dem Vorwurf auszusetzen, dass das KI-System die spätere menschliche Entscheidung faktisch beherrsche.“ (Hervorhebungen durch den Verfasser)

Klein, BB 2024, 266 (267 f.): „Das Kriterium der Maßgeblichkeit bezieht sich nicht auf die Frage, ob eine Entscheidung automatisiert getroffen wird oder nicht, sondern dient der Verortung der Entscheidung im Sinne des Art. 22 DS-GVO. Damit die Score-Wert-Berechnung tatsächlich Entscheidungscharakter erhält, genügt es allerdings nicht, dass dieser Score-Wert abstrakt berechnet wird.“<sup>24</sup>[Fn.: Vgl. GA Pikamäe, Schlussanträge vom 16.3.2023 – C-634/21, Rn. 44, BB 2023, 706 Ls.] Erst der Umstand, dass der berechnete Wert an sich eine Entscheidung vorwegnimmt, qualifiziert ihn zu einer automatisierten Entscheidungsfindung.<sup>25</sup>[Fn.: Vgl. EuGH, 7.12.2023 – C-634/21, BB 2024, 270, Rn. 50.] Das führt zu der Frage, ob es dem EuGH überhaupt auf das Tatbestandsmerkmal der automatisierten Entscheidungsfindung ankommt, also den Prozess der Entscheidungsfindung ohne weiteres menschliches Dazwischentreten.<sup>26</sup>[Fn.: Kritisch bereits zu den Schlussanträgen insoweit Thüsing/Peisker/Musiol, RDV 2023, 82, 84.] Denn zu der Frage der Abläufe bei der weiteren Score-Wert-Verwendung musste der EuGH nach seiner Auffassung gar keine Stellung mehr beziehen: Wird der Score-Wert einmal berechnet, stellt dies die automatisierte Verarbeitung dar, die aufgrund ihrer Maßgeblichkeit für den Dritten dann zu einer automatisierten Entscheidungsfindung wird. Eine Trennung von Verarbeitung einerseits und Entscheidungsprozess andererseits ist nach Auffassung des EuGH wohl nicht geboten.“ (Hervorhebungen durch den Verfasser)

Kremer, CR 2024, 50 (57 f.): „Gerade zur Frage der „Maßgeblichkeit“ hat sich der EuGH aber nicht geäußert (s. II.). Denkbar sind hier zwei Konstellationen, die aus dem Verbot automatisierter Entscheidungen herausführen könnten: Gibt es den – entscheidungsbefugten und auch tatsächlich Entscheidungen treffenden – „human in the loop“ bei der Anwendung des KI-Systems, wäre die vorherige Ermittlung des Wahrscheinlichkeitswerts durch das KI-System vom Verbot des Art. 22 Abs. 1 DS-GVO ausgenommen. Ermittelt das KI-System mehrere unterschiedliche Wahrscheinlichkeitswerte, die sodann vom Anwender in ein Verhältnis zueinander gesetzt werden, um erst hieraus den relevanten, „finalen“ Wahrscheinlichkeitswert zu errechnen, gleich ob dies automatisiert oder menschlich geschieht, lässt dies die Kausalkette zwischen Erstermittlung der Wahrscheinlichkeitswerte und späterer Entscheidung brechen, so dass auch hier die Ermittlung der Wahrscheinlichkeitswerte durch das KI-System vom Verbot des Art. 22 Abs. 1 DS-GVO ausgenommen sein dürfte.“ (Hervorhebungen durch den Verfasser)

Langenbucher, BKR 2024, 66 (67): „In ersten Pressereaktionen hat die SCHUFA verlauten lassen, die von ihr befragten Kreditinstitute legten den SCHUFA-Score der eigenen Entscheidung über eine Kreditgewähr jedenfalls nicht „maßgeblich“ zugrunde. Das Urteil bedinge keine Verhaltensänderung, sofern einzelne Kreditinstitute nicht ausnahmsweise doch „maßgeblich“ auf den Score Bezug nehmen. Das steht in Widerspruch zu den beschriebenen Feststellungen des VG Wiesbaden, auf welche sich der EuGH berufen hatte. Künftige Kläger sind folglich mit

erheblicher Rechtsunsicherheit belastet: Für die nunmehr anstehende Folgeentscheidung des VG Wiesbaden empfiehlt sich eine deskriptiv-typologische Einordnung des Begriffs „maßgeblich“. Das vorliegende Gericht hat den Ausdruck verwendet, um die prominente Stellung des SCHUFA-Scores zu erläutern und, dies abstützend, auf Erfahrungen aus der behördlichen Datenschutzaufsicht verwiesen. Auf dieser Beschreibung setzt der EuGH auf, dem es genügt, dass der Wahrscheinlichkeitswert „die betroffene Person zumindest erheblich beeinträchtigt“ (Rn. 49). Dem lässt sich nicht etwa entgegenhalten, dass einzelne Banken neben dem SCHUFA-Score noch weitere Elemente berücksichtigen oder den Score nicht für „maßgeblich“ halten, etwa weil nach ihren internen Abläufen kein Automatismus zwischen Score und Kreditgewähr (oder -ablehnung) existiert. Hinzu kommt, dass die Bedeutung des SCHUFA-Scores über die Kreditgewährung durch Finanzinstitute hinausreicht und beispielsweise auch Mobilfunkunternehmen, Vermieter, mitunter sogar Arbeitgeber diesen anfragen. Das schließt nicht aus, dass sich im Laufe der Zeit Wettbewerber der SCHUFA ein so erhebliches Marktpotenzial erobert, dass der SCHUFA-Score „unmaßgeblich“ wird. Jedenfalls solange die SCHUFA in Deutschland eine herausragende, wenn nicht sogar monopolartige Stellung innehat, kann hiervon nicht ausgegangen werden.“

Paal/Hüger, MMR 2024, 540 (542 f.) „Grundsätzlich in den Anwendungsbereich des Art. 22 Abs. 1 DS-GVO fallen können sog. Vorschlagssysteme, die einem menschlichen Entscheidungsträger bereits einen konkreten Entscheidungsausgang nahelegen. Beispiele hierfür sind KI-Systeme, die i.R.d. Kredit Scorings eine konkrete Einstufung der Kreditwürdigkeit auf einer abschließenden Punkteskala<sup>16</sup>[Fn.: So die Konstellation in EuGH, MMR 2024, 153 m. Anm. Radtke = ZD 2024, 157 m. Anm. Söbbing/Schwarz und m. Anm. Schild.] oder i.R.d. Recruiting-Kontexts eine automatisierte Vorsortierung von Lebensläufen vornehmen.“<sup>17</sup>[Fn.: Zum KI-Einsatz im Recruiting-Kontext s. statt vieler Hoffmann, NZA 2022, 19; Höpfner/Daum, ZfA 2021, 467.] Für die Annahme eines maßgeblichen Beruhens einer menschlichen Entscheidung auf einem KI-basierten Vorschlag spricht in diesen Fällen eines konkreten KI-basierten Entscheidungsvorschlags insbesondere das als sog. Automatisierungsbias diskutierte sozio-technische Phänomen des besonderen Vertrauens des menschlichen Entscheidungsträgers in die Ausgabe von KI-Systemen, wobei dieses Vertrauen insbesondere durch die Intransparenz des KI-Systems sowie den potenziellen Rechtfertigungsdruck bei Abweichung von dem KI-generierten Vorschlag begünstigt wird.<sup>18</sup> [S. dazu Kolleck/Orwat, Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen, 2020, S. 27 ff.; s. exemplarisch die Untersuchung des Georgia Institute of Technology, bei welchem Versuchspersonen in einem bereits vernebelten Raum einem offenkundig fehleranfälligen Roboter folgten, statt eigenständig den Notausgang zu nutzen, Robinette/Allen/Howard/Wagner, Overtrust of robots in emergency evacuation scenarios, 11th ACM/IEEE International Conference on Human-Robot Interaction 2016, S. 101 ff.; so auch anerkannt als besonderer Gegenstand der erforderlichen menschlichen Aufsicht von Hochrisiko-KI-Systemen nach Art. 14 Abs. 4 KI-VO.] Gleichwohl wird auch in diesen Konstellationen die Maßgeblichkeit des Beruhens der Entscheidung auf dem KI-basierten Vorschlag im Einzelfall widerlegbar sein, wenn eine hinreichend konkrete Auseinandersetzung mit der rechtserheblichen Einzelfallentscheidung durch

einen menschlichen Entscheider sichergestellt ist.<sup>19</sup>[Fn.: Paal, ZfDR 2023, 114 (117) und Schild/Paal, PinG, 2024, 90 (91 f.) verweisen etwa im Kontext der Kreditvergabe auf die gesetzlich erforderliche Einzelfallprüfung nach § 18a KWG, §§ 505a, 505b BGB; EuGH, MMR 2024, 153 m. Anm. Radtke = ZD 2024, 157 m. Anm. Söbbing/Schwarz und m. Anm. Schild betonen die Unzulässigkeit von Banken nach § 25b Abs. 2 KWG, ihr Risikomanagement auf die SCHUFA auszulagern.] Demgegenüber keine Maßgeblichkeit des Beruhens begründen und folglich nicht in den Anwendungsbereich des Art. 22 DS-GVO fallen wird die bloße Nutzung von KI-basierten Assistenzsystemen, welche die menschliche Entscheidungsfindung durch die Aufbereitung, Analyse oder Visualisierung von Informationen lediglich vorbereitend unterstützen, ohne bereits einen hinreichend konkreten Entscheidungsvorschlag zu unterbreiten. In diese Kategorie einzuordnen wäre u.a. die wertungsfreie automatisierte Aufbereitung von Daten oder auch die Nutzung von großen Sprachmodellen wie etwa ChatGPT, um allgemeine Hintergrundinformationen für eine Entscheidung anzusammeln.“ (Hervorhebung durch den Verfasser).

Radtke, Anm. zu EuGH, Urt. v. 7.12.2023 – C-634/21, MMR 2024, 153 (156): „Allerdings legen die Ausführungen in Rn. 48 f. nun nahe, dass die Maßgeblichkeit vermutet werden kann, wenn ein unzureichender Score „in nahezu allen Fällen“ zu Grunde gelegt wird. Selbst wenn die Empfänger also gesetzlich zur Vornahme einer eigenen Prüfung verpflichtet sind, schließt dies nicht zwingend aus, dass der SCHUFA-Score maßgeblich, weil ein regelmäßig ausschlaggebender Faktor ist. Entscheidend ist somit die tatsächliche Bedeutung im Einzelfall. Jedenfalls außerhalb des engmaschig regulierten Bankensektors dürfte das Merkmal der Maßgeblichkeit hiernach oft erfüllt sein.“ (Hervorhebungen durch den Verfasser).

Ziegenhorn, CR 2024, 586 (589): „Unabhängig davon, wie man die Entscheidung des EuGH inhaltlich beurteilen möchte, kommt dieser nur eine geringe praktische Relevanz zu.“<sup>46</sup>[Fn.: So auch Marsch/Kratz, NJW 2024, 392, 393.] Denn der EuGH begrenzt diese Sonderkonstellation auf Fälle, in denen der Score eine „maßgebliche“ Rolle spielt. Diese Maßgeblichkeit ist nach ihm gegeben, wenn „ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen“ dazu führt, dass die Bank den beantragten Kredit ablehnt.<sup>47</sup>[Fn.: EuGH v. 7.12.2023 – C-634/21, ECLI:EU:C:2023:957 Rz. 48, CR 2024, 29 m. Anm. Kerkemeyer.] Dies wird im Kreditwesen bereits wegen den besonderen Anforderungen an die Kreditwürdigkeitsprüfung von Verbraucherdarlehensverträgen (§§ 505a, 505b BGB und § 18a KWG) für die Mehrheit der Fälle des externen Scorings zu Recht bezweifelt.<sup>48</sup>[Fn.: Blasek, ZD 2022, 433, 436; Paal, ZfDR 2023, 114, 131.] Unklar bleibt jedoch, inwiefern der Maßstab der „Maßgeblichkeit“ auf andere Branchen, in denen automatisierte Entscheidungen vorgenommen werden, zu übertragen ist und es damit zu einer Ausweitung des Anwendungsbereichs der judizierten Ausnahme kommen könnte.<sup>49</sup>[Fn.: Zur Bedeutung für KI-Anwendungen, Klein, BB 2024, 266, 268 f.; allgemein zu weiteren denkbaren Fallgestaltungen in anderen Bereichen Thüsing, CB 2024, 45, 50.] Hier wird eine weitere Konkretisierung des Merkmals der „Maßgeblichkeit“ durch die Rechtsprechung abzuwarten sein.<sup>50</sup>[Fn.: Marsch / Kratz, NJW 2024, 392, 393.]“ (Hervorhebungen durch den Verfasser)

Dies knüpft zum Teil an Überlegungen an, die das Schrifttum schon vor der Entscheidung des EuGH unternommen hat. Köhler fasst die Bandbreite dieser Stellungnahmen zusammen und ordnet sie:

„Bereits vor dem Urteil des EuGH zur SCHUFA herrschte weitgehend Einigkeit darüber, dass eine rein formale Zwischenschaltung eines Menschen in den Entscheidungsprozess nicht genügt, um die Anwendung des Art. 22 Abs. 1 DS-GVO auszuschließen.<sup>11</sup>[Fn.: Raji, *Künstliche Intelligenz im öffentlichen Sektor*, 2023, S. 207; Kögel, *ZdW* 2022, 205 (207).] Wird eine menschliche Instanz installiert, die die automatisierten Entscheidungen lediglich alibimäßig abnickt, wird den Gefahren, vor denen Art. 22 Abs. 1 DS-GVO schützen soll, nicht ausreichend begegnet.<sup>12</sup>[Fn.: Paal/Hüger, *MMR* 2024, 540 (541).] Der Mensch muss die Entscheidung stattdessen beeinflussen können.<sup>13</sup>[Fn.: Martini, *Blackbox Algorithmus*, 2019, S. 173.] Erforderlich sind daher zumindest eine eigene inhaltliche (Letzt-)Entscheidungskompetenz und ein eigener Beurteilungsspielraum.<sup>14</sup>[Fn.: Martini/Nink, *NVwZ-Extra* 10 (2017), 1 (3); Kumkar/Roth-Isigkeit, *JZ* 2020, 277 (279).] Der hier nach zum Ausschluss des Verbots mindestens erforderliche Einfluss des Menschen lässt sich mit Paal/Hüger treffend als formelle Hoheit bezeichnen.<sup>15</sup>[Fn.: Paal/Hüger, *MMR* 2024, 540 (542).] In welcher Form darüber hinaus eine materielle Hoheit erforderlich ist, wurde vor dem Urteil des EuGH dagegen nicht einheitlich beurteilt. Eine materielle Hoheit verlangt nach den in diesem Beitrag gewählten Begrifflichkeiten eine inhaltliche Auseinandersetzung der menschlichen Instanz mit dem im Einzelfall ausgegebenen Ergebnis des algorithmischen Systems. In Bezug auf Art. 22 Abs. 1 DS-GVO wurde teilweise vertreten, dass ein menschliches Dazwischentreten im Sinne einer Plausibilitätskontrolle genügt.<sup>16</sup>[Fn.: Kühling/Buchner/Buchner, Art. 22 DS-GVO Rn. 15; BeckOK DatenschutzR/v. Lewinski, Art. 22 DS-GVO Rn. 25.1.] Demnach sollte es für den Ausschluss von Art. 22 DS-GVO Abs. 1 ausreichen, wenn die menschliche Kontrollinstanz einzelne, nicht plausible Entscheidungen herausgreift und inhaltlich überprüft.<sup>17</sup>[Fn.: Kühling/Buchner/Buchner, Art. 22 DS-GVO Rn. 15.] Lediglich rein stichprobenhafte Kontrollen seien unzureichend.<sup>18</sup>[Fn.: Kühling/Buchner/Buchner, Art. 22 DS-GVO Rn. 15.] Andere forderten eine umfassende inhaltliche Auseinandersetzung in jedem Einzelfall.<sup>19</sup>[Fn.: Paal/Pauly/Martini, Art. 22 DS-GVO Rn. 19; Kumkar/Roth-Isigkeit, *JZ* 2020, 277 (279).] Wie eine solche konkret zu erfolgen hat, wurde dabei meist offengelassen. Regelmäßig wird nach dieser Ansicht allerdings erforderlich sein, dass der Mensch weitere Aspekte in die Entscheidung einbezieht.<sup>20</sup>[Fn.: v. Walter in Kaulartz/Braegelmann, *AI und Machine Learning-HdB* Kap. 8.4 Rn. 7.]“

Von ihm stammt auch die bislang ausführlichste Auseinandersetzung mit der hier diskutierten Frage. Er bietet zur Konkretisierung der Maßgeblichkeit ein Drei-Stufen-Modell an:<sup>21</sup>

„Der Ausschluss des in Art. 22 Abs. 1 DS-GVO enthaltenen Verbots der automatisierten Einzelentscheidung setzt die materielle Hoheit des Menschen voraus. Deren konkrete Ausgestaltung ist anhand eines differenzierenden Stufenmodells zu beurteilen:

Stufe	Voraussetzungen	Folgen
1	unwesentlicher Einfluss auf die Entscheidung	Dokumentation der Organisation des Einsatzes entsprechend Art. 6 Abs. 3 UAbs. 2 KI-VO
2	wesentlicher Einfluss auf die Entscheidung	Plausibilitätskontrolle im Einzelfall
3	wesentlicher Einfluss auf die Entscheidung und KI-System und hohes Schutzniveau des Art. 47 GRCh	inhaltliche Auseinandersetzung im Einzelfall durch Berücksichtigung weiterer Aspekte

Weiterführend sind vor allem die Ausführungen, die die KI-Systeme in den Kontext des EuGH-Urteils einbindet – eine Fragestellung, die bereits vorher aufgeworfen wurde.<sup>22</sup> Im hier diskutierten – beschränkteren Kontext reicht die Feststellung, dass auch nach seiner Ansicht eine Plausibilitätskontrolle genügt.

### 3. Erste Duftmarken der Instanzgerichte

Erste Entscheidungen der Instanzgerichte deuten auf einen weiten Anwendungsbereich. So geht das LG Bamberg davon aus, dass eine maßgebliche Leitung des Handelns der kreditgebenden Banken auch vorliegen kann, wenn deren Handeln neben dem Bonitätsscore durch weitere Faktoren bestimmt wird. Ein Indiz für die maßgebliche Leitung des Handelns der kreditgebenden Banken liege in der Zahlung eines Entgelts für die Übermittlung des Bonitätsscores:

„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 vom 7.12.2023 (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 vorgetragen, 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.“<sup>23</sup>

#### Ähnlich sieht es das LG Bayreuth, das sein Urteil ebenfalls mit prozeduralen Argumenten begründet:

„Was also drittens die Voraussetzung betrifft, dass die Entscheidung gegenüber der betroffenen Person „rechtliche Wirkung“ entfalten oder sie „in ähnlicher Weise erheblich“ beeinträchtigen muss, indem das Handeln des Kunden, dem der Wahrscheinlichkeitswert übermittelt wird, „maßgeblich“ von diesem Wert geleitet wird (EuGH, *NJW* 2024, 413 [415, Rn. 48, 50]), so

21 Köhler, *EuDIR* 2025, 16 Rn. 34.

22 Unmittelbar nach der Entscheidung des EuGH Thüsing, Das EuGH-Urteil wird zum Problem für KI, *LTO* v. 10.12.2023, abrufbar unter <https://www.lto.de/recht/meinung/m/eugh-c63421-schufa-scoring-folgen-ki-automatisierte-verarbeitung-kreditauskunft>.

23 LG Bamberg, *Urt.* v. 26.3.2025 – 41 O 749/24, *GRUR-RS* 2025, 7269 Rn. 28.

kann aus dem Umstand, dass die Kunden die kostenpflichtigen Dienste der Beklagten in Anspruch nehmen bzw. nach der erteilten Auskunft konkret in Anspruch genommen haben, die widerlegliche Vermutung aufgestellt werden, dass dies der Fall ist. Die Beklagte ist allgemein bekannt nicht eine Auskunftfei unter Vielen. Im Gegenteil trägt sie selbst ihre zentrale Rolle als Zusammenschluss von Unternehmen der Kreditwirtschaft vor. Der Beklagtenvortrag im Schriftsatz vom 15.4.2025 ist nicht geeignet, die Vermutung zu widerlegen, es ist nicht nachvollziehbar, dass die Tätigkeit der Beklagten für ihre Kunden als irrelevant bzw. unmaßgeblich dargestellt wird. Es besteht auch kein Anlass zum Wiedereintritt in die mündliche Verhandlung, nachdem die Beklagte Beweismittel für eine andere Entscheidungsfindung ihrer Kunden gerade nicht anbietet. Jedenfalls bei einem schlechten Score kann sich die Beklagte auch nicht darauf zurückziehen, dass der Kläger erst nachweisen müsse, dass ein Kunde aufgrund des mitgeteilten Score ohne weitere Überprüfung ein Geschäft mit dem Kläger abgelehnt habe. Aus dem Inhalt der vorgelegten Auskünfte (Anlage K1/B2) spricht dafür der Beweis des ersten Anscheins. Insbesondere im weitgehend automatisierten Betrieb von Massengeschäften wäre es höchst ungewöhnlich, eine ablehnende Entscheidung über die nachteilige S. -Auskunft hinaus noch einmal individuell zu überprüfen. Nur bei darüber hinausgehenden Kreditentscheidungen von erheblichem Gewicht dürfte es üblich sein, selbst eine positive S. -Auskunft nur als ein Kriterium unter mehreren zu betrachten. Das ist hier aber nicht streitgegenständlich.<sup>24</sup>

#### 4. Ordnung der Argumente

Wer sich um eine Ordnung der Argumente bemüht, der muss schrittweise vorgehen. Es ist offensichtlich: Angesichts der nur spärlichen Hinweise des EuGH muss seine Argumentation fortgedacht und konkretisiert werden. Die Schwierigkeit besteht jedoch darin, ihm nicht eigene Vorstellungen gleichsam „in den Mund zu legen“.

##### a) Der Wortsinn hilft nicht allzu viel weiter

In der Tat: Der Wortsinn hilft nicht allzu viel weiter. Zu vage ist der Begriff. Aber etwas Erkenntnis kann man doch hieraus ableiten: Maßgeblich ist mehr als eine Mitursächlichkeit. Ein *conditio sine qua non*-Zusammenhang reicht nicht. Auf der anderen Seite bedeutet maßgeblich etwas anderes als z.B. ausschlaggebend: Wenn ein Enkel seinen Großvater seit Jahren nicht mehr besucht hat und auch nicht zu seinem 80. Geburtstag erscheint, und der Großvater daraufhin den Enkel enterbt, dann ist das Nichterscheinen zum 80. Geburtstag der ausschlaggebende Grund gewesen. Maßgeblich für die Entscheidung der Enterbung war aber das jahrelange Nichtbesuchen davor.

##### b) Systematische Überlegungen

Auch die Systematik hilft nur bedingt weiter, da der Begriff „maßgeblich“ an keiner Stelle in der DS-GVO verwendet wird. Der Begriff kommt zwar zuweilen in anderen Gesetzen vor, wie etwa in Art. 23 Abs. 5 S. 2 GG, wonach bei Angelegenheiten der Europäischen Union, die im Schwerpunkt die Gesetzgebungsbefugnisse der Länder betreffen, „bei der Willensbildung des Bundes insoweit die Auffassung des Bundesrates maßgeblich zu berücksichtigen [ist]“.<sup>25</sup> Unter dem Begriff

„maßgeblich“ wird in diesem Zusammenhang verstanden, „dass die Bundesregierung sich bei ihrer Entscheidungsbildung von der Stellungnahme leiten lassen muss“.<sup>26</sup> Was das konkret bedeutet und ob damit eine Bindungswirkung, also ein Letztentscheidungsrecht des Bundesrats, einhergeht, ist umstritten.<sup>27</sup> Das Beispiel hat nichts mit dem Kontext hier und erst recht nicht mit europarechtskonformer Auslegung zu tun. Es zeigt aber, dass der Begriff „maßgeblich“ auch in anderen Kontexten unscharf ist und sich kaum für juristisch präzise Abgrenzungen eignet – eben darin liegt die Herausforderung.

##### c) Eine teleologische Interpretation, orientiert am *effet utile*

Es kommt damit also entscheidend auf den Sinn und Zweck des Art. 22 DS-GVO an. Ziel ist es, betroffene Personen vor sie beschwerenden Entscheidungen zu schützen, die ausschließlich auf einer automatisierten Verarbeitung beruhen. Die Letztentscheidungsbefugnis muss bei einer natürlichen Person liegen.<sup>28</sup> Das durch den EuGH neu eingeführte Merkmal der Maßgeblichkeit soll verhindern, dass ein Mensch das Ergebnis eines automatisiert erstellten Scores lediglich abnickt und keine weitere Auseinandersetzung stattfindet. Daraus folgt, dass starre Kriterien oder Grenzen, die allein vom Score abhängen und nicht von einem Menschen überstimmt werden können, für eine maßgebliche Beeinflussung sprechen.

##### d) Beispiele maßgeblicher und nicht-maßgeblicher Beeinflussung

Eine „maßgebliche“ Beeinflussung ist damit insbesondere dann anzunehmen, wenn der Verwender des Scores die Entscheidung allein vom Score abhängig macht. Dies ist etwa der Fall, wenn der Verwender ausschließlich den Score über die Bonität der betroffenen Person einholt und keine weiteren Informationen erhebt. In diesem Fall ist der Score alleinentscheidend, dann muss er erst recht maßgeblich sein. Darüber hinaus hängt eine Entscheidung auch dann maßgeblich vom Score ab, wenn der Verwender zwar auch weitere Informationen erhebt, vorher aber einen Mindestscore („Cut-Off-Score“) festlegt, bei dessen Unterschreiten die Entscheidung automatisch negativ ausfällt (z.B. wird bei einem Score von unter 80 % der Antrag der betroffenen Personen automatisch abgelehnt). Denn dann stellt der Score ein „KO-Kriterium“ für die Entscheidung dar.

Keine „maßgebliche“ Beeinflussung liegt hingegen vor, wenn der Score abgefragt wird sowie weitere Informationen erhoben werden und diese offen für die Kompensation eines negativen Scores sind, d.h. es muss die reale Möglichkeit bestehen, dass der Score durch die weiteren Informationen aufgewogen werden kann, auch wenn er es am Ende dann eben nicht wird. Ein Beispiel: Ein Gehaltsnachweis, der ein hohes monatliches Einkommen ausweist, ist grundsätzlich dazu geeignet, etwaige Defizite bei einem Score über die Bonität zu kompensieren. Die Entscheidung darüber, ob das Einkommen den negativen Score tatsächlich aufwiegt, ist eine Frage des Einzelfalles und obliegt dem Verwender des Scores. Dies setzt eine menschliche Auseinandersetzung mit dem abge-

24 LG Bayreuth, Urt. v. 29.4.2025 – 31 O 593/24, GRUR-RS 2025, 13866 Rn. 34 f.

25 Hervorhebung durch den Verfasser.

26 BeckOK GG/Heintschel von Heinegg/Frau, 61. Ed. 15.3.2025, GG Art. 23 Rn. 46.

27 S. hierzu Sodan/Schmahl, 5. Aufl. 2024, GG Art. 23 Rn. 49 m.w.N.

28 Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 22 Rn. 1.

fragten Score und den weiteren Informationen voraus, mit der Folge, dass keine automatisierte Einzelentscheidung i.S.d. Art. 22 DS-GVO vorliegt.

Die § 505b BGB, § 18a KWG zeigen, dass im Kreditwesen neben dem Score auch weitere Informationen über die Zahlungsfähigkeit des Antragstellers einzuholen sind. Das folgt auch aus den Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin, die sich an alle Kreditinstitute und Finanzdienstleistungsinstitute in Deutschland richtet. Dort heißt es:

*MaRisk BTO 1.2 Tz. 4: „Die Verwendung externer Bonitätseinschätzungen enthebt das Institut nicht von seiner Verpflichtung, sich ein Urteil über das Adressenausfallrisiko zu bilden und dabei eigene Erkenntnisse und Informationen in die Kreditentscheidung einfließen zu lassen.“<sup>29</sup>*

Daraus folgt, dass der Bonitätsscore im Kreditwesen schon rechtlich nicht maßgeblich sein darf. Der Kreditgeber muss eigene Erkenntnisse und Informationen in die Entscheidung über die Kreditvergabe einfließen lassen, in dem er diese weiteren Informationen selbst erhebt. Ob der Kreditgeber dies auch tatsächlich macht, ist keine Rechtsfrage, sondern eine Tatfrage.<sup>30</sup>

Wie hoch der Entscheidungsanteil des Scores sein muss, um eine maßgebliche Beeinflussung anzunehmen, lässt sich nicht anhand einer mathematisch berechneten Zahl quantifizieren. Ziel des Art. 22 Abs. 1 DS-GVO ist es, wie bereits angesprochen, dass eine für die betroffene Person belastende Entscheidung nicht ausschließlich von einer Maschine getroffen wird; der Mensch soll darüber entscheiden. Es muss daher eine reale menschliche Auseinandersetzung erfolgen, nur dann kann auch die Entscheidung dem Menschen zugerechnet werden. Eine pro-forma Kontrolle, bei der ein Mensch lediglich als Sachbearbeiter die Entscheidung abnickt und somit ausnahmslos dem Score folgt, genügt nicht diesen Anforderungen. Werden aber neben dem Bonitätsscore weitere Informationen, wie ein Gehaltsnachweis oder mögliche Sicherheiten abgefragt, und diese auch tatsächlich bewertet, findet eine menschliche Auseinandersetzung statt. Der Umstand, dass ein Score eingeholt wird, führt damit allein noch nicht zu einer maßgeblichen Beeinflussung.

#### IV. Zur Frage der Beweislast – Grenzen und Möglichkeiten des Anscheinsbeweises

Der EuGH hat in der Rs. C-634/21 klargestellt, dass es Aufgabe der nationalen Gerichte sei, zu beurteilen, ob die Entscheidung über die Begründung eines Vertragsverhältnisses maßgeblich vom Bonitätsscore abhängt.<sup>31</sup> Demzufolge ist das jeweilige nationale Prozessrecht auf die Frage, ob eine maßgebliche Beeinflussung vorliegt, anzuwenden. Das LG Bayreuth stellte hinsichtlich der Maßgeblichkeit eine widerlegliche Vermutung auf:

*„Was also drittens die Voraussetzung betrifft, dass die Entscheidung gegenüber der betroffenen Person „rechtliche Wirkung“ entfalten oder sie „in ähnlicher Weise erheblich“ beeinträchtigen muss, indem das Handeln des Kunden, dem der Wahrscheinlichkeitswert übermittelt wird, „maßgeblich“ von diesem Wert geleitet wird (EuGH, NJW 2024, 413 [415, Rn. 48, 50]), so kann aus dem Umstand, dass die Kunden die kostenpflichtigen Dienste der Beklagten in Anspruch nehmen bzw. nach der erteilten Auskunft konkret in Anspruch genommen haben, die widerlegliche Vermutung*

*aufgestellt werden, dass dies der Fall ist. Die Beklagte ist allgemein bekannt nicht eine Auskunftsei unter Vielen. Im Gegenteil trägt sie selbst ihre zentrale Rolle als Zusammenschluss von Unternehmen der Kreditwirtschaft vor. Der Beklagtenvortrag im Schriftsatz vom 15.4.2025 ist nicht geeignet, die Vermutung zu widerlegen, es ist nicht nachvollziehbar, dass die Tätigkeit der Beklagten für ihre Kunden als irrelevant bzw. unmaßgeblich dargestellt wird. Es besteht auch kein Anlass zum Wiedereintritt in die mündliche Verhandlung, nachdem die Beklagte Beweismittel für eine andere Entscheidungsfindung ihrer Kunden gerade nicht anbietet.*

*Jedenfalls bei einem schlechten Score kann sich die Beklagte auch nicht darauf zurückziehen, dass der Kläger erst nachweisen müsse, dass ein Kunde aufgrund des mitgeteilten Score ohne weitere Überprüfung ein Geschäft mit dem Kläger abgelehnt habe. Aus dem Inhalt der vorgelegten Auskünfte (Anlage K1/B2) spricht dafür der Beweis des ersten Anscheins. Insbesondere im weitgehend automatisierten Betrieb von Massengeschäften wäre es höchst ungewöhnlich, eine ablehnende Entscheidung über die nachteilige S. -Auskunft hinaus noch einmal individuell zu überprüfen. Nur bei darüber hinausgehenden Kreditentscheidungen von erheblichem Gewicht dürfte es üblich sein, selbst eine positive S. -Auskunft nur als ein Kriterium unter mehreren zu betrachten. Das ist hier aber nicht streitgegenständlich.“<sup>32</sup>*

Die Annahme eines Anscheinsbeweises überrascht. Denn „Voraussetzung seiner Anwendung ist ein sog. typischer Geschehensablauf, also ein sich aus der Lebenserfahrung bestätigender gleichförmiger Vorgang, durch dessen Typizität es sich erübrigt, die tatsächlichen Einzelumstände eines bestimmten historischen Geschehens nachzuweisen.“<sup>33</sup> Aus dem Umstand, dass der Verwender für die Einholung des Scores zahlt, eine maßgebliche Beeinflussung anzunehmen, führt zu weit. Folge wäre, dass jeder genutzte Score automatisch als maßgeblich anzusehen wäre. Der BGH hat jedoch in einer früheren Entscheidung Zurückhaltung bei der Anwendung des Anscheinsbeweises angemahnt, weil er es erlaubt, bei typischen Geschehensabläufen auf Grund allgemeiner Erfahrungssätze auf einen ursächlichen Zusammenhang oder ein schuldhaftes Verhalten zu schließen, ohne dass im konkreten Fall die Ursache bzw. das Verschulden festgestellt ist.<sup>34</sup> Wenn der Verwender einen Score einholt und dafür zahlt, ist es denkbar, einen Anscheinsbeweis dahingehend anzunehmen, dass der Score in die Entscheidung mit einfließt – niemand kauft einen Score, den er nicht nutzen will. In welchem Ausmaß der Score die Entscheidung beeinflusst, ist eine Frage des Einzelfalles. Dafür gibt es schlicht keinen Erfahrungssatz – erst recht keinen, der aus dem bloßen Umstand der Entgeltlichkeit des Scores hergeleitet werden kann.

#### V. Eine Vorlage an den EuGH scheint unumgänglich

Es hat sich gezeigt: Der vom EuGH neu eingeführte Begriff der Maßgeblichkeit wirft Fragen auf, die sich gegenwärtig

<sup>29</sup> Rundsreiben 06/2024 (BA) vom 29.5.2025 – MaRisk, abrufbar unter: [https://www.bafin.de/SharedDocs/Downloads/DE/Rundschriften/dl\\_rs\\_06\\_2024\\_MaRisk\\_pdf\\_BA.html](https://www.bafin.de/SharedDocs/Downloads/DE/Rundschriften/dl_rs_06_2024_MaRisk_pdf_BA.html).

<sup>30</sup> Vgl. zur Abgrenzung zwischen Rechts- und Tatfragen, Stein/Jonas/Jacobs, 23. Aufl. 2018, ZPO § 546 Rn. 3 ff.

<sup>31</sup> EuGH, Ur. v. 7.12.2023 – C-634/21, GRUR-RS 2023, 34905 Rn. 48.

<sup>32</sup> LG Bamberg, Ur. v. 26.3.2025 – 41 O 749/24, GRUR-RS 2025, 7269 Rn. 34 f.

<sup>33</sup> MüKoZPO/Prütting, 7. Aufl. 2025, ZPO § 286 Rn. 50.

<sup>34</sup> BGH, Ur. v. 13.12.2011 – VI ZR 177/10, NJW 2012, 608 Rn. 11.

nicht abschließend – und vor allem nicht rechtsverbindlich – klären lassen. Dass der Gerichtshof es versäumt hat, den Begriff zu konkretisieren und mit Leben zu füllen, ist misslich. Angesichts der Rechtsunsicherheit, die der unbestimmte Rechtsbegriff mit sich bringt, scheint daher eine Vorlage an den EuGH unumgänglich zu sein. Denn auszulegen ist hier, was der EuGH eigentlich meint; das kann nicht das nationale Gericht. Dieses ist nur dazu berufen, die Obersätze des EuGH auf das nationale Recht und den nationalen Sachverhalt anzuwenden, nicht aber den Sinn der Obersätze zu ergründen und zu deuten.<sup>35</sup> Solch ein dialogisches Vorgehen zwischen nationalem Gericht und EuGH hat durchaus Vorbilder – insb. dort, wo die Vorgaben des EuGH allzu sperrig, systemwidrig und dunkel waren. Auf die Entscheidung *Alemo-Herron* folgte die Vorlage *Asklepios* (mit einem ganz anderen Ergebnis)<sup>36</sup>, auf die Vorlage *Schultz-Hoff* folgte *KHS*<sup>37</sup>, oder gerade auch im Datenschutz: Auf die Ausführungen des EuGH insb. in der Entscheidung vom 4.5.2023<sup>38</sup> folgte jüngst die Vorlage des BGH vom 6.5.2025.<sup>39</sup> Wenn Antworten des EuGH weitere Fragen provozieren, dann müssen sie gestellt werden.

## VI. Was bleibt

Ob und wann es zu einer Konkretisierung durch den EuGH kommt, ist unklar. Bis dahin braucht es Kriterien, an denen sich die Praxis orientieren kann. Nach dem oben gesagten, ist eine maßgebliche Beeinflussung dann anzunehmen, wenn der Score ein „KO-Kriterium“ darstellt, d.h.

1. wenn allein der Score eingeholt wird und nur auf dieser Grundlage die Entscheidung getroffen wird. In diesem Fall ist der Score alleinentscheidend, da es gar keine weiteren Kriterien gibt, die überhaupt Berücksichtigung finden könnten. Beispiel hierfür wäre ein Vermieter, der von potenziellen Mietern lediglich eine Bonitätsauskunft verlangt und ausschließlich auf dieser Grundlage entscheidet, ob er sie zu einer Besichtigung einlädt oder nicht.
2. oder wenn neben dem Score zwar weitere Informationen erhoben werden, vorher aber ein Mindestscore („Cut-Off-Score“) festgelegt wurde, bei dessen Unterschreiten die Entscheidung automatisch negativ ausfällt. Setzt eine Bank für die Kreditvergabe bspw. einen Mindestscore von 80 % voraus, mit der Folge, dass Antragsteller mit einem niedrigeren Score automatisch abgelehnt werden, liegt eine maßgebliche Beeinflussung vor. Eine pro-forma Kontrolle durch einen Menschen, der die Entscheidung lediglich abnickt, ändert hieran nichts, da keine inhaltliche Auseinandersetzung durch einen Menschen erfolgt.

Keine maßgebliche Beeinflussung liegt vor, sofern neben dem Score weitere Informationen erhoben werden und diese offen für die Kompensation eines negativen Scores sind, d.h. es muss die reale Möglichkeit bestehen, dass der Score durch die weiteren Informationen aufgewogen werden kann. Dies setzt eine menschliche Auseinandersetzung mit dem abgefragten Score und den weiteren Informationen voraus, mit der Folge, dass keine automatisierte Einzelentscheidung vorliegt. Diese Auslegung entspricht dem Sinn und Zweck des Art. 22 DS-GVO.

Der Umstand, dass ein Score abgefragt wird und der Verwender für diesen bezahlt, kann allein nicht die Vermutung begründen, dass der Score die Entscheidung maßgeblich beeinflusst. Aus der Entgeltlichkeit des Scores kann allenfalls der Schluss gezogen werden, dass er in die Entscheidung mit einfließt. Ob der Score die Entscheidung maßgeblich beeinflusst oder nicht, kann nach den oben genannten Kriterien beurteilt werden.

Verpflichtet sich der Verwender eines Scores, diesen nicht maßgeblich zu benutzen, dann hört hier die Verantwortlichkeit des Verantwortlichen aus. Die Zurechnungskette wird unterbrochen. Die Scoreerstellung kann keine Entscheidung i.S.d. Art. 22 DS-GVO sein, wenn der Scoreersteller die nachfolgende, ja dann pflichtwidrige Verwendung des Scores zwar nicht verhindert (und ggf. auch gar nicht verhindern kann), aber eben auch nicht gebilligt hat. Das Verhalten des Scorenutzers kann ihm nicht zu gerechnet werden – insoweit ist er nicht Verantwortlicher.



### Prof. Dr. Gregor Thüsing

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.

35 S. Thüsing, BB 2024, Editorial, Heft 16, I.

36 EuGH, Urt. v. 18.7.2013 – C-426/11, BeckRS 2013, 81519; Urt. v. 27.4.2017 – C-680/15, C-681/15, BeckRS 2017, 108049.

37 EuGH, Urt. v. 20.1.2009 – C-350/06, C-520/06, BeckRS 2009, 70077; Urt. v. 22.11.2011 – C-214/10, BeckRS 2011, 81665.

38 EuGH, Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972.

39 BGH, Beschl. v. 6.5.2025 – VI ZR 53/23, GRUR-RS 2025, 13267.

Prof. Dr. Petra Gehring/Dr. Christian Person

# Rechtsformwahl: eine Herausforderung für Datentreuhänder

Mit der Idee der Datentreuhand verbinden sich große Hoffnungen, bestehende Hürden des Datenteilens zu überwinden und den Datenaustausch zwischen Individuen und Organisationen zu intensivieren. Das durch den Data Governance Act der EU im Entstehen begriffene, neuartige Regulierungsregime für neue Datenintermediäre schafft hierfür ein innovatives Experimentierfeld. Aktuell versuchen sich zahlreiche Initiativen an der Entwicklung funktionsfähiger Datentreuhänder, was sich an einer eindrucksvollen Vielfalt an Modellen und Betreiberkonstellationen beobachten lässt. Eine zentrale Herausforderung für die nachhaltige Etablierung von Datentreuhändern stellt die Frage der rechtlichen Eigenständigkeit und der gesellschaftsrechtlichen Ausgestaltung dieser Entitäten dar. Der Artikel beleuchtet dies näher und bilanziert auch, dass es jenseits des DGA einer Diskussion über Governance und Geschäftsmodelle für Datentreuhänder bedarf.

## I. Zum Stand der Diskussion über die Datentreuhand

Nachdem Anfang der 2020er Jahre eine zunächst rechtswissenschaftlich geprägte Forschungsdiskussion das Thema Datentreuhand aufgebracht hatte,<sup>1</sup> kann man heute von einem interdisziplinären Experimentierfeld sprechen, das auch durch Projektentwicklungen gekennzeichnet ist. Maßgeblich hierfür waren Initiativen, die auf den Data Governance Act (DGA) der EU reagierten, sowie mehrere Förderinitiativen des Bundes, die an der Schnittstelle von Wissenschaft und Wirtschaft auf eine Intensivierung des Datenteilens abzielten. Der Begriff Datentreuhand als Konkretisierung der Rede von new intermediaries im DGA bleibt zwar durchaus unbestimmt. Er steht aber für Vieles, was „Plattformen“ aus heutiger Sicht gerade nicht zu bieten haben: Marktneutralität, Sicherheit, Vertrauenswürdigkeit, Nachhaltigkeit. Dass ein Datentreuhänder seine Vermittlungsleistung jedenfalls ohne Interesse an den Daten selbst zu erbringen hat, macht den Ausdruck auch symbolisch attraktiv. So wurde ein im geplanten Forschungsdatengesetz vorgesehenes „Deutsches Mikrodatenzentrum“, eigentlich wohl nur eine Schnittstelle, die Daten aus Forschungsdatenzentren (FDZ) zugänglich machen soll, als Datentreuhänder bezeichnet.<sup>2</sup>

Die Idee Datentreuhand „boomt“, kann man mit Blick auf die letzten Jahre sagen – wenngleich sich die Wege zu einem stabilen Lagebild mit einer erfolgreichen Etablierung solcher neuer Intermediäre als langwierig erweisen.<sup>3</sup> Inzwischen ist die Vielfalt und Vielzahl der Ansätze schwer überschaubar. Für unterschiedliche Leistungsmerkmale im Rahmen unterschiedlicher Akteurskonstellationen und Datendomänen werden unterschiedliche Datentreuhandmodelle entworfen – wobei sich alle des Ausdrucks Datentreuhand bedienen. Für die Orientierung aller Beteiligten ist diese inflationäre Verwendung des Terminus technicus sicher nicht nur hilfreich.<sup>4</sup>

Typisierungsversuche in Sachen Datentreuhandmodelle kann man am Schutzbedarf der Daten festmachen, an der Frage der Gemeinwohl- oder Profitorientierung, an Datendomänen, auf die ihre Dienste zugeschnitten sind, oder an existierenden gesellschaftlichen Sektoren (mit Paradigmen wie: medizinische Datentreuhandstellen, sozialwissenschaftliche FDZ, brancheneigene Treuhandkonstrukte für Mobilitätsdaten) oder man kann Datentreuhänder klassisch gemäß des Vektors zwischen Anbieter und Kunden typisieren – also: „B2B“, „B2C“, „G2B“, „G2C“ etc. Ein früher Kandidat für prototypische Treuhandfunktionen waren auch die Personal Information Management Systems (PIMS); hier ging es um eine Art

Wallet für persönliche Daten (Gesundheit, Sport etc.), die eine App mit einem Einwilligungsmanagement zu Zwecken der Datenspende oder des Datenverkaufs versieht. Die Rede von der Datentreuhand changiert also, gerade auch weil der Begriff so attraktiv ist, und die Typisierung der Modelle<sup>5</sup> ist work in progress. Sie läuft den realen Entwicklungen ein Stück weit hinterher. Mit Blick aufs Recht ist zudem zu vermerken, dass „Datentreuhand“ – ungeachtet der rechtlichen Prägung des Konzepts Treuhand und der Einschlägigkeit des DGA – nicht unbedingt als reiner Rechtsbegriff wahrgenommen wird. Eher schon handelt es sich um eine Art Projekttitel, der auf technische, die Leistung der Datenvermittlung und die Governance betreffende sowie letztlich marktliche Innovationen hinausläuft. Aber auch die Vorstellung einer mit dem Zweck der Datenvermittlung verbundenen Aufbewahrung von Daten schwingt – vielleicht sogar fälschlicherweise<sup>6</sup> – mit.

Vor diesem Hintergrund möchten wir im Folgenden eine aus dem noch laufenden Versuch einer möglichst breiten Befragung aller derzeit in Deutschland laufenden Datentreuhandprojekte<sup>7</sup> gewonnene Wissensbasis zu einer Zwischenbilanz nutzen. Im Fokus stehen das Thema der rechtlichen Selbstständigkeit und das Problem der Rechtsformenwahl, mit welcher Datentreuhandprojekte – also Datentreuhänder-im-Werden – konfrontiert sind. In der Frage der geeigneten Rechtsform spiegeln sich sowohl die Schwierigkeiten, den durch den DGA skizzierten neuen Akteur tatsächlich am Markt zu verankern wie auch wichtige rechtliche und die Governance betreffende Aspekte von so etwas wie einem jeweils gewählten Datentreuhand-„Modell“.

1 Pertot/Wendehorst/Schwamberger/Grinzinger, Rechte an Daten, 2020, S. 103; Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne MMR-Beil. 2021, 25; Specht-Riemenschneider/Kerber, Designing Data Trustees, 2020, abrufbar unter <https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf> [9.1.2026].

2 Wir beziehen uns hier auf 2023/24 kursierende Vorfassungen; zu einem Referentenentwurf für ein Forschungsdatengesetz kam es aufgrund des vorzeitigen Endes der Ampel-Regierung nicht.

3 Gehring, Datentreuhänder – dauern Wunder etwas länger?, FAZ vom 11.3.2024, abrufbar unter <https://www.faz.net/aktuell/wirtschaft/datentreuhaender-dauern-wunder-etwas-laenger-19576785.html> [9.1.2026].

4 Gehring, Datentreuhänder – eine unterschätzte Chance?, FAZ vom 21.10.2024, abrufbar unter <https://www.faz.net/aktuell/wirtschaft/unternehmen/petra-gehring-zum-digitalgipfel-datentreuhaender-eine-unterschaetzte-chance-110044062.html> [9.1.2026].

5 Vgl. Buchheim/Möslein/Omlor/Gehring/Laakmann/Person/Seidemann, Handbuch Datentreuhand, 2025, S. 9.

6 Der DGA jedenfalls sieht den Fall einer bloßen Bereitstellung eigener Daten nicht als Vermittlung an.

7 Die empirische Grundlage entstammt dem BMFTR<sup>1</sup> Projekt „ReFo\_Dat – Rechtsformen für Datentreuhänder“, vgl. <https://zevedi.de/themen/refo-dat/> [9.1.2026].

## II. Keineswegs selbstverständlich: die rechtliche Eigenständigkeit

Festzuhalten ist als eine erste Einsicht unserer empirischen Erhebungen, dass Datentreuhänder – ob sie bereits existieren oder projektiert sind – nicht per se eine rechtliche Selbstständigkeit für erstrebenswert erachten. Von den 23 Datentreuhandprojekten, die von uns bisher (Stand März 2025) befragt wurden, strebt lediglich etwas mehr als die Hälfte (13) eine rechtliche Eigenständigkeit an. Weitere 3 Projekte zeigen sich hierfür zwar grundsätzlich offen, sind jedoch noch unentschieden, ob dies zu ihren operativen Belangen passt. Für 4 Projekte ist die Ausformung einer rechtlich selbstständigen Entität keine realistische Handlungsoption.<sup>8</sup>

Dieser Befund mag überraschen – oder auch nicht, schließlich existieren sowohl gewichtige Argumente, die für eine rechtliche Selbstständigkeit sprechen, als auch relevante Einwände dagegen. Nicht zuletzt der DGA selbst scheint den Akteuren eigentlich eine rechtliche Selbstständigkeit nahezulegen, wenn nicht gar zwingend vorzuschreiben: so statuiert Art.12 lit. a) DGA, dass sogenannte Datenvermittlungsdienste durch eine gesonderte juristische Person zu erbringen sind.<sup>9</sup> Die meisten der aktuell diskutierten Datentreuhandmodelle dürften sich problemlos unter die in Art. 10 DGA festgelegte Definition von Datenvermittlungsdiensten subsumieren lassen.<sup>10</sup> In der Terminologie der EU-Legislation handelt es sich bei Datentreuhändern somit jedenfalls potenziell um Datenvermittlungsdienste, die sowohl anmeldepflichtig sind als auch der Haftung fähig sein sollen. Mehr noch als die Haftbarkeit dürften es aber die Unabhängigkeit und das Gebot der (Markt-)Neutralität sein, an welche der europäische Gesetzgeber gedacht haben mag, als er die rechtliche Eigenständigkeit von Datenvermittlungsdiensten normierte.<sup>11</sup>

### 1. Gründe für fehlendes Interesse

Real existierende Datentreuhandprojekte sind in Deutschland gleichwohl häufig anders aufgestellt – sie werden nämlich als funktionale Einheiten vom Typ einer Abteilung oder einer Stabsstelle unter dem Dach größerer, zumeist öffentlich getragener Einrichtungen inkubiert. Dies geschieht etwa in Form von „Datentreuhandstellen“ an großen Klinika oder in Gestalt der FDZ datenhaltender Behörden, die ihre Daten unter kontrollierten Bedingungen ausgewählten Nutzerinnen und Nutzern zugänglich machen. Datenvermittlung heißt hier „Öffnung“ zur Nutzung dessen, was der hauseigene Datenbestand, der eigene Silo, enthält. Datentreuhänder, so könnte man auch sagen, die sich auf das Zurverfügungstellen von Daten fokussieren, die sie primär aus operativ ganz anderen Gründen sammeln, sind „Datenmittler“ allenfalls im Rahmen einer Nebenzwecke erfüllenden Zusatzfähigkeit. Diese kann benevolenter Art sein oder auch – im Zuge der durch die EU statuierten Öffnungsgebote für Public Sector Data<sup>12</sup> – gesetzlich gefordert.

Als Grund für das geringe Interesse an rechtlicher Eigenständigkeit wird man, etwas verallgemeinernd, die oftmals enge Anbindung von Datentreuhändern im Sinne einer Funktionseinheit oder Abteilung an große (oft: auch forschende) Einrichtungen in Betracht ziehen müssen. Tatsächlich stellen medizinische Datentreuhandstellen (in enger Symbiose mit den ebenfalls an Klinika angesiedelten Datenintegrationszentren) in Deutschland die historisch älteste Form der Datentreuhand dar.<sup>13</sup> In der Praxis besteht das Geschäft solcher Treuhandstellen allerdings vor allem in der Pseudonymisierung von Datensätzen sowie in der Verwahrung der die-

sen gleichwohl auf Bedarf zuzuordnenden Einwilligungsdokumente. Solche Treuhandstellen vermitteln also nicht Daten, sondern stellen bereinigte Datensätze für eine z.B. forschende Nutzung (die dann aber an anderer Stelle erfolgt) zur Verfügung, wobei sie zugleich für ein Einwilligungsmanagement sorgen, das den getilgten Personenbezug der Daten reversibel hält. Die hierfür erforderliche Prozesskette ist im Grunde wenig spezifisch für digitale Daten, und sie schließt auch eine Datennutzung online (und durch organisationsfremde Nutzende) nicht unbedingt mit ein. Auch bei den FDZ ist der Remote-Zugang oftmals nicht (ohne Weiteres) möglich.

Die Datennutzung zu Forschungszwecken (etwa in einem Klinikum) gleicht generell eher einem organisationsintern (oder zwischenbehördlich) eingeräumten, formularbasierten Datenzugang, über den der Datengeber in hoheitlichem Stil entscheidet, als einem voll verrechtlichten „B2B“-Szenario, dem detaillierte Leistungsvereinbarungen und beispielsweise auch Abmachungen über Fristen, Schlechtleistung, Haftung etc. zugrunde liegen. Ebenso sieht man sich mehr als Datenausgabestelle bzw. als Ermöglicher eines Datenzugangs denn als ein in zwei Richtungen agierender Mittler.

### 2. Der DGA – ein Realitätsschock?

In der Frage danach, wie man es denn mit der Selbstständigkeit hält, liegt somit zumindest für solche Datentreuhandstellen, die sich im Wesentlichen als Dienstleister eines öffentlich-rechtlich verfassten Datengebers sehen, ein Reflexionsanstoß, vielleicht sogar ein Schockmoment. Schlimm ist das nicht, es spiegelt eher die derzeit weit gefasste Vorstellung von Treuhänderschaft. Sich als Treuhänder zu verstehen mag eben zum Selbstbild von Datenarchiven oder -zentren passen wie auch zu Stellen, die durch Präparation von Datensätzen dem Datenschutz Rechnung tragen – sofern sie sich jeweils als getreuliche Sachwalter einer seriösen Datenverwahrung und Bereitstellung von Daten sehen. Die Anforderungen des DGA haben zwar tatsächlich die Nachnutzung von Daten des öffentlichen Sektors im Blick; gleichwohl zielen sie aber (neben der Mobilisierung von Daten für die Forschung) auf eine etwas andere Konstellation, nämlich diejenige einer wirtschaftlichen Nutzung.<sup>14</sup> Und auch der „data intermediation service“, der Datenvermittlungsdienst selbst, ist im

8 Die übrigen 3 Projekte machten keine Angabe.

9 Auch wenn ein Datentreuhänder als datenaltruistische Organisation anerkannt und dem speziellen Regelungsregime des Kapitel IV DGA unterliegt, sehen die in Art.18 DGA statuierten allgemeinen Eintragungserfordernisse die Notwendigkeit einer rechtlichen Selbstständigkeit vor.

10 Maßgeblich für die Einordnung als Datenvermittlungsdienst sind folgende Bestimmungskriterien: die Bereitstellung technischer, rechtlicher und sonstiger Mittel zur Herstellung von Geschäftsbeziehungen zum Zwecke der gemeinsamen Datennutzung für eine unbestimmte Anzahl von Personen. Ausnahmen existieren beispielsweise für Datenaufbereitungs- und Lizenzierungsdienste, Datenbroker oder Content-Intermediäre.

11 Zu den regulatorischen Anforderungen an Datenvermittlungsdienste vgl. Buchheim/Möslein/Omlor/Jetzen/Villablanca, Handbuch Datentreuhand, 2025, S. 207; von Ditfurth, Datenmärkte, Datenintermediäre und der Data Governance Act, 2024, S. 187 ff.

12 Die Public Sector Information Richtlinie der EU (2003) zog in Deutschland das Informationsweiterverwendungsgesetz (2006, 2016) nach sich, die EU Open Data Richtlinie (2019) wird durch das Datennutzungsgesetz (2021) umgesetzt.

13 So wirbt die Datentreuhandstelle der Universitätsmedizin Greifswald, „mit 10 Jahren Erfahrung“ den Zugriff auf schützenswerte Daten zu organisieren, vgl. <https://www.ths-greifswald.de/> [9.1.2026].

14 Vgl. DGA, ErwG 6: „In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union.“; vgl. auch die Aussagen zum Wettbewerb, etwa in ErwG 13.

Grundsatz, auch wenn eine öffentliche Einrichtung als ein solcher fungieren kann, als ein Marktakteur konzipiert.

So schließt der DGA zwar gem. Art. 12 die Verknüpfung der Datenvermittlungsleistung mit anderen datenbezogenen Dienstleistungen (z.B. Cloud-Services etc.) aus bzw. unterlegt dies engen Grenzen, aber es kann eben auch derjenige, der ausschließlich eigene Daten bereitstellt oder eine bloße Lizenzierung anbietet, ohne eine kommerzielle Beziehung zwischen Datenhaltern und -nutzern zu begründen, schon definitorisch nicht als Datenvermittlungsdienst betrachtet werden.<sup>15</sup> Neben der in Art. 11 geregelten Anmeldepflicht, statuiert Art. 12 DGA darüber hinaus zahlreiche weitere Bedingungen, die bei der Erbringung von Datenvermittlungsdiensten zu beachten sind:<sup>16</sup> hierzu zählen exemplarisch die strenge Zweckbindung<sup>17</sup> der Datenvermittlung, das Gebot der strukturellen Trennung<sup>18</sup>, ein partielles Kopplungsverbot (De-Bundling)<sup>19</sup>, Nutzungsbeschränkungen für Metadaten, die Gewährleistung von Interoperabilität, Vorgaben bezüglich IT-Sicherheit sowie die Maßgabe eines fairen, transparenten und diskriminierungsfreien Zugangs zum eigenen Serviceangebot. Zudem müssen sie über Instrumente verfügen, um Fehlverhalten ihrer Nutzer sanktionieren zu können, und die Einhaltung des Wettbewerbsrechts gewährleisten.<sup>20</sup>

### 3. Vor- und Nachteile der Selbstständigkeit

Die rechtliche Selbstständigkeit ist also – jedenfalls für Treuhänder, die sich im Sinne des DGA als Datenvermittler sehen – unumgänglich. Im Hinblick darauf neigen die von uns befragten Datentreuhandprojekte derzeit zu einem pragmatischen Vorgehen. Die Entscheidung solle, so die Auskunft mehrerer Gesprächspartner, davon abhängig gemacht werden, ob regulatorische Vorgaben existieren, die eine organisatorische Ausgliederung explizit einfordern. Man schlägt den Pfad der rechtlich-organisatorischen Eigenständigkeit also schlicht ein, weil es sein muss. Die Rolle des voll verantwortlichen Akteurs scheint nicht aus sich heraus attraktiv zu sein, sondern eher eine regulatorische Last, der man zähneknirschend nachzukommen hat.<sup>21</sup>

Allerdings legen unsere Erhebungen auch diverse Argumente zugunsten einer rechtlich-organisatorischen Selbstständigkeit nahe. So ermöglicht sie einen klaren Aufgabenfokus, und dieser ist gewünscht: als eigenverantwortliche Entität kann sich ein Datentreuhänder auf seine Kernaufgabe und -kompetenz, die Bereitstellung datentreuhandbezogener Dienstleistungen im Sinne seiner Kunden, konzentrieren. Außerdem lassen sich durch die organisatorische Separierung mögliche Interessenkonflikte vermeiden (sofern die Interessen der Datentreuhandstelle den Interessenlagen der übergeordneten Mutterorganisation widersprechen). Es winkt ein Zugewinn an Freiheitsgraden, da beim eigenen Handeln nicht zwangsläufig die strategischen Ziele der Dachorganisation mit zu berücksichtigen sind. Als eigenständige Organisation wahrgenommen zu werden, kann Vertrauensvorteile schaffen und Geschäftspartnern eine höhere Neutralität vermitteln, insbesondere bei geschickter Ausgestaltung der Trägerstrukturen (z.B. Einbindung von Verbänden, von wissenschaftlichen Einrichtungen oder der öffentlichen Hand). Zudem lassen sich dadurch auch umfangreichere Partizipationsmöglichkeiten für interessierte Stakeholder(-gruppen) schaffen.

Mit einer rechtlichen Eigenständigkeit gehen schließlich Handlungsspielräume und Gestaltungsfreiheiten bezüglich der strukturellen Ausformung der Binnenorganisation, der Entwicklung eines tragfähigen Geschäftsmodells, der Erschließung von Finanzierungsquellen sowie der Handlungs-

fähigkeit im Außenverhältnis (z.B. selbstständige Teilnahme am Rechtsverkehr/Interaktion im Außenverhältnis mit Dritten) einher. Organisatorische Eigenständigkeit bedeutet oftmals auch, dass man sich eines strikten Regelungskorsetts mit starren Vorgaben und Handlungsvorschriften entledigen kann; ein Zugewinn an Flexibilität und Agilität ist die Folge. Ein Datenmittler, der selbstständig ist, kann auch besser „skalieren“ – also die Frequenz seiner Vermittlungsleistungen an die Nachfrage anpassen. Dies ist auch Datentreuhandstellen oder FDZ klar, für welche die Herauslösung aus der Institution, der sie angehören, schwer vorstellbar ist. In der Praxis beschränken solche Treuhänder ihre Angebote tendenziell auf das, was die Bedarfe (und das Budget) ihrer Dachorganisation zulassen.

Allerdings sind auch Nachteile einer Selbstständigkeit nicht von der Hand zu weisen. Technisch-administrative Synergien mit den Infrastrukturen einer Mutterorganisation sind erschwert oder unmöglich, Personal und Technik sind eigenständig bereitzustellen und zu finanzieren, Zugriffe auf spezifisches Knowhow und Serviceleistungen gehen verloren; auch eine (binnenorganisationale) Verantwortungsdelegation im Falle von Fehlern ist nicht mehr ohne Weiteres möglich. Zudem muss Reputation eigenständig aufgebaut werden. Als Treuhänder „des/der ...“ können Reputation und etablierte Vertrauensbindungen gleichsam „übernommen“ werden; die Reputation färbt sozusagen auf die Datentreuhandstelle ab.<sup>22</sup> Generell stellt der Aufbau von Vertrauen eine zentrale Herausforderung dar, die Datentreuhandprojekten sehr bewusst vor Augen steht.<sup>23</sup> Dies schließt im Falle der rechtlichen Selbst-

15 DGA, ErWG 28.

16 Vgl. Buchheim/Möslein/Omlor/Jetzen/Villablanca, Handbuch Datentreuhand, 2025, S. 207.

17 Gem. Art. 12 lit. a) DGA dürfen die Daten für keine anderen Zwecke verwendet werden als für die Bereitstellung für die Datennutzer, insbesondere nicht für eigene Zwecke.

18 Datenvermittlungsdienste sind von einer gesonderten juristischen Person zu erbringen, um Interessenkonflikten vorzubeugen und die Neutralität der Diensteanbieter sicherzustellen. Es wird jedoch keine Weisungsfreiheit oder wirtschaftliche Unabhängigkeit verlangt.

19 Nach Art. 12 lit. b) DGA darf die Nutzung des Datenvermittlungsdienstes bzw. deren Konditionen nicht davon abhängig gemacht werden, dass andere Services des Anbieters (oder eines verbundenen Unternehmens) genutzt werden.

20 DGA, ErWG 36 und 37.

21 So antwortete ein Verantwortlicher eines Datentreuhandprojekts auf die Frage nach rechtlicher Selbstständigkeit: „Vorteile? Gut man hält dann die gesetzlichen Vorgaben aus dem Data Governance Act ein. Ja, aber sonst? Also mir fällt jetzt nicht so viel ein, warum das so besonders vorteilhaft sein sollte“ (Interview #5). Insofern handle es sich auch nicht um eine bewusste, freiwillige Entscheidung, der eine sorgfältige Güterabwägung zugrunde lag, „weil das nie wirklich zur Debatte stand, weil dadurch, dass wir es machen müssen, hat man sich jetzt auch nicht groß damit beschäftigt, Vor- und Nachteile von Eigenständigkeit gegeneinander aufzuwiegen“ (Interview #5).

22 „Was wir jetzt oft zu hören bekommen [...] ist, dass unser Hintergrund, dass wir an einer TU verortet sind, an einer Universität, uns sozusagen sehr vertrauenswürdig macht.“ (Interview #5); „Es kann durchaus sein, dass es eine Organisation ist, an der die Datentreuhand [angegliedert ist], der schon unglaublich viel Vertrauen entgegengebracht wird, und man sagen kann, das ist ein offizielles Institut, wir gehen davon aus, dass deren Datentreuhand auch gut und vertrauenswürdig strukturiert ist. Und es kann genau in die Richtung gehen, dass so einer ganz unabhängigen Datentreuhand misstraut wird, weil man gar nicht weiß, wer dahintersteckt.“ (Interview #6); „Ich weiß nicht, ob es einen Mehrwert bietet, [wenn] dann in die Richtung wieder des Vertrauens, weil [...] man hat schon gewisse Vertrauensbeziehung[en] und ist etabliert.“ (Interview #7). Im Hinblick auf eine mögliche rechtliche Eigenständigkeit werden gerade bezüglich des Reputationsaufbaus Bedenken geäußert: „Das ist, glaube ich, immer das Schwierige, [...] diese Vertrauensbeziehung. Da muss man, glaube ich, sich das wieder aufbauen, das Vertrauen in diese Plattform und in die eigenständige rechtliche Identität.“ (Ebenda).

23 Zentrale Herausforderung „war und ist es, Vertrauen zu erzeugen. Also und Kontrolle und Transparenz sicherzustellen und zu vermitteln. Das waren und werden weiterhin die Hauptaufgaben [sein]“ (Interview #3); „Das ist mit der wichtigste Erfolgsgarant aus unserer Sicht, zumindest für eine Datentreuhand, dass man sagt, da wo keine Neutralität ist, da wo kein Vertrauen irgendwo ist, da werden auch keine Daten hinfließen.“ (Interview #6).

ständigkeit eine möglichst transparente Außerdarstellung der Trägerstrukturen mit ein, um Zweifel und Misstrauen auf Seiten potenzieller Nutzer zu zerstreuen: eine Anstrengung, die aber eben auch nur dann erforderlich ist.

#### 4. Alternativen?

Der DGA kennt u.a. mit der Datengenossenschaft und mit dem Konstrukt datenaltruistischer Organisationen unterschiedliche Varianten der Datenvermittlung. Er belässt jedoch auch Interpretationsspielräume für Formen der Datenweitergabe oder Datenanalysediensten, die möglicherweise nicht ohne Weiteres unter das Gesetz fallen. Dies können dann auf der einen Seite entweder doch „klassische“, nicht neutrale, sondern sich vielleicht lediglich als besonders seriös oder sicher positionierende Plattformen sein – oder aber auf der anderen Seite Konzepte der Treuhandschaft, bei denen es so konsequent allein um die Vermittlungsleistung geht, dass der Treuhänder noch nicht einmal mehr die Daten bewegt, sondern gleichsam blind lediglich Datenzugänge administriert, geschützte Datenauswertungsmöglichkeiten bereitstellt und Datenanalysen durchführt, ohne hierbei direkten Einblick in die Daten nehmen zu können. Letzteres ist bei dem im BMWK-Projekt EuroDaT entwickelten Ansatz der transaktionsbasierten Datentreuhand der Fall.<sup>24</sup>

Dass ein Datentreuhandmodell den DGA von vornherein für sich selbst nicht für einschlägig hält, bleibt unter den von uns untersuchten Vorhaben die Ausnahme. Die oben beschriebene, abwartende Haltung scheint durchweg von der Vermutung begleitet zu sein, dass das noch wenig erprobte Gesetz für das eigene Vorhaben einschlägig ist. Wir sehen hier aus Sicht der Praxis vor allem einen dringenden Beratungsbedarf. Man wird einräumen müssen, dass der DGA es Datenvermittlungsdiensten durchaus nicht leicht macht, da diese – gerade in der nicht altruistischen Variante – vielfältige regulatorische Anforderungen zu erfüllen haben. Der DGA verfolgt hierbei einen One-size-fits-all-Ansatz, der keine Differenzierung nach unterschiedlichen Graden der Marktmacht zwischen den Akteuren vornimmt. Der damit einhergehende starre Regulierungsrahmen legt den Akteuren extensive Verhaltenspflichten auf, bedingt erhebliche Compliance-Kosten und benachteiligt Datenintermediäre im Wettbewerb mit analogen, nicht dem DGA unterliegenden Geschäftsmodellen (wie Datenbroker oder geschlossene Datenplattformen). Kritiker haben daher bilanziert, der regulatorische Rahmen des DGA wirke in wirtschaftlicher Hinsicht unausgegoren: Er hemme die Ausbildung innovativer Geschäftsmodelle und lasse die Tätigkeit als Datenintermediär ökonomisch unattraktiv erscheinen. Worin bestünden überhaupt die Anreize, sich in diesem Geschäftsfeld zu versuchen, lautet die nicht ganz unberechtigte Frage.<sup>25</sup> Der Impuls, den der DGA setzen soll, könnte so womöglich verpuffen.<sup>26</sup>

### III. Aktuelle Entwicklungen „bottom up“

Wie bereits erwähnt fordert der DGA die Bereitstellung von Datenvermittlungsdiensten durch eine gesonderte juristische Person<sup>27</sup>, eine rechtlich eigenständige Entität, deren originäre Aufgabe die Datenvermittlung darstellt. Über diese Vorgabe hinaus bleibt die gesellschaftsrechtliche Ausgestaltung und die Rechtsformwahl jedoch völlig offen. Durch die allgemeine Formulierung des Art. 12 lit. a) DGA steht somit grundsätzlich das vollständige Arsenal gesellschafts- und verbandsrechtlicher Rechtsformen,

sowohl in ihrer öffentlich-rechtlichen als auch privatrechtlichen Ausprägung, zur Verfügung; aus Praktikabilitätsgründen dürfte sich der Kreis möglicher Rechtsformen in vielen Fällen jedoch auf juristische Personen des Privatrechts beschränken.

Datentreuhänder im Werden sind also herausgefordert, aus einem großen Fundus eine passende Rechtsform auszuwählen, um dann die Governance-Arrangements durch geschickte Satzungsgestaltung an die spezifischen Bedürfnisse eines Datenvermittlungsdienstes anzupassen. Dabei gilt es, sowohl den datenrechtlichen Rahmenbedingungen (v.a. die Anforderungen des Art. 12 DGA) als auch den ökonomischen Funktionsvoraussetzungen ihres Datentreuhandmodells (Neutralität, Vertrauenswürdigkeit, Vermeidung von Interessenskonflikten, Fragen der Gewinnerzielung und -ausschüttung) gerecht zu werden, Etwaige sektorspezifische Regulierungen und kartellrechtliche Aspekte können für das Anforderungsprofil der Datentreuhanderschaft ebenfalls bedeutsam sein. Gleichwohl lässt sich diese Komplexität analysieren und im Zuge der Rechtsformwahl beantworten. Mittels der Einrichtung und Ausgestaltung unterschiedlichster Gremien wie auch durch die Festlegung wohldefinierter Satzungszwecke bietet das Gesellschaftsrecht vielfältige Möglichkeiten, eine adäquate Interessenrepräsentation herbeizuführen und die Unabhängigkeit von Einzel- und Sonderinteressen zu gewährleisten.<sup>28</sup>

Wie sehen vor diesem Hintergrund die aktuell in Entwicklung befindlichen Datentreuhandmodelle aus? Und welche Erwägungen hinsichtlich der Rechtsformen treffen wir – jenseits der Varianten, einer rechtlich unselbstständigen Anbindung an eine große öffentliche Einrichtung, an das oben beschriebene, prototypische Universitätsklinikum oder die Behörde oder Forschungseinrichtung mit FDZ – im deutschen Rechtsraum derzeit an?

#### 1. Tendenzen

Im Hinblick auf die Frage der Rechtsformwahl deuten unsere Befragungen auf große Unsicherheit in der Datentreuhand-Community und auf die bereits geschilderte Unentschlossenheit hin. In vielen Projekten war die Rechtsformwahl noch gar kein Thema. Oftmals wurden hierzu allenfalls erste kursorische Überlegungen angestellt, ein systematischer Analyse- und Entscheidungsprozess stand noch aus. Dennoch zeigen unsere Interviews erste Tendenzen und Präferenzen.

Die Mehrzahl der Projekte hält eine privatrechtliche Rechtsform für plausibel; Rechtsformen des öffentlichen Rechts werden eher selten als realistische Option genannt.<sup>29</sup> Erwogen

24 Zur rechtlich-konzeptionellen Einordnung: Buchheim/Augsberg/Gehring JZ 2022, 1139; zu den technischen Grundlagen: Buchheim/Möslein/Omlor/Alldridge, Handbuch Datentreuhand, 2025, S. 325.

25 Hennemann/von Ditfurth, NJW 2022, 1905 (1910); Richter, ZEuP 2021, 634 (662f.); von Ditfurth, Datenmärkte, Datenintermediäre und der Data Governance Act, 2024, S. 582 ff.

26 Eine durch den DGA bedingte mangelnde ökonomische Attraktivität der Rolle des Datenintermediärs könnte erklären, warum in der Gruppe der vom BMBF/BMFTF seit 2020 geförderten datentreuhandbezogenen Forschungsvorhaben kaum privatwirtschaftliche Akteure als Betreiber eines Datentreuhänders auftreten. Vgl. Technopolis, Wissenschaftliche Begleitung und Vernetzung der Projekte zur Entwicklung und praktischen Erprobung von Datentreuhandmodellen in den Bereichen Forschung und Wirtschaft, 2024, abrufbar unter <https://www.technopolis-group.com/wp-content/uploads/2024/04/BMBF-Datentreuhandmodelle-Begleitforschung-Umsetzungshemmnisse-1.pdf> [9.1.2026], S. 34ff.

27 Die tatsächliche, also wirtschaftliche Unabhängigkeit von anderen Unternehmen wird jedoch nicht vorausgesetzt.

28 Vgl. Buchheim/Möslein/Omlor/Möslein/Tuschhoff, Handbuch Datentreuhand, 2025, S. 129.

29 Von 42 Nennungen (Mehrfachnennung möglich) entfielen 30 auf privatrechtliche und lediglich 5 auf öffentlich-rechtliche Rechtsformen. 7 Projekte sahen sich außer Stande, diese Frage zu beantworten.

werden insbesondere der Verein, die Genossenschaft (in einem Fall in ihrer europäischen Variante) oder die GmbH (seltener auch die gemeinnützige GmbH) als denkbare oder bereits geplante Rechtsform; deutlich seltener die Stiftung.<sup>30</sup>

Unabhängig von der konkreten Rechtsform betonen die befragten Datentreuhandprojekte wiederholt die Wichtigkeit einer ausgewogenen und transparenten Zusammensetzung des Betreiberkonsortiums. Es sei darauf zu achten, dass passende Stakeholder ausgewählt und hinreichende Beteiligungsmöglichkeiten geschaffen werden sowie dass einzelne Stakeholder oder Interessengruppen keine zu große Macht, gar dominante Position in den zentralen Steuerungsgremien des Datentreuhänders einnehmen, so dass eine angemessene Berücksichtigung unterschiedlichster Interessen gewährleistet werden kann.

Angesichts dieser Ziele werden insbesondere der (wirtschaftliche) Verein oder die Genossenschaft von unseren Befragten als geeignete Rechtsformen für Datentreuhänder angesehen. Die mitgliederschaftliche Struktur schafft nicht nur vielfältige Partizipationsmöglichkeiten für unterschiedlichste Stakeholder des Datentreuhänders (z.B. Datengeber, Datennutzer) und begünstigt dem genossenschaftlichen Grundgedanken einer Hilfe zur Selbsthilfe folgend eine gemeinsame Interessenverfolgung, die sich mehrwertstiftend für das Kollektiv auswirken kann, sondern bietet auch ausreichenden Raum, einen angemessenen Interessenausgleich zwischen den Mitgliedern herbeizuführen und somit eine hinreichende Unabhängigkeit des Datentreuhänders von Einzel- und Eigeninteressen und damit dessen Neutralität zu gewährleisten, nicht zuletzt da dem demokratischen Grundprinzip folgend jedes Mitglied mit dem gleichen Stimmgewicht ausgestattet ist, d.h. alle gleich behandelt und niemand übervorteilt wird. Durch den community-getriebenen, kooperativen Ansatz werden die Mitglieder in alle relevanten Prozesse eingebunden. Gleichzeitig ermöglicht er eine Kontrollfunktion durch das Kollektiv. Damit wird nicht nur die Selbstwirksamkeit der Mitglieder gewährleistet, sondern auch ein Vertrauensanker für diese geschaffen. Bei der (noch exotischen) Variante der europäischen Genossenschaft (SCE) kommt eine „digitalfreundliche“ Verfasstheit hinzu, da hier viele Prozesse vollständig digital abzuwickeln sind. Als Nachteile beider Rechtsformen wird auf schwerfällige Strukturen und einen hohen administrativen Aufwand für die Durchführung des Tagesgeschäfts verwiesen. Insbesondere bei exotischen Varianten wie der SCE tritt erschwerend hinzu, dass es sich hierbei noch um eine weitgehend unbekannte Rechtsform handelt, zu welcher wenige Erfahrungswerte existieren, was mit einem höheren Gründungsaufwand verbunden ist.<sup>31</sup>

Auch die GmbH wird von vielen Befragten als eine geeignete Rechtsform für Datentreuhänder wahrgenommen. Ähnlich wie die zuvor genannten Rechtsformen weist die GmbH eine mitgliederschaftlich geprägte Struktur auf und ermöglicht somit Partizipationsmöglichkeiten, um einen Interessenausgleich herbeizuführen. Allerdings ist die Mitgliederstruktur nicht durch demokratische Parität (one man, one vote) geprägt, sondern das Stimmgewicht richtet sich nach der Höhe der Unternehmensbeteiligung. Zu den klaren Vorzügen der GmbH gehört, dass sie hinsichtlich der Gesellschafterstruktur maßgeschneiderte Lösungen zulässt. Die weite Verbreitung dieser Rechtsform macht sie zudem zu einem weithin bekannten und im allgemeinen Wirtschaftsverkehr auch anerkannten Rechtskonstrukt, was insbesondere im B2B-Bereich bei Geschäftspartnern des Datentreuhänders Vertrauensprobleme mindert. Die im Vergleich zu

anderen Kapitalgesellschaften geringen Kapitalanforderungen, die Haftungsbegrenzung sowie der geringe administrative Aufwand, der i.d.R. einen zügigen, wenig aufwendigen Gründungsprozess ermöglicht, steigern die Attraktivität zusätzlich. Zudem bietet sie vielfältige Gestaltungsmöglichkeiten auf Ebene der Gesellschaftssatzung, wodurch sie flexibel an die jeweiligen Bedürfnisse des (zu gründenden) Datentreuhänders angepasst – wie auch im laufenden Geschäftsbetrieb modifiziert – werden kann. Allerdings sehen Datentreuhandprojekte, die auf strikte Interessensneutralität ihres zu etablierenden Datentreuhänders Wert legen, die Kopplung von Stimmgewichten an die Höhe des Gesellschafteranteils als kritisch an, wenn Unternehmen aus der Datendomäne, für die der Treuhänder arbeiten soll, unter den Gesellschaftern sind. Es wird befürchtet, dass in einem solchen Fall kleinere, weniger kapitalkräftige Stakeholder übervorteilt werden könnten. Ein weiterer Kritikpunkt besteht in einer – vermeintlichen – Notwendigkeit der Gewinnorientierung einer GmbH. Die GmbH wird v.a. seitens öffentlich finanzierter Forschungseinrichtungen als „kommerzielle“ Rechtsform wahrgenommen.<sup>32</sup> Hierbei ist allerdings festzuhalten, dass dies ein Stück weit ein Vorurteil ist. Die Rechtsform der GmbH ermöglicht zwar grundsätzlich eine Gewinnorientierung, ist hierzu jedoch nicht verpflichtet. So kann im Rahmen der Satzung eine Kostendeckung vorgesehen werden.

Im Gegensatz zu den Vorgenannten ist die Stiftung als Rechtsform für Datentreuhänder deutlich weniger attraktiv. Zwar wird dieser Rechtsform durchaus zugestanden, Neutralität, fehlende Eigeninteressen und Vertrauen als Kernprinzipien der Datentreuhand durch eine geschickte Festlegung des Stiftungszwecks sicherstellen zu können. Als Haupthindernis werden jedoch die hohen Kapitalanforderungen gesehen.<sup>33</sup>

Besondere Aufmerksamkeit erregt die Frage nach der Gewinnorientierung. In unseren Interviews zeigte sich, dass die Mehrzahl der Projekte einer Gewinnorientierung ablehnend gegenübersteht (14); lediglich eine Minderheit kann sich eine (begrenzte) Profitorientierung vorstellen (7). In der Regel zielt man also auf einen kostendeckenden Betrieb des Datentreuhänders, einige wenige Projekte rechnen gar damit, dass der Datentreuhänder dauerhaft von dritter Seite bezuschusst werden muss. Interessanterweise scheint in den Projekten die Frage der Gewinnorientierung unabhängig von der Rechtsform gesehen und diskutiert zu werden: Alle der oben genannten Rechtsformen sind aus Sicht der Befragten so-

30 Konkrete Anzahl der Nennungen: Verein (8), Genossenschaft (7), GmbH (7), gGmbH (5), Stiftung (3).

31 Hürden schafft freilich auch das klassische deutsche Vereinsrecht. Die Tätigkeit nicht-wirtschaftlicher Vereine ist auf spezifische Zwecke ideeller Art begrenzt. Die Rechtsfähigkeit eines wirtschaftlichen Vereins ist an die hohe Hürde staatlicher Verleihung gebunden. Die damit verbundenen Anforderungen dürften in der Praxis kaum erfüllbar sein, da Datentreuhändern i.d.R. alternative Gesellschaftsformen zur Verfügung stehen. Vgl. Buchheim/Möslein/Omlor/Möslein/Tuschhoff, Handbuch Datentreuhand, 2025, S. 129.

32 Um dieser vermeintlichen Schwachstelle zu entgehen, wird häufig die gGmbH als Alternative angesehen (unbeschadet der Tatsache, dass es sich hierbei zivilrechtlich gar nicht um eine eigene Rechtsform handelt; die Gemeinnützigkeit ist lediglich ein steuerrechtliches Qualifikationsmerkmal): „Wir glauben aber schon, dass die Gemeinnützigkeit ein großer Benefit ist, auch für das langfristige Überleben des Datentreuhänders, weil der Datentreuhänder lebt von den Datengebern. Und da glauben wir schon, dass die Gemeinnützigkeit per se noch mal ein Vertrauenspunkt gibt, den man als gewinnbringendes Unternehmen so nicht mitbringt.“ (Interview #19).

33 Als weitere Hindernisse werden im Schrifttum die enge Bindung an den Stiftungszweck benannt, welcher eine dynamische Anpassung an ein sich rasch änderndes Marktumfeld erschwert; ebenso sind Stiftungen Grenzen bei der Verfolgung unternehmerischer Zielsetzungen gesetzt, was – will man dies dennoch nicht ausschließen – verschachtelte Konstruktionen erforderlich macht. Vgl. Buchheim/Möslein/Omlor/Möslein/Tuschhoff, Handbuch Datentreuhand, 2025, S. 129.

wohl in einer gewinnorientierten als auch in einer nicht-gewinnorientierten Variante denkbar.

Manche Befragte sehen eine Gewinnorientierung als erforderlich an, um für Betreiber ökonomische Anreize zu setzen, Datentreuhandmodelle überhaupt erst zu entwickeln und die damit verbundenen Aufwände zu tragen. Zudem könne dadurch die Tragfähigkeit des Finanzierungsmodells und damit dessen finanzielle Nachhaltigkeit sichergestellt werden – nicht zuletzt da aus den Gewinnen auch Rücklagen gebildet werden können, um umsatzschwache Phasen zu überbrücken. Außerdem sei, so die Sicht der Befürworter solcher Ansätze, eine gewisse Gewinnorientierung als unproblematisch einzuschätzen, da sich Datentreuhänder vermutlich sowieso nicht zu „großen Gewinnmaschinen“ entwickeln und ihre „Gewinne [...] nicht ins Unendliche wachsen“ werden (Interview #9). Gewinne dürften bis zu einem gewissen Grade zudem notwendig sein, um die Aktivitäten eines Datentreuhänders skalieren zu können.

Kritiker verweisen jedoch auf das Spannungsverhältnis zwischen Gewinnorientierung und Vertrauenswürdigkeit sowie (Markt-)Neutralität des Datentreuhänders. Man sehe die Profitorientierung skeptisch, da sie die Bereitschaft potenzieller Datengeber hemmen könnte, ihre Daten über den Treuhänder bereitzustellen.<sup>34</sup> Insbesondere bei hochsensiblen Daten wie beispielsweise im Gesundheitsbereich wird befürchtet, der Monetarisierungsgedanke könne zu Fehlanreizen führen und Vertrauen unterminieren.<sup>35</sup> Die Gleichsetzung von Gewinnorientierung mit „Kommerzialisierung“ spiegelt die Sorge wider, dass sich analog zu den Marktkonzentrationstendenzen in der Plattformökonomie Datentreuhänder zu Datenkraken entwickeln könnten, die v.a. daran interessiert sind, möglichst viele Daten zu akkumulieren, um diese gleichsam um jeden Preis gewinnbringend weiterzuvermitteln. Dies gilt besonders, wenn die Höhe des Gewinns unmittelbar vom Umfang der übermittelten Daten abhängt, wenn also Anreize bestehen, möglichst umfangreiche Datenpools zu schaffen.<sup>36</sup> Dem so nahegelegten Argumentationsgang folgend könnte ein bewusster Verzicht auf eine Gewinnorientierung oder auf jedwede Form der Monetarisierung von Daten (z.B. in der Satzung) als vertrauensstiftendes Element wirken, das die (Markt-)Neutralität des Datentreuhänders nach außen besonders überzeugend repräsentiert. Jenseits der reinen Datenmittlung sollte kein (finanzielles) Eigeninteresse etwa an der Frequenz der Dienstleistung bestehen.<sup>37</sup> Zudem scheint mit dem Verzicht auf Gewinnerzielung auch die Erwartung verbunden, dass ein lediglich Kostendeckung anstrebender Datentreuhänder geringere Nutzungskosten auf der Nachfrageseite, d.h. bei den Datennutzenden, verursacht. Er würde also in der Nutzung schlicht günstiger sein.

Wägt man die skizzierten Vor- und Nachteile der einzelnen Rechtsformen gegeneinander ab, erscheint insbesondere die GmbH als Rechtsform für Datentreuhänder geeignet. Dies deckt sich auch mit Einschätzungen im Schrifttum: So sehen Möslein/Tuschhoff deren größte Vorzüge in der hohen Flexibilität bei der Ausgestaltung der Governance-Arrangements, die sich auch nachträglich ohne größeren Aufwand modifizieren lassen, dem flexiblen Satzungszweck, dem relativ niedrigen Gründungsaufwand sowie der vorteilhaften unternehmerischen Außenwirkungen aufgrund des hohen Bekanntheitsgrades dieser Rechtsform.<sup>38</sup>

## 2. Datenaltruismus als Alternative?

Nach Einschätzung der EU-Kommission besteht grundsätzlich eine hohe Bereitschaft, Daten für altruistische, d.h. gemein-

wohlorientierte Zwecke preiszugeben, sofern richtige Rahmenbedingungen und Instrumente gegeben sind. Sie hält allerdings Vertrauen, Transparenz und eine klare Rechtsgrundlage für unverzichtbar, um Vertrauensräume zu schaffen und Nutzungshemmnisse abzubauen.<sup>39</sup> Daher sieht der DGA neben den Datenvermittlungsdiensten auch die Option datenaltruistischer Organisationen vor. Durch diese sollen Sorgen vor einer Zweckentfremdung der Datennutzung entgegengewirkt, Vertrauen gesteigert und die Motivation zum Datenteilen für altruistische Zwecke erhöht werden.<sup>40</sup> Die Anerkennung als datenaltruistische Organisation entbindet von der Einhaltung der strengen Vorgaben für Datenvermittlungsdienste, allerdings unterliegen diese Entitäten bestimmten Anforderungen. Die Datennutzung muss gemeinwohlorientiert erfolgen – ähnlich dem deutschen Gemeinnützigkeitsrecht bemisst sich das an einer Liste hierfür typischer Ziele. Des Weiteren darf das Recht auf Datennutzung nicht vergütet werden (allenfalls eine Entschädigung für die Kosten der Datenbereitstellung ist darstellbar) und die Datenbereitstellung muss auf Freiwilligkeit beruhen (kein Zwang, keine gesetzliche/vertragliche Verpflichtung). Auch datenaltruistische Organisationen müssen über eine eigene Rechtspersönlichkeit verfügen. Allerdings dürfen sie keinen Erwerbszweck verfolgen, d.h. nicht gewinnorientiert agieren und keine privatwirtschaftlichen Ziele anstreben. Im Mittelpunkt steht die Uneigennützigkeit, um Interessenkonflikte zu vermeiden.<sup>41</sup>

Insgesamt wirken diese regulatorischen Vorgaben recht eng und scheinen auf den Fall einer individuellen Spende eigener, persönlicher Daten durch Bürgerinnen und Bürger an eine gemeinwohlorientierte Organisation zugeschnitten zu sein (nicht aber beispielsweise auf B2B-Szenarien oder auch für Konstellationen der Weitergabe von Forschungsdaten an Unternehmen). Das mag erklären, weshalb im Rahmen der Befragungen nur wenig Ambitionen für altruistische Datentreuhandmodelle gemäß DGA zu erkennen waren. Allgemein wird das Konzept des Datenaltruismus als noch unscharf empfunden und ein adäquater Gegenwert oder Mehrwert entsprechender Selbstfestlegungen steht dem aus der Sicht der Datentreuhandprojekte nicht gegenüber. Der einzige Vorteil wird darin gesehen, dass man ein staatliches Siegel erhält und hiermit werben kann. Insgesamt scheint der Datenaltruis-

34 Interview #8: „Wir hoffen, dass wenn es ein nicht gewinnorientiertes Betreibermodell gibt, man solche Probleme eben nicht hat, und man dadurch mehr Akzeptanz schafft zum Datenspenden“.

35 Interview #2: „Es ist sehr wichtig, dass es nicht kommerzielle Vereine sind oder Organisationen, die das betreiben, damit erst mal dieses Vertrauen, Grundvertrauen da ist. [...] Der Datentreuhänder soll in einer Organisation liegen, die keine kommerziellen Absichten mit den Daten hat, um das Vertrauen zu stärken“.

36 Interview #6: „Da haben wir viel drüber nachgedacht, weil aus solchen Gewinnerzielungsabsichten natürlich Risiken, was Datenmissbrauch angeht, wachsen. [...] Also nicht in der Gewinnerzielung an sich vielleicht. Aber wenn der Gewinn direkt mit der Datenübermittlung verbunden wird, dass dann die Personen, die Entscheidungen treffen, ob in bestimmten Fällen Daten weitergegeben werden sollen, einen Anreiz dafür haben, immer ja zu sagen“.

37 Interview #5: „Genau das wäre auch so ein bisschen der Punkt, dass man sagt, man arbeitet nur kostendeckend und eben nicht gewinnorientiert, um schon gar nicht den Anschein zu erwecken, man hat da irgendein finanzielles Interesse an den Daten. In welcher Form auch immer“.

38 Buchheim/Möslein/Omlor/Möslein/Tuschhoff, Handbuch Datentreuhand, 2025, S. 129.

39 Vgl. den Impact Assessment Report zum Entwurf des DGA: SWD(2020) 295 final, S. 71-72.

40 Vgl. ErwG 45 und 46 DGA.

41 Vgl. Buchheim/Möslein/Omlor/Denga/Köbel, Handbuch Datentreuhand, 2025, S. 155.

mus daher wenig attraktiv, die Sinn- und Zweckhaftigkeit des Konstrukts erschließt sich aus Sicht der Praxis noch nicht.<sup>42</sup>

#### IV. Hinweise für Entscheider

Aus unseren Befragungen ergibt sich nicht unbedingt konkretes Rezeptwissen. Dennoch lässt sich für die Zwecke von Entscheidern festhalten: Es ist keineswegs so, dass Datentreuhandmodelle sich aus dem DGA ableiten ließen. Vielmehr werden hierzulande vielfältige Datentreuhandmodelle entwickelt und erprobt, die den DGA eher als (neue und fernliegende) Randbedingung für ein Projektziel auffassen. Suchbewegungen auf dem Weg zu einem Datentreuhandmodell gehen wiederum nicht immer sogleich mit einer von Anfang an verfolgten Suche nach einem Geschäftsmodell (sei es auch nur zur Kostendeckung) einher.

Entscheider sollten hinsichtlich Datentreuhandkonzepten von daher darauf achten

- dass die heterogenen Vorgeschichten der praktischen Konzepte von Datentreuhand mit in Betracht gezogen werden – es gilt, sich zur Vielfalt zu verhalten und dabei einen informierten eigenen Weg zu wählen,
- dass der DGA in seinen Details bekannt ist,
- dass die Frage nach dem Bezug zum jeweiligen „Datenmarkt“ und nach der rechtlichen Selbstständigkeit rechtzeitig durchdacht wird,
- dass das durch den DGA vorgegebene Thema „Altruismus“ hinreichend pragmatisch erwogen und bewertet wird (denn auch nicht-altruistische Datentreuhänder können datenökonomisch höchst sinnvoll sein),
- eine mit EU-Vorgaben auf der Ebene nationaler Umsetzungen generell verbundene Rechtsunsicherheit nicht zu Lasten der Experimentierfreude geht. Denn erkennbar ist die EU-Legislation nicht als Verhinderungsgesetzgebung gedacht, sondern – im Falle des DGA – als Anregung und Stimulation.

Der dringende Rat schließt sich an, sich um Fragen der rechtlichen Selbstständigkeit und der Rechtsformwahl frühzeitig zu kümmern, sie also nicht erst als Thema zu behandeln, das mit der Anwendung der Ergebnisse eines FuE-Projektes verbunden ist.

#### V. Fazit

Auch wenn wir in unsere Befragung nach Kräften Datentreuhand-Projekte jenseits der BMBF/BMFTR-Förderung mit einbezogen haben, sind in unseren Interviews Vorhaben stark repräsentiert, in denen es um die Gewinnung oder um die Nutzbarmachung von Forschungsdaten geht. Das macht es auf der einen Seite erklärlich, dass die Frage der rechtlichen Selbstständigkeit so erstaunlich zögernd adressiert wird – etwa weil man unter dem Dach einer forschenden Einrichtung tätig ist oder auch weil man ein Projekt verfolgt, in dem es gar nicht um eine Marktkonkurrenz geht, sondern vor allem um das Nutzen von Daten, die man ohnehin sammeln kann bzw. besitzt. Auf der anderen Seite mögen Vorbehalte gegen Gewinnerorientierung und (trotz der komplexeren Ausgestaltungsoptionen) etwa auch gegen eine GmbH sich erklären lassen durch eine für die Bereitstellung „öffentlicher“ Daten (und auch von Forschungsdaten) leitende

Vorstellung, hier werde Datenzugang nicht etwa auf zivilrechtlich abgesicherten Wegen vereinbart, sondern gleichsam hoheitlich „gewährt“. Datentreuhandmodelle umschließen bzw. erschließen – Stand heute – eher selten wirklich eine marktliche Rolle, sei diese gewinnorientiert, sei diese altruistisch.

Als umso auffälligeren Befund lässt sich vermerken, dass der durch den DGA skizzierte „altruistische“ Intermediär die Community der deutschen Datentreuhand-Projekte bislang nicht überzeugt, obgleich so viele von ihnen sich um Forschungsdaten (also tendenziell um öffentliche Güter bzw. um ohnehin potenziell gemeinnützige Zielstellungen) drehen. Daraus ergibt sich ein Signal Richtung EU: Der DGA wird nicht wirklich als hilfreiches Instrument erlebt, sondern eher als gut gemeintes, aber unklares und, was die Details angeht, wenig verlässliches Signal.

Aus den empirischen Befunden, die wir hier präsentieren konnten, ergibt sich gleichwohl, dass „bottom up“ eine eher über den EU-Rahmen hinausgehende, geradezu kreativ zu nennende Breite an Datentreuhandmodellen gleichsam darauf wartet, sich zu EU-Vorgaben ins Verhältnis setzen zu können. Zur Unsicherheit der DTM-Projekte, was ihre für sich und ihre Stakeholder optimale rechtliche Verortung angeht, kommen die Unschärfen, welche die EU-Legislation absichtsvoll in Kauf nimmt, hinzu. Nicht zuletzt zur Eröffnung rechtlicher Freiräume auf der nationalstaatlichen Ebene.

Um dem Zielbild der Datentreuhand als Datenvermittlungsdienst gerecht zu werden – wie auch, um die generellere Idee zu realisieren, neue Intermediäre könnten Datenmärkte verändern, sollte jedenfalls der Diskurs nicht nur über Datentreuhandmodelle intensiviert werden, sondern auch derjenige über Marktchancen und über diesen zuträgliche Rechtsformen sowie Geschäftsmodelle.



#### Prof. Dr. Petra Gehring

ist Professorin für Theoretische Philosophie an der TU Darmstadt, sie leitet das BMFTR geförderte Kompetenznetzwerk Datentreuhand und ist wissenschaftliche Direktorin des Zentrums verantwortungsbewusste Digitalisierung (ZEVEDI) des Landes Hessen.



#### Dr. Christian Person

ist Politik- und Verwaltungswissenschaftler, er ist wissenschaftlicher Mitarbeiter im BMFTR-Projekt „Rechtsformen für Datentreuhänder“ sowie einer von zwei Geschäftsstellenleitern des ZEVEDI.

<sup>42</sup> So bemerkt einer unserer Interviewpartner: „Das ist das einzig tolle am Datenaltruismus laut dem DGA, dass Sie sich so einen Badge an die Seite ballern können und sagen: Hey, ich bin zugelassener Datenaltruist. Ja, Sie können so ein Logo führen. Toll. Und dann denken die Bürger: Hey, super, das ist ja ganz tolles Vertrauen, so wie ADAC oder irgendwie so. Aber das heißt: der Gesetzgeber hat die Idee, dass durch ein solches Logo oder durch eine solche Referenz die Transparenz gefördert und das Zutrauen der Bürger gestärkt wird.“ (Interview #25).

Alexander Stichling

# Künstliche Intelligenz im Automobil - Rechtsrahmen und Implikationen von diskriminierender KI

Die zunehmende Anwendung Künstliche Intelligenz (KI) prägt nicht nur das digitale Zeitalter, sondern transformiert auch die Automobilbranche fundamental. KI-Systeme kommen entlang der gesamten automobilen Wertschöpfungskette zum Einsatz insbesondere in (teil-) autonomen Fahrsystemen. Hier übernehmen sie sicherheitskritische Aufgaben wie die Umfeld- oder Innenraumüberwachung. Fahrzeuge mit einer solchen Technik beschleunigen selbst, halten die Spur, bremsen ab, parken ein oder initialisieren eine Vollbremsung in Gefahrensituationen, ohne dass der menschliche Fahrer aktiv handeln muss.<sup>1</sup> Um jedoch breite gesellschaftliche Akzeptanz zu erreichen müssen diese Systeme höchsten Sicherheits- und Ethikstandards genügen.

Ein Problem stellt die potenzielle Diskriminierung durch KI im Straßenverkehr dar. Empirische Studien zeigen, dass bildbasierte Erkennungssysteme in Fahrzeugen People of Color (PoC)<sup>2</sup> sowie Kinder signifikant seltener erkennen als andere Personen.<sup>3</sup>

Solche Erkennungsfehler bergen nicht nur technisch, sondern auch schwerwiegende rechtliche Implikationen, insbesondere bei sicherheitsrelevanten Entscheidungen. Die Gefahr rechtsgutverletzender Fehlentscheidungen durch fehlerhaft trainierte oder voreingenommene KI ist real und gefährdet insbesondere Fußgänger.

Dieser Text legt den Fokus auf die Frage, inwiefern das deutsche und europäische Recht, etwa das AGG, die DS-GVO, oder KI-VO, geeignet sind, Schutzlücken zu schließen und Diskriminierungsfreies automatisiertes Fahren zu gewährleisten.

## I. Die 5 Level des automatisierten Fahrens

Automatisiertes Fahren wird gem. SAE J3016 in Level unterteilt (Level 0-5), abhängig vom Automatisierungsgrad. Während Level 0-2 (keine bis partielle Automatisierung) eine ständige Überwachung durch den Fahrer erfordern, ermöglichen Level 3-5 eine schrittweise Entlastung bis hin zur vollständigen Ablösung des Menschen durch das System.<sup>4</sup> Ab Level 3 übernimmt das Fahrzeug in definierten Betriebsbereichen temporär die Fahraufgabe, der Fahrer muss jedoch die Aufmerksamkeit auf den Verkehr gerichtet haben, um jederzeit die volle Kontrolle über das Fahrzeug übernehmen zu können.<sup>5</sup> Level 4 erlaubt hochautomatisiertes Fahren innerhalb definierter Betriebsbereiche ohne menschliches Eingreifen, mit der Möglichkeit sich nach fehlender Übernahme durch den Fahrer in einen risikominimalen Zustand, meist durch anhalten, zu versetzen. Level 5 beschreibt das vollautonome Fahren ohne Lenkrad oder Fahrintervention unter allen Verkehrsbedingungen und durch fehlende Interventionsmöglichkeit des Fahrers.<sup>6</sup>

In Deutschland ist das autonome Fahren durch das Gesetz zum autonomen Fahren (seit 2022) und Autonome-Fahrzeuge-Genehmigung-und-Betriebs-Verordnung geregelt. Der rechtliche Rahmen erlaubt aktuell die Erprobung und Genehmigung von SAE-Level 3 Fahrzeugen im Realverkehr sowie erste Tests von Level 4 Kleinserien.<sup>7</sup> Bislang kommt dem menschlichen Fahrer neben dem System somit noch immer eine zentrale Rolle zu.

Die EU macht seit 2022 verschiedene Assistenzsysteme zur Pflicht in Neufahrzeugen. Ab 2024 zählen u.a. Notbrems- und Spurhalteassistenten, Müdigkeitserkennung, sowie Unfalldatenspeicher zur Standardausstattung. Die zunehmende Systemverantwortung ab Level 3 und die Pflichtausstattung machen eine juristische Neubewertung der Verantwortlichkeit und Diskriminierungsgefahren durch KI-Systeme erforderlich.<sup>8</sup>

KI ermöglicht durch Fusion aus Kamera-, Radar- und LiDAR-Sensorik und deren Daten eine präzise Umfeldwahrnehmung von Fahrzeugen. Die KI erkennt und klassifiziert dabei Objekte wie Fußgänger in Echtzeit und bewertet de-

ren Verhalten.<sup>9</sup> Weitere Einsatzbereiche sind die Trajektorienplanung welche das Verhalten anderer Verkehrsteilnehmer prognostiziert und darauf reagiert, die Fahrzeuglokalisierung, Sprachsteuerung und die Sicherheitsüberwachung von Fahrsystem.<sup>10</sup> Schwächen bestehen vor allem in der Objekterkennung bei ungünstigen Bedingungen oder gezielter Manipulation der Umwelt.<sup>11</sup> Eine diversifizierte und technisch robuste Trainingsdatenbasis ist somit für derartige Systeme unerlässlich.

## II. Maschinelles Lernen (ML) und neuronale Netzwerke

Um die enge Verzahnung von Technik und Recht sowie deren Problemstellungen nachvollziehen zu können ist es unausweichlich auch die technischen Gegebenheiten von Beginn an mit einzubeziehen.

Moderne KI-Systeme, wie z.B. für das SAE-Level 3, basieren überwiegend auf maschinellem Lernen. Hierbei lernt das System, anhand großer Mengen annotierter Daten Muster zu erkennen, etwa zur Identifikation von Fußgängern.<sup>12</sup> Besonders leistungsfähig, aber schwer durchschaubar, sind neuro-

1 APTIV, Insights, Unsere Geschäftsbereiche, Juli 2024.

2 People of Color (PoC) ist eine internationale Selbstbezeichnung für Menschen mit Rassismuserfahrung bzw. solche, die als nicht-weiß wahrgenommen werden. In dieser Arbeit bezieht sich der Begriff ausschließlich auf sichtbare Hautmerkmale – ohne jede rassistische Konnotation, vgl. Amnesty International, Glossar für diskriminierungssensible Sprache; Universität zu Köln, Chancengerechtigkeit – Antidiskriminierung.

3 Li/Chen/Zhang/Sarro/Zhang/Liu. Bias Behind the Wheel, S. 22.

4 Vgl. SAE, J3016, S.6.

5 Vgl. Becker; Kamal, Selbst ist das Auto, S. 26.

6 Vgl. Becker; Kamal, Selbst ist das Auto, S. 27.

7 KBA, Gesetzgebung zum autonomen Fahren.

8 Vgl. TÜV Rheinland, Assistenzsysteme: Welche es gibt und was 2024 Pflicht wird.

9 Dietmayer, Autonomes Fahren, S. 426-429.

10 Lehrstuhl für Regelungstechnik TU München, Trajektorienplanung fürs Autonome Fahren.

11 DataScientest, Adversarial Examples im Machine Learning.

12 Schmid, Maschinelles Lernen, Bayerisches Forschungsinstitut für Digitale Transformation (bidt).

nale Netzwerke, bei denen Daten durch mehrere Schichten künstlicher Neuronen verarbeitet werden (Deep Learning). Zunächst sind die Gewichte der Neuronen zufällig gesetzt, erst durch wiederholte Anpassung via Backpropagation, einem Rückkopplungsverfahren bei dem das falsche Ergebnis wieder zurück durch jede Schicht und in die einzelnen Neuronen geschickt wird, lernt das Netzwerk, die Parameter so zu optimieren, dass der Output dem gewünschten Ergebnis entspricht.<sup>13</sup> Zwar ermöglichen sie so eine präzise Objekterkennung, ihre Entscheidungen sind jedoch oft nicht nachvollziehbar (Blackbox), ein rechtliches Problem in Bezug auf Haftung und Diskriminierung.<sup>14</sup> Die Qualität und Vielfalt der Trainingsdaten ist entscheidend. Werden bestimmte Gruppen, etwa PoC, nicht ausreichend berücksichtigt, drohen systematische Erkennungsfehler.

### III. Convolutional Neural Networks (CNNs)

CNNs als spezialisierte Klasse der neuronalen Netzwerke sind auf die Verarbeitung von Bilddaten fokussiert und bilden das technische Rückgrat der Objekterkennung. Sie analysieren Bildinhalte Schicht für Schicht und lernen mit Hilfe spezieller Optimierungsverfahren, visuelle Merkmale zuverlässig zu identifizieren.<sup>15</sup> Um reines Auswendiglernen (Overfitting) zu vermeiden und die Robustheit für unbekannte Daten zu erhöhen, werden Validierungsmethoden und gezielte Datenveränderungen (Data Augmentation) eingesetzt. Dennoch können vorhandene Verzerrungen in den Trainingsdaten reproduziert werden, weshalb Fairness und Diskriminierungsfreiheit fortlaufend kontrolliert werden müssen.<sup>16</sup>

### IV. Diskriminierung durch KI

Für die rechtliche Bewertung diskriminierender Entscheidungen autonomer Fahrzeugsysteme ist eine klare Definition von Diskriminierung notwendig. Das Verständnis des AGG und des Art. 3 GG als zentrale Normen zur Bekämpfung von Diskriminierungen werden dazu herangezogen. Zu beachten gilt, dass anders als bei menschlichen Akteuren das Motiv einer KI irrelevant ist, maßgeblich ist allein das Ausgabeergebnis und dessen Wirkung.<sup>17</sup>

Diskriminierung im Sinne des AGG liegt vor, wenn eine ungerechtfertigte Ungleichbehandlung aufgrund geschützter Merkmale erfolgt, § 3 AGG. Diese in § 1 AGG niedergeschriebenen Merkmale, etwa ethnische Herkunft, Behinderung oder Alter sind auch in Art. 3 Abs. 3 GG normiert. Diskriminierungen werden nach dem AGG in unmittelbare (§ 3 Abs. 1 AGG) und mittelbare Benachteiligung (§ 3 Abs. 2 AGG) unterschieden. Im Kontext der KI ist insbesondere die mittelbare Diskriminierung durch scheinbar neutrale Systeme relevant, wenn PoC etwa systematisch seltener als Fußgänger erkannt werden. Auch eine präferenzbedingte Diskriminierung durch voreingenommene Entwicklerentscheidung kann sich negativ auswirken.

Das AGG ist grundsätzlich technologieneutral anwendbar, jedoch erschwert die Intransparenz vieler KI-Systeme die Zurechnung. In der Literatur wird zunehmend gefordert, spezifische gesetzliche Regelungen für algorithmusbasierte Diskriminierung zu schaffen, etwa zur Erweiterung des AGG oder durch neue Diskriminierungskategorien.<sup>18</sup> Dennoch

dient das AGG aufgrund seiner breiten Merkmalsdefinition als geeigneter erster Prüfungsmaßstab.

Grundsätzlich entstehen Diskriminierungen durch KI-Systeme in (teil-) autonomen Fahrzeugen häufig durch unausgewogene Trainingsdaten. Unterrepräsentationen, etwa bei Hautfarbe, Kleidung oder Lichtverhältnissen, führen dazu, dass bestimmte Personengruppen wie PoC seltener korrekt erkannt werden.<sup>19</sup> Auch gesellschaftliche Vorurteile, die in den Datensätzen enthalten sind, sog. Bias, können sich durch das maschinelle Lernen systematisch verstärken.<sup>20</sup> Physikalische Einschränkungen, etwa bei der Beleuchtung, verstärken diesen Effekt zusätzlich. Hinzu kommen Probleme durch falsche Modellarchitekturen, etwa wenn Ausgabeschichten zu wenig differenzierte Kategorien zulassen oder die Feature-Extraktion nicht robust genug ist, um die Vielfalt menschlicher Erscheinungsformen zu erfassen.<sup>21</sup>

### V. Rechtliche Regelungen zu KI in Fahrzeugen

Neben produkthaftungsrechtlichen Normen bilden branchenspezifische Regelungen und die DS-GVO einen zentralen Rechtsrahmen für die Entwicklung und Nutzung von KI-Systemen beim (teil-) autonomen Fahren.

#### 1. Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO schützt, wenn sie anwendbar ist, auch vor diskriminierenden Datenverarbeitungen. Bild- und Videodaten zur Fußgängererkennung gelten regelmäßig als personenbezogene Daten, Art. 2, 4 Nr. 1 DS-GVO, wenn identifizierbare Merkmale wie z.B. Gesichtsgeometrie oder Gangbild enthalten sind.<sup>22</sup> Dies ist durch die bildliche Aufnahme des Fußgängers gegeben. Anonymisierte Daten, etwa durch Unkenntlichmachung von Gesichtern oder ersetzen menschlicher Konturen, können teilweise ausreichen, doch sind reale, unveränderte Verkehrsdaten oft unverzichtbar, um die Leistungsfähigkeit der KI zu sichern. Ziel sollte es jedoch sein stetig mit anonymisierten Daten auszukommen. Die Nutzung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO), wie biometrische Merkmale oder ethnische Herkunft, ist bei der Umfelderkennung nicht primärer Zweck, wird jedoch relevant, wenn gezielt zur Vielfaltserhöhung entsprechende Merkmale erhoben werden.<sup>23</sup> Mithin ist grundsätzlich von personenbezogenen Daten

13 Vgl. Raveling, Was ist ein neuronales Netz?, WFB Wirtschaft Förderung Bremen. Zwar ermöglichen sie so eine präzise Objekterkennung.

14 Vgl. Schmid, Maschinelles Lernen, Bayerisches Forschungsinstitut für Digitale Transformation (bidt).

15 Databricks, Faltungsschichten.

16 Shorten/Koshgoftaar, A survey in Image Data Augmentation for Deep Learning, S. 9.

17 Budelacci, Maschinen haben kein Gewissen. Sie kennen nur 0 und 1, HSLU, Februar 2023.

18 Männing/Hambel, Wie diskriminierend ist Künstliche Intelligenz?, CMS Deutschland Blog.

19 Spiecker/Towfigh, Automatische Benachteiligung, S. 25.

20 Vgl. Holland, Amazon: KI zur Bewerbungsprüfung benachteiligte Frauen.

21 Wilson/Hoffmann/Morgenstern, Predictive Inequity in Object Detection, Februar 2019, S. 2-3.

22 Steege/Winkler, Rechtsfragen zu Testfeldern zur Erforschung automatisierter und vernetzter Mobilität, NZV, 2024, S. 353, Rn. 59.

23 ADAC, Müde oder abgelenkt? Diese Sensoren passen auf, 2022.

auszugehen und im jeweiligen Einzelfall abzuschätzen, ob eine Identifizierung möglich ist.

Verantwortlich im Sinne des Art. 4 Nr. 7 DS-GVO ist in der Regel der Fahrzeughersteller, bei Kooperationen mit Drittfirmen kann eine gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) vorliegen.<sup>24</sup>

Ferner muss eine Verarbeitung gem. Art. 4 Nr. 2 DS-GVO durch den Verantwortlichen stattfinden. Der Begriff der Verarbeitung ist weit auszulegen und umfasst Speicherung, Übermittlung, Löschung sowie jede sonstige Nutzung, auch temporär im Fahrzeug.<sup>25</sup> Ergänzend verpflichtet § 1 g StVG den Halter autonomer Fahrzeuge zur Speicherung spezifischer Betriebs- und Umweltdaten, insbesondere bei Unfällen oder kritischen Ereignissen.

Da die Verarbeitung durch KI-Systeme regelmäßig automatisiert erfolgt, könnte Art. 22 DS-GVO und somit das Verbot der Verarbeitung einschlägig sein, wenn Entscheidungen, etwa zur Erkennung eines Fußgängers, ausschließlich automatisiert getroffen werden und rechtliche Wirkung entfalten.<sup>26</sup> Ziel dieser Vorschrift ist es, die besondere Schutzbedürftigkeit Betroffener zu wahren und zu verhindern, dass Menschen zum bloßen Objekt algorithmischer Entscheidungen degradiert werden. Es ist daher zu klären, ab welchem SAE-Level nicht mehr von einem hinreichenden menschlichen Einfluss ausgegangen werden kann, der eine Anwendung dieser Norm entgegensteht.

Ausnahmen bestehen aktuell bei SAE-Level 3 und niedriger. Die verpflichtende Eingriffsmöglichkeit sowie das Richten der Aufmerksamkeit des Fahrers auf den Straßenverkehr entkräften das Bestehen einer ausschließlich automatisierten Verarbeitung.<sup>27</sup> Der Mensch hat faktisch die Möglichkeit und die Pflicht sich gegen die Entscheidung des Fahrzeuges zu wenden und die Hoheit zu übernehmen.

Ab dem SAE-Level 4 fährt das Fahrzeug in definierten Betriebsbereichen ohne Eingriffspflicht des Menschen. Der Mensch hat keinen hinreichenden Einfluss mehr auf die Entscheidung. In diesen Phasen werden Entscheidungen, auch sicherheitskritische, vollständig durch das System getroffen. Hier liegt in der Praxis erstmals eine rein automatisierte Entscheidung i.S.v. Art. 22 DS-GVO vor, etwa wenn ein Fahrzeug autonom einen Ausweich- oder Bremsvorgang durchführt, der zu einem Unfall mit Personen- oder Sachschaden führt.

Mit dem SAE-Level 5 tritt Vollautonomie ohne menschliche Eingriffsmöglichkeit ein. Jede Fahrentscheidung ist dadurch eine ausschließlich automatisierte Entscheidung. Damit ist Art. 22 DS-GVO hier grundsätzlich einschlägig, und ein Verbot besteht, sofern keine Ausnahme nach Art. 22 Abs. 2 lit. b) DS-GVO greift (z.B. gesetzliche Erlaubnis, wie § 1 g StVG, und geeignete Schutzmaßnahmen durch den Hersteller). Abhilfe könnte durch eine steigende Sensorfusion die entsprechende Nutzung von weiterentwickelten Systemen bringen, die rein mit anonymisierten Daten auskommen.

Ferner muss die Verarbeitung auf einer Rechtsgrundlage des Art. 6 DS-GVO beruhen. Trainingsdaten stützen sich meist auf die Einwilligung, Art. 6 Abs. 1 lit. a) DS-GVO, im Straßenverkehr greift häufig nur die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO.

Im aktiven Straßenverkehr kann sich die Datenverarbeitung nach Art. 6 Abs. 1 lit. f) DS-GVO auf das berechtigte Interesse des Herstellers stützen, vorausgesetzt die Rechte des

Betroffenen überwiegen nicht.<sup>28</sup> Wird auf Pseudonymisierung verzichtet, muss das Interesse des Herstellers an einer effektiven Objekterkennung mit dem Recht auf informationelle Selbstbestimmung vereinbar sein. Dabei gilt der Erforderlichkeitsgrundsatz und es ist zu prüfen, ob der Zweck auch durch mildere, gleich wirksame Mittel erreicht werden kann.

Der Verantwortliche muss dafür einen legitimen Zweck verfolgen. Dieser kann rechtlicher, tatsächlicher, wirtschaftlicher Natur sein oder einen allgemeinen Nutzen haben. Der Automobilhersteller verfolgt primär ein wirtschaftliches Interesse an der Marktreife seines Produktes, sowie das übergeordnete Ziel, die Verkehrssicherheit zu erhöhen und Unfälle zu vermeiden.<sup>29</sup> Zur Erreichung des legitimen Zwecks benötigt es einem ebenso legitimen Mittel. Erst die Außenraumüberwachung ermöglicht es dem Fahrzeug zu „sehen“ und auf Situationen zu reagieren. Mithin ist sie geeignet, den Zweck zu erreichen.

Ferner muss die Verarbeitung erforderlich sein, um berechnete, schutzwürdige, Interessen zu wahren, und es darf kein gleich wirksames milderes Mittel bestehen.<sup>30</sup> Ein solches könnte die Pseudonymisierung der Bilddaten sein, die nach Art. 25 Abs. 1 und 2 DS-GVO ein zentrales Element der Datenminimierung darstellt. Unterbleibt sie, muss der Verantwortliche begründen, warum dies nicht möglich oder zumutbar war. Hohe Sicherheitsanforderungen, wie etwa die notwendige Verarbeitungsgeschwindigkeit in dynamischen Verkehrssituationen, können eine Verarbeitung ohne Pseudonymisierung rechtfertigen, da Verzögerungen zu Fehlentscheidungen führen könnten. Auch für die präzise Trajektorievorhersage ist eine detaillierte Datenerhebung derzeit erforderlich. In Zukunft könnte ein breiterer Datenpool, etwa in einer „Smart-City“, eine stärkere Pseudonymisierung oder Anonymisierung ermöglichen.

Bei der Abwägung ist das allgemeine Interesse am autonomen Verkehr ebenfalls zu beachten. Maßgeblich sind Art und Umfang der Verarbeitung, die Umstände, die Möglichkeit zur Vermeidung der Erfassung, so wie die Zahl der Betroffenen. Fußgänger können sich der Umgebungserkennung kaum entziehen, oft ohne überhaupt von der Verarbeitung zu wissen werden sie Teil dieser. Ein Ausweichen wäre praktisch unzumutbar, zudem ist im öffentlichen Raum ein unbestimmter, großer Personenkreis betroffen.<sup>31</sup>

Aus Sicht des Verarbeiters spricht für die Datenverarbeitung, das nur der unmittelbare Fahrzeugumkreis erfasst und unnötige Daten anonymisiert oder gar nicht erhoben werden. Die Speicherung erfolgt in der Regel nicht dauerhaft, sondern nur bei Unfällen. Aufgrund der Fahrzeugbewegung ist die Erfassung einzelner Personen nur kurzzeitig und be-

24 Sydow/Marsch/Helfrich, DS-GVO/BDSG, 3. Aufl. 2022, Art. 26 DS-GVO Rn. 4.

25 Möller, Die Außenraumüberwachung autonom verkehrender Fahrzeuge, DAR 2021, 608-609.

26 Sydow/Marsch/Helfrich, DS-GVO/BDSG, 3. Aufl. 2022, Art. 22 DS-GVO Rn. 43.

27 Sydow/Marsch/Helfrich, DS-GVO/BDSG, 3. Aufl. 2022, Art. 22 DS-GVO Rn. 44.

28 Möller, Die Außenraumüberwachung autonom verkehrender Fahrzeuge, DAR 2021, 608.

29 Vgl. Möller, Die Außenraumüberwachung autonom verkehrender Fahrzeuge, DAR 2021, 610.

30 Vgl. VG Mainz, Urt. v. 24.9.2020 – 1 K 584/19.MZ, BeckRS 2020, 28535 Rn. 35.

31 Vgl. Möller, Die Außenraumüberwachung autonom verkehrender Fahrzeuge, DAR 2021, 610.

trifft ausschließlich den öffentlichen Raum, nicht die Privat- oder Intimsphäre.<sup>32</sup> Der Eingriff in die informationelle Selbstbestimmung wiegt daher geringer. Zudem dient die Verarbeitung sicherheitsrelevanten Zielen im Interesse der Betroffenen sowie der Allgemeinheit. Mithin überwiegen die Interessen des Verantwortlichen und eine Verarbeitung auf Grundlage des Art. 6 Abs. 1 lit. f) DS-GVO ist zunächst einschlägig.<sup>33</sup>

Führt die Datenverarbeitung zu diskriminierenden Ergebnissen, ist die Interessenabwägung jedoch stets zugunsten der betroffenen Person zu entscheiden. Solche Ergebnisse verstoßen regelmäßig gegen die Grundsätze aus Art. 5 Abs. 1 lit. a) DS-GVO (Rechtmäßigkeit, Treu und Glauben) sowie gegen Art. 25 DS-GVO (Privacy by Design).

Ferner gelten die Datenschutzgrundsätze der DS-GVO uneingeschränkt. Rechtmäßigkeit, Transparenz, Zweckbindung und Datenminimierung müssen ebenso beachtet werden wie präventive technische und organisatorische Maßnahmen nach Art. 24 und 25 DS-GVO. Trotz der Black-Box-Problematik bleibt der Verantwortliche stets zur Auskunft und Nachvollziehbarkeit nach Art. 12-15 DS-GVO verpflichtet und muss die Funktionsweise erläutern können. Die Verletzung datenschutzrechtlicher Pflichten kann infolgedessen zu Schadensersatzansprüchen nach Art. 82 DS-GVO sowie zu Bußgeldern gem. Art. 83 DS-GVO führen.

Ein Problem bleibt die Beweislast, der Betroffene muss die Ursächlichkeit der Diskriminierung durch das System darlegen, was ihm durch technische Intransparenz erschwert wird.<sup>34</sup> Es besteht somit ein rechtliches Risiko für Hersteller, wenn systemische Diskriminierungen nachweisbar sind.

## 2. Branchenspezifische Regelungen

Neben allgemeinen Gesetzen existieren zahlreiche technische Normen und Richtlinien, die speziell auf die Sicherheitsanforderungen von (teil-) autonomen Fahrzeugen zugeschnitten sind.

Zu beachten ist z.B. die von der UNECE als Vorschriften für Typengenehmigungen von Fahrzeugen erlassene UNECE RE 157, welche die automatisierten Spurhaltesysteme (SAE-Level 3) regelt und u.a. die Pflicht zur Datenaufzeichnung bei lernfähigen Algorithmen festlegt.<sup>35</sup> Ferner die UNECE R152, welche Notbremsassistenzsysteme betrifft. Schwachstellen dieser Normen ist ein Fokus auf normale Testbedingungen, das Auslassen von Umgebungsstörungen oder komplexen Verkehrsszenarien, eine fehlende Berücksichtigung von prozessualen Schwächen der KI und zu hohe zugelassene Fehlerquoten im Hinblick auf eine steigende Automatisierung.<sup>36</sup>

Als zentrale ISO-Normen sind die ISO 26262 anzusehen, welche sich mit der funktionalen Sicherheit elektronischer Systeme und Fehlern von sicherheitsrelevanten Komponenten beschäftigt, sowie die ISO/PAS 21448 (SOTIF), welche die ISO 26262 um besondere Fehlfunktionen von KI-Systemen ergänzt und die funktionalen Grenzen prüft. Die SOTIF fördert eine Use-Case-basierte Gefahrenanalyse, etwa für die Fußgängererkennung.<sup>37</sup> Problematisch ist jedoch, dass sich die Norm noch stark an der Rolle des Fahrers als Rückfallebene orientiert (SAE-Level 3), obwohl sich die Verantwortung zunehmend auf das System selbst verlagert.

Die im Dezember 2024 veröffentlichte ISO 8800 ergänzt die SOTIF und schließt eine wesentliche Regelungslücke zur

funktionalen Sicherheit von KI in Straßenfahrzeugen. Sie soll die Entwicklung, Prüfung und den Betrieb von KI-Systemen über den gesamten Lebenszyklus hinweg, von der Trainingsphase bis zum Einsatz im Fahrzeug, standardisieren und befindet sich aktuell in der Anwendung.<sup>38</sup> Ihr Ziel ist es, durch frühzeitige Regulierung diskriminierende Tendenzen zu vermeiden und die Qualität der Daten sowie die Sicherheit auch in Extremsituationen sicherzustellen. Sie klärt die Frage, wie und mit welcher Genauigkeit eine KI im Fahrzeug funktionieren muss damit kein Unfall geschieht. Besonders relevant ist die Festlegung technischer Anforderungen bereits in frühen Entwicklungsphasen. Damit schafft die ISO 8800 erstmals eine fundierte und frühe Grundlage für sichere, innovative KI-Anwendungen in der Automobilbranche.<sup>39</sup> Es bleibt somit abzuwarten, ob sie ihre Wirkung in diesem Bereich vollends entfalten kann.

## 3. Einordnung in deutsches Verfassungsrecht

Das Grundgesetz verpflichtet den Staat zur Gleichbehandlung (Art. 3 Abs. 1 GG) und verbietet Diskriminierung u. a. aufgrund der „Rasse“ (Art. 3 Abs. 3 GG). Im Verhältnis zwischen Privaten, etwa zwischen betroffenen Fußgängern und Fahrzeugherstellern, gilt Art. 3 GG nicht unmittelbar. Eine mittelbare Drittwirkung kann nur unter engen Voraussetzungen greifen, etwa wenn ein strukturelles Machtgefälle besteht und eine Teilhabe am gesellschaftlichen Leben systematisch ausgeschlossen wird.<sup>40</sup>

Im vorliegenden Fall einer potenziellen KI-Diskriminierung durch fehlerhafte Objekterkennung ist eine solche Drittwirkung nicht ohne Weiteres anzunehmen. Weder ist der Automobilhersteller funktional mit dem Staat vergleichbar, noch ist ein gezielter und gewollter Ausschluss von Personen mit bestimmten Merkmalen erkennbar.<sup>41</sup> Zwar kann der Ausschluss von PoC durch algorithmische Verzerrungen faktisch zu Nachteilen führen, doch fehlt es bei SAE-Level 4-5 an der vollständigen Abhängigkeit der betroffenen Person vom System. Um eine derartige Angewiesenheit des Fußgängers bejahen zu können, müssten sämtliche im Straßenverkehr befindliche Fahrzeuge autonom sein und keine Lenkeinrichtung mehr besitzen. Der Straßenverkehr und damit alle in Verbindung stehenden Partizipanten wären somit wesentlich davon abhängig, dass die Systeme sicherheitskritische Aufgaben fehlerfrei ausführen und keine Diskriminierung vornehmen.

Die Rechtsprechung des BVerfG zur mittelbaren Drittwirkung (etwa Stadionverbot-Urteil) wird diskutiert, lässt sich

32 Vgl. Möller, Die Außenraumüberwachung autonom verkehrender Fahrzeuge, DAR 2021, 610.

33 Vgl. Ehmann/Selmayr/Heberlein, 3. Aufl. 2024, Art. 6 DS-GVO Rn. 47.

34 Vgl. AG Bochum, Beschl. v. 11.3.2019 – 65 C 485/18, Rn. 5.

35 Steining, Studie Rechtliche Fragestellungen des automatisierten Fahrens, innocam.NRW, S. 9.

36 Gesmann-Nuissl/Tacke, Funktionale Sicherheit KI-basierter Systeme im Automobilsektor, S. 87.

37 Gesmann-Nuissl/Tacke, Funktionale Sicherheit KI-basierter Systeme im Automobilsektor, S. 87.

38 Held/Bossert/Lenzen/Sutter, KI in sicherheitskritischen Automobilanwendungen, September 2024.

39 Köllner, Christiane, Was leistet der Standard ISO/PAS 8800?, Springer Professional, August 2024.

40 Spiecker/Towfigh, Automatische Benachteiligung, S. 35.

41 Vgl. Härtel, Digitalisierung im Lichte des Verfassungsrechts, LKV 2019, S. 49.

aber nur eingeschränkt übertragen. Eine strukturelle Überlegenheit, wie sie bei KI-gestützten Entscheidungen denkbar ist, müsste aktiv genutzt werden, um Diskriminierung zu bewirken oder in Kauf zu nehmen, was hier mangels bewusster Gestaltung nicht vorliegt.<sup>42</sup>

Eine grundrechtliche Haftung des Herstellers über Art. 3 GG scheidet aus. Fraglich ist, ob diese Schutzlücke durch das einfachgesetzliche Antidiskriminierungsrecht zu schließen ist.

#### 4. Allgemeines Gleichbehandlungsgesetz

Das Allgemeine Gleichbehandlungsgesetz (AGG) schützt vor Diskriminierung u.a. wegen der ethnischen Herkunft, des Geschlechts oder einer Behinderung. Zwar ist das AGG technologieneutral formuliert und grundsätzlich auf KI übertragbar, sein Anwendungsbereich ist jedoch u. a. auf bestimmte schuldrechtliche Konstellationen beschränkt (§ 19 AGG).<sup>43</sup> Die Diskriminierung durch KI im Außenraum eines (teil-) autonomen Fahrzeugs, etwa bei nicht Erkennung eines Fußgängers, fällt mangels Vertragsbeziehungen nicht unter den Schutzbereich des AGG. Anders kann dies im Bereich des Interieur-Sensing sein, etwa bei Benachteiligungen durch Gestensteuerung oder Müdigkeitserkennung, da hier ein verträgliches Schuldverhältnis angenommen werden kann.<sup>44</sup>

Die geschützten Merkmale des § 1 AGG sind grundsätzlich für KI-Anwendungen geeignet, eine Erweiterung auf neue technische Diskriminierungsdimensionen könnten jedoch erforderlich werden und wird diskutiert.

Adressat des AGG ist derjenige, der Einfluss auf das System nimmt, regelmäßig wäre dies also der Fahrzeughersteller.

Die Antidiskriminierungsstelle kann Betroffene unterstützen, besitzt aber keine Auskunftspflicht gegenüber Unternehmen, was den Rechtsschutz Betroffener einschränkt.<sup>45</sup> Beweiserleichterungen (§ 22 AGG) entlasten Betroffene nur teilweise, da die Grundtatsache der Diskriminierung weiterhin selbst zu belegen ist.<sup>46</sup> Ansprüche auf Schadens- und Entschädigungszahlungen (§ 21 AGG) sind somit bei erfolgreicher Geltendmachung möglich, auch für immaterielle Schäden.

Ferner kann eine mittelbare Diskriminierung durch KI unter engen Voraussetzungen gerechtfertigt sein, etwa bei Erreichung eines legitimen Ziels durch verhältnismäßige Mittel (§ 3 Abs. 2 AGG) bei der Airbagauslösung von kleinwüchsigen Menschen.<sup>47</sup> Unmittelbare Benachteiligung wegen der ethnischen Herkunft hingegen sind grundsätzlich nicht gerechtfertigt (§ 20 AGG).

Die Analyse zeigt, trotz technikoffener Formulierungen weist das AGG Schutzlücken bei KI-bedingten Diskriminierungen auf, insbesondere außerhalb vertraglicher Beziehungen. Eine risikobasierte Erweiterung des Anwendungsbereichs oder die Schaffung neuer spezifischer Regelungen sollte weiterhin in Betracht gezogen werden.

## VI. § 823 BGB als Auffanganspruch

Sofern das AGG keine Anwendung findet, bleibt Betroffenen lediglich der zivilrechtliche Weg über § 823 Abs. 1 BGB, um Schadenersatz für Folgen der durch die KI verursachten Diskriminierung geltend zu machen. Im Falle einer physischen Schädigung, bei der Nichterkennung eines Fußgängers durch ein (teil-) autonomes Fahrzeug, sind die Rechtsgüter Körper oder Gesundheit regelmäßig betroffen. Die Entscheidung des

KI-Systems, trotz Vorhandenseins eines Fußgängers sowohl in der realen Situation als auch in den Daten, nicht abzubremsen stellt ein aktives Tun dar, nicht bloß ein Unterlassen da es sich bewusst zur Weiterfahrt entscheidet. Zusätzlich kann das Unterlassen der Fehlerbehebung durch den Automobilhersteller als Handlung aufgrund seiner Garantenstellung gesehen werden.<sup>48</sup> Kausalität, Rechtswidrigkeit und Verschulden, insbesondere in Form fahrlässiger Produktfreigabe oder unzureichender Validierung durch den Hersteller, sind in der Regel ebenfalls zu bejahen.<sup>49</sup> Gleiches gilt für Systeme der Level 3, teilweise bis Level 4, welche den Fahrer als Überprüfendes und eingreifendes Organ besitzen, wenn dieser gem. § 276 Abs. 2 BGB seine im Verkehr erforderliche Sorgfalt außer Acht lässt.

Die deliktische Haftung kann sich je nach Automatisierungsgrad sowohl gegen den Fahrer bzw. Halter (insbesondere bei Level 3-4 mit Eingriffspflicht) als auch gegen den Hersteller richten. Die Herstellerhaftung gewinnt dabei zunehmend an Bedeutung, da dieser letztlich die KI in Verkehr bringt und damit das Risiko setzt. Die Halterhaftung nach § 7 StVG bleibt daneben bestehen, wobei Versicherer im Innenverhältnis Rückgriff gegen den Hersteller nehmen könnten.

Diese Konstellation zeigt, dass trotz Lücken im Antidiskriminierungsrecht zumindest über das Deliktrecht eine individuelle Kompensation erreichbar ist, gleichwohl ohne präventive Wirkung.

## VII. Einfluss der KI-VO

Die im Juni 2024 in Kraft getretene KI-VO schafft erstmals einen umfassenden EU-Rechtsrahmen für den Einsatz von KI. Ziel ist ein grundrechtsschützender, risikobasierter Umgang mit KI bei gleichzeitiger Innovationsförderung (Art. 1 KI-VO). Erfasst werden alle Akteure entlang der KI-Wertschöpfungskette, auch Fahrzeug-KI wie Objekterkennungs- oder Interieur-Sensing-Systeme (Art. 2 KI-VO).<sup>50</sup>

Die Verordnung unterscheidet vier Risikoklassen, wobei Hochrisiko-KI strenge Vorgaben etwa zur Datenqualität und Transparenz erfüllen muss (Art. 6-14 KI-VO).<sup>51</sup> Fahrzeug-KI zählt zwar aufgrund ihres hohen Risikos für die Gesundheit, Sicherheit oder Grundrechte von Menschen zur Hochrisiko-Kategorie, ist jedoch vom Anwendungsbereich ausgenommen, da sie bereits durch sektorale Harmonisierungsrechtsvorschriften (etwa EU-VO 2018/858 oder 2019/2144) reguliert sind (Anhang I Teil B KI-VO).<sup>52</sup> Die Ausnahme, auf Initiative der Automobilindustrie, soll Innovationshemmnisse vermeiden, birgt aber die Gefahr von neuen Regelungslücken, insbesondere im Bereich des Diskriminierungsschutzes.

42 Spiecker/Towfigh, Automatische Benachteiligung, S. 35.

43 MüKoBGB/Thüsing, 9. Aufl. 2021, AGG § 19 Rn. 1.

44 Lehbrink, Manuel, Bei BMW kann man Sitzheizung jetzt als Abonnement buchen.

45 Spiecker/Towfigh, Automatische Benachteiligung, S. 47.

46 MüKoBGB/Thüsing, 9. Aufl. 2021, AGG § 22 Rn. 6.

47 MüKoBGB/Thüsing, 9. Aufl. 2021, AGG § 22 Rn. 6.

48 MüKoBGB/Wagner, 9. Aufl. 2024, BGB § 823 Rn. 221.

49 MüKoBGB/Wagner, 9. Aufl. 2024, BGB § 823 Rn. 86.

50 Schwartmann/Keber/Zenner/Keber/Zenner, KI-VO Leitfaden, S. 42, Rn. 18-20.

51 Schwartmann/Keber/Zenner/Schwartmann/Köhler, KI-VO Leitfaden, S. 53, Rn. 53.

52 Schwartmann/Keber/Zenner/Schwartmann/Pottkämper, KI-VO Leitfaden, S. 80, Rn. 158.

Durch die Ausnahme der Fahrzeug-KI vom Anwendungsbereich der KI-VO greifen zentrale Schutzmechanismen wie Anforderungen an Trainingsdaten (Art. 10 KI-VO), Protokollierung (Art. 12 KI-VO) oder menschliche Aufsicht (Art. 14 KI-VO) nicht. Stattdessen gelten UNECE-Regelung und ISO-Normen wie ISO 26262 oder SOTIF, die jedoch diskriminierungsrelevante Aspekte bislang wenig berücksichtigen.

Zwar setzt die neue ISO 8800 erste Maßstäbe zur Berücksichtigung von Bias und Trainingsdatenqualität, doch ist ihre Umsetzung noch lückenhaft, insbesondere bei bereits eingesetzten Systemen. Der Ansatz der branchenspezifischen Eigenregulierung ist zwar zu begrüßen, jedoch verbleiben, wie aufgezeigt, dadurch noch immer Schutzlücken. Aktuelle Standards adressieren primär funktionale und zu wenig ethische oder diversitätsbezogene Anforderungen.

Kaum umzusetzen ist die in Art. 14 KI-VO vorgesehene menschliche Aufsicht. Sie ist im Straßenverkehr kaum praktikabel, insbesondere bei plötzlichen Gefahrensituationen durch den Einsatz von Teleoperatoren, etwa in SAE-Level 4 Fahrzeugen.<sup>53</sup> Zudem besteht hier das Risiko des Automatisierungsbias, also der unkritischen Übernahme von KI-Entscheidungen durch den Teleoperator.<sup>54</sup>

### VIII. Fazit und Präventionsstrategien

Diskriminierung durch KI in (teil-)autonomen Fahrzeugen, insbesondere gegenüber PoC, sind systemisch bedingt und bislang rechtlich unzureichend adressiert. Hauptursachen sind unausgewogene Trainingsdaten und technische Grenzen der Bilderkennung. Zwar liefern die eingesetzten CNNs präzise Ergebnisse, doch ihre Intransparenz erschwert den rechtlichen Nachweis diskriminierender Entscheidungen.

Für Diskriminierungsfreie KI tragen Entwickler und Fahrzeughersteller besondere Verantwortung. Vielfältiger Trainingsdaten, gegebenenfalls synthetisch ergänzt, sowie optimierte Bildverarbeitung und Sensorfusion können die Erkennung unterrepräsentierter Gruppen

verbessern. Zugleich sind dabei datenschutzrechtliche Vorgaben (Art. 9 DS-GVO) und die Vermeidung indirekter Diskriminierung zu beachten.

Da die KI-VO Fahrzeug-KI nicht erfasst, ist die Vertiefung ihrer Schutzprinzipien insbesondere zur Datenqualität und Protokollierung, in Normen wie die ISO 8800 erforderlich. Auch klare Dokumentationspflichten und vertragliche Regelungen zwischen Herstellern und Zulieferern sind nötig, um Nachbesserungen zu erleichtern und Haftungsfragen abzusichern.

Rechtlich bestehen Schutzlücken, weder das AGG noch Art. 3 GG greifen wirksam und datenschutzrechtliche Mittel entfalten häufig erst post hoc Wirkung. § 823 Abs. 1 BGB bietet betroffenen zivilrechtlichen Schutz, jedoch keine präventive Wirkung. Umso wichtiger wird ein Zusammenspiel aus technischer Verbesserung, verbindlichen Standards und datenethischer Verantwortung angesehen, um einen diskriminierungsfreien KI-Einsatz im Straßenverkehr zu gewährleisten.



#### Alexander Stichling

ist HR Specialist mit Schwerpunkt Datenschutz beim Automobilzulieferer APTIV.

<sup>53</sup> DLR, Teleoperation hilft, wenn das autonome Fahrzeug nicht weiterweiß.

<sup>54</sup> Schwartzmann/Keber/Zenner/Schwartzmann/Keber/Köhler, KI-VO Leitfaden, S. 136, Rn. 344.

# KURZBEITRÄGE

## Prüfen in der „KI-Ära“

Prof. Dr. Rolf Schwartmann/Moritz Köhler\*

Die KI-generierte Hausarbeit ist nur einen Klick entfernt. KI-Systeme wie ChatGPT gehören heute zum festen Bestandteil des universitären Werkzeugkastens: In einer Studie der Hochschule Darmstadt gaben 90 % der befragten Studierenden an, KI-Tools für ihr Studium zu nutzen. Die Anwendungsgebiete reichen von der Literaturrecherche über die Datenanalyse und die Problemlösung bis hin zur Texterstellung. Das Thema drängt Studierende wie Lehrpersonal wünschen sich eine klare Positionierung der Hochschulen, doch diese agieren überwiegend zurückhaltend.

### I. KI-Einsatz durch Studierende

Das mag an nachvollziehbaren Vorbehalten gegenüber dem KI-Einsatz durch Studierende liegen. Schon intuitiv haben wir Bedenken: Wenn KI das Denken übernimmt, kann das zwar kurzfristig zu schnelleren und besseren Ergebnissen führen. Langfristig lagern die Studierenden damit allerdings nicht nur das Denken, sondern auch den Lerneffekt aus. Eine Studie des Massachusetts Institute of Technology (MIT) hat dieses Störfühl kürzlich bestätigt. Die Forscher fanden heraus, dass Studierende „kognitive Schulden“ anhäufen, wenn sie beim Verfassen von Aufsätzen auf KI-Assistenten wie ChatGPT zugreifen. Was Studierende durch den Einsatz von KI also an Denkarbeit einsparen, bezahlen sie später mit geringeren Lernerfolgen.

Sollten wir also Wege suchen, KI aus den Hochschulen zu verbannen? Das dürfte die Studierenden kaum angemessen auf eine Arbeitswelt vorbereiten, in der sich 97 % der Unternehmen mit dem Einsatz generativer KI beschäftigen. Der verantwortungsvolle Einsatz Künstlicher Intelligenz in dieser Welt verlangt menschliche Kontrolle. Diese Kontrolle kann nur gewährleisten, wer neben fachlichen Fähigkeiten auch über Fähigkeiten im Umgang mit KI verfügt. Die KI-Verordnung der Europäischen Union verpflichtet Unternehmen schon heute zur Vermittlung von KI-Kompetenz, wenn sie KI entwickeln oder einsetzen. Sie müssen ihren Mitarbeitern Fähigkeiten und Kenntnisse vermitteln, die einen sachkundigen Einsatz erlauben. Übertragen auf Hochschulen bedeutet das: Sie müssen dafür sorgen, dass die Studierenden eigenständige Leistungen erbringen, um einen fachlichen Lernerfolg zu garantieren. Zugleich müssen sie den Umgang mit KI lehren.

Die Sicherung eigenständiger Leistungen bei gleichzeitiger Vermittlung von KI-Kompetenz ist ein Balanceakt. Dennoch adressieren die wenigsten Prüfungsordnungen an deutschen Hochschulen dieses komplexe Verhältnis. Damit entziehen sich die Einrichtungen ihrer Verantwortung. Denn unter der fehlenden Regelung leidet die Rechtssicherheit und damit schließlich der Prüfling. Wo klare Regelungen zum Einsatz von KI fehlen, müssen die Studierenden die Zulässigkeit anhand der hergebrachten und allgemeinen Bestimmungen des Prüfungsrechts selbst erproben.

### II. Prüfungsrechtliche Bewertung

Nach allgemeinem Prüfungsrecht liegt eine Täuschungshandlung vor, wenn der Prüfling eine selbstständige und reguläre Prüfungsleistung vorspiegelt, obwohl er unerlaubte oder nicht offen gelegte Hilfsmittel genutzt hat. Wer eine ganze Hausarbeit von einer KI formulieren lässt und diese als eigene Leistung einreicht, begeht eine Täuschungshandlung. Für diese Feststellung bedarf es keiner vertieften Kenntnisse im Prüfungsrecht. Allerdings verstecken sich mittlerweile auch hinter einfachen Korrekturhilfen KI-Anwendungen. Täuscht der Studierende also bereits, wenn er von einem Textprogramm Rechtschreibung und Grammatik seiner Arbeit prüfen lässt? Schon dazu dürften verschiedene Prüfer unterschiedliche Ansichten vertreten. Ohne eindeutige Regelung trägt zunächst der Prüfling das Risiko, die Einstellung seines Prüfers zum KI-Einsatz falsch einzuschätzen.

Daneben tritt ein praktisches Problem. Geht ein Studierender gerichtlich gegen den Vorwurf einer Täuschungshandlung vor, liegt die Beweislast bei der Prüfungseinrichtung. Diese hat aber oft keine wirksame Möglichkeit, den Einsatz von KI nachzuweisen. Für andere Täuschungshandlungen im Rahmen schriftlicher Arbeiten helfen den Hochschulen vor den Verwaltungsgerichten die Grundsätze des Anscheinsbeweises. Die Gerichte vermuten, dass ein Studierender getäuscht hat, wenn ein typischer Sachverhalt vorliegt, der diesen Schluss nach allgemeiner Erfahrung zulässt. Nur durch den Nachweis besonderer Umstände, die einen atypischen Geschehensablauf ernsthaft möglich erscheinen lassen, kann der Studierende diese Vermutung widerlegen.

Die Grundsätze des Anscheinsbeweises ermöglichen in vielen Prüfungssituationen eine praktikable und gerechte Lösung. Anders als das Verwaltungsgericht München in einer Entscheidung im November 2023 annahm, dürften sie auf den Einsatz von KI hingegen nicht übertragbar sein. Denn wie sehen ein typischer Sachverhalt und die allgemeine Erfahrung bei einem Phänomen aus, das erst seit wenigen

\* Prof. Dr. Rolf Schwartmann ist Leiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln, ist Mitherausgeber von *Recht der Datenverarbeitung (RDV)* sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Moritz Köhler ist wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln.

Jahren überhaupt vorstellbar ist? Allein auf die Ergebnisse KI-basierter Überprüfungssoftware können und dürfen sich Hochschulen und Gerichte jedenfalls nicht verlassen. Wenn KI einen Text auf KI überprüft, sind Prüfling und Prüfer nur noch Beifahrer eines autonomen Bootes, das unkontrolliert in Richtung Wasserfall beschleunigt. Das ist weder aus gesellschaftlicher, noch aus technischer Perspektive sinnvoll und deshalb zurecht verboten.

### III. Vorschlag zur praktischen Umsetzung

Die Hochschulen müssen also umdenken. Es hilft niemandem, die Realität des KI-Einsatzes in studentischen Hausarbeiten zu ignorieren. Schon aus Gründen der Bestimmtheit müssen die Prüfungsordnungen der Bildungseinrichtungen deshalb die Zulässigkeit des Einsatzes von KI und dessen Grenzen regeln. Dazu braucht es auch neue Prüfungsformate, die die tatsächlichen und rechtlichen Herausforderungen des zunehmenden KI-Einsatzes adressieren und die KI-Kompetenz der Studierenden fördern. Bei der Entwicklung solcher Formate müssen die Hochschulen vieles berücksichtigen: Datenschutz spielt eine Rolle, auch Urheber- und Persönlichkeitsrechte sollten sie im Blick behalten. Richtig umgesetzt leisten derartige Projekte aber nicht nur einen Beitrag zur Entwicklung der Studierenden, sondern auch zur Chancengleichheit. Ansonsten profitiert im Zweifel der Prüfling, der sich die bessere KI leisten kann.

An der Technischen Hochschule Köln existiert bereits ein Prüfungsformat, das die fachlichen Fähigkeiten der Prüflinge ebenso fordert und fördert wie ihre KI-Kompetenz. Statt die Studierenden bei der Bestimmung des zulässigen KI-Einsatzes im Regen stehen zu lassen, bindet etwa der Studiengang Wirtschaftsrecht die Technologie bei einigen Hausarbeiten aktiv in die Prüfung ein. Der Einsatz von KI ist in diesen Hausarbeiten ausdrücklich gestattet. Aufgabe der Studierenden ist es, im Dialog mit dem hauseigenen Chatbot eine Arbeit zu einem vorgegebenen Thema zu verfassen. Neben der inhaltlichen Leistung ist für die Bewertung entscheidend, dass die Prüflinge aufzeigen, an welchen Stellen der Bot an seine Grenzen gestoßen ist – etwa, weil er falsche Informationen ausgegeben oder eine kreative Lösung nicht gefunden hat.

Die Ergebnisse dieser Auseinandersetzung stellen die Studierenden in einer mündlichen Prüfung vor.

Die Hausarbeit wird bei der Bildung der Gesamtnote mit 40 % gewichtet und der mündliche Vortrag mit 60 %. Die Prüfungsordnung der Fakultät lässt den Einsatz von KI als Hilfsmittel nach dieser Maßgabe zu. So kann der Prüfer auf Grundlage des Prüfungsrechts unter Wahrung von Chancengleichheit und Prüfungsgerechtigkeit eine Bewertung vornehmen, die die Leistung des Prüflings unter kontrolliertem Einsatz von KI bewertet. Die Fakultät hat sich aus diesem Grund dafür entschieden, sowohl in Bachelor- als auch in Masterprüfungen eine vergleichbare Kombination aus häuslicher Arbeit und mündlicher Prüfung vorzusehen.

Um in diesem Format gute Ergebnisse zu erzielen, müssen die Prüflinge die Ergebnisse der KI hinterfragen. Dazu müssen sie jedenfalls grundlegend die Funktionsweise der Anwendung verstehen und fachliche Fehler der KI erkennen können. Das Prüfungsformat adressiert damit auch ein psychologisches Phänomen, das die Kontrolle Künstlicher Intelligenz in der Praxis erschwert: den Automatisierungsbias. Bereits 1999 fanden Forscher heraus, dass Menschen dazu neigen, maschinelle Ergebnisse als besonders verlässliche Erkenntnisquelle zu betrachten. Sie stimmen der Maschine zu, obwohl ihre Fachkenntnisse einen anderen Schluss verlangen und sie erkennen nicht, dass die Maschine relevante Informationen unberücksichtigt lässt. Als wirksame Gegenmaßnahme ermittelte die Forschungsgruppe die Zuweisung inhaltlicher Verantwortung. Für den Umgang mit einem Chatbot bedeutet das: Nur wer die KI als fachlich unterlegenen Assistenten begreift, ist im Dialog mit ihr in der Lage, dem Automatisierungsbias zu entgehen.

### IV. Fazit

Prüfungseinrichtungen und Prüfer müssen Verantwortung übernehmen und sich klar zum Einsatz von KI durch die Studierenden positionieren. Nur so können sie Rechtsunsicherheit vermeiden und Prüfungsformate entwickeln, die sowohl fachliche Fähigkeiten als auch KI-Kompetenz fördern. Gelingt die Integration Künstlicher Intelligenz, profitieren Hochschulen ebenso wie Studierende.

# Semantic Risk Classification – need for runtime solutions

Ganesh Srinivasan\*

This is a follow-up to my article on End-User responsibilities on a GPAI system that was published recently at – <https://www.rdv-online.com/print/ausgabe-4-2025/end-user-responsibilities-on-a-generative-ai-conversation/>.

I was contemplating titling this as either “Runtime Ontology” vs being a little more descriptive – in calling out the need for staying dynamic with semantic risk classification. Stuck with the simpler and more descriptive title, as you can see above!

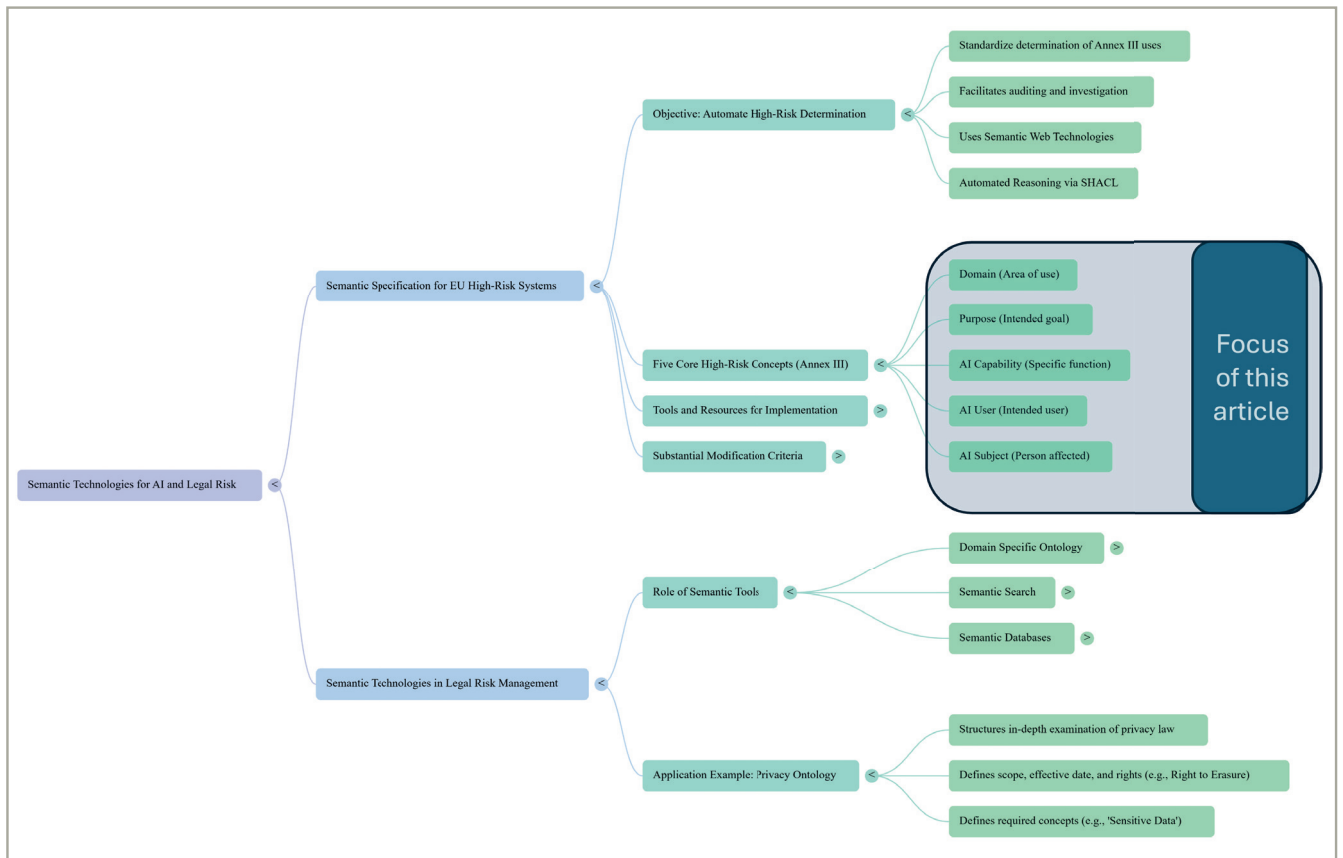
To set some context, we could define Semantic Risk Classification on the following lines:

A dynamic approach to evaluating and categorizing risks in AI systems based on the actual meaning, context, and intent of user interactions, model outputs, and system behaviors—rather than relying solely on static, predefined use cases or domains. This enables real-time identification and mitigation of evolving risks as AI systems operate in unpredictable environments.

## I. Scope

I also used Notebook LM to get me a jump start in this topic on the below lines. Fascinating mind-map, in my view.

The AI act has multiple aspects in relevance, but we will focus primarily on the shaded regions above, that talk about – what defines a High-Risk system.



The Five Core High-Risk Concepts that determine classification are:

1. Domain: The area in which the AI system is used.
2. Purpose: The intended goal of the AI system
3. AI capability: Specific function the AI system performs
4. AI user: Who is the intended user of the AI system
5. AI subject: The person or entity about whom the AI system makes a decision

its domain and capabilities offered and make a determination on whether it qualifies for a high-risk AI system or not. However, given that the model behind the scenes is a GPAI model – that has far reaching capabilities outside of the intended boundaries, it does leave a large gap to our own imagination, which may or may not be captured by guardrails in play.

The current approach seems a little too static where we go about defining the purpose of an AI system, largely based on

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

Just to recap from the previous article, a high-risk AI system could deal with one or more of the following.

High-Risk AI Category
Biometric identification and categorization
Critical infrastructure management
Education and vocational training
Employment, workers management, and self-employment
Access to essential private and public services
Law enforcement
Migration, asylum, and border control management
Administration of justice and democratic processes

## II. Risk of compromise

If we now dig into each of the above parameters that drive a risk classification, they could be examined this way.

Parameter	Ease of compromise (how easily real use deviates from the intended classification)	Typical guardrails and extent of protection
<b>Domain</b>	Medium–High. “Domain drift” in open chat or with broad RAG can pull the system into high risk domains (e.g., HR, credit, law enforcement) without design intent.	Domain whitelists/blacklists; runtime domain classifier + refusal/route; tenant/data segmentation; DLP and egress allow lists.  <b>Protection:</b> moderate if enforced at runtime; weak if only documented in policy.
<b>Purpose</b>	High. Function creep: advisory turns into decisioning; users ask for actions beyond scope; prompt injection reframes intent.	Policy as code for allowed intents; action gating/human in the loop for decisioning; mandatory approvals; prompt signing/constraints; post hoc decision logs.  <b>Protection:</b> moderate–strong if gates block execution, weak if only warnings/disclaimers.

Parameter	Ease of compromise (how easily real use deviates from the intended classification)	Typical guardrails and extent of protection
<b>AI capability</b>	High. Tooling/plugins (code exec, RPA, data writes, email/send, procurement) and model updates constantly bring about further improvements.	Least privilege tool permissions; sandboxed execution; network egress allow list; rate limits; kill switch; capability change reviews/red teaming.  <b>Protection:</b> strong if capabilities are permissioned and sandboxed; moderate otherwise.
<b>AI user</b>	High. Broad access, weak identity, or low literacy raises misuse and insider risk; external users may weaponize prompts.	Strong IAM (MFA, RBAC/ABAC with purpose binding), scoped tokens, session risk scoring, usage education, anomaly detection, audit trails.  <b>Protection:</b> moderate–strong if tied to ABAC + monitoring; weak with generic SSO only.
<b>AI subject</b>	Medium (can be High for vulnerable groups). Bias, unfair impact, or opaque logic affects individuals rights even in “advisory” modes.	Data minimization, PII detection, fairness testing/monitoring, DPIA, notice/contestability, explainability, human review for impactful outcomes, retention/erasure controls.  <b>Protection:</b> moderate; becomes strong with continuous fairness monitoring and enforced review gates.

## III. Runtime Solutions

The current AI solution stack – at an abstracted level has the following options.

Emerging GenAI/LLM-specific security categories.

Category	Purpose (what it does)	Typical risks addressed
LLM Firewall	Filters/blocks malicious inputs/ outputs; enforces rules; prevents exfiltration	Prompt injection, jailbreaks, data leakage, unsafe actions
LLM Automated Benchmarking (incl. vuln scanning)	Probes models to find weaknesses; evaluates behavior across scenarios	Injection/adversarial inputs, leakage, bias, robustness gaps
LLM Guardrails	Constrains model behavior with policies, content filters, intent validation	Harmful/biased content, policy violations, unsafe tool use
AI Security Posture Management (AI-SPM)	Lifecycle posture, governance, and drift/attack monitoring for AI systems	Data poisoning, model drift, adversarial attacks, leakage, compliance gaps

Below is a merged table: your risk parameters + emerging GenAI/LLM categories + best-fit solutions from the OWASP landscape.

Parameter	Ease of compromise	Typical guardrails & protection	Best-fit emerging category	Suggested solutions (examples from OWASP matrix)
Domain	Medium-High	Whitelists/blacklists; runtime domain classifier + refusal/route; tenant/data segmentation; DLP/egress controls. <b>Protection:</b> moderate if enforced at runtime.	LLM Guardrails; LLM Firewall; AI SPM (monitor drift)	Cisco AI Runtime (LLM enabled WAF/guardrails); Lasso Secure Gateway for LLMs; Prompt Security (governance + guardrails); Pangea Prompt Guard; Lakera (monitor); PromptGuard OSS (Meta)

Parameter	Ease of compromise	Typical guardrails & protection	Best-fit emerging category	Suggested solutions (examples from OWASP matrix)
Purpose	High	Policy as code for allowed intents; action gating/HITL; approvals; prompt signing/ constraints; decision logs. <b>Protection:</b> strong if gates block execution.	LLM Guardrails; LLM Firewall; AI SPM (governance)	Lasso Secure Gateway; Prompt Security; Cisco AI Runtime (runtime gating); Pangea Authorization/Authentication (intent bound access); AI Sec Platform (Hidden-Layer) for ongoing posture/compliance
AI capability	High	Least privilege tools; sandbox; egress allow lists; rate limits; kill switch; change reviews/red team. <b>Protection:</b> strong with permissioned/sandboxed tools.	LLM Guardrails; LLM Firewall; AI SPM	Cisco AI Runtime (tool/command guard + RASP); ZenGuard AI (guardrails + DLP); LLM Guard (Protect AI) (runtime protections); Pangea Authorization (scoped tokens); PurpleLlama CodeShield (unsafe code generation)

Parameter	Ease of com-promise	Typical guar-drails & protec-tion	Best-fit emerging category	Suggested solutions (exam-ples from OWASP matrix)
AI user	High	Strong IAM (MFA, RBAC/ ABAC with purpose binding); scoped tokens; session risk scoring; edu-cation; anomaly detec-tion; audit trails. <b>Protec-tion:</b> moderate-strong with ABAC + monito-ring.	LLM Gu-ardrails; AI SPM (monitor users); LLM Firewall (block abusive prompts)	Pangea Authen-tication/ Autho-rization; Cisco AI Runtime (prompt security/filters); AI Sec Platform (Hidden-Layer), SPLX.AI, Lakera (user/ anomaly moni-toring, com-pliance tracking)
AI sub-ject	Medium → High (for vul-nerable groups)	Data minimi-zation; PII detection; fairness testing/ moni-toring; DPIA; explai-nability; HITL for impactful outco-mes; retention/ erasure. <b>Protec-tion:</b> strong with con-tinuous moni-toring + review gates.	AI SPM; LLM Au-tomated Bench-marking; LLM Gu-ardrails	AI Verify (bias/ fairness oversight OSS); Giskard (bias/ adversarial tests OSS); En-krypt AI, Prompt Foo (eval/ bench-marking OSS/prop); Pangea Redact/ Data Guard; Cloaked AI (PII pro-tection); ZenGuard AI, LLM Guard (privacy/ DLP guar-drails)

To summarize the solution alternatives to our Categories:

- Domain: Cisco AI Runtime + Lasso + Lakera.
- Purpose: Lasso + Prompt Security + Pangea Authorization.
- AI capability: Cisco AI Runtime + PurpleLlama Code-Shield + Pangea Authorization.
- AI user: Pangea Authentication + AI Sec Platform.
- AI subject: AI Verify + Giskard + Pangea Redact/Cloaked AI.

#### IV. Risk Assessment priorities

From a risk management perspective, it is better to review every single AI solution on the below lines to better assess the need for external or commercial solutions as the dynamic layer of protection.

Parameter	Assess-ment lines (questions to answer)	Baseline controls (OSS/DIY)	Add dynamic solutions when...
Domain	Regulated domain involved? RAG uses external/ cross tenant data? Do-main drift observed in pilots? Cross border/eg-ress requirements? Evidence of residency/ compliance needed?	Domain allow/deny lists; runti-me domain classifier + refusal/route; tenant/ data seg-mentation; DLP; egress allow lists; audit logs	Drift exceeds threshold; external/ unvetted sources enabled; multi tenant production; cross border data flows; compliance attestation required → add runtime guardrails/ firewall and continuous posture/drift monitoring
Purpose	Advisory vs. action/decision? Users request out of scope actions? Write backs/ emails/pro-curement integrations? HITL enforced?	Policy as code for allowed intents; action gating/approvals; HITL; prompt constraints/ signing; decision logs	Any auto-matic actions beyond advisory; high volume transactions; function creep/ injection reframing detected; auditable approvals mandated → add exe-cution gates, runtime refusal/ route, and governance posture monitoring

Parameter	Assessment lines (questions to answer)	Baseline controls (OSS/DIY)	Add dynamic solutions when...
<b>AI capability</b>	Tools/plugins enable code exec/RPA/data writes? Execution sandboxed? Egress allow lists/rate limits/kill switch in place? Capability changes reviewed/red teamed?	Tool allow list; least privilege scopes; sandboxed execution; egress allow lists; rate limits/kill switch; OSS unsafe code checks	Multiple high impact tools or unsandboxed paths; autonomy in production; persistent exfil attempts; capability changes without review → add runtime protection/guardrails, adaptive throttling, and capability posture monitoring
<b>AI user</b>	External/contractor access? Privileged roles? MFA + ABAC tied to purpose? Anomaly detection and user education?	SSO + MFA; RBAC/ABAC with scoped tokens; session risk scoring; usage education; audit trails	Large/heterogeneous user base; privileged operations; repeated prompt abuse; elevated session risk → add real time prompt filtering, risk based step up auth, user/anomaly monitoring and automated containment

Parameter	Assessment lines (questions to answer)	Baseline controls (OSS/DIY)	Add dynamic solutions when...
<b>AI subject</b>	PII/sensitive data processed? Vulnerable groups impacted? Fairness/explainability obligations? Retention/erasure needed? Human review for impactful outcomes?	Data minimization; PII detection/redaction; OSS fairness/adversarial tests; DPIA; explainability notes; retention/erasure gates; human review	High stakes individual impact; regulated fairness/reporting; high data volumes; drift in fairness metrics → add continuous fairness monitoring, runtime DLP/redaction, enforced review gates and auditable outcomes tracking

### V. Closing thoughts

Static decision making on identifying a high-risk system is challenged already. The push to solutions that operate at runtime on the user prompts, model response, underlying data, behavior/pattern analysis will become mainstream as quickly as the models and GPAI systems evolve.

Ultimately, this shift is driven by the need for compliance. Continuous assessment is the only viable path to demonstrate that a system remains within its defined risk profile, preventing functional drift, managing vulnerability to jailbreaks, and ensuring fairness metrics do not degrade. The risk assessment categories should keep pace with this rate of change.

For any organization deploying AI, especially those falling under the high-risk classification defined by the EU AI Act's Annex III, the regulatory mandate is clear: trustworthiness and compliance must be demonstrable. Moving beyond simple upfront documentation, the incorporation of runtime classifiers, guardrails, and dynamic risk monitoring becomes less of a technical preference and more of a fundamental regulatory requirement for compliance attestation and maintaining control over the five core high-risk parameters.

# Praxisfälle zum Datenschutzrecht XXXVIII: Auftragsverarbeitung oder (gemeinsame) Verantwortlichkeit?

RAin Yvette Reif, LL.M. / RA Dr. Johannes Zhou\*

## I. Sachverhalt

Unternehmer U betreibt einen Online-Shop für Möbel und Wohnaccessoires, der sich großer Beliebtheit erfreut. Umsatz und Mitarbeiterzahl des Unternehmens sind innerhalb kürzester Zeit stark angewachsen. U möchte daher verstärkt Aufgaben an externe Dienstleister auslagern und strategische Partnerschaften eingehen, damit sich das Unternehmen auf das Kerngeschäft fokussieren kann. Bzgl. der Lohn- und Gehaltsabrechnung plant U den spezialisierten Dienstleister D einzuschalten, der auf Basis von U zur Verfügung gestellter Parameter, insbes. des Bruttolohns und relevanter steuerlicher Merkmale der Beschäftigten, die Höhe des jeweils auszahlenden Lohns bestimmt. D entscheidet auch über die zu Abrechnungszwecken eingesetzte Software.

Mit Blick auf das Marketing strebt U eine Kooperation mit dem bekannten Reisebüro R an. Konkret soll ein Gewinnspiel durchgeführt werden, bei dem sowohl Reisen als auch Möbel gewonnen werden können. Die Einladung zur Teilnahme an dem Gewinnspiel soll per herkömmlicher Briefpost unter Rückgriff auf die Kundendatenbestände sowohl von U als auch von R versandt werden, d.h., sowohl die Kunden bzw. Kundinnen von U als auch die von R sollen die Einladung zur Teilnahme am Gewinnspiel erhalten, so die Planung von U und R. Eine Zugriffsmöglichkeit auf die Datenbestände des jeweils anderen Unternehmens wird nicht eingeräumt, d.h., jedes der beiden Unternehmen greift zum Zwecke des Versands nur auf seine eigenen Datenbestände zu.

U hat aufgrund des rasanten Wachstums seines Online-Shops nicht nur mit schönen Dingen zu tun. In letzter Zeit ist er aufgrund fehlerhafter Chargen vermehrt Gewährleistungsanfragen und Schadenersatzforderungen ausgesetzt. Da er sich mit diesen Themen nicht selbst beschäftigen möchte, beauftragt er eine Rechtsanwaltskanzlei mit der Bearbeitung dieser Fälle, die ihn außergerichtlich und – sofern notwendig – auch gerichtlich vertreten soll.

Welche datenschutzrechtliche Rolle kommt den Parteien in den verschiedenen Konstellationen jeweils zu?

## II. Musterlösung

### 1. Rollen in der DS-GVO

Bei der Verarbeitung personenbezogener Daten nach der DS-GVO sind grundsätzlich auf der einen Seite der Verantwortliche und auf der anderen Seite die betroffene Person beteiligt. Der Verantwortliche ist nach Art. 4 Nr. 7 Hs. 1 DS-GVO „jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Betroffene Person ist nach Art. 4 Nr. 1 DS-GVO diejenige natürliche Person, deren personenbezogene Daten verarbeitet werden.

Der Verantwortliche kann sich bei der Verarbeitung personenbezogener Daten jedoch auch anderer Stellen bedienen und mit externen Dienstleistern oder Partnern zusammenarbeiten. In solchen Fällen stellt sich regelmäßig die Frage, in welchem Verhältnis diese anderen Stellen datenschutzrechtlich zum Verantwortlichen stehen. In Betracht kommen vor allem eine Auftragsverarbeitung nach Art. 28 DS-GVO oder eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO. Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Eine gemeinsame Verantwortlichkeit liegt nach Art. 26 Abs. 1 DS-GVO vor, wenn „zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest[legen]“. Möglich ist aber auch eine jeweils alleinige, d.h. getrennte Verantwortlichkeit der Beteiligten. Den Begriffen der Auftragsverarbeitung bzw. der (ggf. gemeinsamen) datenschutzrechtlichen Verantwortlichkeit liegen „funktionelle Konzepte“ zugrunde, die darauf abzielen, Verantwortlichkeiten entsprechend den tatsächlichen Rollen der Parteien zuzuweisen.<sup>1</sup> Folglich ist die Dispositionsfreiheit der Beteiligten bei der datenschutzrechtlichen Verantwortungszuweisung eingeschränkt. Beispielsweise folgt aus einem Auftragsverhältnis nach § 662 BGB oder einem Dienstvertrag nach § 611 BGB nicht zwingend eine Auftragsverarbeitung.<sup>2</sup>

Die Bestimmung, welcher Beteiligte als datenschutzrechtlich Verantwortlicher anzusehen ist, ist vor allem deshalb wichtig, da der Verantwortliche der primäre Normadressat der DS-GVO ist. Dieser ist nach Art. 5 Abs. 2 DS-GVO mit Blick auf die Einhaltung der Datenschutzgrundsätze des Art. 5 Abs. 1 DS-GVO verantwortlich und nachweisspflichtig.<sup>3</sup> Die Beantwortung der Frage, wer Verantwortlicher bezüglich einer personenbezogenen Datenverarbeitung ist, hat insofern weitreichende Auswirkungen. Zudem stellen insbesondere die Art. 26 und 28 DS-GVO unterschiedliche spezifische Anforderungen an die verschiedenen Arten von Beteiligten. Schließlich ist es für die betroffene Person von zentraler Bedeutung, wer datenschutzrechtlich Verantwortlicher und damit Ansprechpartner in Bezug auf ihre Datenschutzrechte ist.

Die DS-GVO definiert darüber hinaus auch die Begriffe „Empfänger“ und „Dritter“. Empfänger ist nach Art. 4 Nr. 9 DS-GVO jede „Stelle, der personenbezogene Daten offenge-

\* 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). RA Dr. Johannes Zhou ist bei der Kanzlei FPS in Frankfurt a.M. im IT- und Datenschutzrecht tätig.

1 EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Vers. 2.0 (7.7.2021), S. 3.

2 Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, 1. Aufl. (2025), Kap. 8 Rn. 3.

3 Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 4.

legt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Auch der Auftragsverarbeiter ist Empfänger im Sinne dieser Definition, da ihm im Rahmen der Auftragsverarbeitung Daten offengelegt werden.<sup>4</sup> Dritter ist nach Art. 4 Nr. 10 DS-GVO jede „Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten“. Damit sind „Außenstehende“ gemeint, die nicht an der Datenverarbeitung beteiligt sind.<sup>5</sup>

## 2. Abgrenzung zwischen Auftragsverarbeitung und (alleiniger/gemeinsamer) Verantwortlichkeit

### a) Kriterien und Merkmale der Auftragsverarbeitung nach Art. 28 DS-GVO

Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Zentrales Merkmal der Auftragsverarbeitung ist die Weisungsgebundenheit des Auftragsverarbeiters. Dieser verarbeitet personenbezogene Daten als „verlängerter Arm“ des Verantwortlichen und unterliegt dessen Vorgaben.<sup>6</sup>

Der Verantwortliche entscheidet nach Art. 4 Nr. 7 Hs. 1 DS-GVO über die Zwecke und Mittel der Datenverarbeitung. Wer über die Zwecke bzw. das „Ob“ einer personenbezogenen Datenverarbeitung entscheidet, ist in jedem Fall als datenschutzrechtlich Verantwortlicher einzuordnen. Bei der Entscheidung bezüglich der Mittel der Datenverarbeitung ist dagegen zu differenzieren: Während die Entscheidung über die „wesentlichen Mittel“ stets beim Verantwortlichen verbleiben muss, darf die Entscheidung über die „nicht wesentlichen Mittel“ auch dem Dienstleister übertragen werden.<sup>7</sup> Wesentliche Mittel sind dem EDSA zufolge solche, die in engem Zusammenhang mit Zweck und Umfang der Verarbeitung stehen, wie die Art der verarbeiteten personenbezogenen Daten, die Dauer der Verarbeitung, die Kategorien von Empfängern und die Kategorien betroffener Personen. Im Gegensatz dazu geht es bei den nicht wesentlichen Mitteln um die „praktischen Aspekte“ der Datenverarbeitung, wie etwa die Wahl der Hard- bzw. Software oder der konkreten Sicherheitsmaßnahmen.<sup>8</sup> In diesem Zusammenhang ist es ausreichend, dass der Verantwortliche dem Auftragsverarbeiter die wesentlichen Grundzüge der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO vorgibt.<sup>9</sup>

Ob eine Auftragsverarbeitung vorliegt, kann im Einzelfall schwierig zu beurteilen sein. Die nachfolgenden Kriterien sprechen für das Vorliegen einer Auftragsverarbeitung nach Art. 28 DS-GVO:

- keine Entscheidungsbefugnis über die Zwecke der Datenverarbeitung und deren wesentliche Mittel (z.B. Art der verarbeiteten Daten, Speicherdauer, Kategorien von Empfängern), sondern allenfalls bzgl. der nicht wesentlichen Mittel der Verarbeitung (z.B. Hard- und Software, Sicherheitsmaßnahmen im Detail),
- keine Verfolgung eigener Zwecke mit den verarbeiteten Daten,

- Vorliegen ausführlicher Weisungen, die wenig Spielraum geben,
- Ausübung einer Unterstützungs-/Hilfsfunktion sowie
- Wahrnehmung einer konkreten Tätigkeit in einem spezifischen Kontext.<sup>10</sup>

Spiegelbildlich dazu sprechen die folgenden Kriterien für das Vorliegen einer (ggf. gemeinsamen) Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO:

- Entscheidungshoheit hinsichtlich der Datenverarbeitung insgesamt,
- Entscheidung über Zwecke und wesentliche Mittel (z.B. Art der verarbeiteten Daten, Speicherdauer, Kategorien von Empfängern) der Datenverarbeitung,
- Entscheidung über die rechtliche Grundlage der Datenverarbeitung sowie
- Vorliegen einer direkten Beziehung zur betroffenen Person.<sup>11</sup>

### b) Anwendung der Kriterien auf die hier zu beurteilenden Fälle

Gemessen an diesen Grundsätzen stellt die Einschaltung des Dienstleisters für die Lohn- und Gehaltsabrechnung in der ersten Fallgestaltung eine Auftragsverarbeitung nach Art. 28 DS-GVO dar. Mit Blick auf die Ausführung des Auftrags besteht kein nennenswerter eigener Entscheidungsspielraum des Dienstleisters, sondern es kommt im Wesentlichen darauf an, dass routinemäßig eine korrekte Berechnung auf Grundlage der gesetzlichen Abrechnungsmaßgaben erfolgt.<sup>12</sup> D führt insofern für U eine klar umrissene Tätigkeit in einem spezifischen Kontext durch und hat nur Unterstützungsfunktion mit Blick auf die personenbezogene Datenverarbeitung. Auch die Entscheidung über den Einsatz einer bestimmten Software stellt keinen Hinderungsgrund dar, eine Auftragsverarbeitung anzunehmen, weil sich dieser Spielraum lediglich auf nicht wesentliche Mittel der Datenverarbeitung bezieht.<sup>13</sup>

Die Einordnung der hier beschriebenen Konstellation als Auftragsverarbeitung kann im Wesentlichen als unstrittig angesehen werden.<sup>14</sup> Abgrenzungsprobleme entstehen in der Praxis insbes. in Fällen, in denen die Lohn- und Gehalts-

4 Taeger/Gabel/Arning/Rothkegel, DS-GVO Art. 4 Rn. 271.

5 Taeger/Gabel/Arning/Rothkegel, DS-GVO Art. 4 Rn. 279.

6 Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 20 f.

7 EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Vers. 2.0 (7.7.2021), Rn. 40.

8 EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Vers. 2.0 (7.7.2021), Rn. 40.

9 Kühling/Buchner/Hartung, DS-GVO Art. 28 Rn. 43.

10 S. hierzu bereits Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 29 mit weiteren Kriterien.

11 S. hierzu bereits Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 30 mit weiteren Kriterien.

12 Taeger/Pohle/Polenz, Computerrechts-Handbuch, 40. EL März 2025, Teil 3. 36.3.

13 Vgl. auch EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Vers. 2.0 (7.7.2021), Rn. 40.

14 Vgl. auch DSK, Kurzpapier Nr. 13: Auftragsverarbeitung, Art. 28 DS-GVO (Stand: 17.12.2018), Anlage A: „DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung“.

abrechnung an Steuerberater/-innen ausgelagert wird, denn § 57 Abs. 1 Steuerberatungsgesetz (StBerG) bestimmt, dass Steuerberater ihren Beruf „unabhängig“ und „eigenverantwortlich“ ausüben haben. Jedenfalls Beratungsleistungen von Steuerberatern, die mit weitgehenden Entscheidungsspielräumen verbunden sind, werden daher weisungsfrei erbracht und der Steuerberater kann insofern nicht Auftragsverarbeiter sein.<sup>15</sup> Bereits vor Geltung der DS-GVO war umstritten, ob dagegen zumindest die bloße Lohnbuchführung durch Steuerberater/-innen noch als Auftragsverarbeitung (damals: Auftragsdatenverarbeitung) eingestuft werden kann.

Den Streit, ob Steuerberater Auftragsverarbeiter sein können, wollte der nationale Gesetzgeber durch eine Klarstellung im nationalen Recht beenden. Seit dem 18.12.2019 heißt es daher in § 11 Abs. 2 S. 2 StBerG: „Die Personen und Gesellschaften nach § 3 sind bei Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche gem. Art. 4 Nr. 7 der Datenschutz-Grundverordnung (EU) 2016/679<sup>16</sup>.“ Da allerdings die Europarechtskonformität der Regelung in § 11 Abs. 2 S. 2 StBerG angezweifelt wird, besteht insofern im Ergebnis nach wie vor Rechtsunsicherheit.<sup>17</sup>

Im zweiten Fall liegt hingegen keine Auftragsverarbeitung vor, da das Verhältnis zwischen U und R insofern durch eine gemeinsame Festlegung der Zwecke und wesentlichen Mittel der Datenverarbeitung geprägt ist und sich keine der Parteien den Weisungen der jeweils anderen mit Blick auf die Datenverarbeitung unterwirft.

Auch in der letzten Fallgestaltung, der Beauftragung der Anwaltskanzlei, ist eine Auftragsverarbeitung abzulehnen. Zwar liegt mit der Vertretung in Rechtsstreitigkeiten durch die Anwaltskanzlei ein „auftragsähnliches“ Verhältnis vor, nämlich ein Dienstvertrag mit Geschäftsbesorgungscharakter nach § 611 BGB i.V.m. § 675 Abs. 1 BGB.<sup>18</sup> Die Beauftragung der Rechtsanwaltskanzlei zielt jedoch nicht auf die Verarbeitung personenbezogener Daten ab, sondern auf die außergerichtliche Vertretung, die Vertretung vor Gericht sowie die Beratung des Mandanten.<sup>19</sup> Eine Auftragsverarbeitung scheidet auch aufgrund der standesrechtlichen Stellung des Rechtsanwalts regelmäßig aus, denn als Organ der Rechtspflege handelt dieser weitgehend unabhängig bei der Erledigung seiner Aufgaben und entscheidet selbstständig, welche personenbezogenen Informationen er in diesem Zusammenhang verarbeitet.<sup>20</sup>

### 3. Abgrenzung zwischen alleiniger und gemeinsamer Verantwortlichkeit

#### a) Kriterien und Merkmale der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO

Nach ErwG 79 DS-GVO bedarf es zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter einer klaren Zuteilung der Verantwortlichkeiten durch die DS-GVO. Liegt keine Auftragsverarbeitung vor, ist insofern zu prüfen, ob die Akteure alleinige, also getrennte oder aber gemeinsame Verantwortliche im Sinne des Art. 26 DS-GVO sind.

Wesentlicher Anknüpfungspunkt ist auch hier die Begriffsbestimmung in Art. 4 Nr. 7 Hs. 1 DS-GVO sowie Art. 26 Abs. 1 DS-GVO, wonach eine gemeinsame Verantwortlichkeit

vorliegt, wenn zwei oder mehrere Verantwortliche gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Der EuGH hat die gemeinsame Verantwortlichkeit in mehreren Entscheidungen weit ausgelegt.<sup>21</sup> Nach seiner Rechtsprechung genügt für die Annahme einer gemeinsamen Verantwortlichkeit bereits die rein faktische Zusammenarbeit für gleiche oder ähnliche Zwecke im Eigeninteresse.<sup>22</sup>

Nicht erforderlich für das Vorliegen einer gemeinsamen Verantwortlichkeit ist nach dem EuGH, dass eine gleichwertige Verantwortlichkeit der verschiedenen Akteure gegeben ist. So müssen nicht alle Akteure hinsichtlich der Verarbeitung identische Handlungsoptionen haben oder gegenüber der betroffenen Person in Erscheinung treten.<sup>23</sup> Auch muss nicht jeder Akteur Zugang zu den verarbeiteten Daten haben.<sup>24</sup> Vielmehr können die Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß einbezogen sein, sodass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.<sup>25</sup>

Zusammengefasst sprechen u.a. folgende Kriterien für eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO:

- Verfolgung gemeinsamer oder eng miteinander verknüpfter bzw. sich ergänzender Zwecke mit Blick auf die Datenverarbeitung,
- gemeinsame Entscheidung über die „wesentlichen Elemente“ der Mittel der Datenverarbeitung (z.B. „Welche Daten werden verarbeitet?“, „Wie lange werden die Daten verarbeitet?“, „Wer hat Zugang zu den Daten?“),
- Verarbeitung auf Grundlage einer einheitlichen Datenbasis (z.B. durch eine gemeinsame Datenbank) und/oder
- Entwicklung eines gemeinsamen Konzepts für die Datenverarbeitung.<sup>26</sup>

#### b) Anwendung der Kriterien auf die hier zu beurteilenden Fälle

Unter Berücksichtigung der genannten Kriterien liegt im zweiten Fall eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO mit Blick auf die personenbezogene Datenverarbeitung im Zusammenhang mit der Versendung der Einladungen zur Gewinnspielteilnahme vor. Die Unternehmen U und R haben gemeinsam Zweck und wesentliche Mittel der Datenverarbeitung bestimmt, indem sie sich mit Blick auf die

<sup>15</sup> Lauck, ZD-Aktuell 2020, 06965.

<sup>16</sup> Ausführlich dazu Kramer/Schmidt, ZD 2020, 194.

<sup>17</sup> Lauck, ZD-Aktuell 2020, 06965.

<sup>18</sup> Vollkommer/Greger/Heinemann/Heinemann, Anwaltschaftsrecht, 5. Aufl. 2021, § 1 Rn. 4.

<sup>19</sup> EDSA, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO, Vers. 2.0 (7.7.2021), Rn. 27.

<sup>20</sup> Taeger/Pohle/Polenz, Computerrechts-Handbuch, 40. EL März 2025, Teil 3. 36.3 Rn. 21.

<sup>21</sup> EuGH, Urt. v. 29.7.2019 – C-40/17; Urt. v. 10.7.2018 – C-25/17; Urt. v. 5.6.2018 – C-210/16.

<sup>22</sup> EuGH, Urt. v. 10.7.2018 – C-25/17, Rn. 68.

<sup>23</sup> S. hierzu ausführlich Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 69.

<sup>24</sup> EuGH, Urt. v. 5.6.2018 – C-210/16, Rn. 38.

<sup>25</sup> EuGH, Urt. v. 5.6.2018 – C-210/16, Rn. 43.

<sup>26</sup> S. hierzu bereits Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 70 mit weiteren Kriterien.

Konzeption, den Ablauf und die Datenbasis für die Aussendung verständigt haben. Die von U bzw. R mit der Datenverarbeitung jeweils verfolgten werblichen Zwecke sind zumindest eng miteinander verknüpft. Dem Vorliegen einer gemeinsamen Verantwortlichkeit steht nach der Rechtsprechung des EuGH, wie bereits angesprochen, auch nicht entgegen, dass U und R keinen Zugriff auf die Datenbestände haben, welche die jeweils andere Partei für die Aktion einsetzt.<sup>27</sup> Ob auch die Datenverarbeitung mit Bezug auf die Durchführung des Gewinnspiels in gemeinsamer Verantwortung erfolgt, hängt davon ab, inwieweit die gemeinsame Konzeption sich auch hierauf bezieht.

Im dritten Fall handelt die Anwaltskanzlei, wie bereits erörtert, grundsätzlich weisungsfrei mit Blick auf die im Zusammenhang mit der Mandatierung stattfindenden personenbezogenen Datenverarbeitungen. Der Auftraggeber ist an der Entscheidung mit Blick auf diese Verarbeitungen nicht beteiligt. Es handelt sich insofern um eine getrennte datenschutzrechtliche Verantwortlichkeit. Die Verantwortlichkeit von U beschränkt sich auf die Datenweitergabe an die Kanzlei.

#### 4. Ergebnis

Im ersten Fall ist der spezialisierte Dienstleister, der die Abwicklung der Lohn- und Gehaltsabrechnung übernimmt, als Auftragsverarbeiter nach Art. 28 DS-GVO einzuordnen.

Im zweiten Fall ist eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO von U und R anzunehmen mit Blick auf die Datenverarbeitung zum Zweck der Einladung zum Gewinnspiel.

Im dritten Fall sind U und die Anwaltskanzlei jeweils eigenständig datenschutzrechtlich verantwortlich.

### III. Ergänzende Hinweise

#### 1. Pflichten im Fall der Auftragsverarbeitung, Art. 28 DS-GVO

Eine Auftragsverarbeitung darf nach Art. 28 Abs. 3 S. 1 DS-GVO nur auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgen. Für Unternehmen ist vor allem der Abschluss von Auftragsverarbeitungsverträgen relevant.<sup>28</sup> Dem Vertrag kommt jedoch keine konstitutive Wirkung zu.<sup>29</sup> Das bedeutet: Eine Auftragsverarbeitung kann auch in Fällen anzunehmen sein, in denen keine diesbezügliche Vereinbarung getroffen wurde.

Der Vertrag muss insbesondere Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Pflichten und Rechte des Verantwortlichen regeln. Ziel ist es, die konkreten Verarbeitungstätigkeiten und -umstände für die Beteiligten verbindlich festzuhalten.<sup>30</sup>

Weitere Mindestinhalte sind in Art. 28 Abs. 3 S. 2 DS-GVO geregelt und umfassen die Bindung an Weisungen (lit. a)), Verschwiegenheitsverpflichtungen der beim Auftragsverarbeiter tätigen Personen (lit. b)), technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (lit. c)), die Beauftra-

gung weiterer Auftragsverarbeiter (lit. d)), die Wahrung der Betroffenenrechte (lit. e)), Unterstützungspflichten (lit. f)), die Rückgabe und Löschung nach Beendigung der Auftragsverarbeitung (lit. g)) und Überprüfungen (lit. h)). Diese Inhalte sind jedoch nicht abschließend, sodass auch weitere Aspekte geregelt werden können.

Der Auftragnehmer ist sorgfältig auszuwählen und entsprechend zu überwachen.

#### 2. Pflichten bei gemeinsamer Verantwortlichkeit, Art. 26 DS-GVO

Art. 26 Abs. 1 S. 2 DS-GVO bestimmt, dass die Verantwortlichen im Fall einer gemeinsamen Verantwortlichkeit in einer transparenten Vereinbarung festlegen, wer von ihnen welche Pflichten gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gem. den Art. 13 und 14 DS-GVO nachkommt. Die Vereinbarung muss nach Art. 26 Abs. 2 S. 1 DS-GVO die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.

Ziel der Vereinbarung ist nach ErwG 79 DS-GVO die klare Zuteilung der Verantwortlichkeiten. Der Abschluss einer entsprechenden Vereinbarung ist jedoch keine konstitutive Voraussetzung der gemeinsamen Verantwortlichkeit,<sup>31</sup> vielmehr ist sie Rechtsfolge derselben.

Nach Art. 26 Abs. 2 S. 2 DS-GVO ist das „Wesentliche“ der Vereinbarung der betroffenen Person zur Verfügung zu stellen. Angesichts der komplexen und von außen oftmals nicht überschaubaren Verarbeitungssituation in Fällen der gemeinsamen datenschutzrechtlichen Verantwortlichkeit soll diese insbes. nachvollziehen können, wie sie ihre Rechte wirksam ausüben kann.<sup>32</sup> „Wesentlich“ sind mindestens eine nachvollziehbare Beschreibung des Kreises der beteiligten Verantwortlichen, ihres Zusammenwirkens und ihrer Rollen, ihrer jeweiligen Beziehung zur betroffenen Person sowie eine Erläuterung, wie die Betroffenenrechte ausgeübt werden können.<sup>33</sup>

Für die Geltendmachung von Betroffenenrechten kann von den Verantwortlichen eine gemeinsame Anlaufstelle eingerichtet werden gem. Art. 26 Abs. 1 S. 3 DS-GVO. In diesem Fall bleibt die betroffene Person allerdings weiterhin berechtigt, ihre Rechte gegenüber jedem einzelnen Verantwortlichen geltend zu machen. Sie ist also nicht verpflichtet, sich an die gemeinsame Anlaufstelle zu wenden.

<sup>27</sup> EuGH, Urt. v. 5.6.2018 – C-210/16, Rn. 38.

<sup>28</sup> Kühling/Buchner/Hartung, DS-GVO Art. 28 Rn. 62.

<sup>29</sup> Taeger/Gabel/Gabel/Lutz, DS-GVO Art. 28 Rn. 36.

<sup>30</sup> Taeger/Gabel/Gabel/Lutz, DS-GVO Art. 28 Rn. 37.

<sup>31</sup> EuGH 5.12.2023 – C-683/21; EuGH 5.12.2023 – C-807/21; Taeger/Gabel/Lang, DS-GVO Art. 26 Rn. 93.

<sup>32</sup> Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 87.

<sup>33</sup> Schwartmann/Benedikt/Reif/Reif/Brink, Datenschutz im Internet, Kap. 8 Rn. 88.

# RECHTSPRECHUNG

## HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

### Neues zum Personenbezug: Die SRB-Entscheidung des EuGH

(EuGH, Urteil vom 4. September 2025 - C-413/23 P -)

#### Relevanz für die Praxis

Wieder einmal hatte sich der EuGH in der vorliegenden Entscheidung mit dem Personenbezug von Daten zu befassen. Die Ausführungen beziehen sich zwar auf Art. 3 Nr. 1 der Verordnung 2018/1725. Dieser ist aber wortgleich zur Bestimmung des Begriffs der personenbezogenen Daten in Art. 4 Nr. 1 DS-GVO. Im Kern ging es in dem Verfahren um die Frage, ob pseudonymisierte Daten aus Sicht eines Datenempfängers personenbezogene Daten darstellen, auch wenn der Datenempfänger die natürlichen Personen selbst nicht identifizieren kann. Der EuGH hat sich im vorliegenden Urteil für ein relatives Verständnis des Personenbezugs ausgesprochen: Daten sind nicht allein deshalb personenbezogen, weil irgendjemand den Personenbezug herstellen kann. Entscheidend ist vielmehr die Perspektive des Datenempfängers.

**Pseudonymisierte Daten müssen nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden. Entscheidend ist, ob die Pseudonymisierung andere Personen als den Verantwortlichen nach den Umständen des Einzelfalls tatsächlich an einer Identifizierung der betroffenen Person hindert, so dass letztere für sie nicht oder nicht mehr identifizierbar ist.**

*(Nicht amtlicher Leitsatz)*

#### Zum Rechtsmittel:

2. Zum zweiten Teil des ersten Rechtsmittelgrundes: falsche Auslegung der Voraussetzung gem. Art. 3 Nr. 1 der Verordnung 2018/1725, dass sich die Informationen auf eine „identifizierbare“ natürliche Person beziehen

Mit dem zweiten Teil des ersten Rechtsmittelgrundes macht der EDSB geltend, das Gericht habe in den Rn. 76 bis 106 des angefochtenen Urteils zu Unrecht festgestellt, dass es die Informationen, die sich aus den an Deloitte übermittelten Stellungnahmen ergäben, nicht als Informationen betrachten könne, die sich im Sinne von Art. 3 Nr. 1 der Verordnung 2018/1725 auf eine „identifizierbare“ Person bezögen. Dieser Teil besteht aus zwei separaten Rügen.

a) Zur ersten Rüge des zweiten Teils des ersten Rechtsmittelgrundes:

[...] Die erste Rüge des zweiten Teils des ersten Rechtsmittelgrundes wird im Wesentlichen auf die Erwägung gestützt, dass pseudonymisierte Daten wie die an Deloitte übermittelten Stellungnahmen – allein aufgrund des Vorliegens von Informationen, die eine Identifizierung der betroffenen Person ermöglichen – in jedem Fall personenbezogene Daten darstellen, ohne dass konkret geprüft werden müsste, ob die Person, auf die sich diese Daten beziehen, trotz der Pseudonymisierung identifizierbar ist.

In diesem Zusammenhang ist darauf hinzuweisen, dass sich eine Information nach dem Wortlaut von Art. 3 Nr. 1 der Verordnung 2018/1725 auf eine „identifizierte oder identifizierbare“ natürliche Person beziehen muss, um unter den Begriff der personenbezogenen Daten im Sinne dieser Bestimmung zu fallen. Die Anwendung dieser Verordnung setzt grundsätzlich also eine Prüfung voraus, ob die von der in Rede stehenden Information betroffene Person identifiziert oder identifizierbar ist.

Diese Auslegung wird durch den fünften und den sechsten Satz des 16. ErwG der Verordnung 2018/1725 gestützt, nach denen unter die Definition des Begriffs „personenbezogene Daten“ weder „anonyme Informationen ...“, d.h. ... Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen“, fallen noch „personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“ (vgl. entsprechend Ur. v. 5.12.2023, Nacionalinis visuomenės sveikatos centras, C 683/21, EU:C:2023:949, Rn. 57).

Was konkret pseudonymisierte Daten betrifft, ist als Erstes darauf hinzuweisen, dass diese Daten in der Legaldefinition des Begriffs „personenbezogene Daten“ in Art. 3 Nr. 1 der Verordnung 2018/1725 nicht genannt werden, sich ihre Eigenschaften aber aus Art. 3 Nr. 6 dieser Verordnung ergeben. Die letztgenannte Bestimmung definiert den Begriff „Pseudonymisierung“ als „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 vom Generalanwalt im Wesentlichen in den Nr. 46 und 48 seiner Schlussanträge ausgeführt, ist die Pseudonymisierung somit kein Element der Definition des Begriffs „personenbezogene Daten“. Sie bezieht sich vielmehr auf die Umsetzung technischer und organisatorischer Maßnahmen, die das Risiko verringern sollen, dass ein bestimmter Datensatz mit der Identität der betroffenen Personen in Verbindung gebracht wird. Nach dem 17. ErwG der Verordnung 2018/1725 kann die Pseudonymisierung „[nur] die Risiken“ einer solchen

Korrelation für die betroffenen Personen „senken“ und damit „die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen“.

Als Zweites ergibt sich aus Art. 3 Nr. 6 der Verordnung 2018/1725, dass der Begriff „Pseudonymisierung“ das Vorliegen von Informationen voraussetzt, die eine Identifizierung der betroffenen Person ermöglichen. Die bloße Existenz solcher Informationen spricht dagegen, dass Daten, die pseudonymisiert wurden, in jedem Fall als anonymisierte Daten betrachtet werden können, die vom Anwendungsbereich dieser Verordnung ausgenommen sind.

Als Drittes deutet indes das in Art. 3 Nr. 6 der Verordnung 2018/1725 vorgesehene Erfordernis, die Informationen zur Identifizierung gesondert aufzubewahren und technische und organisatorische Maßnahmen zu ergreifen, „die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“, darauf hin, dass die Pseudonymisierung insbesondere darauf abzielt, zu verhindern, dass die betroffene Person allein anhand pseudonymisierter Daten identifiziert werden kann.

Sofern solche technischen und organisatorischen Maßnahmen nämlich tatsächlich ergriffen werden und geeignet sind, eine Zuordnung der in Rede stehenden Daten zu der betroffenen Person zu verhindern, so dass diese nicht oder nicht mehr identifizierbar ist, kann sich die Pseudonymisierung auf die Personenbezogenheit dieser Daten im Sinne von Art. 3 Nr. 1 der Verordnung 2018/1725 auswirken.

Hierzu ist klarzustellen, dass der SRB vorliegend – wie dies bei dem Verantwortlichen, der die Pseudonymisierung vorgenommen hat, normalerweise der Fall ist – über zusätzliche Informationen verfügt, die eine Zuordnung der an Deloitte übermittelten Stellungnahmen zur betroffenen Person ermöglichen. Daher bleiben diese Stellungnahmen für den SRB trotz der Pseudonymisierung personenbezogen.

Im Hinblick auf Deloitte, an die der SRB pseudonymisierte Stellungnahmen übermittelt hat, können, wie im Wesentlichen vom SRB ausgeführt, die technischen und organisatorischen Maßnahmen gem. Art. 3 Nr. 6 der Verordnung 2018/1725 bewirken, dass diese Stellungnahmen für Deloitte nicht personenbezogen sind. Dies setzt jedoch zum einen voraus, dass Deloitte nicht in der Lage ist, diese Maßnahmen bei der Bearbeitung der Stellungnahmen, die unter ihrer Kontrolle erfolgt, aufzuheben. Zum anderen müssen diese Maßnahmen auch tatsächlich geeignet sein, zu verhindern, dass Deloitte diese Stellungnahmen der betroffenen Person zuordnet, und zwar auch anhand anderer Mittel zur Identifizierung, wie etwa eines Abgleichs mit anderen Elementen, so dass die betroffene Person für Deloitte nicht oder nicht mehr identifizierbar ist.

Diese Auslegung wird durch den 16. ErwG der Verordnung 2018/1725 gestützt, in dem es nach dem Hinweis im ersten Satz, dass „[d]ie Grundsätze des Datenschutzes ... für alle Informationen gelten [sollten], die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“, im zweiten Satz heißt, dass „[e]iner Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, ... als Informationen über eine identifizierbare natürliche Person betrachtet werden [sollten]“.

Im Anschluss an diese Ausführungen zu personenbezogenen bzw. pseudonymisierten Daten wird nämlich mit dem dritten Satz des 16. ErwG klargestellt, dass, bei der Prüfung der Identifizierbarkeit einer natürlichen Person „alle Mittel“ berücksichtigt werden sollten, die von dem Verantwortlichen oder „einer anderen Person nach allgemeinem Ermessen wahrscheinlich“ genutzt werden, um die natürliche Person „direkt oder indirekt“ zu identifizieren. Außerdem sollten gemäß dem vierten Satz dieses Erwägungsgrundes bei der Prüfung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, „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“.

Wie vom Generalanwalt im Wesentlichen in Nr. 51 seiner Schlussanträge ausgeführt, würde diesen Ausführungen zur Beurteilung, ob die betroffene Person identifizierbar ist oder nicht, jegliche Wirksamkeit genommen, wenn pseudonymisierte Daten für die Zwecke der Anwendung der Verordnung 2018/1725 in jedem Fall und in Bezug auf jede Person als personenbezogene Daten zu betrachten wären.

Insoweit ist darauf hinzuweisen, dass sich der Gerichtshof in Bezug auf eine Pressemitteilung, die gewisse Angaben zu einer namentlich nicht genannten Person enthielt, in seinem Urteil v. 7.3.2024, OC/Kommission (C 479/22 P, EU:C:2024:215, Rn. 52 bis 64), nicht auf die Feststellung beschränkt hat, dass die diese Pressemitteilung veröffentlichende Stelle der Union über sämtliche Informationen verfügte, die die Identifizierung dieser Person ermöglichten. Vielmehr hat er geprüft, ob die Angaben in dieser Pressemitteilung der betroffenen Öffentlichkeit nach allgemeinem Ermessen eine Identifizierung dieser Person ermöglichten, insbesondere durch einen Abgleich dieser Angaben mit im Internet verfügbaren Informationen.

Außerdem hat der Gerichtshof bereits entschieden, dass ein Mittel nach allgemeinem Ermessen wahrscheinlich nicht genutzt wird, um die betreffende Person zu identifizieren, wenn das Risiko einer Identifizierung de facto unbedeutend erscheint, weil die Identifizierung dieser Person gesetzlich verboten oder praktisch nicht durchführbar ist, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde (vgl. i.d.S. Urteil v. 7.3.2024, OC/Kommission, C 479/22 P, EU:C:2024:215, Rn. 51 und die dort angeführte Rechtsprechung). Diese Rechtsprechung bestätigt die Auslegung, wonach die Existenz von zusätzlichen, die Identifizierung der betroffenen Person ermöglichenden Informationen für sich genommen nicht bedeutet, dass pseudonymisierte Daten für die Zwecke der Anwendung der Verordnung 2018/1725 in jedem Fall und für jede Person als personenbezogene Daten zu betrachten sind.

Gleichermaßen hat der Gerichtshof insbesondere in den Urteilen v. 19.10.2016, Breyer (C 582/14, EU:C:2016:779, Rn. 44, 47 und 48), sowie v. 7.3.2024, IAB Europe (C 604/22, EU:C:2024:214, Rn. 43 und 48), im Wesentlichen entschieden, dass an sich nicht personenbezogene Daten, die vom Verantwortlichen erhoben und gespeichert wurden, sich dennoch auf eine identifizierbare Person bezogen, da der Verantwortliche über rechtliche Möglichkeiten verfügte, von Dritten zu-

sätzliche Informationen zu erlangen, die die Identifizierung dieser Person erlaubten. Unter diesen Bedingungen war nämlich der Umstand, dass sich die zur Identifizierung der betroffenen Person erforderlichen Informationen in den Händen verschiedener Personen befanden, nicht geeignet, die Identifizierung der betroffenen Person tatsächlich so zu verhindern, dass sie für den Verantwortlichen nicht identifizierbar war.

Vor allem können nach der Rechtsprechung aus dem Urv. v. 9.11.2023, Gesamtverband Autoteile-Handel (Zugang zu Fahrzeuginformationen) (C 319/22, EU:C:2023:837, Rn. 46 und 49), an sich nicht personenbezogene Daten dann zu „personenbezogenen“ Daten werden, wenn der Verantwortliche sie anderen Personen überlässt, die über Mittel verfügen, die nach allgemeinem Ermessen wahrscheinlich die Identifizierung der betroffenen Person ermöglichen. Diesem Urteil ist insbesondere zu entnehmen, dass die betreffenden Daten – im Zusammenhang mit einer solchen Überlassung – personenbezogen sind, und zwar sowohl für diese Personen als auch indirekt für den Verantwortlichen.

Angesichts der in der vorstehenden Randnummer wiedergegebenen Rechtsprechung macht der EDSB daher zu Unrecht geltend, dass der Umstand, wonach pseudonymisierte Daten für Personen, denen der Verantwortliche solche Daten übermittle, gegebenenfalls keinen Personenbezug aufweisen, es ermögliche, diese Daten zu Unrecht vom Anwendungsbereich des Unionsrechts zum Schutz personenbezogener Daten auszunehmen. Nach dieser Rechtsprechung wirkt sich dieser Umstand insbesondere im Zusammenhang mit einer etwaigen späteren Übermittlung an Dritte nämlich nicht auf die Beurteilung der Personenbezogenheit dieser Daten aus. Sofern nämlich nicht ausgeschlossen werden kann, dass diese Dritten nach allgemeinem Ermessen in der Lage sind, die pseudonymisierten Daten anhand von Mitteln wie etwa einem Abgleich mit anderen ihnen zur Verfügung stehenden Daten der betroffenen Person zuzuordnen, ist diese Person sowohl in Bezug auf die Übermittlung der Daten als auch in Bezug auf die spätere Verarbeitung dieser Daten durch Dritte als identifizierbar anzusehen. Unter solchen Umständen müssten pseudonymisierte Daten als personenbezogene Daten betrachtet werden.

Folglich müssen – entgegen dem Vorbringen des EDSB – pseudonymisierte Daten für die Zwecke der Anwendung der Verordnung 2018/1725 nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden. Denn die Pseudonymisierung kann – je nach den Umständen des Einzelfalls – andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, so dass letztere für sie nicht oder nicht mehr identifizierbar ist.

Der vom EDSB angeführte Umstand, wonach der vierte Satz des 16. ErwG der Verordnung 2018/1725 den Verantwortlichen oder „ein[e] ander[e] Person“ betrifft, vermag diese Auslegung nicht in Frage zu stellen. Aus dem in Rn. 79 des vorliegenden Urteils wiedergegebenen Wortlaut dieses Satzes ergibt sich nämlich, dass er sich nur auf Personen bezieht, die über Mittel verfügen oder Zugang zu Mitteln haben, die nach allgemeinem Ermessen wahrscheinlich für die Identifizierung der betroffenen Person genutzt werden. Wie in den Rn. 75 bis 77 des vorliegenden Urteils ausgeführt, kann die

Pseudonymisierung also je nach den Umständen des Einzelfalls andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, so dass letztere für die anderen Personen nicht oder nicht mehr identifizierbar ist.

Was das Vorbringen des EDSB zum Ziel der Gewährleistung eines hohen Schutzniveaus für personenbezogene Daten angeht, bringt zwar der Wortlaut von Art. 3 Nr. 1 der Verordnung 2018/1725 das Ziel des Unionsgesetzgebers zum Ausdruck, dem Begriff „personenbezogene Daten“ eine weite Bedeutung beizumessen. Dieser Begriff ist indes nicht unbegrenzt, da die genannte Bestimmung u.a. voraussetzt, dass die betroffene Person identifiziert oder identifizierbar ist.

Insbesondere enthält die Verordnung 2018/1725, wie vom Generalanwalt in Nr. 58 seiner Schlussanträge dargelegt, Pflichten – etwa jene nach Art. 15 dieser Verordnung, die die betroffene Person zu informieren –, deren Erfüllung die Identifizierung der betroffenen Person voraussetzt. Solche Pflichten können keiner Einrichtung auferlegt werden, die nicht in der Lage ist, diese Identifizierung vorzunehmen.

Folglich ist die erste Rüge des zweiten Teils des ersten Rechtsmittelgrundes als unbegründet zurückzuweisen.

b) Zur zweiten Rüge des zweiten Teils des ersten Rechtsmittelgrundes:

[...] Das Gericht hat insbesondere in den Rn. 97 bis 100 des angefochtenen Urteils im Wesentlichen entschieden, dass der EDSB gem. der auf das Urv. v. 19.10.2016, Breyer (C 582/14, EU:C:2016:779), zurückgehenden Rechtsprechung verpflichtet gewesen wäre, zu prüfen, ob die an Deloitte übermittelten Stellungnahmen aus der Sicht von Deloitte personenbezogene Daten darstellten. Um zu diesem Schluss zu gelangen, hat das Gericht u.a. darauf hingewiesen, dass der in der streitigen Entscheidung festgestellte Verstoß gegen Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 die Übermittlung dieser Stellungnahmen durch den SRB an Deloitte betroffen habe und nicht nur die Tatsache, dass der SRB über diese verfügt habe.

Zunächst ist darauf hinzuweisen, dass Art. 3 Nr. 1 der Verordnung 2018/1725 nicht ausdrücklich festlegt, welche Sicht für die Beurteilung der Identifizierbarkeit der betroffenen Person maßgeblich ist, während der 16. ErwG dieser Verordnung undifferenziert auf den „Verantwortlichen“ oder „ein[e] ander[e] Person“ abstellt. Überdies ist es nach ständiger Rechtsprechung für die Einstufung von Daten als „personenbezogene Daten“ nicht erforderlich, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden (vgl. in diesem Sinne Urteile vom 19.10.2016, Breyer, C 582/14, EU:C:2016:779, Rn. 43, und vom 7.3.2024, OC/Kommission, C 479/22 P, EU:C:2024:215, Rn. 48).

Nach der Rechtsprechung, die insbesondere auf das Urv. v. 19.10.2016, Breyer (C 582/14, EU:C:2016:779), zurückgeht und auf die in den Rn. 81 bis 84 des vorliegenden Urteils verwiesen wird, richtet sich die maßgebliche Sicht für die Beurteilung der Identifizierbarkeit der betroffenen Person wesentlich nach den Umständen der Datenverarbeitung im Einzelfall.

Im vorliegenden Fall hat der EDSB in der streitigen Entscheidung festgestellt, dass der SRB gegen seine Informationspflicht gem. Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 verstoßen habe, indem er Deloitte in der Datenschutzerklärung, die zum Zeitpunkt der Einholung der Stellungnahmen

veröffentlicht worden sei, nicht als potenzielle Empfängerin der Stellungnahmen genannt habe.

Art. 15 Abs. 1 der Verordnung 2018/1725 bestimmt, welche Informationen der Verantwortliche der betroffenen Person zur Verfügung zu stellen hat, wenn bei ihr personenbezogene Daten erhoben werden, und stellt zudem klar, dass diese Informationen der betroffenen Person „zum Zeitpunkt der Erhebung dieser Daten“ zur Verfügung zu stellen sind. Bereits aus dem Wortlaut dieser Bestimmung ergibt sich, dass der für die Verarbeitung Verantwortliche diese Informationen sofort zu geben hat, d.h. zum Zeitpunkt des Erhebens dieser Daten (vgl. entsprechend Urteil vom 29.7.2019, Fashion ID, C 40/17, EU:C:2019:629, Rn. 104 und die dort angeführte Rechtsprechung).

Was konkret die Information zu potenziellen Empfängern personenbezogener Daten nach Art. 15 Abs. 1 lit. d) dieser Verordnung betrifft, so handelt es sich dabei um eine der Informationen, die zum Zeitpunkt des Erhebens der Daten bei der betroffenen Person zur Verfügung zu stellen ist.

Nach Art. 14 Abs. 1 der Verordnung 2018/1725 trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person die u.a. in Art. 15 dieser Verordnung genannten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, und um diese Person so in die Lage zu versetzen, die an sie gerichteten Informationen in vollem Umfang zu verstehen (vgl. entsprechend Ur. v. 4.5.2023, Österreichische Datenschutzbehörde und CRIF, C 487/21, EU:C:2023:369, Rn. 38, sowie v. 11.7.2024, Meta Platforms Ireland [Verbandsklage], C 757/22, EU:C:2024:598, Rn. 55 und 56).

Die Bedeutung der Erfüllung einer solchen Informationspflicht wird durch den 35. ErwG der Verordnung 2018/1725 bestätigt, nach dessen ersten beiden Sätzen es die Grundsätze einer fairen und transparenten Verarbeitung erforderlich machen, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Dabei sollte der Verantwortliche auch alle weiteren Informationen zur Verfügung stellen, die unter Berücksichtigung der besonderen Umstände und Rahmenbedingungen, unter denen die personenbezogenen Daten verarbeitet werden, notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten, wie in Art. 15 Abs. 2 dieser Verordnung vorgesehen (vgl. entsprechend Ur. v. 11.7.2024, Meta Platforms Ireland [Verbandsklage], C 757/22, EU:C:2024:598, Rn. 57 und die dort angeführte Rechtsprechung).

Beruhet die Erhebung solcher Daten bei der betroffenen Person – wie im vorliegenden Fall im Rahmen des Anhörungsverfahrens – auf der Einwilligung der betroffenen Person, so hängt die Gültigkeit der von dieser Person erteilten Einwilligung somit u.a. davon ab, ob diese Person zuvor die Informationen über alle Umstände im Zusammenhang mit der Verarbeitung der fraglichen Daten erhalten hat, auf die sie nach Art. 15 der Verordnung 2018/1725 Anspruch hat und die ihr ermöglichen, die Einwilligung in voller Kenntnis der Sachlage zu geben (vgl. entsprechend Ur. v. 11.7.2024, Meta Platforms Ireland [Verbandsklage], C 757/22, EU:C:2024:598, Rn. 60).

Was im Übrigen den Fall einer Pflicht der betroffenen Person zur Übermittlung von personenbezogenen Daten an den Verantwortlichen angeht, wird im vierten Satz des 35. ErwG

der Verordnung 2018/1725 klargestellt, dass der betroffenen Person mitgeteilt werden sollte, ob sie zur Bereitstellung der personenbezogenen Daten verpflichtet ist und welche Folgen eine Zurückhaltung der Daten nach sich ziehen würde. Dies belegt, welche Bedeutung der gem. Art. 15 dieser Verordnung erforderlichen Information zum Zeitpunkt des Erhebens der Daten bei der betroffenen Person zukommt.

Vor diesem Hintergrund zielt die Pflicht, der betroffenen Person – zum Zeitpunkt des Erhebens der mit ihr verbundenen personenbezogenen Daten – die potenziellen Empfänger dieser Daten mitzuteilen, u.a. darauf ab, es dieser Person zu ermöglichen, in voller Kenntnis der Sachlage zu entscheiden, ob sie die bei ihr erhobenen personenbezogenen Daten zur Verfügung stellt oder dies verweigert.

Zwar ist, wie im Wesentlichen von der Kommission in der mündlichen Verhandlung dargelegt, die Information über potenzielle Empfänger auch unerlässlich, damit die betroffene Person später gegenüber diesen Empfängern ihre Rechte verteidigen kann. Die Pflicht, diese Information zum Zeitpunkt des Erhebens der personenbezogenen Daten zur Verfügung zu stellen, gewährleistet jedoch insbesondere, dass diese Daten vom Verantwortlichen nicht gegen den Willen der betroffenen Person erhoben oder gar an Dritte übermittelt werden.

Daraus folgt, wie vom Generalanwalt in Nr. 69 seiner Schlussanträge dargelegt, dass die Informationspflicht gem. Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 im Rechtsverhältnis zwischen der betroffenen Person und dem Verantwortlichen besteht und sie daher die mit dieser Person verbundenen Informationen zum Gegenstand hat, wie sie dem Verantwortlichen übermittelt wurden, also vor einer möglichen Übermittlung an Dritte.

Für die Zwecke der Anwendung der Informationspflicht nach Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 ist folglich davon auszugehen, dass die Identifizierbarkeit der betroffenen Person zu dem Zeitpunkt des Erhebens der Daten und aus der Sicht des Verantwortlichen zu beurteilen ist.

Daraus ergibt sich, wie im Wesentlichen vom Generalanwalt in Nr. 79 seiner Schlussanträge ausgeführt, dass die dem SRB obliegende Informationspflicht im vorliegenden Fall vor der Übermittlung der fraglichen Stellungnahmen und unabhängig davon bestand, ob es sich dabei aus der Sicht von Deloitte nach ihrer etwaigen Pseudonymisierung um personenbezogene Daten handelte oder nicht.

Das auf den Wortlaut von Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 – „Empfänger ... der personenbezogenen Daten“ – gestützte Argument des SRB vermag diese Auslegung nicht in Frage zu stellen. Aus den Rn. 102 bis 108 des vorliegenden Urteils ergibt sich nämlich, dass diese Bestimmung die Informationspflicht regelt, die dem Verantwortlichen zum Zeitpunkt des Erhebens solcher Daten obliegt. Die Frage, ob der Verantwortliche zu diesem Zeitpunkt seine Informationspflicht erfüllt hat, kann nicht von den Möglichkeiten zur Identifizierung der betroffenen Person abhängen, über die ein potenzieller Empfänger nach einer späteren Übermittlung der in Rede stehenden Daten gegebenenfalls verfügen könnte.

Wie vom Generalanwalt im Wesentlichen in Nr. 77 seiner Schlussanträge ausgeführt, würde das Argument des SRB, wonach für die Prüfung der Erfüllung dieser Informations-

pflicht die Perspektive des Empfängers einzunehmen sei, zu einer zeitlichen Verlagerung dieser Kontrolle führen. Da diese Kontrolle zwingend bereits an den Empfänger übermittelte personenbezogene Daten beträfe, verkennt dieses Argument auch den Zweck der Informationspflicht, der untrennbar mit dem Verhältnis zwischen dem Verantwortlichen und der betroffenen Person verbunden ist.

Das Gericht hat somit einen Rechtsfehler begangen, als es in den Rn. 97, 98, 100, 101 und 103 bis 105 des angefochtenen Urteils festgestellt hat, dass der EDSB für die Beurteilung, ob der SRB seine Informationspflicht nach Art. 15 Abs. 1 lit. d) der Verordnung 2018/1725 erfüllt habe, hätte prüfen müssen, ob die an Deloitte übermittelten Stellungnahmen aus der Sicht von Deloitte personenbezogene Daten darstellten.

Daraus folgt, dass die zweite Rüge des zweiten Teils des ersten Rechtsmittelgrundes begründet ist, ohne dass die übrigen, in den Rn. 93 und 94 des vorliegenden Urteils zusammengefassten Argumente des EDSB geprüft zu werden brauchen.

### Zur Vertiefung

*Simwinga, SRB Rechtssache C-413/23P: Der Begriff „personenbezogene Daten“ und das Risiko der Identifizierung = RDV 4/2025*

*Simwinga, Pseudonymised data is not in all cases personal data: from Breyer to SRB, the concept of personal data under EU law = EuDIR 6/2025*

[Urteil] Kein Personenbezug bei fehlenden Mitteln des Datenempfängers zur Re-Identifizierung = RDV 4/2023

## Es bleibt dabei: Kontrollverlust allein ist immaterieller Schaden

(BGH, Urteil vom 11. November 2025 – VI ZR 396/24 –)

### Relevanz für die Praxis

Das vorliegende Urteil des BGH ist gleich aus zwei Gründen von Bedeutung für die Praxis: Zunächst bestätigt der Gerichtshof seine Rechtsprechung aus dem vergangenen Jahr, wonach ein bloßer Kontrollverlust genügt, um einen immateriellen Schaden der betroffenen Person anzunehmen. Entwickeln sich aus dem Kontrollverlust besondere Befürchtungen oder Ängste, sind diese geeignet, den immateriellen Schaden zu vertiefen oder zu vergrößern. Zur Begründung des Schadens sind sie allerdings nicht erforderlich. Daneben trifft der BGH im vorliegenden Urteil wichtige Aussagen zu den Pflichten des Verantwortlichen nach Beendigung einer Auftragsverarbeitung. Demnach genügt es nicht, mit dem Auftragsverarbeiter einen Vertrag abzuschließen, in dem diesem die vertragliche Verpflichtung zur Löschung der Daten und zum Nachweis der Löschung bei Auftragsbeendigung auferlegt wird. Der Verantwortliche hat darüber hinaus Maßnahmen zu ergreifen, um sicherzustellen, dass der Auftragsverarbeiter die personenbezogenen Daten auch tatsächlich nicht länger speichert.

1. Der Verantwortliche hat auch im Zusammenhang mit der Beendigung einer Auftragsverarbeitung den Schutz der Rechte der betroffenen Personen zu gewährleisten. Er hat sicherzustellen, dass – vorbehaltlich etwaiger gesetzlicher Speicherpflichten – keinerlei personenbezogene Daten mehr beim Auftragsverarbeiter verbleiben, die diesem vom Verantwortlichen zwecks Auftrags Erfüllung überlassen wurden. Er hat daher das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass es bei Auftragsende tatsächlich zur Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragsverarbeiter kommt.
2. Verbleiben personenbezogene Daten nach Beendigung des Auftrags beim Auftragsverarbeiter, werden sie dort abgegriffen und im Darknet zum Verkauf angeboten, stellt dies einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO dar. Ein solcher ist nicht allein deshalb ausgeschlossen, weil die Daten schon zuvor rechtswidrig abgegriffen worden sind.

### Aus den Gründen:

B. Die Revision ist begründet.

I. Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen hält dessen Beurteilung, dem Kläger sei kein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DS-GVO entstanden, der revisionsrechtlichen Prüfung nicht stand. [...]

3. Nach ständiger Rechtsprechung des Gerichtshofes der Europäischen Union (im Folgenden: Gerichtshof) erfordert ein Schadenersatzanspruch im Sinne des Art. 82 Abs. 1 DS-GVO einen Verstoß gegen die DS-GVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. nur EuGH, Urt. v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 140; weitere Nachweise im Senatsurteil v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 21). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft grundsätzlich die Person, die auf der Grundlage von Art. 82 Abs. 1 DS-GVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH a.a.O. Rn. 141 sowie Senatsurteil a.a.O. m.w.N.). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadenersatzanspruches nach Art. 82 Abs. 1 DS-GVO ein Verschulden des Verantwortlichen. Art. 82 DS-GVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DS-GVO dem Verantwortlichen (vgl. EuGH, Urt. v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 44 ff. sowie Senatsurteil a.a.O. m.w.N.).

a) Rechtlich nicht zu beanstanden ist die Beurteilung des Berufungsgerichts, dass die Beklagte bei Vorliegen eines Schadens (dazu unten b)) haftungsrechtlich dafür einzustehen hat, dass die Daten des Klägers bei dem Unternehmen O. nach Beendigung des Auftragsverarbeitungsverhältnisses nicht gelöscht wurden, so dass sie bei dem Unternehmen O. (durch Hacking oder infolge unbefugter Weitergabe durch Mitarbeiter des Unternehmens O.) abgegriffen und anschließend im Darknet zum Verkauf angeboten werden konnten. Dabei geht es nicht lediglich um einen Verstoß des Auftragsverarbeiters O. gegen die DS-GVO, für den die Beklagte –

vorbehaltlich der Möglichkeit einer Exkulpation nach Art. 82 Abs. 3 DS-GVO – gem. Art. 82 Abs. 2 S. 1 DS-GVO einzustehen hat. Vielmehr liegt darüber hinaus ein eigener Verstoß der Beklagten gegen die DS-GVO vor, der, wie vom Berufungsgericht zutreffend gesehen, darin besteht, dass sie sich bei Beendigung des Vertrages mit ihrem Auftragsverarbeiter O. mit dessen Ankündigung einer Datenlöschung begnügt und nicht die Bestätigung einer erfolgten umfassenden Datenlöschung einholte (dazu aa)). Wegen dieser eigenen schadensursächlichen Pflichtverletzung gelingt ihr eine Exkulpation nach Art. 82 Abs. 3 DS-GVO nicht (bb)).

aa) Die Beklagte hat jedenfalls ihre Pflichten aus Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 lit. c), e) und f) DS-GVO sowie aus Art. 32 Abs. 1 DS-GVO verletzt.

(1) Überträgt ein Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO die Datenverarbeitung auf einen Auftragsverarbeiter, kann er sich dadurch von seinen datenschutzrechtlichen Pflichten nicht befreien (Taeger/Gabel/Gabel/Lutz, DS-GVO-BDSG-TTDSG, 4. Aufl., Art. 28 Rn. 2). Er bleibt "Herr der Verarbeitung" und daher gegenüber der betroffenen Person für die Einhaltung der datenschutzrechtlichen Vorschriften bei der Verarbeitung ihrer Daten durch den Auftragsverarbeiter als seinem "verlängerten Arm" verantwortlich (Paal/Pauly/Martini, DS-GVO BDSG, 3. Aufl., Art. 28 Rn. 2; Kühling/Buchner/Bergt, DS-GVO BDSG, 4. Aufl., Art. 82 Rn. 55). Lediglich im Falle eines sogenannten Aufgaben- oder Auftragsverarbeiterexzesses, bei dem der Auftragsverarbeiter unter Verstoß gegen die DS-GVO selbst die Zwecke und Mittel der Verarbeitung bestimmt (Art. 28 Abs. 10 DS-GVO), wird dieser Verantwortliche und der ursprüngliche Verantwortliche unter Umständen aus seiner Haftung entlassen (vgl. für den Fall einer Haftung nach Art. 83 DS-GVO EuGH, Urt. v. 5.12.2023 – C-683/21, ZD 2024, 209 Rn. 85). Das gilt unter anderem dann, wenn der Auftragsverarbeiter Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche zugestimmt hätte (EuGH a.a.O.). Auch in diesen Fällen kommt allerdings eine Haftung des Verantwortlichen in Betracht, wenn er es versäumt, mit den Mitteln des Vertragsrechts auf ein vertragskonformes Verhalten des Auftragsverarbeiters zu drängen (vgl. Simitis/Hornung/Spiecker gen. Döhmman/Petri, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 28 Rn. 94).

Der Verantwortliche hat auch im Zusammenhang mit der Auftragsbeendigung den Schutz der Rechte der betroffenen Personen zu gewährleisten. Insoweit ist von Bedeutung, dass die Übermittlung von personenbezogenen Daten seitens des Verantwortlichen an den Auftragsverarbeiter einen Eingriff in die durch Art. 7 und 8 GRCh garantierten Rechte der betroffenen Personen auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellt, der nur solange gerechtfertigt ist, als die Voraussetzungen der Auftragsverarbeitung vorliegen. Wenn aber das Auftragsverhältnis nicht mehr besteht, gibt es keine Rechtfertigung mehr dafür, dass sich die Daten noch beim Auftragsverarbeiter befinden (BeckOK Datenschutzrecht/Spoerr, 53. Ed., Stand: 1.8.2025, DS-GVO Art. 28 Rn. 78). Es ist daher auch und gerade durch den Verantwortlichen sicherzustellen, dass – vorbehaltlich etwaiger

gesetzlicher Speicherpflichten – keinerlei personenbezogene Daten mehr beim Auftragsverarbeiter verbleiben, die diesem vom Verantwortlichen zwecks Auftrags Erfüllung überlassen wurden (BeckOK/Spoerr a.a.O., Art. 28 Rn. 79; Simitis/Hornung/Spiecker gen. Döhmman/Petri, Datenschutzrecht, 2. Aufl., DS-GVO Art. 28 Rn. 78; Kühling/Buchner/Hartung, a.a.O., Art. 28 Rn. 77). Das Zugriffsrecht des Auftragsverarbeiters auf diese Daten entfällt mit dem Auftragsende, der Zugang zu ihnen muss ihm daher ab diesem Zeitpunkt verwehrt sein (Martini a.a.O., Art. 28 Rn. 50). In Art. 28 Abs. 3 S. 2 lit. g) DS-GVO ist dementsprechend geregelt, dass in dem Vertrag oder anderen Rechtsinstrument, auf dessen Grundlage die Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO zu erfolgen hat, vorzusehen ist, dass der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Ferner ist gem. Art. 28 Abs. 3 S. 2 lit. h) DS-GVO vorzusehen, dass der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten, also auch der Löschungs- bzw. Rückgabepflicht, zur Verfügung stellt und Überprüfungen seitens des Verantwortlichen oder eines von diesem beauftragten Prüfers ermöglicht und dazu beiträgt.

Der Verantwortliche darf sich allerdings grundsätzlich nicht damit begnügen, mit dem Auftragsverarbeiter einen Vertrag abzuschließen, in dem diesem die vertragliche Verpflichtung zur Löschung der Daten und zum Nachweis der Löschung bei Auftragsbeendigung auferlegt wird. Er hat vielmehr bei Beendigung des Auftragsverhältnisses das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass der Auftragsverarbeiter seine vertragliche Verpflichtung erfüllt, die personenbezogenen Daten also tatsächlich nicht länger bei ihm gespeichert bleiben, so dass er tatsächlich keinen Zugriff mehr auf diese hat. Ob sich diese Pflicht aus Art. 28 DS-GVO ergibt, weil dessen Abs. 1 und Abs. 3 S. 2 lit. h) bei verständiger Auslegung der Vorschrift eine Kontrollpflicht des Verantwortlichen impliziert (vgl. Gabel/Lutz a.a.O., Art. 28 Rn. 27, 31; BeckOK/Spoerr a.a.O., Art. 28 Rn. 35; Martini a.a.O., Art. 28 Rn. 20; Hartung a.a.O., Art. 28 Rn. 60), kann dahinstehen. Denn jedenfalls ergibt sie sich aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) und insbesondere dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DS-GVO), der den Zeitraum der Speicherung betrifft und dessen Ausfluss die Löschungs- bzw. Rückgabepflicht bei Beendigung des Auftragsverhältnisses ist (Martini a.a.O., Art. 28 Rn. 50; Simitis/Hornung/Spiecker gen. Döhmman/Petri, Datenschutzrecht, 2. Aufl., DS-GVO Art. 28 Rn. 78). Für die Einhaltung dieser Grundsätze ist der Verantwortliche gem. Art. 5 Abs. 2 DS-GVO "verantwortlich". Ferner ergibt sich seine Pflicht, sicherzustellen, dass dem Auftragsverarbeiter mit Beendigung des Auftrags der Zugang zu den personenbezogenen Daten der betroffenen Personen entzogen wird, aus der aus Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 DS-GVO folgenden Pflicht, eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. So hat der Verantwortliche gem.

Art. 32 Abs. 1 DS-GVO unter Berücksichtigung unter anderem der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Gem. Art. 32 Abs. 2 DS-GVO sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Datenverarbeitung verbunden sind, unter anderem durch den unbefugten Zugang zu gespeicherten Daten. Das Risiko eines unbefugten Zugriffs auf die gespeicherten Daten besteht nicht erst bei einem Cyberangriff durch außenstehende Dritte, sondern schon dann, wenn die Daten nach Beendigung des Auftragsverhältnisses beim Auftragsverarbeiter gespeichert bleiben, obwohl dessen Zugriffsrecht mit der Beendigung des Auftrags erloschen ist. Dies hat der Verantwortliche durch geeignete Maßnahmen "so weit wie möglich" zu verhindern (zu dieser Einschränkung vgl. EuGH, Urt. v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 30). Er hat daher das seinerseits nach den Umständen des Einzelfalls Erforderliche dazu beizutragen, dass sichergestellt ist, dass es bei Auftragsende tatsächlich zur Rückgabe bzw. Löschung der personenbezogenen Daten beim Auftragsverarbeiter kommt. Die Beweislast für die Geeignetheit seiner insoweit getroffenen Sicherheitsmaßnahmen liegt beim Verantwortlichen (vgl. EuGH a.a.O. Rn. 52, 56).

Hat der Verantwortliche diese ihm selbst obliegende Pflicht verletzt und insbesondere nicht auf ein vertragskonformes Verhalten des Auftragsverarbeiters hinsichtlich der Datenlöschung bzw. -rückgabe bei Auftragsende gedrängt, so kann er sich seiner Verantwortung hierfür nicht schon durch den Hinweis auf einen Aufgabenexzess entziehen, den der Auftragsverarbeiter dadurch begeht, dass er die Daten vertragswidrig behält und weiter verarbeitet. Für die Folgen seines eigenen Pflichtenverstößes hat der Verantwortliche selbst einzustehen. [...]

b) Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen ist dessen Beurteilung, dem Kläger sei kein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DS-GVO entstanden, rechtsfehlerhaft. Nach den Feststellungen des Berufungsgerichts waren von dem Vorfall folgende personenbezogene Daten des Klägers betroffen: Vor- und Nachname, Geschlecht, E-Mail-Adresse, Sprache sowie sein Registrierungsdatum bei der Beklagten. Der Kläger hat nicht nur die Kontrolle über diese Daten dadurch verloren, dass nach Beendigung der Auftragsverarbeitung das Unternehmen O. und Dritte (Hacker) unbefugten Zugriff auf die Daten hatten. Vielmehr ist es darüber hinaus anschließend zu einer missbräuchlichen Verwendung der Daten dadurch gekommen, dass sie im Darknet zum Verkauf angeboten wurden. Spätestens damit ist dem Kläger ein immaterieller Schaden entstanden. Ferner ist ein solcher Schaden durch die entgegen der Auffassung des Berufungsgerichts als begründet anzusehende Befürchtung des Klägers eingetreten, es könne zu einer (weiteren) missbräuchlichen Verwendung der im Darknet veröffentlichten Daten durch Versendung von Spam-Mails kommen.

aa) Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (st. Rspr., vgl.

nur EuGH, Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 55; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 139 m.w.N.; weitere Nachweise bei Senatsurteil v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 28). 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 DS-GVO 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) erforderlich (st. Rspr., vgl. EuGH, Urt. v. 4.9.2025 – C-655/23, a.a.O. Rn. 56; v. 4.10.2024 – C-200/23, a.a.O. Rn. 140 m.w.N.; weitere Nachweise bei Senatsurteil v. 18.11.2024 – VI ZR 10/24, a.a.O.).

Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DS-GVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat oder eine "Bagatellgrenze" überschreitet (EuGH, Urt. v. 4.9.2025 – C-655/23, a.a.O. Rn. 58; v. 4.10.2024 – C-200/23, a.a.O. Rn. 149 m.w.N.; weitere Nachweise bei Senatsurteil v. 18.11.2024 – VI ZR 10/24, a.a.O. Rn. 29). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DS-GVO verpflichtet ist, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die DS-GVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden i.S.v. Art. 82 dieser Verordnung darstellen (vgl. EuGH, Urt. v. 4.10.2024 – C-200/23, a.a.O. Rn. 142; weitere Nachweise bei Senatsurteil v. 18.11.2024 – VI ZR 10/24, a.a.O.).

bb) Wie der Senat in seinem – der angefochtenen Entscheidung allerdings zeitlich nachfolgenden – Urt. v. 18.11.2024 – VI ZR 10/24 (BGHZ 242, 180) zu einem Scraping-Vorfall bei Facebook unter Bezugnahme auf die Rechtsprechung des Gerichtshofs ausgeführt hat, kann ein immaterieller Schaden i.S.d. Art. 82 Abs. 1 DS-GVO auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die DS-GVO sein (a.a.O. Rn. 30 f.). Hat die betroffene Person den Nachweis erbracht, dass sie einen in einem bloßen Kontrollverlust als solchem bestehenden Schaden erlitten hat, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese sind lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern (a.a.O. Rn. 31).

(1) Diese Rechtsauffassung, die der Senat in dem genannten Urteil nachfolgenden Entscheidungen wiederholt hat (Senatsurteile v. 28.1.2025 – VI ZR 109/23, NJW 2025, 1060 Rn. 16 f.; v. 11.2.2025 – VI ZR 365/22, NJW 2025, 1656 Rn. 15) und die das Bundesarbeitsgericht teilt (vgl. BAG, Urt. v. 8.5.2025 – 8 AZR 209/21, NZA 2025, 1248 Rn. 24), soll nach in Teilen der Literatur vertretener Meinung (vgl. Mörsdorf/Momtazi, JZ 2025, 425, 428 f.; Paal, NJW 2025, 261, 263 f.; Spittka, DSB 2024, 311, 312 f.; Schürgers/Hirschberger, NZA 2025, 216, 221 f.) sowie

nach Auffassung der Revisionserwiderung im Widerspruch zur Rechtsprechung des Gerichtshofs stehen. Insbesondere wird vertreten, der Gerichtshof habe den Kontrollverlust als solchen nur als mögliche Ursache für einen immateriellen Schaden, nicht aber als den immateriellen Schaden selbst angesehen.

(2) Gegen diese Meinung spricht, dass, worauf der Gerichtshof zuletzt in seinem Urt. v. 4.9.2025 – C-655/23 (NJW 2025, 3137 Rn. 59) hingewiesen hat, in den Erwägungsgründen der DS-GVO die Hinderung der betroffenen Person daran, "die sie betreffenden personenbezogenen Daten zu kontrollieren" (ErwG 75 DS-GVO) und der "Verlust der Kontrolle über ihre personenbezogenen Daten" (ErwG 85 DS-GVO) als Beispiele für einen möglichen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO aufgeführt sind. Unter Bezugnahme auf ErwG 85 DS-GVO hat der Gerichtshof wiederholt und auch in seinen jüngsten Entscheidungen zu diesem Thema darauf hingewiesen, dass der Unionsgesetzgeber unter den Begriff des Schadens auch den "bloßen Verlust der Kontrolle" über die eigenen personenbezogenen Daten dieser Personen infolge eines Verstoßes gegen die DS-GVO "fassen" wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten erfolgt sein sollte (EuGH, Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 60; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 145; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 82). Ähnlich heißt es im Urteil des Gerichtshofs v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 42, dass der 85. ErwG der DS-GVO ausdrücklich den "Verlust der Kontrolle" zu den Schäden "zählt", die durch eine Verletzung personenbezogener Daten verursacht werden können. In demselben Urteil (a.a.O.) sowie in seinem Urt. v. 20.6.2024 – C-590/22, ZD 2024, 519 Rn. 33 hat der Gerichtshof ausgeführt, dass der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden i.S.v. Art. 82 Abs. 1 DS-GVO "darstellen" (englische Fassung: "constitute", französische Fassung: "constituer") kann, der einen Schadenersatz begründet, sofern die betroffene Person den Nachweis erbringt, dass sie tatsächlich "einen solchen Schaden" – so geringfügig er auch sein mag – erlitten hat. Dies stützt die vom Senat vertretene Auffassung, dass bereits der Kontrollverlust als solcher ein Schaden im Sinne von Art. 82 Abs. 1 DS-GVO sein kann und dementsprechend nur dieser nachgewiesen werden muss, um einen Schadenersatzanspruch zu begründen.

Allerdings ist die Wortwahl, auch im Vergleich der Sprachfassungen, nicht einheitlich. In der deutschen Fassung des Urteils des Gerichtshofs v. 25.1.2024 – C-687/21, CR 2024, 160 Rn. 66 heißt es, dass die betroffene Person durch den kurzzeitigen Verlust der Kontrolle einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO "erleiden" kann, in den Urteilen des Gerichtshofs v. 14.12.2023 – C-456/22, NZA 2024, 56 Rn. 22 und v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 150, dass der Verlust der "Hoheit" über diese Daten einen Schaden "zufügen" kann. In der englischen und der französischen Fassung werden insoweit aber einheitlich die Begriffe "loss of control" bzw. "perte de contrôle" verwendet, die Verknüpfung mit dem immateriellen Schaden wird einheitlich durch die Wörter "cause/causing" bzw. "causer" hergestellt. In den deutschen Sprachfassungen findet sich das Wort "verursachen" (erst) in Rn. 156 des Urteils des Gerichtshofs v. 4.10.2024 – C-200/23 (a.a.O.) sowie im Urteil des Gerichtshofs

v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 60, wo es heißt, dass ein zeitlich begrenzter Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten ausreichen kann, um einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO zu "verursachen", sofern die betroffene Person nachweist, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat, ohne dass dieser Begriff des immateriellen Schadens den Nachweis "zusätzlicher spürbarer negativer Folgen" erfordert (Hervorhebungen nur hier). Bei isolierter Betrachtung dieses Satzes könnte der bloße Kontrollverlust nur Ursache für einen davon zu trennenden immateriellen Schaden sein, den die betroffene Person nachweisen müsste, wobei der Nachweis zusätzlicher spürbarer negativer Folgen nicht erforderlich wäre. Damit würde sich allerdings die Frage stellen, worin genau der immaterielle Schaden als Zwischenstufe zwischen Kontrollverlust und zusätzlichen spürbaren negativen Folgen bestehen soll. Insbesondere wäre diese Interpretation mit dem (im Urt. v. 4.9.2025 – C-655/23 unmittelbar zuvor in Rn. 60 wiederholten) Hinweis des Gerichtshofs darauf, dass der Unionsgesetzgeber bei der beispielhaften Aufzählung der Schäden ("types of damage") unter diesen Begriff insbesondere auch den "bloßen Verlust der Kontrolle" über die eigenen personenbezogenen Daten dieser Personen infolge eines Verstoßes gegen die DS-GVO fassen wollte ("intended to include in that concept, inter alia, mere loss of control") und der vom Gerichtshof in anderen Urteilen verwendeten Formulierung, dass der Kontrollverlust den immateriellen Schaden "darstellen" kann, kaum in Einklang zu bringen. Der Generalanwalt beim Gerichtshof (Szpunar) hat in den Schlussanträgen v. 18.9.2025 in der Rechtssache C-526/24 unter Bezugnahme unter anderem auf das Urteil des Gerichtshofs v. 4.9.2025 – C-655/23 das Wort "darstellen" ("constitute", "constituer") und nicht "verursachen" ("cause", "causer") verwendet (Rn. 89). Zu berücksichtigen sind in diesem Zusammenhang ferner das mit der DS-GVO verfolgte Ziel der Gewährung eines hohen Schutzniveaus für natürliche Personen bei der Verarbeitung personenbezogener Daten sowie ErwG 146 S. 3 DS-GVO, der eine weite Auslegung des Begriffs des Schadens in einer Art und Weise gebietet, die den Zielen der DS-GVO in vollem Umfang entspricht.

cc) Auf diese für den Kontrollverlust als immateriellen Schaden – auch nach der Rechtsprechung des Gerichtshofs – sprechenden Gesichtspunkte kommt es im vorliegenden Fall allerdings letztlich nicht entscheidungserheblich an. Denn hier ist es wie auch in den Facebook-Scraping-Fällen (hierzu Senatsurteil v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180) nicht nur zu einem Kontrollverlust, sondern in dessen Folge zu einer missbräuchlichen Verwendung der personenbezogenen Daten gekommen, womit ein immaterieller Schaden vorliegt.

(1) Ohne Zweifel lässt sich der Rechtsprechung des Gerichtshofs entnehmen, dass ein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DS-GVO jedenfalls dann vorliegt, wenn der Kontrollverlust nicht folgenlos geblieben, sondern es zu einer missbräuchlichen Verwendung der betreffenden Daten tatsächlich gekommen ist. Aus der vom Gerichtshof auch jüngst wiederholten Wendung, dass der Unionsgesetzgeber unter den Begriff des Schadens insbesondere auch den bloßen Verlust der Kontrolle über die eigenen personenbezogenen Daten fassen wollte, selbst wenn konkret keine

missbräuchliche Verwendung der betreffenden Daten erfolgt sein sollte (EuGH, Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 60; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 145; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 82, Hervorhebung nur hier), lässt sich schließen, dass erst recht ein immaterieller Schaden zu bejahen ist, wenn die Daten tatsächlich missbräuchlich verwendet wurden. Dasselbe ergibt sich aus der Rechtsprechung des Gerichtshofs, wonach auch die durch einen Verstoß gegen die DS-GVO ausgelöste Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten von Dritten missbräuchlich verwendet werden, für sich genommen einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO darstellen kann, sofern diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als "begründet" angesehen werden kann, das Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten also nicht rein hypothetischer Natur ist (vgl. nur EuGH, Urt. v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 143 f. m.w.N.; v. 25.1.2024 – C-687/21, CR 2024, 160 Rn. 65, 67, 68; Senatsurteil v. 13.5.2025 – VI ZR 186/22, CR 2025, 585 Rn. 28 f.; dazu näher unten dd)). Wie beim Kontrollverlust ist es also für die Qualifizierung einer Befürchtung als immaterieller Schaden nicht erforderlich, dass es zu der befürchteten missbräuchlichen Verwendung der Daten kommt. Hat sich das Risiko der missbräuchlichen Verwendung aber verwirklicht, so liegt ein immaterieller Schaden erst recht vor.

Insbesondere bedarf es hierfür nicht zusätzlich eines durch die missbräuchliche Datenverwendung hervorgerufenen "emotionalen" Schadens. Letzteres lässt sich nicht darauf stützen, dass der Gerichtshof in Rn. 64 des Urt. v. 4.9.2025 – C-655/23 (NJW 2025, 3137) auf die dortige vierte Vorlagefrage des Senats geantwortet hat, "dass Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass der Begriff 'immaterieller Schaden' in dieser Bestimmung negative Gefühle umfasst, die die betroffene Person infolge einer unbefugten Übermittlung ihrer personenbezogenen Daten an einen Dritten empfindet, wie z.B. Sorge oder Ärger, und die durch einen Verlust der Kontrolle über diese Daten, ihre mögliche missbräuchliche Verwendung oder eine Rufschädigung hervorgerufen werden, sofern die betroffene Person nachweist, dass sie solche Gefühle samt ihrer negativen Folgen aufgrund des in Rede stehenden Verstoßes gegen die DS-GVO empfindet." Denn die vierte Vorlagefrage betraf nicht etwa die Frage, ob und unter welchen Voraussetzungen ein Kontrollverlust oder gar eine missbräuchliche Verwendung der Daten einen immateriellen Schaden darstellt, sondern, ob Art. 82 Abs. 1 DS-GVO dahingehend auszulegen ist, dass für die Annahme eines immateriellen Schadens im Sinne dieser Bestimmung bloße negative Gefühle wie z.B. Ärger, Unmut, Unzufriedenheit, Sorge und Angst, die an sich Teil des allgemeinen Lebensrisikos und oft des täglichen Erlebens sind, genügen (a.a.O. Rn. 35). Die Antwort, dass nachgewiesene negative Gefühle samt ihrer negativen Folgen, die durch einen Kontrollverlust etc. hervorgerufen werden, vom Begriff des immateriellen Schadens umfasst sind, lässt nicht den Schluss zu, dass es zur Begründung eines Schadens zwingend solcher negativer Gefühle bedarf.

(2) Nach diesen Maßstäben ist vorliegend von einem immateriellen Schaden im Sinne von Art. 82 DS-GVO jedenfalls ab dem Zeitpunkt auszugehen, zu dem die personenbezo-

genen Daten des Klägers im Darknet veröffentlicht und dort zum Verkauf angeboten wurden. Zuvor hatte der Kläger die Kontrolle über diese Daten dadurch verloren, dass seine personenbezogenen Daten trotz Beendigung des Auftragsverhältnisses bei dem Unternehmen O. gespeichert blieben und damit sowohl das Unternehmen O. unbefugten Zugriff auf die Daten hatte als auch Dritte, die die Daten hackten oder von Mitarbeitern des Unternehmens O. erhielten. Mit ihrer anschließenden Veröffentlichung im Darknet wurden die Daten sodann missbräuchlich verwendet.

Allein darauf, ob die hier betroffenen Daten des Klägers auch schon vor dem streitgegenständlichen Vorfall gehackt worden waren, wie den Feststellungen des Berufungsgerichts zufolge der Website "haveibeenpwned.com" zu entnehmen ist, kommt es für das Vorliegen eines Schadens nicht an. Denn mit jedem rechtswidrigen Abgriff der Daten wird der Kontrollverlust intensiviert und die Gefahr eines Missbrauchs (durch denselben oder einen anderen Personenkreis) erhöht. Der Umstand, dass dieselben Daten schon einmal gehackt wurden, kann deshalb für sich genommen nur bei der Bemessung der Schadenshöhe eine Rolle spielen.

dd) Ein immaterieller Schaden wird vorliegend zudem durch die mit Bekanntwerden des Vorfalls ausgelöste Befürchtung des Klägers begründet, die im Darknet veröffentlichten Daten könnten (nun ein weiteres Mal) missbräuchlich verwendet werden. Die Beurteilung des Berufungsgerichts, diese Befürchtung sei nicht als begründet anzusehen, beruht auf Rechtsfehlern.

(1) Durch die Rechtsprechung des Gerichtshofs ist geklärt, dass die durch einen Verstoß gegen die DS-GVO ausgelöste (empfundene) Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten infolge eines Verstoßes gegen die DS-GVO von Dritten missbräuchlich verwendet werden, "für sich genommen" einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO darstellen kann, sofern diese Befürchtung samt ihrer negativen Folgen ordnungsgemäß nachgewiesen ist (EuGH, Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 61; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 143 f.; v. 20.6.2024 – C-590/22, ZD 2024, 519 Rn. 32, 35, 36; v. 25.1.2024 – C-687/21, CR 2024, 160 Rn. 65; Senatsurteile v. 13.5.2025 – VI ZR 186/22, CR 2025, 585 Rn. 28; v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 32). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (EuGH, Urt. v. 20.6.2024 – C-590/22, a.a.O. Rn. 35; v. 25.1.2024 – C-687/21, a.a.O. Rn. 68; Senatsurteile v. 13.5.2025 – VI ZR 186/22, a.a.O. Rn. 29; v. 18.11.2024 – VI ZR 10/24, a.a.O.). Die Befürchtung muss unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als "begründet" angesehen werden können (EuGH, Urt. v. 4.10.2024 – C-200/23, a.a.O. Rn. 143 m.w.N.; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 85; Senatsurteil v. 13.5.2025 – VI ZR 186/22, a.a.O.). Ebenso wenig wie beim Kontrollverlust ist es dagegen erforderlich, dass es zu einer missbräuchlichen Verwendung der Daten tatsächlich kommt (s.o. sub cc) (1)). Die mit der begründeten Befürchtung einer missbräuchlichen Datenverwendung verbundenen negativen Folgen können auch negative Gefühle wie Sorge und Ärger sein, auch wenn

diese Teil des allgemeinen Lebensrisikos sein können (vgl. EuGH, Urt. v. 4.9.2025 – C-655/23, a.a.O. Rn. 62, 64).

Die Anforderungen an die Darlegung der Befürchtung eines Datenmissbrauchs dürfen nicht überspannt werden. Allein der Umstand, dass sich in einer Vielzahl von Klageschriften nach einem Vorfall, der eine Vielzahl von Personen betroffen hat, gleichlautende Formulierungen zu Sorgen und Ängsten über einen Datenmissbrauch finden, steht der Schlüssigkeit der jeweiligen Klage noch nicht entgegen (vgl. Senatsurteil v. 18.11.2024 – VI ZR 10/24, a.a.O. Rn. 36). Je plausibler die Befürchtung eines Datenmissbrauchs im konkreten Fall erscheint, desto geringere Anforderungen sind an ihre Darlegung zu stellen.

(2) Die Beurteilung des Berufungsgerichts, die vom Kläger vorgetragene Befürchtung eines Datenmissbrauchs könne nicht als begründet angesehen werden, steht nicht in Einklang mit der Rechtsprechung des Gerichtshofs.

Nach seinem vom Berufungsgericht festgestellten Vortrag befürchtet der Kläger aufgrund des streitgegenständlichen Vorfalls insbesondere den Erhalt von Spam-Mails mit auch betrügerischem Inhalt sowie einen Identitätsdiebstahl. Werden wie hier Name und E-Mail-Adresse einer natürlichen Person im Darknet zum Verkauf angeboten, so darf es als sehr wahrscheinlich angesehen werden, dass diese Daten dazu verwendet werden, Werbemails, aber auch Mails mit betrügerischem Inhalt an diese Person zu senden. Das stellt wohl auch das Berufungsgericht nicht in Frage. Ferner besteht die konkrete Gefahr, dass unter dem Namen der betroffenen Person und scheinbar von ihrem E-Mail-Account aus Mails mit betrügerischem Inhalt an Dritte geschickt werden. Schon mit der Versendung dieser Spam-Mails an den Kläger bzw. scheinbar von ihm als Absender an Dritte würden die Daten des Klägers (nach ihrer Veröffentlichung im Darknet ein weiteres Mal) missbräuchlich verwendet, so dass die Befürchtung eben dieser – objektiv naheliegenden – Verwendung als solche einen immateriellen Schaden darstellt, sofern diese Befürchtung samt ihrer negativen Folgen nachgewiesen ist. Darauf, welches Gefahrenpotenzial mit Spam-Mails verbunden ist, welche Vorsichtsmaßnahmen insoweit ergriffen werden können und wann solche Mails zu einem materiellen Schaden führen, kommt es entgegen der Auffassung des Berufungsgerichts für die Qualifizierung der Befürchtung als begründet hier nicht an. Da die missbräuchliche Datenverwendung nur befürchtet werden, aber nicht erfolgen muss, ist ferner unerheblich, ob der Kläger gerade infolge des streitgegenständlichen Vorfalls Spam-Mails erhalten hat oder erhalten wird. Mit den weiteren Erwägungen, es handle sich bei den gehackten Daten nicht um besonders sensible Daten, Spam-Mails würden auch andere Personen erhalten, deren Daten nicht gehackt worden seien, das Unwohlsein des Klägers gehe nicht über das hinaus, was alle sich im Internet bewegenden Privatpersonen beim Erhalt ungebetener Nachrichten erduldeten, zudem habe der Kläger nach Bekanntwerden des Vorfalls seine E-Mail-Adresse nicht geändert, hat das Berufungsgericht im Ergebnis eine Erheblichkeitsschwelle für die Annahme eines Schadens angenommen, die es nach der oben aufgezeigten Rechtsprechung des Gerichtshofs nicht gibt. Diese Überlegungen können erst bei der Ermittlung der Schadenshöhe eine Rolle spielen (vgl. Senatsurteil v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 99). Dabei wird allerdings zu berücksichtigen sein, dass die Be-

fürchtung einer missbräuchlichen Datenverwendung und die damit verbundene Sorge stärker empfunden werden kann, wenn die betroffene Person positiv weiß, dass ihre Daten im Darknet zum Verkauf angeboten wurden.

Schließlich entzieht der Umstand, dass die Daten des Klägers der Webseite "haveibeenpwned.com" zufolge schon vor dem streitgegenständlichen Vorfall gehackt worden sein sollen, der Befürchtung, dass sie infolge des streitgegenständlichen Vorfalls erneut – von denselben oder anderen Personen – missbräuchlich verwendet werden, nicht die Grundlage. Insbesondere fehlt es entgegen der Ansicht der Revisionserwiderung nicht an der Kausalität zwischen dem streitgegenständlichen Verstoß und der Befürchtung als immateriellem Schaden. [...]

### Zur Vertiefung

*Kremer/Laue, Kontrollverlust als Schaden beim Scraping sowie Tenorierung von Unterlassungsansprüchen im Datenschutz = EuDIR 1/2025*

*Allgayer, Die Rechtsprechung des BGH zum Datenschutzrecht im Jahr 2024 = EuDIR 2/2025*

*[Urteil] Schadenersatzanspruch allein aufgrund des Kontrollverlustes über die eigenen Daten = RDV 1/2025*

## WICHTIGES AUS DER RECHTSPRECHUNG

### Kein Plattformprivileg im Anwendungsbereich der DS-GVO

(EuGH, Urteil vom 2. Dezember 2025 – C-492/23 –)

1. **Art. 5 Abs. 2 und die Art. 24 bis 26 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) sind dahin auszulegen, dass der Betreiber eines Online-Marktplatzes als Verantwortlicher im Sinne von Art. 4 Nr. 7 dieser Verordnung für die Verarbeitung der personenbezogenen Daten, die in Anzeigen enthalten sind, die auf seinem Online-Marktplatz veröffentlicht werden, vor der Veröffentlichung der Anzeigen und mittels geeigneter technischer und organisatorischer Maßnahmen verpflichtet ist,**
  - Anzeigen, die sensible Daten im Sinne von Art. 9 Abs. 1 dieser Verordnung enthalten, zu identifizieren,
  - zu prüfen, ob es sich bei dem inserierenden Nutzer, der im Begriff ist, eine solche Anzeige zu platzieren, um diejenige Person handelt, deren sensible Daten in dieser Anzeige enthalten sind, und, wenn dies nicht der Fall ist,
  - deren Veröffentlichung zu verweigern, es sei denn, der inserierende Nutzer kann nachweisen, dass die betroffene Person im Sinne von Art. 9 Abs. 2 lit. a) der Richtlinie ausdrücklich in die Veröffentlichung der fraglichen

Daten auf diesem Online-Marktplatz eingewilligt hat oder dass eine der anderen in Art. 9 Abs. 2 lit. b) bis j) vorgesehenen Ausnahmen erfüllt ist.

2. Art. 32 der Verordnung 2016/679 ist dahin auszulegen, dass der Betreiber eines Online-Marktplatzes als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung der personenbezogenen Daten, die in Anzeigen enthalten sind, die auf seinem Online-Marktplatz veröffentlicht werden, verpflichtet ist, geeignete technische und organisatorische Schutzmaßnahmen zu treffen, um zu verhindern, dass dort veröffentlichte Anzeigen, die sensible Daten im Sinne von Art. 9 Abs. 1 DS-GVO enthalten, kopiert und auf anderen Websites unrechtmäßig veröffentlicht werden.
3. Art. 1 Abs. 5 lit. b) der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) und Art. 2 Abs. 4 der Verordnung 2016/679 sind dahin auszulegen, dass sich der Betreiber eines Online-Marktplatzes als Verantwortlicher im Sinne von Art. 4 Nr. 7 der Verordnung 2016/679 für die Verarbeitung der personenbezogenen Daten, die in Anzeigen enthalten sind, die auf seinem Online-Marktplatz veröffentlicht wurden, in Bezug auf einen Verstoß gegen die Verpflichtungen aus Art. 5 Abs. 2 sowie den Art. 24 bis 26 und 32 dieser Verordnung, nicht auf die Art. 12 bis 15 der Richtlinie 2000/31 über die Verantwortlichkeit der Vermittler berufen kann.

### Zu den Vorlagefragen:

#### Zu den Fragen 2 bis 4 betreffend die Auslegung der DS-GVO

Vorbemerkungen:

Vorab ist erstens festzustellen, dass ausweislich des Vorabentscheidungsersuchens die in Rede stehende Anzeige die Klägerin des Ausgangsverfahrens als Anbieterin sexueller Dienstleistungen darstellte und dass diese Anzeige u.a. Fotos der Klägerin des Ausgangsverfahrens enthielt, die ohne ihre Einwilligung verwendet wurden, sowie ihre Telefonnummer.

Es steht fest, dass solche Informationen personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO darstellen: Hierunter sind nach der Begriffsbestimmung dieser Vorschrift „alle Informationen [zu verstehen], die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen“, wobei klargestellt wird, dass „als identifizierbar ... eine natürliche Person angesehen [wird], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Nach ständiger Rechtsprechung kommt nämlich darin, dass die Wendung „alle Informationen“ in der Definition des Begriffs „personenbezogene Daten“ in Art. 4 Nr. 1 DS-GVO Verwendung findet, das Ziel des Unionsgesetzgebers zum Ausdruck, diesem Begriff eine weite Bedeutung beizumessen,

sen, die potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen umfasst, unter der Voraussetzung, dass es sich um Informationen „über“ die in Rede stehende Person handelt. Es handelt sich um eine Information über eine identifizierte oder identifizierbare natürliche Person, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer identifizierbaren Person verknüpft ist (Urt. v. 3.4.2025, Ministerstvo zdravotníctví [Daten über den Vertreter einer juristischen Person], C-710/23, EU:C:2025:231, Rn. 21 und die dort angeführte Rechtsprechung).

Darüber hinaus sieht Art. 9 Abs. 1 DS-GVO bei diesen personenbezogenen Daten eine spezielle Schutzregelung für besondere Kategorien von Daten vor, darunter Daten zum Sexualleben oder zu der sexuellen Orientierung einer natürlichen Person.

Der Gerichtshof hat klargestellt, dass der Zweck von Art. 9 Abs. 1 DS-GVO darin besteht, einen erhöhten Schutz vor Datenverarbeitungen zu gewährleisten, die aufgrund der besonderen Sensibilität der Daten, die Gegenstand der Verarbeitungen sind, einen besonders schweren Eingriff in die durch die Art. 7 und 8 der Charta verbürgten Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen können (Urt. v. 21.12.2023, Krankenversicherung Nordrhein, C-667/21, EU:C:2023:1022, Rn. 41 und die dort angeführte Rechtsprechung).

Ein solcher verstärkter Schutz erfordert jedoch zwangsläufig, für solche „sensiblen Daten“ ein weites Begriffsverständnis zugrunde zu legen. Demnach hat der Gerichtshof entschieden, dass Art. 9 Abs. 1 DS-GVO für Verarbeitungen gilt, die sich nicht nur auf die intrinsisch sensiblen Daten beziehen, auf welche diese Vorschrift Bezug nimmt, sondern auch auf Daten, aus denen sich mittels eines Denkvorgangs der Ableitung oder des Abgleichs indirekt sensible Informationen ergeben (Urt. v. 5.6.2023, Kommission/Polen [Unabhängigkeit und Privatleben von Richtern], C-204/21, EU:C:2023:442, Rn. 344 und die dort angeführte Rechtsprechung).

Im Rahmen dieses weiten Begriffsverständnisses können Daten, die das Sexualleben oder die sexuelle Orientierung einer natürlichen Person betreffen, nicht deshalb ihre Einstufung als „sensible Daten“ i.S.v. Art. 9 Abs. 1 DS-GVO einbüßen, weil sie ihrer Art nach unwahr und schadensstiftend sind.

Zweitens ist festzustellen, dass die in Rede stehende Verarbeitung in der Veröffentlichung dieser Anzeige und damit dieser Daten auf dem Online-Marktplatz von Russmedia besteht. Denn der Vorgang, der darin besteht, personenbezogene Daten auf einer Website zu zeigen, stellt eine Verarbeitung i.S.v. Art. 4 Nr. 2 der DS-GVO dar (Urt. v. 1.8.2022, Vyriausioji tarnybinės etikos komisija, C-184/20, EU:C:2022:601, Rn. 65 und die dort angeführte Rechtsprechung).

Drittens ist darauf hinzuweisen, dass sich die Fragen 2 bis 4 darauf beziehen, dass der Betreiber des in Rede stehenden Online-Marktplatzes für die Verarbeitung personenbezogener Daten verantwortlich ist. Es zeigt sich jedoch, dass die personenbezogenen Daten, deren Veröffentlichung Gegenstand des Ausgangsrechtsstreits ist, von einem anonymen inserierenden Nutzer in die fragliche Anzeige eingefügt wurden, ohne dass dieser Betreiber einen konkreten Einfluss auf den Inhalt dieser Anzeige ausgeübt hätte und ohne dass er sich ihres irreführenden und schadensstiftenden Charakters bewusst gewesen wäre. Daher sind Klarstellungen zu den

Begriffen „Verantwortlicher“ und „gemeinsam Verantwortliche“ i.S.v. Art. 4 Nr. 7 bzw. von Art. 26 DS-GVO vorzunehmen.

Der Begriff „Verantwortlicher“ wird in Art. 4 Nr. 7 DS-GVO weit definiert als die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Durch diese weite Definition soll im Einklang mit dem Ziel der DS-GVO ein wirksamer Schutz der Grundfreiheiten und Grundrechte natürlicher Personen und insbesondere ein hohes Schutzniveau für das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten gewährleistet werden (Urt. v. 5.12.2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, Rn. 29 und die dort angeführte Rechtsprechung).

Somit kann jede natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung solcher Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als für diese Verarbeitung Verantwortlicher angesehen werden (Urt. v. 5.12.2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, Rn. 30 und die dort angeführte Rechtsprechung).

Zudem verweist der Begriff des „Verantwortlichen“, da er sich, wie Art. 4 Nr. 7 DS-GVO ausdrücklich vorsieht, auf die Stelle bezieht, die „allein oder gemeinsam mit anderen“ über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, nicht zwingend auf eine einzige Stelle und kann mehrere an dieser Verarbeitung beteiligte Akteure betreffen, wobei dann jeder von ihnen den Datenschutzvorschriften unterliegt (vgl. i.d.S. Urt. v. 29.7.2019, *Fashion ID*, C-40/17, EU:C:2019:629, Rn. 67 und die dort angeführte Rechtsprechung).

Art. 26 DS-GVO, der sich in den begrifflichen Rahmen des „Verantwortlichen“ nach Art. 4 Nr. 7 DS-GVO einfügt, sieht im Wesentlichen vor, dass zwei oder mehr Verantwortliche, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, als „gemeinsam Verantwortliche“ für diese Verarbeitung einzustufen sind.

Eine solche gemeinsame Verantwortlichkeit erfordert nicht notwendigerweise das Vorliegen gemeinsamer Entscheidungen über die Festlegung der Zwecke und Mittel der Verarbeitung der betreffenden personenbezogenen Daten. Der Gerichtshof hat nämlich entschieden, dass die Mitwirkung an der Entscheidung über diese Zwecke und Mittel verschiedene Formen annehmen und sich sowohl aus einer gemeinsamen Entscheidung von zwei oder mehr Einrichtungen als auch aus übereinstimmenden Entscheidungen ergeben kann, die sich in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Festlegung der Verarbeitungszwecke und -mittel auswirkt (vgl. i.d.S. Urt. v. 5.12.2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, Rn. 43).

Insoweit setzt die gemeinsame Verantwortlichkeit mehrerer Akteure für dieselbe Verarbeitung nach Art. 4 Nr. 7 DS-GVO nicht voraus, dass jeder von ihnen Zugang zu den betreffenden personenbezogenen Daten hat (Urt. v. 29.7.2019, *Fashion ID*, C-40/17, EU:C:2019:629, Rn. 69 und die dort angeführte Rechtsprechung, sowie v. 5.12.2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, Rn. 42).

Im selben Sinne hat der Gerichtshof klargestellt, dass aus einer gemeinsamen Verantwortlichkeit nicht zwangs-

läufig folgt, dass die verschiedenen Akteure für dieselbe Verarbeitung personenbezogener Daten eine gleichwertige Verantwortlichkeit trifft. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist (vgl. i.d.S. Urt. v. 10.7.2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, Rn. 66 und die dort angeführte Rechtsprechung, sowie v. 5.12.2023, *Nacionalinis visuomenės sveikatos centras*, C-683/21, EU:C:2023:949, Rn. 42).

Im vorliegenden Fall steht fest, dass der inserierende Nutzer, der die irreführende, schadenstiftende und personenbezogene Daten der Klägerin des Ausgangsverfahrens enthaltende Anzeige auf dem von Russmedia betriebenen Online-Marktplatz platzierte, als derjenige anzusehen ist, der über die Zwecke und Mittel der Verarbeitung dieser Daten hauptsächlich entschieden hat, und daher unter den Begriff des „Verantwortlichen“ im Sinne von Art. 4 Nr. 7 DS-GVO fällt.

Gleichwohl ist erwiesen, dass diese Anzeige nur dank dem von Russmedia betriebenen Online-Marktplatz im Internet veröffentlicht und den Internetnutzern somit zugänglich gemacht wurde.

Zwar ergibt sich aus der in Rn. 58 des vorliegenden Urteils angeführten Rechtsprechung, dass eine Person nur dann als „Verantwortlicher“ für die Verarbeitung personenbezogener Daten eingestuft werden kann, wenn sie diese Verarbeitung aus Eigeninteresse beeinflusst, doch ist festzustellen, dass dies u.a. dann der Fall sein kann, wenn der Betreiber eines Online-Marktplatzes relevante personenbezogene Daten zu kommerziellen Zwecken oder Werbezwecken veröffentlicht, die über die bloße Erbringung einer Dienstleistung, die er dem inserierenden Nutzer erbringt, hinausgehen.

Im vorliegenden Fall geht aus der Vorlageentscheidung hervor, dass Russmedia auf ihrem Online-Marktplatz aus kommerziellem Eigeninteresse heraus Anzeigen veröffentlicht. Insoweit werden Russmedia durch die allgemeinen Nutzungsbedingungen dieses Marktplatzes große Freiräume eingeräumt, um die auf diesem Marktplatz veröffentlichten Informationen zu nutzen. Insbesondere behält sich Russmedia nach den Angaben des vorlegenden Gerichts das Recht vor, veröffentlichte Inhalte zu nutzen, zu verbreiten, zu übermitteln, zu vervielfältigen, zu ändern, zu übersetzen, an Partner weiterzugeben und jederzeit zu entfernen, ohne dass es insoweit eines „triftigen Grundes“ bedürfte. Russmedia veröffentlicht daher die in den Anzeigen enthaltenen personenbezogenen Daten nicht oder nicht nur für die inserierenden Nutzer, sondern verarbeitet diese Daten und kann zu ihren eigenen Werbezwecken und aus kommerziellen Eigeninteressen Profit aus ihnen ziehen.

Somit ist davon auszugehen, dass Russmedia aus Eigeninteresse auf die Veröffentlichung der personenbezogenen Daten der Klägerin des Ausgangsverfahrens im Internet Einfluss genommen und damit an der Festlegung der Zwecke dieser Veröffentlichung und somit der Zwecke der in Rede stehenden Verarbeitung mitgewirkt hat.

Diese Feststellung wird nicht dadurch in Frage gestellt, dass offensichtlich der irreführende und schadenstiftende Zweck, den der inserierende Nutzer mit der Veröffentlichung

der im Ausgangsverfahren in Rede stehenden Anzeige verfolgt hat, ohne Mitwirkung von Russmedia festgelegt wurde. An der Festlegung desjenigen Zwecks der Verarbeitung, der darin bestand, den Internetnutzern die in der im Ausgangsverfahren fraglichen Anzeige enthaltenen personenbezogenen Daten zugänglich zu machen, um aus diesen Veröffentlichungen Profit zu ziehen, hat Russmedia nämlich mitgewirkt. Darüber hinaus hat Russmedia es erleichtert, dass solche Daten ohne Einwilligung der betroffenen Person veröffentlicht wurden, indem das Unternehmen es ermöglicht hat, anonym Anzeigen auf ihrem Online-Marktplatz zu platzieren.

Außerdem hat Russmedia dadurch, dass das Unternehmen dem inserierenden Nutzer seinen Online-Marktplatz, der der Veröffentlichung der im Ausgangsverfahren in Rede stehenden Anzeige gedient hat, zur Verfügung gestellt hat, an der Festlegung der Mittel dieser Veröffentlichung mitgewirkt.

Der Gerichtshof hat nämlich im Wesentlichen bereits entschieden, dass an der Festlegung der Mittel zur Verarbeitung diejenige natürliche oder juristische Person beteiligt ist, die das Erheben und die Übermittlung von personenbezogenen Daten maßgeblich beeinflusst, oder auch eine Person, die durch ihre Parametrierung entsprechend ihren Zielen der Steuerung oder Förderung ihrer Tätigkeiten auf die Verarbeitung solcher Daten Einfluss nimmt (vgl. i.d.S. Ur. v. 5.6.2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, Rn. 36, sowie v. 29.7.2019, Fashion ID, C-40/17, EU:C:2019:629, Rn. 78). Gleiches gilt für eine Suchmaschine, wenn ihre Tätigkeit insofern maßgeblichen Anteil an der weltweiten Verbreitung personenbezogener Daten hat, als sie diese Daten in organisierter und aggregierter Weise online öffentlich zugänglich macht (vgl. i.d.S. Ur. v. 8.12.2022, Google [Auslistung eines angeblich unrichtigen Inhalts], C-460/20, EU:C:2022:962, Rn. 50 und die dort angeführte Rechtsprechung).

Daher ist festzustellen, dass der Betreiber eines Online-Marktplatzes wie Russmedia, wenn er die Parameter für die Verbreitung der Anzeigen, die personenbezogene Daten enthalten können, nach Maßgabe des Zielpublikums festlegt, die Darstellung, die Dauer dieser Verbreitung oder die Rubriken, in denen die veröffentlichten Informationen strukturiert werden, festlegt oder das Ranking organisiert, von dem die Einzelheiten einer solchen Verbreitung abhängen, an der Festlegung der wesentlichen Mittel zur Veröffentlichung der betreffenden personenbezogenen Daten mitwirkt und damit maßgeblich auf die weltweite Verbreitung dieser Daten Einfluss nimmt.

Insoweit kann der Inhalt der allgemeinen Nutzungsbedingungen des betreffenden Online-Marktplatzes Anhaltspunkte dafür liefern, dass der Betreiber dieses Marktplatzes die betreffende Verarbeitung personenbezogener Daten maßgeblich beeinflusst und somit die Mittel dieser Verarbeitung festlegt. Dies scheint für die allgemeinen Nutzungsbedingungen des Online-Marktplatzes von Russmedia zu gelten, in denen sich Russmedia u.a. das Recht vorbehält, die in den Anzeigen enthaltenen Informationen einschließlich der darin enthaltenen personenbezogenen Daten zu verbreiten, zu übermitteln, zu veröffentlichen, zu löschen oder auch zu vervielfältigen.

Jedenfalls kann sich der Betreiber eines Online-Marktplatzes als für die Verarbeitung personenbezogener Daten Verantwortlicher nicht mit der Begründung seiner Verantwortung entziehen, dass er den Inhalt der auf diesem Marktplatz veröffentlichten Anzeige nicht selbst festgelegt hat. Es liefe nämlich nicht nur dem klaren Wortlaut, sondern auch dem Zweck von Art. 4 Nr. 7 DS-GVO zuwider, der darin besteht, durch eine weite Definition des Begriffs „Verantwortlicher“ einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten, wenn ein solcher Betreiber allein aus diesem Grund von dieser Definition ausgenommen würde.

Daher ist festzustellen, dass das vorliegende Gericht seine Fragen 2 bis 4 zu Recht auf die Prämisse gestützt hat, dass der Betreiber des Online-Marktplatzes bei einer Sachlage wie der im Ausgangsverfahren in Rede stehenden im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung der personenbezogenen Daten verantwortlich ist, die in einer auf diesem Online-Marktplatz veröffentlichten Anzeige enthalten sind. [...]

### Zur ersten Frage: Auslegung der Richtlinie 2000/31

Wie in den Rn. 45 und 46 des vorliegenden Urteils ausgeführt, möchte das vorliegende Gericht ferner wissen, ob sich der Betreiber eines Online-Marktplatzes als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung der personenbezogenen Daten, die in Anzeigen enthalten sind, die auf seinem Online-Marktplatz veröffentlicht wurden, in Bezug auf einen Verstoß gegen die Verpflichtungen aus Art. 5 Abs. 2 sowie aus den Art. 24 bis 26 und 32 DS-GVO, die in den Rn. 106 und 126 des vorliegenden Urteils festgestellt worden sind, auf die Art. 12 bis 15 der Richtlinie 2000/31 über die Verantwortlichkeit der Vermittler berufen kann.

Daher stellt sich die Frage nach dem Zusammenspiel dieser beiden Unionsrechtsakte. Insbesondere ist zu prüfen, ob die Art. 12 bis 15 der Richtlinie 2000/31 in die in der DS-GVO vorgesehene Haftungsregelung eingreifen können.

Hierzu ist zum einen festzustellen, dass die Richtlinie 2000/31 nach ihrem Art. 1 Abs. 5 lit. b) keine Anwendung auf Fragen betreffend die Dienste der Informationsgesellschaft findet, die von den Richtlinien 95/46 und 97/66 erfasst werden.

Diese Bestimmung ist vom Gerichtshof dahin ausgelegt worden, dass Fragen, die mit dem Schutz der Vertraulichkeit der Kommunikation und personenbezogener Daten zusammenhängen, anhand der DS-GVO und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) zu beurteilen sind, die an die Stelle der Richtlinie 95/46 bzw. der Richtlinie 97/66 getreten sind, wobei der Schutz, den die Richtlinie 2000/31 gewährleisten soll, auf keinen Fall die Anforderungen, die sich aus der DS-GVO und der Richtlinie 2002/58 ergeben, beeinträchtigen darf (Ur. v. 6.10.2020, La Quadrature du Net u.a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 200 und die dort angeführte Rechtsprechung).

Daraus folgt insbesondere, dass die etwaige Inanspruchnahme der in Art. 14 Abs. 1 der Richtlinie 2000/31 vorgesehenen Befreiung, auf die sich der Betreiber eines Online-Marktplatzes in Bezug auf die auf seiner Website gehosteten

Informationen berufen könnte, nicht in die Regelung der DS-GVO eingreifen kann, die für einen solchen Betreiber wie für jeden anderen Wirtschaftsteilnehmer gilt, der in den Anwendungsbereich dieser Verordnung fällt.

Gleiches gilt für Art. 15 der Richtlinie 2000/31, wonach die Mitgliedstaaten den Diensteanbietern hinsichtlich der Erbringung der u.a. in Art. 14 dieser Richtlinie genannten Dienste keine allgemeine Überwachungspflicht auferlegen dürfen. Im Übrigen kann die Verpflichtung des Betreibers eines Online-Marktplatzes, die sich aus der DS-GVO ergebenden Anforderungen zu erfüllen, jedenfalls nicht als eine solche allgemeine Überwachungspflicht eingestuft werden.

Zum anderen sieht Art. 2 Abs. 4 DS-GVO vor, dass die Verordnung die Anwendung der Richtlinie 2000/31 und zwar insbesondere der Vorschriften der Art. 12 bis 15 dieser Richtlinie zur Verantwortlichkeit der Vermittler unberührt lässt.

Art. 2 Abs. 4 DS-GVO ist dahin zu verstehen, dass der Umstand, dass ein Wirtschaftsteilnehmer Träger von in der DS-GVO vorgesehenen Pflichten ist, nicht automatisch ausschließt, dass sich dieser Wirtschaftsteilnehmer in anderen Fragen als solchen, die den Schutz personenbezogener Daten betreffen, auf die Art. 12 bis 15 der Richtlinie 2000/31 berufen kann.

Somit ergibt sich aus Art. 1 Abs. 5 lit. b) der Richtlinie 2000/31 in Verbindung mit Art. 2 Abs. 4 DS-GVO, dass die Bestimmungen dieser Richtlinie, insbesondere ihre Art. 12 bis 15, nicht in die Regelung der DS-GVO eingreifen können.

Nach alledem ist auf die erste Frage zu antworten, dass Art. 1 Abs. 5 lit. b) der Richtlinie 2000/31 und Art. 2 Abs. 4 DS-GVO dahin auszulegen sind, dass sich der Betreiber eines Online-Marktplatzes als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO für die Verarbeitung der personenbezogenen Daten, die in Anzeigen enthalten sind, die auf seinem Online-Marktplatz veröffentlicht wurden, in Bezug auf einen Verstoß gegen die Verpflichtungen aus Art. 5 Abs. 2 sowie aus den Art. 24 bis 26 und 32 DS-GVO nicht auf die Art. 12 bis 15 der Richtlinie 2000/31 über die Verantwortlichkeit der Vermittler berufen kann. [...]

## Rechtfertigung der Übermittlung personenbezogener Positivdaten

(BGH, Urteil vom 14. Oktober 2025 – VI ZR 431/24 –)

1. Ein Unterlassungsantrag, der auch datenschutzrechtlich nicht zu beanstandende Verhaltensweisen erfasst, ist zu weit gefasst und damit unbegründet
2. Die Übermittlung personenbezogener Positivdaten (hier: zum Identitätsabgleich erforderliche Stammdaten der Verbraucher sowie die Information, dass ein Vertragsverhältnis mit diesen begründet oder beendet wurde) seitens eines Mobilfunkdiensteanbieters an eine Wirtschaftsauskunftei kann gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO durch das Interesse an einer Betrugsprävention gerechtfertigt sein.

### Aus den Gründen:

B. Die Revision ist unbegründet. [...]

4. Der Klageantrag zu 1.a ist im Haupt- und Hilfsantrag unbegründet, weil er auch datenschutzrechtlich nicht zu be-

anstandene Verhaltensweisen erfasst und damit zu weit gefasst ist (vgl. BGH, Urte. v. 18.10.2012 – I ZR 137/11, NJW 2013, 1373 Rn. 22 m.w.N. – Steuerbüro; OLG Köln, GRUR-RS 2023, 34611 Rn. 20-23; OLG München, ZD 2025, 463 Rn. 44 ff.; LG Stuttgart, GRUR-RS 2025, 6262 Rn. 24). Der Antrag ist darauf gerichtet, der Beklagten jede Übermittlung der Positivdaten von Verbrauchern an die SCHUFA nach Abschluss eines Telekommunikationsvertrages zu verbieten, die wie in Anlage K 3 "beschrieben", erfolgt, also insbesondere nicht an das Vorliegen konkreter Anhaltspunkte für ein Ausfallrisiko oder einen Betrug im Einzelfall geknüpft ist (s.o. 1.b; vom Kläger als "anlasslose", "pauschale" Übermittlung bezeichnet). Eine Einschränkung des Unterlassungsantrags durch die Formulierung von Ausnahmen (vgl. dazu BGH, Urte. v. 18.10.2012 – I ZR 137/11, NJW 2013, 1373 Rn. 21 m.w.N. – Steuerbüro) hat der Kläger nur im Hilfsantrag und dort nur hinsichtlich des Vorliegens einer Einwilligung vorgenommen, und – wie sich aus der Formulierung "insbesondere nicht auf der Basis von Art. 6 Abs. 1 f) DS-GVO" ergibt – ausdrücklich nicht für eine Rechtfertigung gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO. Eine solche hält er im Gegenteil für ausgeschlossen und zwar auch dann, wenn es um die ("pauschale", "anlasslose") Übermittlung von Positivdaten zum Zwecke der Betrugsprävention geht.

Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen hält aber dessen Beurteilung, die Übermittlung der hier betroffenen Positivdaten der Verbraucher seitens der Beklagten an die SCHUFA lasse sich gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO durch das Interesse der Beklagten an einer hinreichenden Betrugsprävention rechtfertigen, der revisionsrechtlichen Nachprüfung stand. Damit schränkt der Klageantrag zu 1.a den der Beklagten datenschutzrechtlich eingeräumten Gestaltungsspielraum beim Umgang mit Positivdaten zu weitgehend ein. Der Hauptantrag ist darüber hinaus auch deshalb unbegründet, weil auch eine wirksame Einwilligung des Verbrauchers die Datenübermittlung rechtfertigen würde; dies hat der Kläger erst im Hilfsantrag berücksichtigt.

a) Die Rechtmäßigkeit der streitgegenständlichen Datenübermittlung richtet sich allein nach der DS-GVO, deren zeitlicher (Art. 99 Abs. 2 DS-GVO), räumlicher (Art. 3 DS-GVO) und sachlicher Anwendungsbereich (Art. 2 Abs. 1 DS-GVO) eröffnet ist. Die Übermittlung der personenbezogenen Daten durch die Beklagte als Verantwortliche an die SCHUFA stellt eine Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO dar. § 31 BDSG ist unabhängig von der umstrittenen Frage, ob diese Regelung unionsrechtskonform ist (offengelassen: EuGH, Urte. v. 7.12.2023 – C-634/21, EuGRZ 2023, 642 Rn. 72; verneinend mangels Öffnungsklausel für den nationalen Gesetzgeber: Simitis/Hornung/Spiecker gen. Döhmman/Ehmann, Datenschutzrecht, 2. Aufl., § 31 BDSG Rn. 6 ff.; Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl., Art. 6 DS-GVO Rn. 161 und Rn. 199 f.), nicht einschlägig, da diese Vorschrift nicht unmittelbar die Übermittlung von Daten an Auskunfteien (sog. Einmeldung) regelt (Ehmann a.a.O. Rn. 115; Taeger/Gabel/Taeger, DS-GVO-BDSG-TTDSG, 4. Aufl., § 31 BDSG Rn. 24-26).

b) Art. 6 Abs. 1 UAbs. 1 DS-GVO enthält eine erschöpfende und abschließende Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Daher muss eine Verarbeitung unter einen der in dieser Bestimmung vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können. Nach Art. 6

Abs. 1 UAbs. 1 lit. a) DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung i.S.v. Art. 4 Nr. 11 DS-GVO dazu für einen oder mehrere bestimmte Zwecke gegeben hat (st. Rspr. des EuGH, vgl. nur Urt. v. 12.9.2024 – C-17/22 und C-18/22, NJW 2024, 3637 Rn. 34 m.w.N., 36).

Dies berücksichtigt der Hauptantrag, anders als der Hilfsantrag, nicht, so dass das mit dem Hauptantrag erstrebte Unterlassungsgebot schon deshalb zu weit geht.

c) Liegt keine wirksame Einwilligung vor, ist eine Verarbeitung personenbezogener Daten gleichwohl gerechtfertigt, wenn sie aus einem der in Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) DS-GVO genannten Gründe erforderlich ist, wobei diese Rechtfertigungsgründe eng auszulegen sind (st. Rspr. des EuGH, vgl. Urt. v. 12.9.2024 – C-17/22 und C-18/22, NJW 2024, 3637 Rn. 36 f. m.w.N.).

aa) Nach dem hier allein in Betracht kommenden Rechtfertigungsgrund des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie "zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen...". Nach ständiger Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) ist die Verarbeitung personenbezogener Daten nach dieser Bestimmung unter drei kumulativen Voraussetzungen rechtmäßig: Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein, und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (EuGH, Urt. v. 9.1.2025 – C-394/23, NJW 2025, 807 Rn. 45 m.w.N.). Was erstens die Voraussetzung der Wahrnehmung eines berechtigten Interesses betrifft, ist zu berücksichtigen, dass es nach Art. 13 Abs. 1 lit. d) DS-GVO dem Verantwortlichen obliegt, einer betroffenen Person zu dem Zeitpunkt, zu dem personenbezogene Daten bei ihr erhoben werden, die verfolgten berechtigten Interessen mitzuteilen, wenn diese Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO beruht. In Ermangelung einer Definition des Begriffs "berechtigtes Interesse" durch die DS-GVO kann ein breites Spektrum von Interessen grundsätzlich als berechtigt gelten. Insbesondere ist dieser Begriff nicht auf gesetzlich verankerte und bestimmte Interessen beschränkt (EuGH a.a.O. Rn. 46 m.w.N.). Das geltend gemachte berechtigte Interesse muss allerdings rechtmäßig sein (EuGH, Urt. v. 4.10.2024 – C-621/22, NJW 2024, 3769 Rn. 40). Was zweitens die Voraussetzung der Erforderlichkeit der Verarbeitung personenbezogener Daten zur Verwirklichung des wahrgenommenen berechtigten Interesses betrifft, ist zu prüfen, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere in die durch Art. 7 und 8 GRCh garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen, wo-

bei eine solche Verarbeitung innerhalb der Grenzen dessen erfolgen muss, was zur Verwirklichung dieses berechtigten Interesses unbedingt notwendig ist. Die Voraussetzung der Erforderlichkeit der Datenverarbeitung ist gemeinsam mit dem Grundsatz der Datenminimierung zu prüfen, der in Art. 5 Abs. 1 lit. c) DS-GVO verankert ist und verlangt, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (EuGH, Urt. v. 9.1.2025 – C-394/23, NJW 2025, 807 Rn. 48 f. m.w.N.). Was schließlich drittens die Voraussetzung betrifft, dass die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen, gebietet diese Voraussetzung eine den nationalen Gerichten obliegende Abwägung der einander gegenüberstehenden Rechte und Interessen, die grundsätzlich von den konkreten Umständen des Einzelfalls abhängt. Wie sich aus ErwG 47 DS-GVO ergibt, können die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen insbesondere dann überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet (EuGH a.a.O. Rn. 49 f.). Zu berücksichtigen ist ferner der Umfang der fraglichen Verarbeitung und deren Auswirkungen auf die betroffene Person (EuGH, Urt. v. 12.9.2024 – C-17/22 und C-18/22, NJW 2024, 3637 Rn. 62).

bb) Nach diesen Grundsätzen lässt sich auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen die Übermittlung der zum Identitätsabgleich erforderlichen Stammdaten der Verbraucher sowie der Information, dass ein Vertragsverhältnis mit diesen begründet oder beendet wurde, seitens der Beklagten an die SCHUFA gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO durch das Interesse der Beklagten an einer hinreichenden Betrugsprävention rechtfertigen.

(1) Bei dem von der Beklagten den Verbrauchern in den Datenschutzhinweisen (Anlage K 3) mitgeteilten Interesse an Betrugsprävention handelt es sich um ein berechtigtes, insbesondere rechtmäßiges, wirtschaftliches Interesse der Beklagten. Das Interesse an der Verhinderung von Betrug ist in ErwG 47 DS-GVO ausdrücklich als berechtigtes Interesse angeführt. Soweit dort vom für die Verhinderung von Betrug "unbedingt erforderlichen Umfang" die Rede ist, betrifft dies die Frage der Erforderlichkeit.

(2) Auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen kann die Übermittlung der hier betroffenen Positivdaten zur Verhinderung von Betrug als unbedingt erforderlich angesehen werden.

(a) Nach den tatbestandlichen Feststellungen des Berufungsgerichts übermittelte die Beklagte (bis Oktober 2023) nur bei Postpaid-Mobilfunkverträgen Positivdaten von Kunden an die SCHUFA, nämlich zumindest die zum Identitätsabgleich erforderlichen Stammdaten sowie die Information, dass ein Vertragsverhältnis mit dem Verbraucher begründet oder beendet wurde. Weiter nimmt das Berufungsurteil konkret Bezug auf den Vortrag der Beklagten zur Betrugsprävention in der Klageerwiderung und fasst diesen dahingehend zusammen, dass in den Fällen, in denen potenzielle Kunden in kurzer Zeit unerklärlich viele Mobilfunkverträge abschließen, auf ihre Absicht geschlossen werden könne, an die teure

Hardware zu gelangen. Ferner müssten Name und Geburtsdatum übermittelt werden, um die Identität sicher feststellen zu können. Die Beklagte hat zu ihrem Interesse an Betrugsprävention in der Klageerwidern näher ausgeführt, dass Betrugsfälle zulasten von Mobilfunkdiensteanbietern bei Postpaid-Mobilfunkverträgen dadurch gekennzeichnet seien, dass die Täter durch "gefälschte existente oder fiktive" Personendaten ihre Identität verschleiern und über ihr Wollen oder Können täuschen, die entstehenden Forderungen zu bedienen, um einen Vertragsschluss zu erwirken. Ein Indiz für einen möglichen Betrugsversuch könne sein, dass eine Person mittleren Alters wirtschaftlich bislang überhaupt nicht in Erscheinung getreten sei; dies sei statistisch unwahrscheinlich und daher ein Indiz dafür, dass es sich um eine fiktive Identität handle. Ein weiteres typisches Indiz für einen Betrugsversuch sei der Abschluss zahlreicher Mobilfunkverträge in kurzer zeitlicher Abfolge bei verschiedenen Mobilfunkdiensteanbietern, z.B. von sechs Verträgen binnen einer Woche. Das wirtschaftliche Interesse der Beklagten an der Nutzung von Positivdaten belaufe sich allein im Hinblick auf den Zweck der Betrugsprävention pro Jahr auf einen siebenstelligen Betrag. In der Vergangenheit habe die Beklagte auf Basis der von den Auskunftseien gespeicherten Positivdaten eine Vielzahl von Aufträgen wegen des Abschlusses auffällig vieler Verträge mit der Absicht, an die Hardware zu gelangen, oder wegen fiktiver Identitäten abgelehnt. Der Schaden entstehe durch Hardwareverlust und Serviceerschleichung.

(b) Nach den tatbestandlichen Feststellungen des Berufungsgerichts ist der Vortrag der Beklagten zu Betrugsversuchen bei der Eingehung von Mobilfunkverträgen und dazu, dass die Auskunftseien hierzu nähere Bewertungsmethoden entwickelt hätten, vom Kläger nicht angegriffen worden. Dem Einwand der Revision, der Kläger habe den Vortrag mit Nichtwissen bestritten, steht schon die Beweiskraft dieser tatbestandlichen Feststellung entgegen (§ 314 ZPO). Abgesehen davon verweist die Revision insoweit lediglich darauf, dass der Kläger zum Ausdruck gebracht habe, die pauschale, anlasslose und uneingeschränkte Übermittlung der personenbezogenen Daten sei durch das Interesse der Beklagten nicht gerechtfertigt. Dabei handelt es sich aber nicht um ein Bestreiten des tatsächlichen Vortrags der Beklagten mit Nichtwissen, sondern um die Darstellung der Rechtsauffassung des Klägers zur Interessenabwägung.

(c) Wie das Berufungsgericht weiter festgestellt hat, ruft die Beklagte ihrem unbestrittenen Vortrag zufolge die Zahl der bereits (mit anderen Mobilfunkdiensteanbietern) abgeschlossenen (und von diesen eingemeldeten) Verträge bei der SCHUFA vor Abschluss des Vertrages mit ihrem Kunden ab. Ihrerseits meldet sie die Positivdaten des Kunden einschließlich der Information über den Vertragsschluss sodann nach Abschluss des Vertrages. Dieses System der Einmeldung der Positivdaten seitens der Mobilfunkdiensteanbieter bei den Wirtschaftsauskunftseien erscheint geeignet, die Mobilfunkdiensteanbieter über die genannten Indizien eines Eingehungsbetrugs, insbesondere über eine ungewöhnliche Anzahl bereits abgeschlossener Mobilfunkverträge binnen kurzer Zeit, zu informieren.

(d) Die Revision weist zwar zu Recht darauf hin, dass die Beklagte die Erforderlichkeit der Einmeldung der Positivdaten für die Betrugsprävention darzulegen und zu beweisen hat. Es erschließt sich jedoch nicht, wie das Interesse der Be-

klagten an der Bekämpfung der genannten Betrugszenarien in zumutbarer Weise ebenso wirksam mit milderem Mitteln erreicht werden könnte. Die Einholung einer freiwilligen (zu den hohen Anforderungen vgl. Art. 7 Abs. 4 DS-GVO) und zudem gem. Art. 7 Abs. 3 DS-GVO jederzeit widerruflichen Einwilligung des Kunden in die Übermittlung der Positivdaten wäre nicht ebenso wirksam, weil der Vertragsschluss von der Einwilligung nicht abhängig gemacht werden dürfte und gerade etwaige Betrüger der Übermittlung der Daten nicht zustimmen oder ihre Zustimmung sofort widerrufen würden (vgl. OLG Koblenz, GRUR-RS 2025, 10143 Rn. 21). Negativdaten, deren Übermittlung an die SCHUFA der Kläger nicht angreift, können zwar unter Umständen ebenfalls auf eine Betrugsabsicht hinweisen, allerdings liegen sie gerade in den Fällen, in denen ein Kunde in kurzer Zeit außergewöhnlich viele Verträge abschließt, typischerweise noch nicht vor. Zudem schützt ihre Übermittlung nicht vor dem Abschluss eines Vertrages unter falscher Identität. Die Übermittlung der Positivdaten nur bei einem vom Kläger geforderten "Anlass", etwa wenn Auffälligkeiten (welche?) bereits vorliegen, erscheint deshalb nicht ebenso wirksam für die Betrugsprävention, weil es gilt, eben diese Auffälligkeiten rechtzeitig zu ermitteln und zu diesem Zweck Positivdaten von Anfang an vollständig zusammenzutragen. Der Einwand der Revision, die Übermittlung der Positivdaten sei allenfalls dann erforderlich, wenn Vertragsgegenstand auch die vom Berufungsgericht angesprochene Überlassung von teurer Hardware (z.B. eines Smartphones) sei, in diesen Fällen könne die Beklagte als milderes Mittel allerdings ihr Geschäftsmodell ändern und reine Mobilfunkleistungen und Abzahlungsgeschäfte über Hardware getrennt anbieten und ihre Zusammenarbeit mit den Wirtschaftsauskunftseien auf die Abzahlungsgeschäfte beschränken, greift nicht durch. Bei der gebotenen Prüfung, ob das berechnete Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen, ist auf das von dem jeweiligen Verantwortlichen gewählte (legale) Leistungsangebot abzustellen. Sie erlaubt es nicht, dem Verantwortlichen unter Missachtung seiner unternehmerischen Freiheit (Art. 16 GRCh) den Wechsel zum Angebot anderer Leistungen aufzuerlegen. Zudem ergibt sich aus dem vom Berufungsgericht in Bezug genommenen und oben referierten Vortrag der Beklagten aus der Klageerwidern, dass mit der Einmeldung der Positivdaten betrügerisches Verhalten bei der Eingehung eines Postpaid-Mobilfunkvertrages auch, aber nicht nur dann bekämpft werden soll, wenn mit dem Vertrag teure Hardware überlassen wird.

(3) Entgegen der Ansicht der Revision überwiegen die Interessen oder Grundrechte und Grundfreiheiten der Verbraucher, deren oben genannte Positivdaten von der Beklagten bei Postpaid-Mobilfunkverträgen an die SCHUFA eingemeldet werden, das berechnete Interesse der Beklagten an einer hinreichenden Betrugsprävention nicht.

(a) Die Zulässigkeit der Übermittlung von Positivdaten an Wirtschaftsauskunftseien ist umstritten.

(aa) Die überwiegende Meinung in der Rechtsprechung (OLG Koblenz, GRUR-RS 2025, 10143 Rn. 10 ff., 52 ff.; OLG Bamberg, GRUR-RS 2025, 8805 Rn. 9 ff.; OLG Nürnberg, GRUR-RS 2025, 17454 Rn. 41 ff.; beispielhaft aus der Rechtsprechung der Landgerichte: LG Stuttgart, GRUR-RS 2025, 6262 Rn. 17 ff.;

LG Bad Kreuznach, GRUR-RS 2025, 1169 Rn. 71 ff.; LG Frankfurt am Main, Urt. v. 18.12.2024 – 2-28 O 33/24, juris Rn. 45 ff.; LG Freiburg im Breisgau, GRUR-RS 2024, 30639 Rn. 32 ff.; LG Weiden i. d. OPf., GRUR-RS 2024, 23031 Rn. 44 ff.; weitere umfangreiche Nachweise bei AG Lüdenscheid, GRUR-RS 2025, 17403 Rn. 43) hält die Übermittlung der Positivdaten von Verbrauchern im Zusammenhang mit dem Abschluss von Telekommunikationsverträgen, insbesondere Postpaid-Mobilfunkverträgen, an Wirtschaftsauskunfteien zum Zweck der Betrugsprävention für rechtmäßig. Teilweise wird vertreten, dass jedenfalls ein Unterlassungsantrag, der die Ausnahme des berechtigten Interesses einer Betrugsprävention nicht aufnehme, zu weit gehe (OLG München, ZD 2025, 463 Rn. 44-46; OLG Köln, GRUR-RS 2023, 34611 Rn. 20-23; LG Köln, GRUR-RS 2023, 9811 Rn. 51; LG Stuttgart, GRUR-RS 2025, 6262 Rn. 24).

Auch Teile der Literatur sprechen sich – allgemein oder für bestimmte Branchen – für die Zulässigkeit der Übermittlung von Positivdaten an Auskunfteien aus (Paal, NJW 2024, 1689, insbes. Rn. 13-20; Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl., Art. 6 DS-GVO Rn. 164; Schulz, RDV 2022, 117, 119 ff.; Assion/Hauck, Beilage ZD 12/2020, 1, 5 f.; Taeger/Gabel/Taeger, DS-GVO-BDSG-TTDSG, 4. Aufl., § 31 BDSG Rn. 26, 52; Auer-Reinsdorff/Conrad/Conrad, Handbuch IT- und Datenschutzrecht, 19. Aufl., § 34 Rn. 767; von Lewinski/Pohl, ZD 2018, 17, 20 f.).

(bb) Aus Sicht der Gegenmeinung, der die Revision folgt, überwiegt das Interesse der Verbraucher am Schutz ihrer personenbezogenen Daten das Interesse der die Positivdaten einmeldenden Stelle an einer Betrugsprävention. Sie betont, dass die anlasslos – da erst nach Vertragsschluss und unabhängig von einem eigenen Fehlverhalten des Verbrauchers – erfolgende Vorratsdatensammlung zur Betrugsprävention weit überwiegend Verbraucher betreffe, bei denen weder ein kreditorisches Risiko noch das Risiko eines Identitätsdiebstahls oder eines sonstigen betrügerischen Verhaltens bestehe. Das Interesse der Verbraucher am Schutz vor einer anlasslosen und unterschiedslosen Erhebung ihrer personenbezogenen Daten zur Erreichung abstrakt-genereller Ziele, in deren Vorteil sie in der Regel allenfalls mittelbar kommen könnten, überwiege das Interesse des Verantwortlichen erheblich (LG München, ZD 2024, 46 Rn. 114 ff.; LG Lübeck, GRUR-RS 2025, 511 Rn. 39 ff.; ähnlich Ziebarth, RDV 2024, 330, 333 ff.). Eine pauschale und präventive Übermittlung sämtlicher Daten im Zusammenhang mit dem Vertragsverhältnis sei weder üblich noch werde sie vernünftigerweise erwartet (LG Köln, GRUR-RS 2023, 9811 Rn. 51; LG Stuttgart, GRUR-RS 2024, 28242 Rn. 27). Ein überwiegendes Interesse der Verbraucher wird teilweise auch daraus hergeleitet, dass die Datenübermittlung zum Zwecke der Erstellung eines Persönlichkeitsprofils erfolge, welches in einen Gesamtscore zur Erfassung der Bonität der Betroffenen kulminiere, wobei hierzu eine große Zahl von an sich nicht miteinander verbundenen Datenpunkten nach einem für die Betroffenen weitgehend intransparenten System miteinander verkettet würden (LG Lübeck, a.a.O. Rn. 45).

(cc) Die Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, DSK) hat in ihren Beschl. v. 11.6.2018 und 22.9.2021 die Ansicht vertreten, dass die Übermittlung und Verarbeitung von Positivdaten an bzw. durch Handels- und Wirtschaftsauskunfteien grundsätzlich nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO gestützt werden könne, weil regelmäßig das schutzwürdige

Interesse der betroffenen Personen überwiege, selbst über die Verwendung ihrer Daten zu bestimmen. Regelmäßig bedürfe es daher einer wirksamen Einwilligung unter Beachtung der hohen Anforderungen an die Freiwilligkeit ihrer Erteilung. Im Beschl. v. 22.9.2021 hat die DSK ergänzt, dass dies auch für die Übermittlung und Verarbeitung von Positivdaten zu Verträgen über Mobilfunkverträge und Dauerhandelskonten gelte. Dabei gehe es um längerfristige Verträge, die durch Vorausleistungsverpflichtungen oder Finanzierungs- bzw. Stundungselemente als kreditorisches Risiko betrachtet würden, aber keine Vertragstörungen aufwiesen. Die Daten würden bei der Bildung von Scorewerten der betroffenen Personen, die Handel oder Kreditwirtschaft zur Bonitätsprüfung heranzögen, regelmäßig neben einer Vielzahl weiterer Sachverhalte einbezogen. Es bestünden zwar berechnete Interessen der Mobilfunkdiensteanbieter und der Handelsunternehmen, die Qualität der Bonitätsbewertungen zu verbessern und die beteiligten Wirtschaftsakteure vor kreditorischen Risiken zu schützen. Besondere Umstände, die – wie bei Kreditinstituten aufgrund deren spezifischer Verpflichtungen nach dem Kreditwesengesetz – ein die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person überwiegendes Interesse der Verantwortlichen oder Dritter an der Verarbeitung bestimmter Positivdaten vermitteln würde, habe die DSK im Rahmen ihrer Überprüfung jedoch nicht feststellen können. Auch bei Positivdaten zu Verträgen über Mobilfunkdienste und Dauerhandelskonten komme den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person, selbst darüber zu entscheiden, ob sie die sie betreffenden Positivdaten zur Bonitätsbewertung preisgeben wolle, entscheidende Bedeutung zu. Ansonsten würden unterschiedslos große Datenmengen über übliche Alltagsvorgänge im Wirtschaftsleben erhoben und verarbeitet, ohne dass die betroffenen Personen hierzu Anlass gegeben hätten. Deshalb könnten weder Verantwortliche noch Dritte ein überwiegendes Interesse an diesen Verarbeitungen geltend machen.

(dd) Der aufgrund Art. 68 DS-GVO eingerichtete Europäische Datenschutzausschuss (EDSA) hat sich bislang zur Zulässigkeit der Übermittlung und Verarbeitung von Positivdaten an Auskunfteien nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO, soweit ersichtlich, nicht geäußert.

(b) Der Senat schließt sich auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen für den vorliegenden Fall der herrschenden Meinung insoweit an, als bei einer Übermittlung der oben genannten Positivdaten (zum Identitätsabgleich erforderliche Stammdaten der Verbraucher sowie die Information, dass ein Vertragsverhältnis mit diesen begründet oder beendet wurde) an die SCHUFA zum Zwecke der Betrugsprävention die Rechte und Interessen der betroffenen Verbraucher diejenigen der Beklagten nicht überwiegen.

(aa) Die DSK betrachtet bei ihrer grundsätzlichen Bewertung in den (rechtlich nicht bindenden) Beschl. v. 11.6.2018 und 22.9.2021 die Übermittlung und Verarbeitung von Positivdaten im Hinblick auf den Zweck der Bonitätsbewertung, bezieht aber den besonderen Zweck der Betrugsprävention nicht, jedenfalls nicht ausdrücklich ein. Zudem stellt sie im Rahmen der Begründung des Beschl. v. 22.9.2021 wiederholt darauf ab, dass es an einem überwiegenden Interesse der Verantwortlichen oder Dritter an der Verarbeitung von Positivdaten fehle. Gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO fällt die Abwägung aber

nur dann zugunsten der betroffenen Person aus, wenn deren Interessen, Grundrechte oder Grundfreiheiten überwiegen.

(bb) Den Kritikern der Übermittlung von Positivdaten durch Mobilfunkdiensteanbieter ist darin Recht zu geben, dass sie präventiv, pauschal und insofern anlasslos erfolgt, als nicht der Einzelne durch ein Fehlverhalten Anlass zu dieser Maßnahme gegeben haben muss. Anlass besteht allerdings insoweit, als auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen Betrugsstraftaten durch die Täuschung über die Identität und/oder die Zahlungsfähigkeit und -willigkeit von Verbrauchern beim Abschluss von Postpaid-Mobilfunkverträgen mit der Beklagten Wirklichkeit sind und im Hinblick auf deren Vorleistungspflicht in dem Dauerschuldverhältnis, das durch den Mobilfunkvertrag begründet wird, auch und gerade, aber nicht nur bei der Überlassung von Hardware (insbesondere Smartphones), einen hohen finanziellen Schaden anrichten können. Dem durch Art. 16 GRCh (unternehmerische Freiheit) geschützten Interesse der Beklagten, sich vor einem Vertragsabschluss mit Betrügnern zu schützen, kommt vor diesem Hintergrund ein hohes Gewicht zu. Über die Betroffenheit des einzelnen Anbieters hinaus geht es bei der Betrugsprävention um schutzwürdige sozioökonomische Interessen der Telekommunikationsbranche und nicht zuletzt um die wirtschaftlichen Interessen ihrer Kunden, da hohe Betrugsschäden negative Auswirkungen auf die Preisgestaltung haben können. Zudem können Kunden von einem Identitätsdiebstahl durch Dritte betroffen sein und von einer Abfrage bei der SCHUFA daher profitieren.

Der Senat verkennt nicht die grundsätzliche Bedeutung der durch Art. 7 und Art. 8 GRCh garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, die durch die Übermittlung der Positivdaten betroffen sind. Geschieht die Datenübermittlung allerdings zur Prävention von Betrugsstraftaten, wie sie nach den Feststellungen des Berufungsgerichts bei Postpaid-Mobilfunkverträgen der Beklagten ernsthaft zu befürchten sind, so überwiegen die genannten Rechte der betroffenen Person die zuvor genannten Interessen der Verantwortlichen nicht. Der Senat teilt die Ansicht des Berufungsgerichts, dass es sich bei den hier in Rede stehenden Positivdaten – im Ergebnis also bei der Information, dass eine bestimmte Person einen Postpaid-Mobilfunkvertrag abgeschlossen oder beendet hat – nicht um sensible Daten handelt. Damit unterscheiden sie sich wesentlich von Negativdaten (vgl. z.B. EuGH, Urt. v. 7.12.2023 – C-26/22 und C-64/22, EuGRZ 2023, 632 Rn. 94 zur Verarbeitung von Daten über die Erteilung einer Restschuldbefreiung), gegen deren Übermittlung an Auskunfteien sich der Kläger nicht wendet. Bei dem Abschluss eines Mobilfunkvertrages handelt es sich um einen gewöhnlichen Geschäftsvorgang im Leben eines erwachsenen Verbrauchers. Die Information hierüber an einen begrenzten Empfängerkreis lässt keine Rückschlüsse auf persönliche Vorlieben zu und gibt keinen Einblick in das sonstige geschäftliche oder gar das private Verhalten des Verbrauchers; er wird dadurch nicht zum "gläsernen Verbraucher".

(cc) Angesichts des Umstands, dass Mobilfunkdiensteanbieter mit dem Abschluss von Postpaid-Mobilfunkverträgen ein hohes kreditorisches Risiko eingehen, insbesondere (aber nicht nur) dann, wenn sie mit Abschluss des Vertrages

ein Smartphone überlassen, dürfte für einen Verbraucher die Erwartung, dass seine Daten, auch seine Positivdaten, an die SCHUFA übermittelt werden, bei vernünftiger Betrachtung nicht fernliegen. Zudem kann er dies aus den Datenschutzhinweisen der Beklagten erkennen.

(dd) Die im Rahmen der Abwägung zu berücksichtigenden Auswirkungen der Übermittlung der Positivdaten seitens der Beklagten an die SCHUFA zum Zwecke der Betrugsprävention könnten auch davon abhängen, wie und in welchem Umfang die Daten von der SCHUFA zum Zwecke der Betrugsprävention verarbeitet und an ihre Vertragspartner weitergegeben werden (bzw. bis Oktober 2023 wurden).

Feststellungen hierzu hat das Berufungsgericht nicht getroffen. Das war allerdings auch nicht veranlasst. Denn die "näheren Einzelheiten der Verarbeitung der Daten durch die Auskunfteien (Bewertung, Lösungsfristen)" sind, wie das Berufungsgericht tatbestandlich und damit für das Revisionsverfahren bindend festgestellt hat, vom Kläger "nicht angegriffen" worden. Zudem verlangt der Kläger mit der weiten Fassung des Klageantrags zu 1.a die Unterlassung der Übermittlung von Positivdaten unabhängig davon, wie die nicht streitgegenständliche Verarbeitung der Positivdaten bei der SCHUFA gerade im Rahmen der Betrugsprävention erfolgt, beispielsweise, ob sie in diesem Rahmen überhaupt in das Bonitätsscoring einfließt und wenn ja, wie sie dieses beeinflusst. Dass eine Reaktion seitens der SCHUFA erfolgt, wenn Auffälligkeiten vorliegen, die als Indizien für einen Betrug zu werten sind, etwa weil außergewöhnlich viele Verträge binnen kurzer Zeit abgeschlossen worden sind, ist gerade Sinn und Zweck der Übermittlung der Positivdaten zur Betrugsprävention und kann deshalb für sich genommen noch nicht zur Rechtswidrigkeit der Übermittlung von Positivdaten zur Betrugsprävention führen. Auf die rechtlichen Anforderungen an die Zulässigkeit des Bonitätsscoring (Profiling) seitens der SCHUFA im Hinblick auf Art. 22 DS-GVO (vgl. EuGH, Urt. v. 7.12.2023 – C-634/21, EuGRZ 2023, 642 Rn. 40 ff.) kommt es daher hier nicht an.

(ee) Soweit die Revision schließlich aus der "anlasslosen", d.h. von einem konkreten Betrugsverdacht im Einzelfall losgelösten, Übermittlung der Positivdaten die Vermutung herleitet, die Beklagte bezwecke mit den Meldungen auch und in erster Linie das Heraussuchen von "Vertragshoppnern", was sie hinter dem angeblichen Zweck der Betrugsprävention zu verbergen versuche, sind Feststellungen, die diese Annahme stützen würden, nicht getroffen. Die Revision benennt auch keinen diesbezüglichen Vortrag, den das Berufungsgericht gehörswidrig übergangen haben könnte. In der insoweit von ihr in Bezug genommenen Klageschrift hat der Kläger lediglich auf die Ansicht der DSK in ihrem Beschl. v. 15.3.2021 verwiesen, wonach die Einmeldung der Positivdaten von Verbrauchern durch Energieversorger mit dem Ziel, "Schnäppchenjäger" zu identifizieren, nicht gerechtfertigt wäre. Dass die Beklagte mit der Einmeldung von Positivdaten auch oder in erster Linie das Ziel der Identifizierung von "Vertragshoppnern" verfolge, hat er dort nicht behauptet. Im Übrigen ließe sich damit eine Übermittlung der Positivdaten zum Zwecke der Betrugsprävention, die aber vom Unterlassungsantrag erfasst ist, nicht verbieten. [...]

# BERICHT AUS BRÜSSEL

Axel Voss/Moritz Köhler\*

## Der Fahrplan der Kommission für den Digitalen Omnibus

Am 19.11.2025 hat die Europäische Kommission ihre Vorschläge für ein digitales Omnibuspaket veröffentlicht. Damit sollen die KI-Regulierung<sup>1</sup> sowie andere europäische Verordnungen und Richtlinien aus dem Bereich des Datenrechts<sup>2</sup> geändert werden. Ziel ist es, Bürokratie abzubauen und die Gesetze auch im Sinne der Rechtssicherheit besser aufeinander abzustimmen. Der Digitale Omnibus ist bereits das siebte Omnibuspaket, das die Kommission von Ursula von der Leyen während ihrer zweiten Amtszeit auf den Weg gebracht hat. Sechs weitere sollen folgen.<sup>3</sup> Der folgende Überblick gibt eine erste Orientierung zu den vorgeschlagenen Änderungen.

### Umstrukturierung des Datenrechts

Der wohl auffälligste Änderungsvorschlag betrifft die Struktur des Datenrechts. In den vergangenen Jahren hat die DS-GVO den Kern des europäischen Datenschutzrechts gebildet. Um sie herum hat der europäische Gesetzgeber zahlreiche Rechtsakte zum Datennutzungsrecht platziert. Nun sollen zentrale Regeln des Data Governance Acts,<sup>4</sup> der Free Flow of non-personal Data-VO<sup>5</sup> sowie der Open Data-RL<sup>6</sup> in den Data Act<sup>7</sup> aufgenommen werden, um ein „einzelnes, konsolidiertes Instrument für Europas Datenwirtschaft“ zu schaffen.<sup>8</sup>

Im Bereich des Datenschutzrechts will die Europäische Kommission die Schaffung einer eigenen ePrivacy-VO endgültig aufgeben. Bereits am 12.2.2025 hatte sie die Rücknahme des Kommissionsvorschlags angekündigt, am 6.10.2025 wurde die Ankündigung vollzogen. An die Stelle einer eigenen Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation sollen spezielle Regeln über die Verarbeitung personenbezogener Daten in den Endgeräten natürlicher Personen treten. Diese speziellen Regeln sollen nach dem Willen der Europäischen Kommission in die DS-GVO integriert werden. Auffällig daran ist, dass die Einwilligung im Einzelfall nicht mehr der einzig gangbare Weg zur Rechtfertigung der Verarbeitung sein soll. Der Cookie-Banner könnte damit bald Geschichte sein.

### Klarstellungen bei der Definition personenbezogener Daten

Jedenfalls auf den ersten Blick von herausragender Bedeutung ist die vorgeschlagene Änderung der Legaldefinition des Begriffs der personenbezogenen Daten. Der bestehenden Begriffsbestimmung soll folgender Zusatz angefügt werden:

„Informationen über eine natürliche Person sind nicht unbedingt personenbezogene Daten für jede andere Person oder Entität, nur weil eine andere Entität diese natürliche Person identifizieren kann. Informationen gelten für eine bestimmte Entität nicht als personenbezogene Daten, wenn diese Entität die natürliche Person, auf die sich die Informa-

tionen beziehen, nicht identifizieren kann, unter Berücksichtigung der Mittel, die von dieser Entität vernünftigerweise eingesetzt werden können. Solche Informationen werden für diese Entität nicht allein deshalb zu personenbezogenen Daten, weil ein potenzieller späterer Empfänger über Mittel verfügt, die vernünftigerweise eingesetzt werden können, um die natürliche Person, auf die sich die Informationen beziehen, zu identifizieren.“

Letztlich will die Europäische Kommission damit lediglich die Rechtsprechung des EuGH, ganz aktuell aus der Rechtssache SRB,<sup>9</sup> in den Verordnungstext aufnehmen, was aus Gründen der Rechtssicherheit und -klarheit begrüßenswert ist.

### Datenverarbeitungen zur KI-Entwicklung und zum KI-Betrieb

Ein weiterer Gegenstand aktueller Debatten, den die Europäische Kommission im Digitalen Omnibus adressiert, ist die Zulässigkeit von Datenverarbeitungen zum KI-Training. Betroffen ist einerseits die Rechtmäßigkeit der Datenverarbeitungen gem. Art. 6 Abs. 1 KI-VO, andererseits die Zulässigkeit einer Verarbeitung besonderer Kategorien personenbezogener Daten. Obwohl das KI-Training als berechtigtes Interesse jedenfalls in der deutschen rechtswissenschaftlichen Literatur bislang nicht ernsthaft bezweifelt wurde,<sup>10</sup> will die Kommission im Verordnungstext ausdrücklich festhalten, dass

\* 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 Proposal for a Regulation of the European Parliament and of the Council Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final.
- 2 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final.
- 3 Europäische Kommission, Simplification, [https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification\\_en](https://commission.europa.eu/law/law-making-process/better-regulation/simplification-and-implementation/simplification_en) (zuletzt abgerufen am 5.12.2025).
- 4 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30.5.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152 S. 1, 2023 ABl. L 90204 S. 1.
- 5 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14.11.2018 über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, ABl. L 303 S. 59.
- 6 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20.6.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Neufassung), ABl. L 172 S. 56.
- 7 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl. L 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>.
- 8 COM(2025) 836 final, S. 5 (Übersetzung durch die Verfasser).
- 9 EuGH Urt. v. 4.9.2025 – C-413/23 P, RDV 2026, 39.
- 10 Ausführlich Paal, ZfDR 2024, 129 (149-154). Ebenso Franke, RD 2023, 565 (566-568); Hüger, ZfDR 2024, 263 (271-275); Piltz/Weiss, EuDIR 2025, 90 (92 f.); Werry, MMR 2023, 911 (912 f.).

Datenverarbeitungen zur KI-Entwicklung grundsätzlich auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO gestützt werden können.

Von erheblich größerer Bedeutung sind die Änderungsvorschläge zur Verarbeitung besonderer Kategorien personenbezogener Daten. Art. 9 Abs. 1 DS-GVO stellt nach geltendem Recht ein Verarbeitungsverbot auf, das nur in eng umgrenzten Ausnahmefällen, die in Art. 9 Abs. 2 DS-GVO genannt werden, durchbrochen werden darf. Die existierenden Ausnahmetatbestände helfen KI-Entwicklern in zahlreichen Anwendungsfällen indes nicht weiter. Da ein konsequentes Prüfen und Filtern von Datensätzen unter Berücksichtigung sensibler Daten im Sinne von Art. 9 Abs. 1 DS-GVO in der Praxis nicht konsequent umsetzbar ist und auch keine Einwilligung aller betroffenen Personen eingeholt werden kann, bestand die Gefahr, dass das Verarbeitungsverbot für besondere Kategorien personenbezogener Daten zum Sargnagel für datenschutzkonforme KI-Entwicklung in der Europäischen Union wird. Der Europäische Datenschutzausschuss hatte sich in einer Stellungnahme zur Entwicklung von generativen KI-Modellen im Dezember 2024 jedenfalls auffällig um eine Position zu diesem Problem gedrückt, das er erkannte, aber nicht berücksichtigt hat.<sup>11</sup> Das OLG Köln stellte sich der Herausforderung und erklärte das Verbot des Art. 9 Abs. 1 DS-GVO in einer Eilentscheidung im Mai 2025 auf Verarbeitungsvorgänge im Rahmen der KI-Entwicklung erst nach einer „Aktivierung“ durch Betroffene für anwendbar.<sup>12</sup> Diese Auslegung sah sich in der Folge allerdings einiger Kritik ausgesetzt.<sup>13</sup>

Die Europäische Kommission schlägt nun einen neuen Ausnahmetatbestand vor, der die Verarbeitung besonderer Kategorien personenbezogener Daten für die Entwicklung und den Betrieb von KI-Systemen und KI-Modellen zulässt. Einschränkend sollen in einem neuen Art. 9 Abs. 5 DS-GVO technische und organisatorische Maßnahmen verlangt werden, die eine Erhebung und anderweitige Verarbeitung besonderer Kategorien personenbezogener Daten im Grundsatz ausschließen. Sofern der Verantwortliche erkennt, dass trotz dieser Maßnahmen sensible Daten verarbeitet werden, soll er diese entfernen. Sofern das mit einem unverhältnismäßigen Aufwand verbunden ist, soll der Verantwortliche zumindest sicherstellen müssen, dass die Daten nicht im Output des KI-Systems reproduziert oder anderweitig gegenüber Dritten veröffentlicht werden. Es wird eine vertiefte Prüfung und Debatte zur Klärung erforderlich sein, ob diese Maßnahmen ausreichen, um dem grundrechtlich vorgesehenen Schutzniveau für sensible Daten im Sinne von Art. 9 Abs. 1 DS-GVO zu genügen.

### Neue Fristen für Hochrisiko-KI-Systeme

Mit Spannung haben Beobachter außerdem die Reformvorschläge zur KI-VO erwartet.<sup>14</sup> Der Druck war entsprechend hoch, doch jedenfalls den Hoffnungen der Industrie dürfte die Europäische Kommission in weiten Teilen gerecht geworden sein. Dafür war eine Aussetzung der Fristen für den Geltungsbeginn der Vorgaben für Hochrisiko-KI-Systeme zentral. Wie die Kommission in den Erwägungsgründen zum Digitalen Omnibus ausführt, würde es Unternehmen vor erhebliche Herausforderungen und beträchtliche Umsetzungskosten stellen, wenn an den existierenden Geltungsfristen festgehalten wird. Sie begründet diese unvorhergesehenen Auswirkungen zuvorderst mit der verspäteten Bereitstellung

von harmonisierten Normen, gemeinsamen Spezifikationen und alternativer Hilfestellung.<sup>15</sup>

In den vergangenen Wochen war tatsächlich aus der Industrie zu hören, dass eine Umsetzung der Vorgaben für Hochrisiko-KI-Systeme ohne Standards der europäischen Normungsorganisationen CEN und CENELEC unsicher und kostspielig sei.<sup>16</sup> Die KI-VO enthält als allgemeines Produktsicherheitsrecht für KI-Systeme eine ganze Reihe unbestimmter Rechtsbegriffe, die es zu konkretisieren gilt. Um die Unternehmen dabei zu unterstützen, statuiert Art. 40 Abs. 1 KI-VO eine gesetzliche Vermutung, wonach Hochrisiko-KI-Systeme den Anforderungen der KI-VO entsprechen, wenn sie mit entsprechenden harmonisierten Normen übereinstimmen. Der Haken: Bereits im September 2024, einen Monat nach Inkrafttreten der KI-VO und knapp zwei Jahre vor dem ursprünglich geplanten Geltungsbeginn der Vorschriften am 2.8.2026, gaben CEN und CENELEC Verzögerungen bei den Normungstätigkeiten bekannt. Es stellte sich heraus, dass die technisch komplexen und neuartigen Fragen einer KI-Regulierung nicht nur Unternehmen, sondern auch Normungsorganisationen vor Herausforderungen stellen. Die Kommission erließ daraufhin am 23.6.2025 einen neuen Durchführungsbeschluss über einen Normungsauftrag. Demnach sollten die Organisationen harmonisierte Normen bis zum 31.8.2025 ausarbeiten, also knapp einen Monat nach geplantem Geltungsbeginn der entsprechenden Vorschriften.

Mit dem Digitalen Omnibus will die Kommission den Unternehmen und den Normungsorganisationen nun also gleichermaßen etwas Luft verschaffen: Der Vorschlag für eine neue Fassung des Art. 113 KI-VO sieht vor, dass sich der Geltungsbeginn der Vorschriften für Hochrisiko-KI-Systeme an einer Entscheidung der Kommission orientieren soll, der bestätigt, dass angemessene Maßnahmen zur Unterstützung der Einhaltung der Vorgaben verfügbar sind. Erst zum 2.12.2027 sollen die Vorschriften auch ohne Entscheidung der Kommission gelten. Bis zu diesem Zeitpunkt hätte die Kommission eine faktische Entscheidungshoheit über den Geltungsbeginn, zumal die „Entscheidung über angemessene Maßnahmen“ zumindest nicht ausdrücklich an das Vorliegen der harmonisierten Normen gekoppelt ist. Es bleibt abzuwarten, ob das Parlament eine derart wichtige Entscheidung an die Kommission abtritt oder ob im Gesetzgebungsprozess weitere Sicherungsmechanismen aufgenommen werden.

### Fazit

Eines muss sich die Europäische Kommission mit den Vorschlägen zum Digitalen Omnibus nicht vorwerfen lassen: Die vorgeschlagenen Änderungen sind mehr als bloße Kosmetik. Wurde im Laufe des Jahres als wesentliche Änderung

11 Europäischer Datenschutzausschuss, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, [https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects\\_de](https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de), Rn. 17 (zuletzt aberufen am 5.12.2025).

12 OLG Köln, Urt. v. 23.5.2025 – 15 UKI 2/25, RDV 2025, 264 (271 f.).

13 Glocker, RD 2025, 427 (431); Hornung, KIR 2025, 407 (411); Paal, RDV 2025, 230 (234 f.); Wasilewski, CR 2025, 461 (463). In einem obiter dictum hat auch das OLG Schleswig diese Auslegung kritisch beurteilt, OLG Schleswig, Urt. v. 12.8.2025 – 6 UKI 3/25, GRUR-RS 2025, 19976 Rn. 30 f.

14 Dazu bereits Voss/Köhler, RDV 2025, 342.

15 ErwG 22 des Digital Omnibus on AI.

16 Dazu bereits Voss/Köhler, RDV 2025, 342.

der DS-GVO noch eine Einschränkung der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten als große Reform gepriesen,<sup>17</sup> enthalten die Vorschläge nun tiefgreifende materielle Änderungen des europäischen Digitalrechts. Von manchen werden sie angesichts des immer wieder betonten Reformbedarfs entsprechend gelobt.<sup>18</sup> Andere sehen in dem Vorschlagspaket einen Ausverkauf des Grundrechts auf Privatheit.<sup>19</sup> Gerade hinsichtlich der Änderungen der DS-GVO darf deshalb ein intensives Trilog-Verfahren erwartet werden. Vor diesem Hintergrund ist zu begrüßen, dass die Kommission die Änderungsvorschläge, insbesondere hinsichtlich der Geltungsfristen, in ein eigenes Omnibus-Paket ausgelagert hat, über das nun separat beraten werden kann.

Jede Verzögerung bedeutet hier weitere Rechts- und Planungsunsicherheit.

17 Dazu ausführlich Dugall, Müssen wir bald kein Verarbeitungsverzeichnis mehr führen?, <https://www.datenschutz-notizen.de/muessen-wir-bald-kein-verarbeitungsverzeichnis-mehr-fuehren-1854886/> (zuletzt abgerufen am 5.12.2025).

18 Hennemann/Kühling, Entschlackung des EU-Rechts dringend nötig, <https://www.faz.net/pro/digitalwirtschaft/kuenstliche-intelligenz/digital-omnibus-juraprofessoren-fordern-entschlackung-des-eu-rechts-accg-200240064.html> (zuletzt abgerufen am 5.12.2025).

19 Dachwitz, Auf Crash-Kurs mit digitalen Grundrechten, <https://netzpolitik.org/2025/digitaler-omnibus-auf-crash-kurs-mit-digitalen-grundrechten/> (zuletzt abgerufen am 5.12.2025).

# Orientierung im Beschäftigtendatenschutz

## mit dem Standardwerk für Profis

9. komplett überarbeitete Auflage mit Co-Autor Prof. Dr. Thüsing



*Wer mit Beschäftigtendaten zu tun hat, kommt an diesem Handbuch kaum vorbei. Es ist keine leichte Lektüre für den Feierabend, aber ein zuverlässiger Sparringspartner für den Berufsalltag. Wer es nutzt, spart nicht nur Zeit bei der Recherche, sondern auch graue Haare bei schwierigen Auslegungsfragen. Kurz: Gola/Thüsing ist wieder das, was es immer war – ein Klassiker im besten Sinne. Nur eben aktueller, umfangreicher und praxisnäher als je zuvor.“*

**RA Levent Ferik, LL.M.**

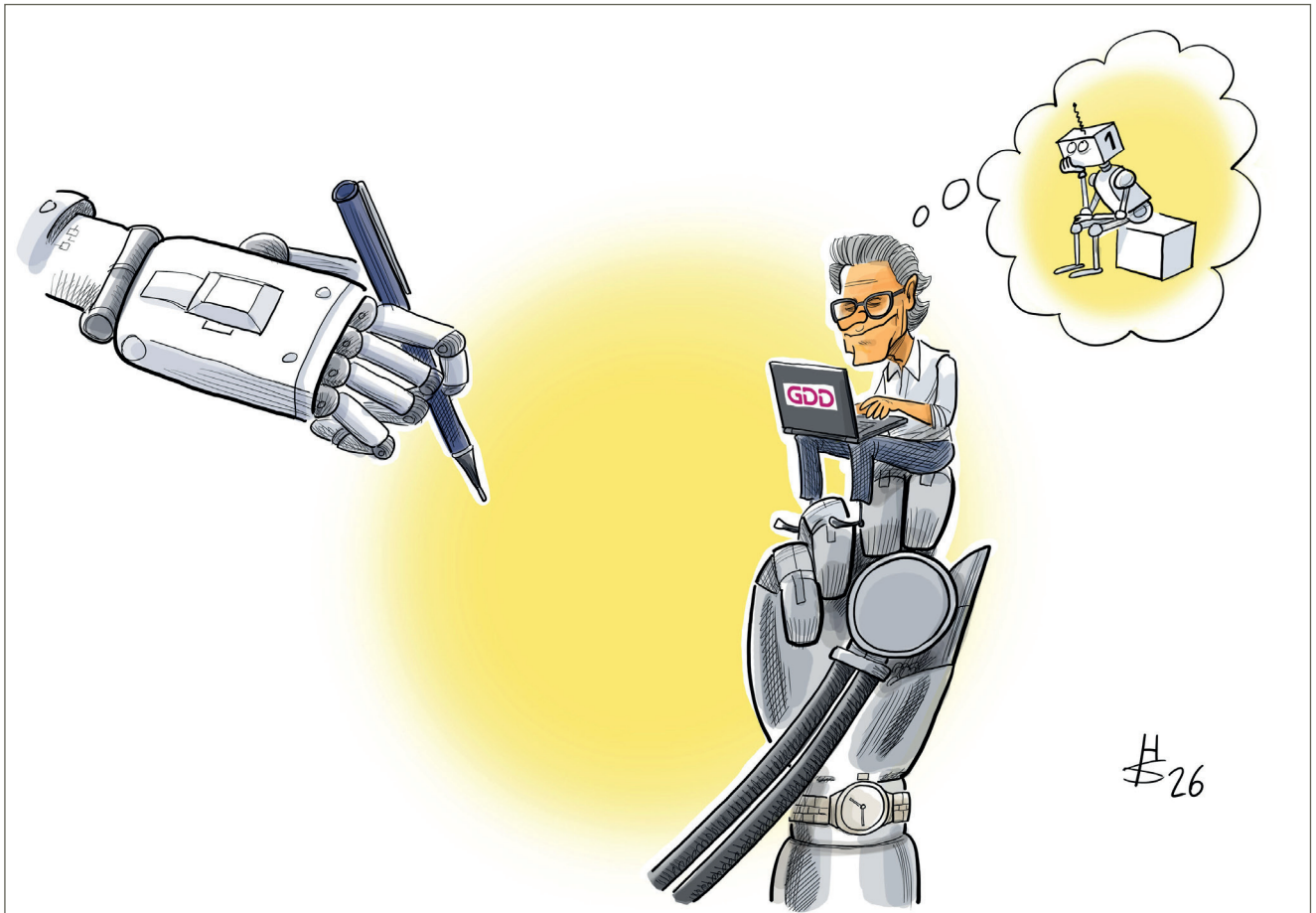
Datenschutzbeauftragter/Syndikusrechtsanwalt,  
HIL GmbH



Jetzt bestellen:

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





## Die „Eins im Sinn“ im Leben mit KI



„KI-Ära“. Diesen Begriff hat die Gesellschaft für deutsche Sprache zum Wort des Jahres 2025 erkoren. Zeithistorisch betrachtet ist das die Instantsuppe unter den Epochen – so schnell und gewissermaßen aus dem Nichts ist sie samt ihren Anführern über unsere Welt hereingebrochen. Das „Time“-Magazin hat die wichtigsten Unternehmer im Bereich der Künstlichen Intelligenz zu den Persönlichkeiten des Jahres 2025 gekürt. Sie hätten das „Ruder der Geschichte“ übernommen. Bots sprechen mit uns wie Menschen. Sie sind aber nur Bedienelemente eines emotionslosen, seelenlosen, geistlosen und zustandslosen Zahlenapparats. Wir haben KI mit unserem Weltwissen gefüttert. Wir stellen ihr Fragen und sie antwortet in Texten und Bildern aus dem Reich der Zahlen. KI tauscht sich mit uns aus, ohne menschliches Bewusstsein zu haben. Mathematische Impulse in Wort und Bild prägen

unsere Gedanken und wir setzen sie um. KI darf uns nicht beherrschen, sondern wir müssen sie kontrollieren. Was ist ein passendes Bild für KI, die hilft und nicht herrscht? Für Albert Einstein soll Mathematik aus Bildern bestanden haben, die er nach Belieben aufrufen, verändern und miteinander kombinieren konnte. Andere Mathematiker nutzen sprachliche Darstellungen von Zahlen. Auch ich habe ein Bild von der KI. Sie ist einerseits ein mächtiges Werkzeug aber andererseits nur ein Hilfsmittel. Aus der Schule habe ich für das Rechnen mit Übertrag eine kleine Formel im Kopf behalten. Sie lautet „Eins im Sinn“. Beim Einsatz von KI geht es um einen Übertrag mathematischer Impulse in das Denken des Menschen. Diese Formel ist ein Sinnbild für KI als ein Hilfsmittel, das den Menschen unterstützt, aber sein Denken nicht ersetzt. KI ist, wenn man so will, die „Eins im Sinn“ im Leben mit KI.