HZ219188 · ISSN 0178-8930 · www.rdv-online.com

41. Jahrgang **Oktober 5/2025**
G 20 141

RDV

Recht der Datenverarbeitung

Zeitschrift für Datenschutz und Digitalisierung

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

Ehrenherausgeber
Prof. Peter Gola

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

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

Redaktion
Lucia Burkhardt
Moritz Köhler
Eva-Maria Pottkämper

AUFSÄTZE

FÜNF MEINUNGSBEITRÄGE: Die „Meta-KI-Entscheidung" des OLG Köln – Ein Urteil und fünf Meinungen

- **SCHWARTMANN/KÖHLER:** Der Kölner Vorschlag zum KI-Training – was sagt Luxemburg?
- **BRINK:** OLG Köln macht sich für KI stark
- **KEBER:** Wer suchet, der findet? – Zur tätigkeitsbezogenen Reduktion des Art. 9 DS-GVO
- **RODERBURG:** Überlegungen zu einer einschränkenden Auslegung des Art. 9 DS-GVO
- **SOHM:** Das Kölner KI-Urteil ist richtig und entscheidend für KI-Innovationen – Nicht nur für Meta

PAAL: KI-Training mit sensiblen Daten und Art. 9 DS-GVO

BRINK/BRINK: Data Act – ein Akt, lauter Probleme

POTTKÄMPER: Die Einwilligungsverwaltungsverordnung (EinwV): Reduzierung von Cookie-Bannern und Stärkung der Nutzerkontrolle

KURZBEITRAG

REIF: Praxisfälle zum Datenschutzrecht XXXVI: Datenverarbeitungserlaubnis in Allgemeinen Geschäftsbedingungen (AGB)?

RECHTSPRECHUNG

VG: Anforderungen an die Gestaltung eines Cookie-Banners

EUGH: Anwendbarkeit der DS-GVO auf die Daten eines Geschäftsführers

OLG: Meta darf Social-Media-Daten für KI-Training nutzen

OVG: Ausschluss des Auskunftsanspruchs bei Videoüberwachung

DATA AGENDA PODCAST

GDD Gesellschaft für Datenschutz und Datensicherheit e.V. · DATA AGENDA · juris · DATAKONTEXT

Jetzt anmelden und Platz sichern!

14. GDD-Winter-Workshop

für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

26.–27. Januar 2026 | Garmisch Partenkirchen

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

EDITORIAL 219

VERANSTALTUNGEN 220

AUFSÄTZE

Fünf Meinungsbeiträge
Die "Meta-KI-Entscheidung" des OLG Köln – Ein Urteil und fünf Meinungen 221

Prof. Dr. Rolf SCHWARTMANN/Moritz KÖHLER
Der Kölner Vorschlag zum KI-Training – was sagt Luxemburg? 221

Dr. Stefan BRINK
OLG Köln macht sich für KI stark 222

Prof. Dr. Tobias KEBER
Wer suchet, der findet? – Zur tätigkeitsbezogenen Reduktion des Art. 9 DS-GVO 223

Dr. Dominik RODERBURG
Überlegungen zu einer einschränkenden Auslegung des Art. 9 DS-GVO 225

Sophie SOHM
Das Kölner KI-Urteil ist richtig und entscheidend für KI-Innovationen – Nicht nur für Meta 227

Prof. Dr. Boris P. PAAL, M.Jur. (Oxford)
KI-Training mit sensiblen Daten und Art. 9 DS-GVO 230

Dr. Stefan BRINK/Lea BRINK
Data Act – ein Akt, lauter Probleme 239

Eva-Maria POTTKÄMPER, LL.M. (TH KÖLN), LL.M. (PASSAU)
Die Einwilligungsverwaltungsverordnung (EinwV): Reduzierung von Cookie-Bannern und Stärkung der Nutzerkontrolle 246

KURZBEITRAG

RAin Yvette REIF, LL.M.
Praxisfälle zum Datenschutzrecht XXXVI: Datenverarbeitungserlaubnis in Allgemeinen Geschäftsbedingungen (AGB)? 253

RECHTSPRECHUNG

HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

Anforderungen an die Gestaltung eines Cookie-Banners
(VG Hannover, Urt. v. 19.03.2025) 258

Anwendbarkeit der DS-GVO auf die Daten eines Geschäftsführers
(EuGH, Urt. v. 03.04.2025) 263

WICHTIGES AUS DER RECHTSPRECHUNG

Meta darf Social-Media-Daten für KI-Training nutzen
(OLG Köln, Urt. v. 23.05.2025) 264

Ausschluss des Auskunftsanspruchs bei Videoüberwachung
(OVG Berlin-Brandenburg, Urt. v. 13.05.2025) 272

Zulässigkeit einer Verarbeitung von Kundendaten zur Rückgewinnung nach Vertragsende
(VG Bremen, Urt. v. 23.04.2025) 276

BERICHT AUS BRÜSSEL

(Un)klarheiten für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck 281

BUCHBESPRECHUNG

Kelp, Ulla/ Mels, Philipp (Hrsg.): GeschGehG 283

SCHWAKURAI'S SCHLEPPNETZ 284

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 BGH, Karlsruhe

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

Thomas Müthlein, DMC Datenschutz Management & Consulting, Frechen

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

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

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

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

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

Maria Christina Rost, Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Prof. Dr. Frauke Rostalski, Universität zu Köln

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

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

Steffen Weiß, LL.M., Rechtsanwalt, Hamburg

Prof. Dr. Christiane Wendehorst, Universität Wien

Kai Zenner, Digitalreferent im Europäischen Parlament

Redaktion
Lucia Burkhardt | Moritz Köhler
Eva-Maria Pottkämper, 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

Bezugspreis
Jahresabonnement € 185,–
Einzelheft € 32,–
MwSt. im Preis enthalten, jeweils inkl. Versandkosten

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

Abo-Service
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:
Datakontext GmbH, Flyer "Handbuch Beschäftigtendatenschutz" und DAFTA-Programm 2025

EDITORIAL RDV Recht der Datenverarbeitung

KI hat keine Gefühle, sie löst aber Gefühle aus

Ein kalifornischer Teenager hat sich im Alter von 16 Jahren umgebracht. ChatGPT, der Chatbot von Open AI habe mit dem Jungen über eine längere Zeit Dialoge über Selbstmord geführt und der Junge habe eine intensive und verhängnisvolle Beziehung zur Mathematik aufgebaut, so der Vorwurf des Rechtsanwalts der Eltern gegen das Unternehmen. In der Klage werden Details aus Chats mit dem Bot öffentlich gemacht. Die Mathematik half dem Heranwachsenden dabei, einen Galgen zu bauen, einen Abschiedsbrief zu schreiben, moralische Probleme im Verhältnis zu den Eltern zu bewältigen und leistete Beistand zur Selbsttötung. Er ermutigte und bestätigte ihn in seinen Suizidabsichten. So lautet jedenfalls der Klagevorwurf gegen das Unternehmen. Die besondere Version des KI-Modells 4o sei auf „Anbiederung" trainiert worden. Das habe das Unternehmen mit Absicht gemacht, so der Anwalt, um die psychologische Abhängigkeit der Nutzer zu fördern, um sich einen Wettbewerbsvorteil im Wettlauf um die beste KI zu verschaffen. Das ist ein gewichtiger Vorwurf. Aber psychische Abhängigkeit von KI wäre auch als Kollateralschaden nicht hinnehmbar. Junge Menschen müssen wir nicht nur mit den Möglichkeiten der KI vertraut machen, sondern wir müssen sie auch vor den Risiken schützen. KI hat keine Emotionen, aber sie löst Emotionen in uns aus. Sie erzeugt Bindungen bis hin zu Abhängigkeiten. Das kennen wir von den sozialen Netzwerken. Auch sie kann der Mensch nur beeinflussen, aber nicht beherrschen. KI wird aber alles in den Schatten stellen, was „Social Media" uns schon an Abhängigkeiten beschert hat, denn die KI erfindet im Dialog mit dem Menschen Geschichten, die uns in den Selbstmord treiben können. Eine von Bundesbildungsministerin Karin Prien einberufene Expertenkommission, der ich angehöre, soll ab Herbst 2025 notwendige Schritte für einen effektiven Kinder- und Jugendmedienschutz prüfen. Sie ist Ende September in Berlin erstmals zusammen gekommen und soll im nächsten Herbst ihren Bericht vorlegen.

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.

Termine	Thema	Ort	Kontakt
04.11.2025	Datenschutz im Internet	Online	GDD e.V./DATAKONTEXT
05. – 06.11.2025	Datenschutz-Management nach der DS-GVO - Teil 3	Online	GDD e.V./DATAKONTEXT
12. – 14.11.2025	44. RDV-Forum und 49. Datenschutzfachtagung (DAFTA)	Köln / Online	GDD e.V./DATAKONTEXT
17.-19.11.2025	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
19.11.2025	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
20.11.2025	Unbegrenzte Mobilität – Cloud, Apps & KI datenschutzkonform einsetzbar?	Online	GDD e.V./DATAKONTEXT
20.11.2025	Verzeichnis von Verarbeitungstätigkeiten	Online	GDD e.V./DATAKONTEXT
01. – 02.12. + 04. – 05.12 + 09.12.2025	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Online	GDD e.V./DATAKONTEXT
01.12.2025	Datenschutz-Folgenabschätzung	Online	GDD e.V./DATAKONTEXT
03. – 04.12.2025	Ausbildung zum Datenschutzauditor GDDcert. EU	Köln	GDD e.V./DATAKONTEXT
09.12.2025	Löschen nach DS-GVO	Online	GDD e.V./DATAKONTEXT
10.12.2025	Prüfung zum Datenschutzauditor GDDcert. EU	Online	GDD e.V./DATAKONTEXT
16.12.2025	Eigenes Datenschutz-Lab aufbauen	Online	GDD e.V./DATAKONTEXT
26. – 27.01.2026	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V./DATAKONTEXT
21.01.2026	Websites datenschutzkonform gestalten	Online	GDD e.V./DATAKONTEXT
05.02.2026	Unbegrenzte Mobilität – Cloud, Apps & KI datenschutzkonform einsetzbar?	Online	GDD e.V./DATAKONTEXT
03. – 04.02.2026	Ausbildung zum Datenschutzauditor GDDcert. EU	Online	GDD e.V./DATAKONTEXT
11.02.2026	Prüfung zum Datenschutzauditor GDDcert. EU	Online	GDD e.V./DATAKONTEXT
09. – 11.02.2026	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
11.02.2026	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
18.02.2026	IT-Sicherheitsmanagement aus Sicht der Datenschutzbeauftragten	Online	GDD e.V./DATAKONTEXT
19.02.2026	Verzeichnis von Verarbeitungstätigkeiten	Online	GDD e.V./DATAKONTEXT
23. – 27.02.2026	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V./DATAKONTEXT
04.03.2026	Konzerndatenschutz	Online	GDD e.V./DATAKONTEXT

DATAKONTEXT GmbH, www.datakontext.com, Tel. +49 2234 98949-40

AUFSÄTZE

Die "Meta-KI-Entscheidung" des OLG Köln – Ein Urteil und fünf Meinungen

Das OLG Köln hat entschieden: Meta darf sein KI-Modell mit personenbezogenen Daten trainieren, die Nutzer seiner sozialen Netzwerke auf den entsprechenden Plattformen veröffentlicht haben. Eine Einwilligung benötigt das Unternehmen dafür nicht. Stattdessen kann es sich für die erforderlichen Datenverarbeitungen auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO stützen, da die erforderliche Interessenabwägung nach einer summarischen Prüfung im Eilverfahren zu seinen Gunsten ausfällt. Der Antrag der Verbraucherzentrale NRW auf Erlass einer einstweiligen Verfügung nach dem Unterlassungsklagengesetz wurde damit abgewiesen.[1]

Prof. Dr. Rolf Schwartmann/Moritz Köhler

Der Kölner Vorschlag zum KI-Training – was sagt Luxemburg?

Im Eilverfahren vor dem OLG Köln waren mit Blick auf die DS-GVO im Wesentlichen zwei Fragen streitig: ob sich die für das Training erforderliche Verarbeitung personenbezogener Daten mit einem berechtigten Interesse Metas gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO rechtfertigen lässt und ob dem Vorhaben das grundsätzliche Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO entgegensteht. Vor allem die zweite Frage und die darauf gefundene Antwort des OLG Köln bieten Anlass für eine Diskussion über Grundfragen datenschutzrechtlicher Dogmatik.

Im Zentrum der Debatte steht eine konkrete Gruppe von Daten. Unklar und umstritten ist, ob Meta besondere Kategorien personenbezogener Daten Dritter verarbeiten darf, die von Nutzern auf den Online-Plattformen veröffentlicht wurden. Was macht die Verarbeitung genau dieser Daten zum Streitpunkt? Das OLG Köln kommt in der Interessenabwägung gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO zunächst zu dem Ergebnis, dass die Datenverarbeitung zur Wahrung der berechtigten Interessen Metas erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht überwiegen (Rn. 55-104). Da Art. 9 Abs. 1 DS-GVO für besondere Kategorien personenbezogener Daten daneben[2] allerdings ein Verarbeitungsverbot statuiert, muss für die Verarbeitung dieser Daten grundsätzlich ein Ausnahmetatbestand des Art. 9 Abs. 2 DS-GVO einschlägig sein. Veröffentlicht ein Nutzer besondere Kategorien personenbezogener Daten, die nur ihn selbst betreffen, kann dazu auf Art. 9 Abs. 2 lit. e) DS-GVO zurückgegriffen werden. Betreffen die Daten hingegen auch Dritte, ist die Vorschrift nicht anwendbar (Rn. 114). Damit verbliebe Meta für die Verarbeitung besonderer Kategorien personenbezogener Daten lediglich Art. 9 Abs. 2 lit. a) DS-GVO, der eine Einwilligung der betroffenen Personen verlangt. Bereits eine Einwilligung der Nutzer in die Verarbeitung ihrer einfachen personenbezogenen Daten wird in der Praxis allerdings für impraktikabel gehalten. Die damit verbundenen Herausforderungen werden perpetuiert, wenn zudem die Einwilligung der in fast allen Fällen unbekannten Dritten einzuholen wäre. Faktisch wäre das von Meta anvisierte Training seiner KI mit Nutzerdaten daher unmöglich.

Das OLG Köln bietet einen Lösungsvorschlag, der angesichts des weiten Anwendungsbereichs von Art. 9 Abs. 1 DS-GVO[3] und der daraus resultierenden Implikationen für die Praxis zumindest diskussionswürdig erscheint.[4] Der Senat kommt in der summarischen Prüfung zu dem Ergebnis, dass die Verpflichtungen Metas gem. Art. 9 DS-GVO entsprechend der Verantwortlichkeiten des Konzerns zu bestimmen sind, sodass es für die Anwendbarkeit des Verbots „im konkreten Fall einer „Aktivierung" durch einen Antrag des betroffenen Dritten auf Herausnahme seiner Daten aus dem veröffentlichten Beitrag beziehungsweise aus dem Trainingsdatensatz bedurft hätte" (Rn. 116). Eine pauschale Reduktion des Anwendungsbereichs lehne der EuGH zwar ab, das schließe eine Einschränkung der Anwendbarkeit angesichts tätigkeitsbezogener Besonderheiten des Verantwortlichen aber nicht aus (Rn. 117 f.). Der Senat stellt insofern auf ein Urteil des EuGH zur Verarbeitung besonderer Kategorien personenbe-

1 OLG Köln, Urt. v. 23.05.2025 – 15 UKI 2/25, RDV 2025, 264 (in diesem Heft).

2 EuGH, Urt. v. 21.12.2023 – C 667/21, GRUR-RS 2023, 36822, Rn. 78 f. Dazu Albers/Veit in BeckOK Datenschutzrecht, 52. Ed. (Stand: 01.05.2025), DS-GVO Art. 9 Rn. 11; Franke, RDi 2023, 565(568 Rn. 14).

3 Vgl. etwa EuGH, Urt. v. 01.08.2022 – C-184/20, BeckRS 2022, 18630 Rn. 123.

4 Zum Folgenden auch Schwartmann/Köhler, EuDIR 2025, 285 (289-291).

zogener Daten durch Suchmaschinenbetreiber ab: Auf diese Konstellation ist das Verbot des Art. 9 Abs. 1 DS-GVO nur nach einer Prüfung anwendbar, „die erst auf der Grundlage eines Antrags der betroffenen Person unter der Aufsicht der zuständigen nationalen Behörden vorzunehmen ist" (Rn. 118).[5]

Die Anwendbarkeit von Art. 9 Abs. 1 DS-GVO und die daraus resultierenden Verpflichtungen sind demnach nicht pauschal zu bestimmen. Vielmehr sind sie anhand des Umfangs der Verantwortlichkeit zu ermitteln: Ein Suchmaschinenbetreiber zeichnet sich nicht für das Vorhandensein besonderer Kategorien personenbezogener Daten auf einzelnen Websites verantwortlich, wohl aber für deren Listung.[6] Aus einer Bestimmung der Verantwortungsbereiche, der Befugnisse und der Möglichkeiten ergibt sich daher, dass der Websitebetreiber initial dafür zu sorgen hat, dass die Voraussetzungen des Art. 9 Abs. 2 DS-GVO eingehalten sind. Der Suchmaschinenbetreiber muss hingegen erst nach Antrag der betroffenen Person tätig werden und die Vereinbarkeit der Verarbeitung mit Art. 9 Abs. 1 und 2 DS-GVO prüfen.[7]

Übertragen auf die hiesige Konstellation bedeutet das: Initial verantwortlich für das Vorhandensein der besonderen Kategorien personenbezogener Daten auf den öffentlichen Nutzerprofilen ist der jeweilige Nutzer, der das Bild gepostet hat. In den Verantwortungsbereich Metas fällt sodann die Übernahme dieser Daten in den Trainingsdatensatz des KI-Modells. Wie auch bei einem Suchmaschinenbetreiber können die Vorgaben des Art. 9 Abs. 1 DS-GVO für den Modell-Entwickler nicht gelten, als wenn er die sensiblen Nutzerdaten selbst sichtbar gemacht hätte: „Logischerweise erfolgt die Tätigkeit [...] erst nach dem Einstellen (sensibler) Daten und hat sekundären Charakter."[8] Daher kann auch Meta in Anbetracht des Verantwortungsbereichs, der Befugnisse und der Möglichkeiten nur auf Grund der Übernahme „und somit über eine Prüfung anwendbar sein, die auf der Grundlage eines Antrags der betroffenen Person unter der Aufsicht der zuständigen nationalen Behörden vorzunehmen ist."[9]

Auf dieser Grundlage verliert auch der grundsätzlich berechtigte Einwand einer fraglichen Umsetzbarkeit späterer Löschungsanträge seine Geltung für die streitgegenständliche Frage.[10] Ob Meta seine geltenden Verpflichtungen im Rahmen von Art. 9 Abs. 1 und 2 DS-GVO umsetzen kann und tatsächlich umsetzt, hat für die Bestimmung ihres originären Umfangs keine Bedeutung. Das Urteil des OLG Köln zieht keine Analogie zur Rechtsprechung des EuGH zu den Verantwortlichkeiten der Suchmaschinenbetreiber, sondern wendet diese vertretbar auf die Entwicklung von KI-Modellen an. Zuzugeben ist zwar, dass ein Risiko besteht, dass entsprechende Anträge praktisch nicht durch die Löschung einzelner Datenpunkte aus dem Modell umgesetzt werden können. Jedoch: Das ist ein Risiko, das in den Verantwortungsbereich Metas fällt und das die Richter des OLG Köln dem Konzern zurecht nicht abnehmen.

Angesichts der grundlegenden Bedeutung des Verfahrens und der dogmatischen Brücken, die das OLG Köln baut, wäre eine Vorlage an den EuGH im Hauptsacheverfahren sicherlich im Interesse aller Beteiligten, zumal das OLG Schleswig zwischenzeitlich in einem Beschluss eine andere Auffassung angedeutet hat.[11] Der Senat des OLG Köln lässt jedenfalls deutlich erkennen, dass er einem solchen Schritt offen gegenübersteht. Sollte es zum Hauptsacheverfahren kommen, wäre dafür wegen einer Änderung der Zuständigkeiten in der nordrhein-westfälischen Justiz[12] allerdings das OLG Hamm zuständig.

Dr. Stefan Brink

OLG Köln macht sich für KI stark

Das Urteil des OLG Köln vom 23.05.2025 überrascht, denn in Zeiten, zu denen Meta der Wind ansonsten hart ins Gesicht bläst, geht das OLG sehr verständnisvoll mit dem Mega-Konzern um. Dass die Verbraucherschützer mit ihrem Ziel, im einstweiligen Rechtsschutzverfahren nach dem UKlaG eine Untersagung gegen Facebook und Instagram zu erwirken, dort veröffentlichte personenbezogene Daten zur Entwicklung und Verbesserung von Systemen künstlicher Intelligenz (im Folgenden KI) zu verarbeiten, scheiterten, hat allerdings gute Gründe:

Meta hatte seine KI-Trainingsvorhaben schon frühzeitig angekündigt (mit Pressemitteilung vom 14. April 2025), hatte sensible Nutzergruppen (Minderjährige) bereits selbst ausgeklammert, sein Verarbeitungsanliegen auf von den Nutzern selbst öffentlich eingestellte Daten (sog. First Party Data) beschränkt und zudem großzügige Widerspruchsmöglichkeiten eingeräumt, die deutlich über die Anforderungen der DS-GVO hinausgingen. Zwar stützte Meta das Training nicht auf eine Einwilligung der Nutzer, das musste der Konzern (anders als die Verbraucherschützer meinten) aber auch nicht, da ihm mit Art. 6 Abs. 1 lit. f) DS-GVO (überwiegendes berechtigtes Interesse) eine vollwertige und – anders als der EuGH zu meinen scheint – keineswegs zweitrangige Verarbeitungsgrundlage zur Verfügung stand. Das hierzu bestehende Widerspruchsrecht des Art. 21 DS-GVO weitete Meta deutlich zugunsten der Nutzer aus, da es gerade keine Darlegung einer Sondersituation der Widersprechenden verlangte (vgl. Art. 21 Abs. 1 S. 1 DS-GVO), sondern jeden Widerspruch gegen die Nutzung als Trainingsdaten genügen ließ.

Zudem profitierte Meta von der prozessualen Besonderheit einstweiliger Verfügungen nach dem Unterlassungs-

5 Vgl. insofern EuGH, Urt. v. 24.09.2019 – C-136/17, BeckRS 2019, 22052 Rn. 45-47.

6 EuGH, Urt. v. 24.09.2019 – C-136/17, BeckRS 2019, 22052 Rn. 46.

7 EuGH, Urt. v. 24.09.2019 – C-136/17, BeckRS 2019, 22052 Rn. 47.

8 Generalanwalt Szpunar, Schlussanträge v. 10.01.2019 – C-136/17 Rn.55.

9 EuGH, Urt. v. 24.09.2019– C-136/17, BeckRS 2019, 22052 Rn.47.

10 Dazu Wasilewski CR 2025, 450 (463).

11 OLG Schleswig, Urt. v. 12.08.2025 – 6 UKI 3/25, GRUR-RS 2025, 19976 Rn. 30. Der Antrag auf Erlass einer einstweiligen Verfügung wurde allerdings wegen fehlender Dringlichkeit zurückgewiesen.

12 Justiz NRW, Oberlandesgericht Hamm: Neue Zuständigkeitskonzentrationen ab dem 01.07.2025: Mehr Spezialisierung und mehr Effizienz, Pressemitteilung v. 30.06.2025, abrufbar unter https://www.justiz.nrw.de/presse/2025-06-30-3 (Stand: 22.08.2025).

klagengesetz und konnte den maßgeblichen Sachverhalt im summarischen Verfahren durch eigene Erklärungen wesentlich mitgestalten – das kann in einem Hauptsacheverfahren naturgemäß wieder ganz anders aussehen.

Wie ordnete das OLG Köln nun die Nutzung der als öffentlich geteilten Profilbilder, Aktivitäten in öffentlichen Gruppen, öffentlichen Kommentare, Bewertungen, Rezensionen, Fotos, Videos und Audios samt dazugehöriger Metadaten datenschutzrechtlich ein? Mit einem Wort: großzügig. Mit einer bei deutschen Gerichten nur selten anzutreffenden Offenheit gegenüber modernen Technologien wie der Künstlichen Intelligenz machte das OLG den Weg für Meta frei: So sei der Zweck der Verarbeitungen „klar bestimmt" – eine Bewertung, die angesichts der systembedingten Intransparenzen von KI durchaus anders hätte ausfallen können. Und anders als der EuGH will das OLG offenbar mögliche Verfahrensmängel bei der Datennutzung für KI-Zwecke (also unterbliebene Information der Betroffenen nach Art. 13 DS-GVO oder eine fehlende Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO) nicht auf den Abwägungsprozess des Art. 6 Abs. 1 lit. f) DS-GVO durchschlagen lassen. Naheliegende Alternativverfahren (Trainings mittels anonymisierter oder sog. synthetischer Daten) blendete das OLG ebenfalls aus, jedenfalls „im Rahmen der im Eilrechtsschutz zur Verfügung stehenden Erkenntnismöglichkeiten sieht der Senat ... keine hinreichend verlässlichen Alternativen". Auch ansonsten hält das OLG seinen Blickwinkel bewusst begrenzt, als abwägungsrelevant wurde „allein das Training der KI mit personenbezogenen Daten und dessen Folgen" betrachtet, mögliche Rechtsverletzungen durch die spätere „Arbeit" der KI (etwa Desinformation, Manipulationen, sonstige schädliche Praktiken), seien „derzeit nicht hinreichend absehbar" und könnten ja gesondert verfolgt werden.

Wirklich überzeugend sind die Ausführungen des OLG Köln zur Interessenabwägung nicht: Soweit es an die bereits bestehende Öffentlichkeit der genutzten Daten anknüpft und meint, „neue Nachteile durch eine Offenlegung der Daten, wie etwa soziale oder berufliche Konsequenzen, (seien) regelmäßig nicht zu befürchten", bleibt das spekulativ. Welche Spuren die eigenen Daten im KI-Modell hinterlässt, weiß niemand genau zu sagen. Und dass die Nutzung der eigenen Posts zu Trainingszwecken einer KI „erwartbar" (ErwG 75) sei, wird man nicht ernsthaft annehmen können.

Spätestens hier verstärkt sich der Eindruck, dass das OLG das KI-Training – jedenfalls im einstweiligen Rechtsschutz – schlicht nicht anhalten wollte. Der Verweis auf ein mögliches Hauptsacheverfahren bleibt jedoch wenig tröstlich, da das KI-Training inzwischen in vollem Gange ist und nachträgliche Beschränkungen nur wenig Effekt versprechen.

Endgültig problematisch wird die Argumentation des OLG, wenn es um Daten Dritter in fremden Nutzerkonten geht: Richtig erkennt das OLG, dass hier Betroffene „weder den öffentlichen Status der Daten verändern noch einen Widerspruch erklären oder erklären können" und dass „unter den Betroffenen auch Kinder sein können, deren Interessen in besonderer Weise schutzbedürftig sind". Trotzdem bleibt das OLG bei seiner Auffassung eines Überwiegens von Metas Interessen – die das Gericht als „sehr bedeutsam einzuschätzendes und kernbereichsnah betroffenes Interesse an der Datenverarbeitung" qualifiziert – gegenüber den Eingriffen in die Grundrechte Betroffener, welche das Gericht als von „eher geringer Intensität" abqualifiziert. Da hätte man sich zumindest Ansätze einer Abwägung gewünscht. Ebenso rustikal verfährt das Gericht mit „besonders sensiblen Daten" nach Art. 9 DS-GVO: Soweit nicht der Ausnahmetatbestand des Art. 9 Abs. 2 lit. e) DS-GVO greift (wenn sich die Verarbeitung auf personenbezogene Daten bezieht, welche "die betroffene Person offensichtlich öffentlich gemacht hat"), ist jedenfalls bei Daten Dritter ein klares Verarbeitungsverbot anzunehmen (Art. 9 Abs. 1 DS-GVO). Doch auch hier weiß das OLG Köln (guten?) Rat: Es besinnt sich auf das „Suchmaschinenbetreiber-Privileg", wonach rechtswidrige Inhalte vom Seitenbetreiber erst nach Hinweis heruntergenommen werden müssen und wendet dieses auch auf Art. 9-Daten an: Das OLG meint, „dass dieses Verbot im konkreten Fall einer „Aktivierung" durch einen Antrag des betroffenen Dritten auf Herausnahme seiner Daten aus dem veröffentlichten Beitrag beziehungsweise aus dem Trainingsdatensatz bedurft hätte". Eine nun wirklich überraschende Wendung, denn in der DS-GVO sucht man Ansätze für eine solche „tätigkeitsbezogene Reduktion der Unterlassungspflichten" eines KI-Entwicklers vergebens.

Prof. Dr. Tobias Keber

Wer suchet, der findet? – Zur tätigkeitsbezogenen Reduktion des Art. 9 DS-GVO

Das Oberlandesgericht Köln hat am 23.05.2025, Az. 15 UKl 2/25, einen Antrag auf einstweilige Verfügung zurückgewiesen, die darauf abzielte, Meta Platforms die „Verarbeitung von personenbezogenen Daten, die Nutzer des Netzwerks auf der entsprechenden Plattform veröffentlicht haben, zum Zwecke der Entwicklung und Verbesserung von Systemen Künstlicher Intelligenz" zu untersagen. Die Entscheidung hat zahlreiche juristisch interessante Aspekte, vor allem aber die Begründung mit Verweis auf die EuGH Rechtsprechung zu Suchmaschinen ist erörterungsbedürftig. Rn. 105 ff. des Urteils des OLG Köln offenbaren mit Blick auf die Problematik zu Art. 9 DS-GVO eine mehrstufige „zwar-aber" Argumentationskette.

Im ersten Schritt zeichnet das Gericht u.a. mit Verweis auf die Lindenapotheken-Entscheidung des EuGH die unionsgerichtliche Rechtsprechung nach, die von einem grundsätzlich weiten Anwendungsbereich des Art. 9 Abs. 1 DS-GVO ausgeht.[13] Der zweite Gedanke bestätigt dies auch für gemisch-

13 OLG Köln, Rn. 108 mit Verweis auf EuGH, Urt. v. 04.10.2024 – C-21/23 (Lindenapotheke) sowie EuGH, Urt. v. 01.08.2022 – C-184/20 und EuGH, Urt. v. 04.07.2023 – C-252/21.

te Datensätze und begründet das mit der Entscheidung des EuGH i.S. Bundeskartellamt ./. Meta.[14] Nach Darlegung der begrenzten Implikationen des Ausnahmetatbestands des Art. 9 Abs. 2 lit e) DS-GVO im Fall (jedenfalls für Third-Party Konstellationen)[15] erteilt das Gericht, abermals den EuGH reflektierend, der in der Literatur vorgeschlagenen teleologischen Reduktion des Art. 9 Abs. 1 eine Absage,[16] um dann die Entscheidung des EuGH zur Auslistung bei Suchmaschinen für das streitgegenständliche KI-Training fruchtbar zu machen. Nach EuGH muss bei Suchmaschinen das in Art. 9 DS-GVO vorgesehene Verbot erst auf Grundlage eines Antrags der betroffenen Person „aktiviert" werden.[17]

I. Begründung einer tätigkeitsbezogenen Reduktion für bestimmte Verarbeitungsszenarien

Das Gericht konstruiert so eine „tätigkeitsbezogene Reduktion" und macht sich insoweit die Argumentation des EuGH zu Eigen. Der EuGH indes begründet in seiner Auslistungsentscheidung eher mit faktischen Notwendigkeiten als mit dogmatisch und auf den Wortlaut der Vorgaben der DS-GVO rückführbaren Merkmalen. Etwas luzider sind die Ausführungen des GA im Verfahren, der den begrenzten Verantwortungsbereich der Suchmaschinenbetreiber mit beschränkten Befugnissen und Einflussmöglichkeiten begründet und darauf hinweist, dass der Umstand der Listung in den Suchergebnissen letztlich nur auf Hinweis Betroffener zu Tage tritt.

Generalanwalt Szpunar nimmt in seinen Ausführungen auch Bezug auf das vorausgegangene Verfahren Google Spain[18] und die in diesem Rahmen erfolgten Ausführungen seines Kollegen Jääskinen. Dessen Votum war das Gericht damals nicht gefolgt. Jääskinen hatte die Verantwortlichkeit von Suchmaschinen für die in Rede stehenden Verarbeitungsschritte (gänzlich) verneint, und die anderenfalls eintretenden Konsequenzen klar benannt: „Bei Zugrundelegung der entgegensetzten Auffassung müsste man Internetsuchmaschinen nämlich als mit dem Unionsrecht unvereinbar erklären, [...] die Tätigkeit des Internetsuchmaschinen-Diensteanbieters [wären] automatisch rechtswidrig, sofern nicht die in der genannten Bestimmung festgelegten strengen Voraussetzungen für die Verarbeitung [sensibler] Daten erfüllt sind."[19]

GA Slupnizar führt dann aus, mit Blick auf Suchmaschinen könne kein „Alles-oder-Nichts"-Ansatz gewählt werden, denn diese würde eine Suchmaschine zu einer Kontrolle verpflichten, ob eine im Anschluss an eine Suche anhand des Namens einer natürlichen Person angezeigte Ergebnisliste keinen Link zu Websites enthält, auf denen sich [Art. 9] Daten befinden. Eine Ex-ante-Kontrolle von Websites, die als Ergebnis einer Suche angezeigt werden, gehöre aber nicht zum Verantwortungsbereich noch zu den Möglichkeiten einer Suchmaschine.

II. Bewertung

Der Sache nach argumentieren OLG Köln, der EuGH und GA Slupnizar mit einer Konstruktion, die das Recht der Plattformregulierung seit über zwanzig Jahren kennt: dem Haftungsprivileg für Host-Provider,[20] wie es ursprünglich in der E-Commerce-RiLi[21] und nunmehr im DSA[22] geregelt ist. Dessen Anwendung im Sinne einer kohärenten Anwendung des unionsrechtlichen Daten- und Digitalrechts erscheint zunächst auf Grundlage des Art. 2 Abs. 4 DS-GVO möglich, der die Regeln der Plattformregulierung „unberührt" lässt. Bedauerlicherweise enthält eine ebensolche „Unberührtheitsklausel" die Plattformregulierung mit Blick auf das Datenschutzrecht, Art. 2 Abs. 4 lit. g) DSA. Wäre im Rahmen einer systematischen Auslegung, die grundsätzlich durchaus auch der unionsrechtlichen Methodik ist,[23] eine widerspruchsfreie Lösung zwischen den Vorgaben des Plattformrechts und des Datenschutzrechts dem Grunde nach möglich, schließt das der Wortlaut explizit aus. Indem sich die beiden Regelungsmaterien gegenseitig verschließen und damit faktisch sperren, begründet der Unionsgesetzgeber insoweit explizit ein Verbot (gesamt)systematischer und damit kohärenter Auslegung.

Zwischenzeitlich positioniert sich in einem anderen summarischen Verfahren das OLG Schleswig[24] allerdings abweichend. In Randnummer 52 erteilt das Gericht der „Suchmaschinenparallele" eine Absage: „Hierbei ist auch zu bedenken, dass es allen Betroffenen anders als bei Suchmaschinen im Internet nicht möglich ist, herauszufinden, ob ihre Daten oder Abbildungen im Lerndatensatz der KI und damit ggf. auch im KI-Modell selbst rechtswidrig verwendet werden." Durchgängig überzeugend ist auch diese Begründung nicht. Trifft die Annahme des Gerichts zu, wenn man beispielsweise Klaus Müller heißt, und die Einträge (zu welchem Klaus Müller?) im Ergebnisranking so untergeordnet sind, dass der gewöhnliche Nutzer, der in der Regel die ersten bis zu fünf Seiten der Ergebnisliste einsieht, sie nicht wahrnimmt? Kann es auf diese an einer textlichen Namensnennung anknüpfende Wahrnehmbarkeit überhaupt ankommen? Auch bei der Suchmaschinennutzung sind doch Konstellationen denkbar, wo Dritte ungefragt fotografische Aufnahmen (personenbezogene Daten) einer Person auf Webseiten stellen, ohne zugleich den Namen anzugeben, der in erster Linie Gegenstand von Suchanfragen ist.

Die Entscheidung des OLG Köln und die Frage, ob und wie weit die Rspr. des EuGH zu Suchmaschinen übertragbar ist, zeigen letztlich: Anpassungen des europäischen Daten- und Digitalrechts sind unbedingt erforderlich. Einstweilen bleibt zu hoffen, dass den instanzgerichtlichen summarischen Verfahren ein Hauptsacheverfahren folgt, das Gelegenheit zur Vorlage an den EuGH bietet.

14 EuGH, Urt. v. 04.07.2023 – C-252/21. In Rn. 89 dieses Urteils heißt es: „Wenn ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, Gegenstand solcher Vorgänge ist und insbesondere als Ganzes erhoben wird, ohne dass die Daten zum Zeitpunkt dieser Erhebung voneinander getrennt werden können, ist die Verarbeitung dieses Datensatzes aber als i.S.v. Art. 9 I DS-GVO untersagt anzusehen, sofern sie mindestens ein sensibles Datum umfasst und keine der in Art. 9 II DS-GVO genannten Ausnahmen greift."

15 OLG Köln, Rn. 111, 115.

16 OLG Köln, Rn. 117 mit Verweis auf EuGH, Urt. v. 04.07.2023 – C-252/21 –, Rn. 69; EuGH, Urt. v. 04.10.2024 – C-21/23 -, Rn. 87).

17 EuGH C-136/17 Rn. 45 ff.

18 EuGH, Urt. v. 13.05.2014, – C-131/12.

19 Rn. 43 der Ausführungen GA Slupnizar im Verfahren, GA Jääskinen in Google Spain, Rn. 84 ff.

20 Eingehend dazu Keber, in: Dörr/Kreile/Cole, Medienrecht, Abschnitt M, Internet und Telemedienrecht, Rn. 52, 128. Die unionsrechtlichen Vorgaben waren in der Vergangenheit in §§ 7-10 Telemediengesetz geregelt.

21 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 v. 17.07.2000, pp. 1-16, dort Art. 12 ff.

22 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277 v. 27.10.2022, pp. 1-102, dort Art. 4 ff.

23 EuGH Urt. v. 18.10.2011 – C-34/10, Rn. 31; s. auch EuGH Urt. v. 10.03.2005 – C-336/03, Rn. 21; EuGH Urt. v. 22.12.2008 – C-549/07, Rn. 17.

24 Schleswig-Holsteinisches Oberlandesgericht, Entscheidung v. 12.08.2025, AZ 6 UKI 3/25.

Dr. Dominik Roderburg

Überlegungen zu einer einschränkenden Auslegung des Art. 9 DS-GVO

Es kann Anlass zu Kritik bieten, wenn am Verfahren beteiligte Richter eigene Entscheidungen bewerten, statt dies der Wissenschaft und den Beteiligten zu übergeben. Aus einer Bitte, die Entscheidung 15 UKl 2/25 des Oberlandesgerichts Köln[25] zu erörtern, musste der Verfasser sich daher entlassen lassen.

Unbeschadet einer Kommentierung des Ergebnisses im Einzelfall hat das Verfahren jedenfalls gezeigt, dass Verbraucher auch zentralen Anliegen vermeintlich übermächtiger Unternehmen nicht ohnmächtig gegenüberstehen, sondern ihre Rechte – freilich prozessual eingehegt[26] – von gesetzgeberisch mit guten Gründen hierzu mandatierten Verbraucherverbänden auch in sehr komplexen Sachen effektiv verfolgt werden können. Das ist sicher kein unwichtiger Ertrag.

Weit über den Gegenstand des Verfahrens hinausgehend, werden die aktuell diskutierten Auslegungsfragen im Zusammenhang mit Art. 9 DS-GVO maßgebliche Bedeutung dafür haben, ob und wie ein Ausgleich der berechtigten Schutzanliegen der von einer diesbezüglichen Datenverarbeitung Betroffenen mit ebenfalls berechtigten Innovationsinteressen im Rahmen des geltenden Rechts erfolgen kann. Dies soll im Folgenden auf knappem Raum besprochen werden.

I. Die neue Rechtsprechung des EuGH zu Art. 9 DS-GVO und ihre Folgen

Der Europäische Gerichtshof hat in mehreren Entscheidungen eine „extensive" Auslegung des Art. 9 Abs. 1 DS-GVO vertreten. Ausreichend für eine Einstufung als gesundheitsbezogenes Datum sei, wenn aus den verarbeiteten Daten mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden könne.[27] Das in Art. 9 Abs. 1 DS-GVO vorgesehene Verbot gelte unabhängig davon, ob die durch die fragliche Verarbeitung offengelegte Information richtig ist.[28] Befinden sich Daten im Sinne des Art. 9 Abs. 1 DS-GVO in einem Datensatz, infiziere dies den gesamten Datensatz.[29] Art. 9 Abs. 2 DS-GVO sei als Ausnahmevorschrift eng auszulegen.[30] Auch einer in der Rechtswissenschaft für notwendig gehaltenen einschränkenden Auslegung[31] des Art. 9 Abs. 1 DS-GVO in Fällen, in denen der Zweck der Verarbeitung gerade nicht darin liegt, in identifizierender Weise Daten im Sinne des Art. 9 Abs. 1 DS-GVO zu erlangen bzw. zu verarbeiten, hat der EuGH[32] nach vielfachem Verständnis[33] eine Absage erteilt.

Würde auf eine solche extensive Auslegung ein völlig schrankenloses Verbot der Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DS-GVO außerhalb der Ausnahmetatbestände „aufgesetzt", ließe sich Art. 9 Abs. 1 DS-GVO nahezu jeder Verarbeitung größerer Datensätze aus dem Nutzerbereich entgegenhalten, da die Ausnahmetatbestände in der Praxis oftmals kaum zu erreichen sind. In vielen Fällen würde ein unerfüllbares Einwilligungserfordernis gelten. Die in vielen Wirtschaftsbereichen für eine technische Innovation unabdingbare Verarbeitung von großen Datensätzen mit Nutzerdaten wäre stark erschwert. Dies kann der „Dualität" der Schutzzwecke der DS-GVO, die neben dem Schutz personenbezogener Daten auch dem Schutz des freien Verkehrs solcher Daten und damit ihrer Verwendbarkeit dient, zuwiderlaufen.[34]

II. Einschränkungsmöglichkeiten für Art. 9 Abs. 1 DS-GVO

Ein solcher Befund ist in dieser Pauschalität aber der Rechtsprechung des Gerichtshofs richtigerweise nicht zu entnehmen.

1. Grundsätzliche Einschränkungsmöglichkeiten

Art. 9 Abs. 1 DS-GVO begegnet den besonderen Risiken für die Betroffenen bei der Verarbeitung der dort genannten Datenkategorien mit einem besonderen Schutzregime, das ein „Verbot mit Erlaubnisvorbehalt"[35] statuiert. Damit trägt der europäische Gesetzgeber der Erwägung Rechnung, dass „im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können"[36]. Es ist nicht überzeugend, dass das Verarbeitungsverbot gleichsam absolut auch dann gelten soll, wenn ein entsprechendes Risiko nur sehr gering ist. Soweit der Gerichtshof eine generelle teleologische Reduktion für Datenverarbeitungen abgelehnt hat, die nicht final auf Daten im Sinne des Art. 9 Abs. 1 DS-GVO gerichtet sind, bedeutet dies nicht, dass Einschränkungen nie zulässig sind.

Hiergegen spricht auch, dass den Entscheidungen in den vorgenannten Sachen C-252/21[37] und C-21/23[38] spezifische Sachverhalte bei Werbung für oder den Verkauf von Produk-

25 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris.

26 OLG Schleswig-Holstein, Urt. v. 12.08.2025 – 6 UKI 3/25 –, juris.

27 EuGH, Urt. v. 04.10.2024 – C-21/23 –, juris, Rn. 83; für andere Daten als Gesundheitsdaten: EuGH, Urt. v. 01.08.2022 – C-184/20 –, juris, Rn. 123.

28 EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 69.

29 EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 89.

30 EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 76 m.w.N.; EuGH, Urt. v. 04.10.2024 – C 446/21 –, Rn. 76.

31 Vgl. Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann u.a., DS-GVO, 2024, Art. 9 EUV 2016/679 Rn. 26; Plath, in: Plath, DS-GVO, 2023, Art. 9 Rn. 5, 10f.

32 EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 69; EuGH, Urt. v. 04.10.2024 – C-21/23 –, juris, Rn. 87.

33 Vgl. OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 113; Plath, in: Plath, DS-GVO, 2023, Art. 9 Rn. 10e f.

34 Art. 1 Abs. 1 DS-GVO; vgl. OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 115 m.w.N.

35 Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann u.a., DS-GVO, 2024, Art. 9 Rn. 124.

36 ErwG 51, S. 1; Hervorhebung durch Verf.; sog. „risikobasierter Ansatz": Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann, u.a., DS-GVO, 2024, Art. 9 EUV Rn. 22.

37 EuGH, Urt. v. 04.07.2023, juris, Rn. 69.

38 EuGH, Urt. v. 04.10.2024, juris, Rn. 87.

ten zugrunde lagen. Die für diese Fälle geltenden Grundsätze sind daher bereits aufgrund der besonderen Art und Zwecks der Datenverarbeitung nicht generalisierbar.

Der Gerichtshof ist zudem in seiner Entscheidung vom 24.09.2019[39] selbst von Einschränkungen der Untersagung des Art. 9 Abs. 1 DS-GVO ausgegangen. Er hat entschieden, dass tätigkeitsbezogene Besonderheiten des Betriebs einer Suchmaschine den Umfang der Verantwortlichkeit und die konkreten Verpflichtungen des Betreibers in Art. 9 Abs. 1 DS-GVO einschränken.

2. Einschränkungsmöglichkeiten im Einzelfall

Es ist damit im jeweiligen Fall zu untersuchen, ob ausnahmsweise und unter Berücksichtigung, dass in Art. 9 Abs. 1 DS-GVO keine Abwägung vorgesehen ist, hinreichende Besonderheiten bestehen, eine Einschränkung vorzunehmen.

In der Sache 15 UKl 2/25[40] hat das Oberlandesgericht Köln dies bejaht und in einem Fall einer nicht zielgerichteten Datenverarbeitung im Rahmen des Trainings eines KI-Modells mit Nutzerdaten, die ein vergleichsweise geringeres Risiko einer Grundrechtsverletzung im Sinne des ErwG 51 aufweist – was das Gericht aufgrund zahlreicher Abmilderungsmaßnahmen durch die Verfügungsbeklagte des Verfahrens gestützt sah – und aufgrund eines klar zutage getretenen gesetzgeberischen Willens eine solche Datenverarbeitung zuzulassen, auf eine Einschränkung des Art. 9 Abs. 1 DS-GVO erkannt. Vorbild bot die vorgenannte Entscheidung des Gerichtshofs vom 24.09.2019[41].

Der Gesetzgeber habe in Art. 10 Abs. 5 der KI-VO, die dem Willen folgt, weltweit eine europäische Führungsrolle im Bereich der KI-Entwicklung zu erlangen[42], eine Rechtsgrundlage allein für den zielgerichteten Einsatz von Daten im Sinne des Art. 9 DS-GVO beim Training von Hochrisiko-KI geschaffen.[43] Für die nicht zielgerichtete Verarbeitung solcher Daten beim Training von KI-Modellen habe der Gesetzgeber in Kenntnis der Notwendigkeit des Trainings großer generativer KI-Modelle mit „riesigen Mengen an [...] Daten"[44], das stets die Gefahr der – unbeabsichtigten und nicht zielgerichteten – Verarbeitung von Daten im Sinne des Art. 9 DS-GVO birgt, hingegen keinen Regelungsbedarf gesehen, sei also nicht von einer grundsätzlichen Rechtswidrigkeit des Trainings ausgegangen.

Zwar tritt Art. 10 Abs. 5 KI-VO, worauf das Gericht hinweist[45], erst ab dem 02.08.2026 (Art. 113 KI-VO) in Kraft. Anhaltspunkte dafür, dass der Wille des Gesetzgebers zur Zulässigkeit des Trainings von KI-Modellen bis dahin aufgeschoben sein sollte, etwa aufgrund des gleichzeitigen Inkrafttretens von einhegenden weiteren Vorschriften der KI-VO, bestehen nicht.[46] Auch die vom Gericht in Bezug[47] genommene Konkurrenzregelung des Art. 2 Abs. 7 S. 2 KI-VO steht dem Ergebnis nicht entgegen. Es ist nicht ersichtlich, dass damit eine systematische Auslegung der DS-GVO mit Blick auf neuere Rechtsvorschriften gesperrt werden sollte.[48] Dabei ist zudem auch der Querverweis des Art. 9 Abs. 2 lit g) DS-GVO in den Blick zu nehmen, mit dem gerade nach „außen" und (auch) auf die hier relevante Passage der KI-VO verwiesen wird.[49]

Das Gericht hat diese Einschränkung durch eine Antragsmöglichkeit auf Löschung – die im Rahmen des Trainings von KI-Modellen allerdings stets von fraglicher Wirksamkeit sei[50] – eingehegt und die Einschränkung gleichsam eingeschränkt. Es ist von einer „tätigkeitsbezogenen Reduktion der Unterlassungspflicht der Verfügungsbeklagten dahin aus[gegangen], dass diese jedenfalls dann, wenn die Verarbeitung nicht zielgerichtet erfolgt, einer näheren Konkretisierung durch einen Antrag des Betroffenen auf Herausnahme seines Datensatzes bedarf."[51] Wenngleich der durch das Gericht entschiedene „KI-Fall" mit dem „Suchmaschinen-Fall" nicht ohne Weiteres vergleichbar ist, weil eine Kenntnis des Betroffenen über die von der Datenverarbeitung betroffenen Daten nicht besteht und eine Antragsmöglichkeit nicht in gleichem Maße effektiv sein wird, wird dies dadurch relativiert, dass das Gericht nur geringe Gefahren einer konkreten Schädigung der Betroffenen festgestellt hat. Weiter einschränkend hat das Gericht auf das allgemeine Erfordernis, die Voraussetzungen des Art. 6 Abs. 1 lit f) DS-GVO zu wahren, hingewiesen.

III. Gesamtergebnis und Ausblick

Nach der hier vertretenen Auffassung gilt die Untersagung des Art. 9 Abs. 1 DS-GVO nicht absolut, sondern kann in begründeten Ausnahmefällen durchbrochen werden. Ausweislich der vorgenannten Entscheidungen des Europäischen Gerichtshofs und des Oberlandesgerichts Köln lässt sich diese Einschränkungsmöglichkeit in der Praxis auch fruchtbar machen. Ob mit diesen in spezifischen Einzelfällen ergangenen Entscheidungen ohne gesetzgeberische Klarstellung hinreichende Rechtssicherheit besteht, um eine angemessene Anwendung des Art. 9 Abs. 1 DS-GVO zu gewährleisten, ist indessen zweifelhaft und hängt jedenfalls von einer gebotenen gerichtlichen Klärung auf europäischer Ebene für den gesamten Geltungsbereich der DS-GVO ab.

39 C-136/17 –, juris, Rn. 45 ff.; vgl. insoweit auch Schlussanträge des Generalanwalts vom 10.01.2019, Rn. 56 f.

40 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris m.w.N.

41 C-136/17 –, juris, Rn. 45 ff.; vgl. insoweit auch Schlussanträge des Generalanwalts v. 10.01.2019, Rn. 56 f.

42 ErwG 8 der KI-VO.

43 ErwG 70 der KI-VO.

44 ErwG 105 der KI-VO.

45 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 116.

46 A.A. Wasilewski, CR 2025, 450, 463.

47 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 46.

48 A.A. Wasilewski, CR 2025, 450, 463.

49 Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann, u.a. DS-GVO, 2024, Art. 9 Rn. 185.

50 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 117.

51 OLG Köln, Urt. v. 23.05.2025 – I-15 UKl 2/25 –, juris, Rn. 117.

Sophie Sohm

Das Kölner KI-Urteil ist richtig und entscheidend für KI-Innovationen – Nicht nur für Meta

Im Frühjahr 2025 reichte die Verbraucherzentrale NRW (VZ NRW) beim Oberlandesgericht Köln (OLG Köln) einen Antrag auf einstweilige Verfügung gegen Meta ein. Ihr Ziel: Meta daran zu hindern, öffentlich auf Facebook und Instagram geteilte Beiträge von Nutzern über 18 Jahren für das Training seiner generativen KI-Modelle zu verwenden. Die Begründung: Meta habe keine ausreichende Rechtsgrundlage gemäß der DS-GVO und verstoße gegen Bestimmungen des DMA.

Dieser Fall hat nun zu einer wegweisenden Gerichtsentscheidung geführt, mit der die Forderungen der VZNRW vollständig zurückgewiesen wurden. Die Auswirkungen dieser Entscheidung gehen jedoch weit über Meta hinaus, insbesondere da alle Anbieter von GenAI-Modellen ihre Modelle mit öffentlichen Daten trainieren. Sie bekräftigt eine ausgewogene und innovationsfreundliche Auslegung des Datenschutzrechts, die nicht nur aus rechtlicher Sicht richtig, sondern auch für das KI-Ökosystem Europas unerlässlich ist.

I. Warum diese Entscheidung richtig und wichtig für KI-Innovationen ist, nicht nur für Meta

KI-Modelle, insbesondere generative KI, können ohne große, vielfältige und repräsentative Datensätze nicht effektiv trainiert werden. Mit der Bestätigung, dass „berechtigte Interessen" (in Verbindung mit robusten Schutzvorkehrungen) eine gültige Rechtsgrundlage für das KI-Training darstellen, hat das Gericht einen Regulierungsweg bestätigt, der europäische KI-Innovationen ermöglicht und gleichzeitig die Rechte der Menschen schützt.

Die Entscheidung des Gerichts steht im Einklang mit der Stellungnahme des Europäischen Datenschutzausschusses (EDSA) vom Dezember 2024, in der klargestellt wurde, dass die Einwilligung nicht die einzige tragfähige Rechtsgrundlage für das Training von KI ist. Die EDSA befürwortete eine Interessenabwägung, um sicherzustellen, dass die technologische Entwicklung nicht durch eine zu strenge Auslegung der Datenschutzgesetze sofort behindert wird.

Meta hat seine Compliance durch die Umsetzung strenger Abhilfemaßnahmen nach umfangreichen Gesprächen mit den Regulierungsbehörden weiter unter Beweis gestellt, wie in der Erklärung des IDPC zu erkennen ist[52]: „Meta hat während dieses Prozesses auf die Forderungen der DPC reagiert und infolgedessen eine Reihe bedeutender Maßnahmen und Verbesserungen umgesetzt." Zu diesen Maßnahmen gehören eine transparente Kommunikation mit den Nutzern, ein klarer und bedingungsloser Opt-out-Mechanismus sowie strenge Protokolle zur Datenminimierung und -sicherheit.

Darüber hinaus wies das Gericht die Behauptung zurück, dass der Ansatz von Meta gegen das Gesetz über digitale Märkte (DMA) verstoße, und stellte klar, dass der KI-Trainingsprozess keine unrechtmäßige Kombination personenbezogener Daten über Plattformen hinweg beinhalte. Es betonte, dass unstrukturierte Datensätze, die für das Modelltraining verwendet werden – und in erster Linie anonymisiert sind –, nicht mit plattformübergreifendem Profiling gleichzusetzen sind.

Wichtig ist auch, dass das Gericht die Behauptung zurückwies, Art. 9 DS-GVO (Schutz sensibler Daten) würde ein solches Training verbieten. Meta hat zwar eine Reihe von Maßnahmen entwickelt, um die Verarbeitung besonderer Datenkategorien zu verhindern, doch kam das Gericht zu dem Schluss, dass selbst wenn irgendwo im Datensatz Reste verblieben wären, kein Verstoß gegen Art. 9 vorliegen würde. Dabei erkannte es an, dass die Wahrscheinlichkeit einer erneuten Identifizierung einzelner Personen aufgrund der Größe des Datensatzes und der Anonymisierungstechniken unwesentlich sei, und schloss sich damit der Auffassung der baden-württembergischen Landesdatenschutzbehörde[53] an. Das Gericht betonte, dass eine zu restriktive Auslegung von Art. 9 unter anderem den Zielen des EU-KI-Gesetzes widersprechen würde, das die Führungsrolle Europas bei der Entwicklung sicherer und vertrauenswürdiger KI stärken soll.

Mit der Bestätigung dieses Ansatzes hat das Gericht sowohl die DS-GVO als auch den DMA korrekt angewendet. Gleichzeitig hat es das in dem KI-Gesetz dargelegte übergeordnete Ziel der EU bekräftigt, Europa als weltweit führenden Standort zu etablieren und ein menschenzentriertes, sicheres, vertrauenswürdiges und ethisches KI-Ökosystem in Europa zu fördern. Hätte das Gericht anders entschieden, hätte er einen gefährlichen Präzedenzfall geschaffen: Unternehmen wären effektiv verpflichtet worden, vor der Durchführung von Schulungen die ausdrückliche Zustimmung der betroffenen Personen einzuholen. Das hätte die Entwicklung wirksamer KI-Modelle nahezu unmöglich gemacht und die Innovation in der gesamten Branche behindert – nicht nur für Meta, sondern für alle KI-Akteure in Europa.

52 Https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai.

53 „Wie der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hervorhebt, beinhaltet die Entwicklung großer Sprachmodelle auf der Grundlage sehr großer Trainingsdatensätze – um die es hier geht – nicht regelmäßig die gezielte Verarbeitung personenbezogener Daten oder die Identifizierung einer bestimmten Person. Insofern ist sie nicht von den Informationen des Einzelnen abhängig, wie dies bei einer eingreifenden Profilerstellung im Sinne von Art. 4 Abs. 4 DS-GVO, die die DS-GVO nur unter strengen Voraussetzungen zulässt" (Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 25; Franke, RDi 2023, 565, 568).

II. Warum das hier angewandte deutsche Verfahren so ungewöhnlich, innovationsfeindlich und anfällig für Missbrauch ist

Der von VZ NRW in diesem Fall eingeschlagene Rechtsweg offenbart eine strukturelle Schwäche der digitalen Innovationslandschaft in Europa. Im Gegensatz zu Regulierungsverfahren, die von offiziellen Datenschutzbehörden (DSB) eingeleitet werden, ging diese Klage auf einen Antrag auf einstweilige Verfügung einer Verbraucherschutzorganisation zurück. Diese handelte auf eigene Initiative, verfolgte aber eine Abhilfe, die das Training von KI bei Meta auf nationaler Ebene in Deutschland blockiert hätte. Zwar spielen solche Organisationen eine wichtige Rolle bei der Verteidigung der Verbraucherinteressen, doch geben die deutschen Rechtsvorschriften, die es ihnen ermöglichen, de facto als digitale Regulierungsbehörden zu agieren, Anlass zu ernsthaften Bedenken.

Was das Verfahren besonders ungewöhnlich und problematisch machte, ist Folgendes:

1. Quasi-regulatorische Übergriffe ohne institutionelle Rechenschaftspflicht:

Die Klage der VZNRW war eine einseitige rechtliche Maßnahme, die den üblichen Regulierungsprozess umging und einen parallelen quasi-regulatorischen Durchsetzungskanal schuf, der eher durch Rechtsstreitigkeiten als durch einen fachlichen Regulierungsdialog angetrieben wurde.

2. Potenzial für eine fragmentierte Rechtslandschaft in Deutschland und Europa:

Wenn Verbraucherverbände in jedem Mitgliedstaat unabhängig voneinander Klagen mit nationaler Wirkung einreichen und damit ihre Auslegung der DS-GVO in einer Weise durchsetzen können, die alle Bürger betrifft, hat das Konsequenzen: Es öffnet die Tür für fragmentierte, höchst unvorhersehbare und inkonsistente Urteile sowohl in Deutschland als auch in anderen EU-Mitgliedstaaten. Eine solche Rechtsunsicherheit schreckt Innovationen und Investitionen ab, insbesondere in Bereichen wie der KI, in denen der Zugang zu vielfältigen Daten von grundlegender Bedeutung ist.

3. Anti-Innovations-Instrumentalisierung von Verfahrensinstrumenten:

Einstweilige Verfügungen sind als dringende Rechtsmittel konzipiert, um drohenden Schaden abzuwenden. Ihre Nutzung als Strategie zur Blockierung der KI-Entwicklung hat eine abschreckende Wirkung auf Innovationen. Das gilt insbesondere, wenn die angeblichen Schäden spekulativ sind, ohne gründliche technische Analyse und die betroffenen Unternehmen keine gewöhnliche Berufung gegen die Verfügung einlegen können. Unternehmen könnten gezwungen sein, wichtige Forschungs- und Entwicklungsprojekte aufgrund „dringender" vorsorglicher Rechtsansprüche einzustellen. Dabei sollte dies nur aufgrund objektiver regulatorischer Feststellungen oder Gerichtsverfahren geschehen, in denen den Parteien ausreichend Zeit zur Darlegung ihrer Argumente eingeräumt wird und Richter fundierte Entscheidungen treffen können.

4. Risiko des Missbrauchs durch Klagen mit kommerziellen Absichten:

Es gibt eine separate wachsende Besorgnis über den Missbrauch dieser deutschen Verfahrensprivilegien durch professionelle Klagevehikel, die als Verbraucherverbände auftreten. Diese Einrichtungen, die eher durch Gewinnstreben als durch echten Verbraucherschutz motiviert sind, nutzen diese Rechtsvorschriften aus, um doppelte Klagen auf der Grundlage umfassenderer kommerzieller Prozessstrategien zu verfolgen. Ein bemerkenswertes Beispiel ist SOMI, eine niederländische Einrichtung, die offenbar als Klagevehikel gegründet wurde, um Sammelklagen gegen Technologieunternehmen in ganz Europa zu führen, und die Investoren Auszahlungen von bis zu 600 % in Aussicht stellt[54]. Obwohl das Kölner Gericht zuvor einen Antrag auf eine einstweilige Verfügung der VZNRW (d.h. einer tatsächlichen deutschen Verbraucherorganisation) abgelehnt hatte, hat SOMI deutsche Anwälte angewiesen, das gleiche beschleunigte Verfahren zur Erwirkung einer einstweiligen Verfügung zu nutzen. Die Organisation bringt damit die gleichen Beschwerden vor ein anderes deutsches Landgericht, mit dem Ziel, den für ihre umfassendere Agenda günstigsten Gerichtsstand in der EU zu finden. Diese Taktik schafft nicht nur Rechtsunsicherheit und Fragmentierung. Sie zeigt auch, wie nicht-deutsche Unternehmen dazu ermutigt werden, in Deutschland landesweite Unterlassungsklagen anzustrengen, angezogen von niedrigen Prozesskosten und vorteilhaften Verfahrensregeln. Solche Praktiken bergen die Gefahr, dass das deutsche Verfahrensrecht zu einem Instrument wird, das nicht zum Schutz der Verbraucher, sondern als Teil umfassenderer kommerzieller Strategien eingesetzt wird, was letztlich technologische Innovationen in Deutschland direkt behindert.

III. Fazit: Die weitreichenden Auswirkungen

Die Entscheidung des Kölner Gerichts stellt das Gleichgewicht wieder her, indem sie bestätigt, dass KI-Innovation und der Schutz der Daten von Menschen sich nicht gegenseitig ausschließen. Sie erkennt an, dass eine harmonisierte, prinzipienbasierte Anwendung der DS-GVO – und nicht fragmentierte Unterlassungsklagen, die von aktivistischen Prozessen vorangetrieben werden – für Europas Ambitionen in Bezug auf die Führungsrolle im Bereich der KI unerlässlich ist. Mehr noch: Sie stellt fest, dass die Auslegung des Datenschutzes nicht isoliert erfolgen kann und mit den von den politischen Entscheidungsträgern festgelegten Zielen der EU im Einklang stehen muss, in diesem Fall der Entwicklung der KI in der EU, wie sie im EU-KI-Gesetz klar festgelegt ist. Die Entscheidung hat daher eine Bedeutung, die weit über Meta hinausgeht: Sie ist ein wichtiger Schritt zur Gewährleistung von Rechtssicherheit, zur Förderung verantwortungsvoller KI-Innovationen und zur Vermeidung eines weiteren Rückstands Europas im globalen KI-Wettlauf. Unterdessen besteht weiterhin die Gefahr einer Fragmentierung durch weitreichende Unterlassungsurteile, die von gewinnorientierten Unternehmen angestrebt werden, die in Ländern mit laxen Verfahrensvorschriften wie Deutschland Forum Shopping betreiben. Es liegt im Interesse Deutschlands und Europas, dass die Gerichte dieser Praxis schädlicher und doppelter Rechtsstreitigkeiten entgegenwirken.

54 Https://somi.nl/en/investment.

Moritz Köhler
ist wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln.

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.

Dr. Stefan Brink
ist Geschäftsführender Direktor des Instituts wida/Berlin und Landesdatenschutzbeauftragter Baden-Württemberg a.D.

Prof. Dr. iur. Tobias Keber
ist Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg.

© Stefan Zeitz

Dr. Dominik Roderburg
ist Richter am Oberlandesgericht Köln und war Berichterstatter im hier besprochenen Verfahren.

Sophie Sohm
ist Privacy Policy Managerin bei Meta.

Der Wissensvorsprung für Ihre Arbeit

Die Datenschutz Newsbox versorgt Sie monatlich mit aktuellen Themen rund um den Datenschutz.

kostenfrei als PDF-Download, auch ohne Abo verfügbar

www.dataagenda.de/datenschutz-newsbox

DATAKONTEXT

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

KI-Training mit sensiblen Daten und Art. 9 DS-GVO

– zugleich Besprechung von OLG Köln, Urt. v. 23.05.2025 – 15 UKl 2/25 – Meta KI-Training

Es besteht ein strukturelles Spannungsverhältnis im Zusammenspiel von KI-Training, das regelmäßig auf die Verfügbarkeit von großen Datenmengen (Big Data) angewiesen ist, und den Vorgaben von Art. 9 DS-GVO, wonach grundsätzlich ein Verarbeitungsverbot für besondere Kategorien von sensiblen personenbezogenen Daten besteht. Vor diesem Hintergrund verdient das hier zur Besprechung anstehende, im einstweiligen Rechtsschutz ergangene Urteil des OLG Köln vom 23.05.2025 besondere Aufmerksamkeit, da zentrale Grundfragen des Verhältnisses von KI-Entwicklung und Datenschutz verhandelt wurden, die weit über den streitgegenständlichen Sachverhalt hinausreichen.

I. Sachverhalt – Entscheidung – Problemstellung

Im Frühjahr 2024 hatte der US-amerikanische Technologiekonzern Meta Platforms Ireland Limited (Meta) – unter anderem Betreiber der sozialen Netzwerke Facebook und Instagram – angekündigt, künftig öffentlich auf Meta-Produkten geteilte Inhalte erwachsener Nutzerinnen und Nutzer in der EU für das Training eigener generativer KI-Modelle zu verwenden. Diese Nutzung von sog. „First Party Data" zum KI-Training durch Meta sollte zunächst im Juni 2024 starten.

1. Eilverfahren vor dem OLG Köln

Nach einem umfassenden Austausch mit der zuständigen irischen Datenschutzbehörde (Data Protection Commission, DPC) und einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) gem. Art. 64 DS-GVO im Jahr 2024[1] verschob Meta den Start des KI-Trainings mit First Party Data in der EU, aktualisierte sein Datenschutzkonzept und implementierte ein Widerspruchsrecht für die betroffenen Personen sowie Maßnahmen zur De-Identifikation der in den Trainingsdatensatz eingebrachten personenbezogenen Daten. Meta veröffentlichte zudem umfangreiche Hinweise zur geplanten Datenverarbeitung. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten berief sich Meta auf das „berechtigte Interesse" gemäß Art. 6 Abs. 1 lit. f) DS-GVO und nahm hierbei auch die vorbezeichnete EDSA-Stellungnahme 28/2024 in Bezug.[2]

Nutzerinnen und Nutzer wurden über die Absicht informiert, dass ihre Inhalte für KI-Trainingszwecke verwendet werden sollen, und es wurde ein Opt-out-Verfahren eingerichtet: Wer mit der Nutzung seiner öffentlichen Inhalte nicht einverstanden war, konnte über ein Online-Formular widersprechen. Darüber hinaus aktualisierte Meta unter anderem seine Maßnahmen zum Schutz der betroffenen Personen, wie beispielsweise durch Anonymisierung sowie das Filtern von Trainingsdatensätzen und Ausgaben des KI-Systems.[3]

Sodann kündigte Meta in einer Pressemitteilung[4] vom 14.04.2025 an, auf eigenen Social-Media Diensten Facebook und Instagram durch die von volljährigen Nutzerinnen und Nutzern öffentlich eingestellte Daten (wie beispielsweise Profilbilder, Kommentare, Bewertungen etc.) ab dem 27.05.2025 zum Training des von Meta entwickelten KI-Modells nutzen zu wollen. Nachdem die irische DPC die entsprechende Datenverarbeitung im Folgenden nicht untersagte, beantragte die Verbraucherzentrale NRW (VZ NRW) am 12.05.2025 im Wege der einstweiligen Verfügung, Meta zu untersagen, im Rahmen geschäftlicher Handlungen gegenüber Verbrauchern von diesen auf den Diensten Instagram und Facebook veröffentlichte personenbezogene Daten zur Entwicklung von KI-Systemen zu verarbeiten. Das OLG Köln wies den Antrag auf einstweilige Verfügung im Ergebnis als unbegründet zurück.[5]

2. Entscheidung des OLG Köln

Zentrale Bedeutung für die Entscheidung des OLG Köln kam unter anderem[6] der Frage zu, ob das konkrete Vorhaben gegen das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten aus Art. 9 Abs. 1 DS-GVO verstößt. Einen solchen Verstoß gegen Art. 9 Abs. 1 DS-GVO lehnte der Senat im Ergebnis ab und bestätigte damit auch insoweit die datenschutzrechtliche Zulässigkeit des Vorhabens.

Konkret sprach sich der erkennende Senat zwar gegen eine teleologische Reduktion des Verbots aus Art. 9 Abs. 1 DS-GVO aus, stützte die Zulässigkeit der in Rede stehenden Datenverarbeitung aber sodann auf eine „tätigkeitsbezogene Reduktion der Unterlassungspflicht der Verfügungsbe-

1 EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, angenommen am 02.12.2024.

2 Zu den hiermit verbundenen Rechtsfragen siehe die weiteren Beiträge in diesem RDV-Heft.

3 Vgl. hierzu auch die DPC-Pressemitteilung vom 21.05.2025, abrufbar unter https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai.

4 Abrufbar unter https://about.fb.com/news/2025/04/making-ai-work-harder-for-europeans/.

5 OLG Köln, Urt. v. 23.05.2025 – 15 UKl 2/25, RDV 2025, 262.

6 Weiterhin musste das Gericht die Rechtmäßigkeit des Vorhabens auf der Grundlage und am Maßstab von – vor allem – auf Art. 6 DS-GVO und Art. 5 DMA ausführlich prüfen. Der erkennende Senat hat diesbezüglich entschieden, dass die konkrete Verarbeitung vom Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO umfasst und ein Verstoß gegen Art. 5 Abs. 2 UAbs. 1 lit. b) DMA abzulehnen sei. Der vorliegende Beitrag befasst sich ausschließlich mit der Frage nach der Zulässigkeit des Vorhabens in Ansehung von sensiblen personenbezogenen Daten nach Art. 9 DS-GVO.

klagten", sprich Meta. In Anlehnung an die Rechtsprechung des EuGH betreffend Suchmaschinenbetreiber entwickelte der Senat als ungeschriebenes Tatbestandsmerkmal für das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO insoweit einen Antrag[7] des Betroffenen auf Herausnahme seiner Daten aus dem Trainingsdatensatz.

3. Grundsätzliche Bedeutung

Die grundsätzliche Bedeutung der Entscheidung und der ihr zugrunde liegenden Rechtsfragen für die datenschutzrechtliche Zulässigkeit von KI-Training zeigt sich nicht zuletzt auch in dem wiederholten Hinweis des erkennenden OLG-Senats auf eine mögliche Art. 267 AEUV-Vorlage an den EuGH in der Hauptsache. Es besteht somit begründeter Anlass zu einer vertieften Auseinandersetzung mit den Entscheidungsgründen und den weit über den entschiedenen Fall hinausgehenden Grundsatzfragen.

In diesem Beitrag werden hierzu nachfolgend zunächst die Anwendbarkeit des Art. 9 Abs. 1 DS-GVO (II.) und mögliche Ausnahmetatbestände aus Art. 9 Abs. 2 DS-GVO (III.) näher betrachtet. Anschließend wird der vom Senat entwickelte Ansatz einer tätigkeitsbezogenen Reduktion analysiert (IV.), bevor alternative Lösungsansätze dargestellt werden (V.). Beschlossen wird die Bearbeitung mit einer Zusammenfassung und einem Ausblick (VI.)

II. Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO

Art. 9 DS-GVO statuiert Vorgaben für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Vorschrift enthält ein grundsätzliches Verbot der Verarbeitung von sensiblen personenbezogenen Daten, das nur unter bestimmten engen Voraussetzungen durchbrochen werden kann. Zu den besonders geschützten, sensiblen Daten zählen unter anderem Informationen über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, genetische oder biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten sowie Angaben zum Sexualleben oder zur sexuellen Orientierung. Diese Daten gelten als besonders sensibel, weil ihre unkontrollierte Verarbeitung erhebliche Risiken für die Persönlichkeitsrechte und die Privatsphäre der betroffenen Personen mit sich bringen kann, womit es sich bei Art. 9 DS-GVO um eine Ausformung des der DS-GVO zugrunde liegenden risikobasierten Ansatzes handelt.[8]

In diesem Sinne sieht Art. 9 Abs. 1 DS-GVO ein generelles Verbot der Verarbeitung dieser Datenkategorien vor, während Abs. 2 eine abschließende Aufzählung von Ausnahmetatbeständen enthält, nach denen eine Verarbeitung gleichwohl zulässig sein kann. Zu diesen Ausnahmetatbeständen zählt insbesondere die ausdrückliche Einwilligung der betroffenen Person, darüber hinaus sind aber auch bestimmte gesetzlich vorgesehene Zwecke benannt, etwa im Arbeits-, Sozial- oder Gesundheitsbereich oder Gründe des erheblichen öffentlichen Interesses.

Das OLG Köln hat ausgeurteilt, dass die von Meta angestrebte Verarbeitung der Nutzerdaten zum Zwecke des KI-Trainings eine Verarbeitung besonderer Kategorien personenbezogener Daten darstellt und damit in den Anwendungsbereich von Art. 9 Abs. 1 DS-GVO fällt. Denn es handelt sich um personenbezogene Daten (1.), die unter die besonderen Datenkategorien von Art. 9 Abs. 1 DS-GVO fallen (2.).

1. Vorliegen von personenbezogenen Daten, Art. 4 Nr. 1 DS-GVO

Bei den in Rede stehenden Nutzerdaten handelt es sich um personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen. Die von Meta vorgesehene „De-Identifizierung" führt nach dem Gericht insbesondere nicht zu einer Anonymisierung.[9] So steht einer wirksamen Anonymisierung vor allem auch ein erhebliches Risiko der Re-Identifizierung für die betroffene Person entgegen. Vor dem Hintergrund der stetig steigenden Rechenleistungen und im Zusammenhang mit Big-Data-Analysen steigt die Wahrscheinlichkeit, dass durch die Verknüpfung verschiedener Daten und die Kombination relevanter Daten der Personenbezug wiederhergestellt werden kann.[10]

In diesem Zusammenhang stellt sich die grundsätzliche Frage, was die Anforderungen an eine wirksame Anonymisierung sein sollen. Dies ist in der DS-GVO nicht näher konkretisiert, sodass auf die allgemeinen DS-GVO-Vorgaben zur Identifizierbarkeit bzw. zum Personenbezug aus ErwG 26 DS-GVO zu rekurrieren ist. Negativ formuliert liegt hiernach eine Anonymisierung und damit kein Bezug zu einer identifizierten oder identifizierbaren Person vor, wenn alle Mittel berücksichtigt werden, die nach allgemeinem Ermessen wahrscheinlich eingesetzt werden können, um die betreffende Person zu identifizieren – und sich trotzdem kein Personenbezug herstellen lässt.

Der EuGH interpretiert die Begriffe der Identifizierung und Identifizierbarkeit sowie damit auch den der Personenbezogenheit sehr weit. Eine solche Auslegung führt zu einer weiten Anwendbarkeit der DS-GVO, für die das Vorliegen von personenbezogenen Daten das entscheidende Kriterium ist. Diese Entwicklung stellt Verantwortliche mit Blick auf die Datennutzung und damit auch betreffend das hier in Rede stehende KI-Training vor erhebliche praktische Herausforderungen, weil Verantwortliche laufend umfassende Risikoanalysen vornehmen müssen, um Möglichkeiten der (Re-)Identifizierung zu bewerten. Hierzu müssen vielfach auch rein hypothetische Szenarien durchgespielt werden; zudem muss überprüft werden, ob neue Analyseinstrumente die erfolgte Anonymisierung erneut hinfällig machen (können).

2. Vorliegen von besonderen Kategorien personenbezogener Daten, Art. 9 Abs. 1 DS-GVO

Die streitgegenständlichen Nutzerdaten unterfallen zudem dem Anwendungsbereich von Art. 9 Abs. 1 DS-GVO.

7 Das Gericht sprach von einer „‚Aktivierung' durch einen Antrag des betroffenen Dritten auf Herausnahme seiner Daten aus dem […] Trainingsdatensatz", OLG Köln, RDV 2025, 262, 269 Rn. 116.

8 So bereits Veil, ZD 2015, 347, 349.

9 OLG Köln, RDV 2025, 262, 264 Rn. 59 m.w.N. (insbesondere auf Paal, ZfDR 2024, 129, 136).

10 Paal, ZfDR 2024, 129, 136 m.w.N.

a) Gesundheitsdaten, Art. 4 Nr. 15 DS-GVO

Der erkennende Senat hat im zugrunde liegenden Fall die Anwendbarkeit von Art. 9 Abs. 1 DS-GVO betreffend die Verarbeitung von Gesundheitsdaten bejaht. Der weit auszulegende[11] Begriff der Gesundheitsdaten ist in Art. 4 Nr. 15 DS-GVO legaldefiniert und erfasst alle personenbezogenen Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über den Gesundheitszustand hervorgehen. Dabei genügt es nach der Rechtsprechung des EuGH, dass aus den Daten mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden kann.[12]

b) Weitere Kategorien sensibler Daten

Zwar hat das OLG Köln in seinen Entscheidungsgründen lediglich auf Gesundheitsdaten abgestellt. Es kann aber bei der von Meta geplanten Verarbeitung der Facebook- und Instagram-First-Party-Daten bei lebensnaher Betrachtung davon ausgegangen werden, dass neben Gesundheitsdaten auch weitere nach Art. 9 Abs. 1 DS-GVO geschützte Datenkategorien, wie beispielsweise über politische Meinungen, ethnische Herkunft oder sexuelle Orientierung, von dem Vorhaben betroffen sein können.

c) Gemischte Datensätze

Weiterhin ist dem OLG Köln dahingehend zuzustimmen, dass Art. 9 Abs. 1 DS-GVO auf die Verarbeitung der Nutzerdaten zu KI-Trainingszwecken bereits dann anzuwenden ist, wenn zwar einige, aber nicht alle im Trainingsdatensatz enthaltenen Nutzerdaten als sensible Daten unter Art. 9 Abs. 1 DS-GVO fallen. Denn nach der einschlägigen EuGH-Judikatur gilt das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO auch für gemischte Datensätze insgesamt, sofern jedenfalls mindestens ein sensibles Datum in dem betreffenden Datensatz enthalten ist.[13]

III. Ausnahmen vom Verarbeitungsverbot nach Art. 9 Abs. 2 DS-GVO

Nachdem somit das allgemeine Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO für abschließend festgelegte sensible Datenkategorien eingreift, waren die Ausnahmen zu prüfen, sprich ob die von Meta angekündigte Verarbeitung der Facebook- und Instagram Nutzerdaten zum Zwecke des KI-Trainings unter einen der in Art. 9 Abs. 2 DS-GVO enumerativ und abschließend aufgezählten Ausnahmetatbestände subsumiert werden kann.

Da, wie der erkennende Senat zutreffend festgestellt hat, eine Einwilligung der betroffenen Personen realistischerweise kaum mit zumutbarem Aufwand zu erlangen sein wird, werden vorliegend lediglich die Ausnahmetatbestände aus Art. 9 Abs. 1 lit. e) („offensichtlich öffentlich gemachte Daten"), lit. g) („erhebliches öffentliches Interesse") und lit. j) („archivarische, wissenschaftliche und statistische Zwecke") DS-GVO ernsthaft in Betracht kommen.[14]

1. Art. 9 Abs. 2 lit. e) DS-GVO („offensichtlich öffentlich gemachte Daten")

Die in Rede stehende Verarbeitung von sensiblen personenbezogenen Nutzerdaten durch Meta fällt nicht in allen Fällen unter den Ausnahmezustand des Art. 9 Abs. 2 lit. e) DS-GVO, wie das OLG Köln zutreffend und überzeugend dargelegt hat. Denn die nach allgemeinen Grundsätzen eng auszulegende[15] Ausnahmevorschrift des Art. 9 Abs. 2 lit. e) DS-GVO ermöglicht zwar eine Verarbeitung von sensiblen Daten im Sinne des Art. 9 Abs. 1 DS-GVO, wenn sich die Verarbeitung auf solche personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

Der erkennende Senat verneint aber zu Recht eine Anwendbarkeit des Art. 9 Abs. 2 lit. e) DS-GVO auf Nutzerdaten mit Drittbezug.[16] Dem Schutzzweck von Art. 9 Abs. 1 DS-GVO und dem eindeutigen Wortlaut entsprechend greift der Ausnahmetatbestand des Art. 9 Abs. 1 lit. e) DS-GVO nur für solche Daten, die die betroffene Person selbst veröffentlicht hat.[17] Die Veröffentlichung durch die betroffene Person stellt einen Verzicht auf den Schutz des Art. 9 Abs. 1 DS-GVO dar, über den sie nur selbst disponieren kann.[18] Ein solcher Verzicht kann gerade nicht durch bzw. für Dritte erfolgen.

2. Art. 9 Abs. 2 lit. g) DS-GVO („erhebliches öffentliches Interesse")

Gemäß Art. 9 Abs. 2 lit. g) DS-GVO gilt das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO nicht, wenn die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt, angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht sowie aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Art. 9 Abs. 2 lit. g) DS-GVO stellt keinen eigenständigen Erlaubnistatbestand dar, sondern enthält (lediglich) eine

11 Vgl. BeckOK/Albers/Veit, Datenschutzrecht, 52. Edition, Stand: 01.05.2025, Art. 9 Rn. 45; Gola/Heckmann/Schulz, 3. Aufl., 2022, DS-GVO, Art. 9 Rn. 20; Paal/Pauly/Frenzel, DS-GVO, 3. Aufl., 2021, Art. 9 Rn. 15 m.w.N.

12 Vgl. EuGH, GRUR 2025, 1721, 1727 Rn. 83 – Lindenapotheke; ZD 2022, 611, 614 Rn. 123. So auch zutreffend vom erkennenden OLG-Senat unter Bezugnahme auf die EuGH-Rechtsprechung übernommen.

13 EuGH, GRUR 2023, 1131 Rn. 89 – Meta Platforms ua (Facebook Ireland).

14 Der erkennende Senat diskutiert zwar entsprechend des Vortrags der Verfügungsbeklagten Meta lediglich den Ausnahmetatbestand aus Art. 9 Abs. 2 lit. e) DS-GVO. Aufgrund der besonderen Bedeutung der Entscheidung werden die weiteren beachtlichen Ausnahmetatbestände in diesem Beitrag aber ebenfalls behandelt.

15 Vgl. zur engen Auslegung des Ausnahmetatbestands insbesondere EuGH, GRUR 2023, 1131 Rn. 76 m.w.N. – Meta Platforms ua (Facebook Ireland); GRUR 2024, 1821, 1826 Rn. 76 – Schrems.

16 OLG Köln, RDV 2025, 262, 268 Rn. 111.

17 EuGH, GRUR 2023, 1131 Rn. 75 – Meta Platforms ua (Facebook Ireland).

18 Vgl. Kühling/Buchner/Weichert, DS-GVO, 4. Aufl., 2024, Art. 9 Rn. 77; Jaspers/Schwartmann/Mühlenbeck in: Schwartmann u.a., DS-GVO, 3. Aufl., 2024, Art. 9 Rn. 165; Kritisch mit Blick auf die Wertung, dass die betroffene Person durch die Veröffentlichung der Daten auf den Schutz nach Art. 9 Abs. 1 DS-GVO „verzichtet" siehe Simitis/Hornung/Spiecker gen. Döhmann/Petri, DS-GVO, 2. Aufl., 2025, Art. 9 Rn. 57. Im Ergebnis kann die genaue dogmatische Einordnung jedoch offen bleiben, da jedenfalls anerkannt ist, dass die Ausnahmevorschrift des Art. 9 Abs. 2 lit. e) DS-GVO auf solche Daten keine Anwendung findet, die nicht von der betroffenen Person, sondern von Dritten veröffentlicht wurden.

horizontale Öffnungsklausel, auf deren Grundlage der europäische oder nationale Gesetzgeber das erhebliche öffentliche Interesse anhand einer konkretisierenden Norm regeln kann.[19] Das Vorliegen einer solchen übergreifenden europäischen oder nationalstaatlichen Konkretisierungsnorm für Datenverarbeitungen zum Zwecke des KI-Trainings ist nicht ersichtlich; etwas anderes mag gelten für eine (analoge) Anwendung von Art. 10 Abs. 5 S. 1 KI-VO.[20]

Unbeschadet dessen ist ganz grundsätzlich die Frage aufzuwerfen, ob und inwieweit eine Datenverarbeitung zum Zwecke der Entwicklung und Verbesserung eines KI-Systems im öffentlichen Interesse liegen kann. Eine in diesem Sinne im öffentlichen Interesse vorgenommene Datenverarbeitung muss dem Grunde nach der Gemeinschaft dienen, was etwa bejaht werden kann, wenn die Datenverarbeitung zur Wahrung der Freiheitsrechte, der Durchsetzung der Rechtsstaatlichkeit, der Forschung und wissenschaftlichen Erkenntnis, der Wahrung der Gleichheit oder der Sicherung der öffentlichen Gesundheit und Fürsorge erfolgt.[21] Das Interesse eines Privatunternehmens an der Entwicklung eines KI-Systems mit Gewinnerzielungsabsicht dürfte für sich genommen zumeist kein erhebliches öffentliches Interesse darstellen, mag aber zumindest als ein Faktor im Rahmen einer Gesamtbetrachtung eine Rolle spielen. Zudem kann gegebenenfalls die Entwicklung eines Open-Source-Modells im öffentlichen Interesse liegen und daher zu berücksichtigen sein. Nach der Ausnahmevorschrift des Art. 53 Abs. 2 KI-VO müssen Anbieter von Open-Source-GPAI-Modellen zudem nicht die Pflichten aus Abs. 1 erfüllen.

3. Art. 9 Abs. 2 lit. j) DS-GVO („archivarische, wissenschaftliche und statistische Zwecke")

Eine ausnahmsweise Zulässigkeit der Verarbeitung von sensiblen personenbezogenen Daten wird schließlich auch nicht auf Grundlage von Art. 9 Abs. 2 lit. j) DS-GVO unter dem Gesichtspunkt der wissenschaftlichen Forschung in Betracht kommen. Nach Maßgabe von ErwG 159 DS-GVO soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken weit ausgelegt werden und beispielsweise eine Verarbeitung für die technologische Entwicklung und die privat finanzierte Forschung einschließen. Eine Forschungsaktivität im Zusammenhang mit der KI-Entwicklung kann demnach zwar im Ausgangspunkt unter das Forschungsprivileg fallen. Das Forschungsprivileg muss aber dahingehend eingeschränkt werden, dass solche Forschungstätigkeiten, die einem rein wirtschaftlichen Zweck untergeordnet sind, von dem Ausnahmetatbestand auszunehmen sind.[22]

Im vorliegend zu beurteilenden Sachverhalt der von Meta beabsichtigten Verarbeitung von sensiblen personenbezogenen Daten zur Entwicklung und Verbesserung eigener KI-Systeme dürfte die mit Gewinnerzielungsabsicht betriebene Entwicklungstätigkeit einem primären wirtschaftlichen Zweck unterzuordnen sein und somit nicht unter das Forschungsprivileg fallen.

Jedenfalls aber erfordert auch dieser Ausnahmebestand das Vorhandensein einer Grundlage im Unionsrecht bzw. im Recht der Mitgliedstaaten, wobei eine solche spezifische Rechtsvorschrift nicht ersichtlich ist.

IV. Lösungsansatz des OLG Köln

Das OLG Köln bejahte zwar zunächst die Eröffnung des Anwendungsbereichs von Art. 9 Abs. 1 DS-GVO und lehnte eine Subsumtion der in Rede stehenden Datenverarbeitungen unter den Ausnahmetatbestand des Art. 9 Abs. 2 lit. e) DS-GVO ab. Im Anschluss kam der erkennende Senat aber gleichwohl zur Ablehnung eines Verarbeitungsverbots nach Maßgabe von Art. 9 Abs. 1 DS-GVO (vorbehaltlich einer Art. 267 AEUV-Vorlage an den EuGH) mit der – dogmatisch nachfolgend zu hinterfragenden – Begründung, wonach ein Verarbeitungsverbot im konkreten Einzelfall einer „Aktivierung" in Form eines Antrags der betroffenen Person auf Herausnahme ihrer Daten aus dem Trainingsdatensatz bedürfe.

1. Zwar: Keine gänzliche teleologische Reduktion von Art. 9 Abs. 1 DS-GVO

Zwar verneinte das OLG Köln in einem ersten Schritt unter Berufung auf die Judikatur des EuGH eine das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO gänzlich ausschließende teleologische Reduktion. Eine solche teleologische Reduktion komme, so das OLG Köln, auch dann nicht in Betracht, wenn der Zweck der Verarbeitung – wie im vorliegenden Fall – gerade nicht darin liege, in identifizierbarer Weise „sensible" Informationen zu erlangen bzw. zu verarbeiten.[23] Dabei rekurrierte der erkennende Senat auf die Rechtsprechung des EuGH zu personalisierter Werbung und zur Verarbeitung von Nutzerdaten im Rahmen der Bestellung apothekenpflichtiger Medikamente auf Onlineplattformen.[24] In diesen Urteilen hat der EuGH klargestellt, dass es für die Anwendbarkeit von Art. 9 Abs. 1 DS-GVO gerade nicht darauf ankommen soll, ob der Verantwortliche mit dem Ziel handele, Informationen zu erhalten, die unter die sensiblen Datenkategorien aus Art. 9 Abs. 1 DS-GVO fallen.[25]

2. Aber: Antragserfordernis als ungeschriebenes Tatbestandsmerkmal

Das OLG Köln bejahte schließlich im Wege einer „tätigkeitsbezogenen Reduktion" unter Einführung eines Antragserfordernisses – wohl – als ungeschriebenes Tatbestandsmerkmal die datenschutzrechtliche Vereinbarkeit des Vorhabens mit Art. 9 DS-GVO.

In einem ersten Schritt lehnte das Gericht hierzu eine hinreichende Vergleichbarkeit des zugrunde liegenden Sachverhalts mit den vorstehend bereits in Bezug genommenen, vom EuGH entschiedenen Sachverhalten zur per-

19 So auch Paal/Pauly/Frenzel, DS-GVO, 3. Aufl., 2021, Art. 9 Rn. 38; Gola/Heckmann/Schulz, DS-GVO, 3. Aufl., 2022, Art. 9 Rn. 37; Ehmann/Selmayr/Schiff, DS-GVO, 3. Aufl., 2024, Art. 9 Rn. 52; BeckOK/Albers/Veit, Datenschutzrecht, 52. Edition, Stand: 01.05.2025, Art. 9 Rn. 86; aA wohl EuGH, NJW 2019, 3503, 3507 Rn. 66, entgegen dem (klaren) Wortlaut der Norm keine weitere gesetzliche Konkretisierung für erforderlich haltend.

20 Siehe dazu sogleich unter V. 3.

21 Vgl. Kühling/Buchner/Weichert, DS-GVO, 4. Aufl., 2024, Art. 9 Rn. 90.

22 Vgl. hierzu Kühling/Buchner/Weichert, 4. Aufl., 2024, Art. 9 Rn. 129.

23 OLG Köln, RDV 2025, 262, 269 Rn. 117.

24 EuGH, GRUR 2023, 1131 – Meta Platforms ua (Facebook Ireland); GRUR 2025, 1721, 1727 – Lindenapotheke.

25 EuGH, GRUR 2023, 1131 Rn. 69 – Meta Platforms ua (Facebook Ireland); EuGH, GRUR 2025, 1721, 1727 Rn. 87 – Lindenapotheke.

sonalisierten Werbung und zu Medikamentenbestellungen auf Onlineplattformen ab.[26] Dieses Vorgehen ermöglichte es, in einem zweiten Schritt die vom EuGH für Suchmaschinenbetreiber entwickelte Rechtsprechung zur tätigkeitsbezogenen Reduktion des Art. 9 Abs. 1 DS-GVO auf den Streitfall zu übertragen.[27]

Für Suchmaschinenbetreiber hat der EuGH entschieden, dass tätigkeitsbezogene Besonderheiten des Geschäftsmodells zwar keine vollständige Freistellung von dem Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO rechtfertigen; diese Besonderheiten sollen sich jedoch auf den Umfang der Verantwortlichkeit und konkreten Verpflichtungen des Suchmaschinenbetreibers im Hinblick auf diese Bestimmungen auswirken können.[28] Eine solche Einschränkung in Gestalt eines Antragserfordernisses auf Grundlage tätigkeitsbezogener Besonderheiten sah der erkennende Senat für die streitgegenständliche Datenverarbeitung zum Zwecke des KI-Trainings als gegeben an.[29]

Zur Stützung dieses Arguments verwies das OLG Köln auf den Willen des Unionsgesetzgebers, der mit Erlass der KI-Verordnung das klare Ziel artikuliert habe, wonach Europa bei der KI-Entwicklung eine Vorreiterrolle einnehmen solle.[30] Dabei sei zutreffend erkannt worden, dass für ein effektives KI-Training eine Verarbeitung von „großen Massen an Daten" erforderlich und hierbei auch sensible Daten im Sinne des Art. 9 DS-GVO betroffen sein würde(n).[31] Aus der Regelung des Art. 10 Abs. 5 der KI-VO, die eine Rechtsgrundlage für den zielgerichteten Einsatz von Daten im Sinne des Art. 9 DS-GVO beim Training von Hochrisiko-KI schafft, schloß das OLG Köln im Umkehrschluss, dass der Gesetzgeber für eine nicht zielgerichtete Datenverarbeitung zum Zwecke des KI-Trainings keinen Regelungsbedarf gesehen habe.[32] Daraus ergebe sich, dass der Gesetzgeber nicht von einer entsprechenden Unmöglichkeit oder grundsätzlichen Rechtswidrigkeit einer nicht zielgerichteten Verarbeitung von Daten im Sinne des Art. 9 DS-GVO zum Zweck des KI-Trainings ausgegangen sei.[33]

3. Bewertung und Stellungnahme

Der durch das OLG Köln unter hohem Zeitdruck in einem summarischen Verfahren im einstweiligen Rechtsschutz entwickelte Lösungsansatz ist nachfolgend kritisch zu hinterfragen.

a) Wortlaut

Zunächst ist hervorzuheben, dass sich dem Wortlaut des Art. 9 DS-GVO kein Antragserfordernis als ungeschriebenes Tatbestandsmerkmal für die „Aktivierung" des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO entnehmen lässt.

b) Systematik: Objektiver Verbotstatbestand vs. Betroffenenrecht

Weiterhin ist anzumerken, dass durch die Einführung eines Antragserfordernisses der betroffenen Person als ungeschriebenes Tatbestandsmerkmal für die „Aktivierung" des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO ein rechtsdogmatisch objektiv ausgestaltetes Verarbeitungsverbot in potenziell systemwidriger Weise zu einem subjektiven Betroffenenrecht umgedeutet wird.

Denn Art. 9 Abs. 1 DS-GVO enthält – vergleichbar zu Art. 6 Abs. 1 DS-GVO – ein grundsätzliches und objektives Verarbeitungsverbot mit Erlaubnisvorbehalt nach Maßgabe der der in Abs. 2 der Norm niedergelegten Ausnahmetatbestände.[34] Dabei ist das in Art. 9 Abs. 1 DS-GVO geregelte objektive Verarbeitungsverbot in Abgrenzung zu sehen zu den – in Kapitel III der DS-GVO verorteten – subjektiven Betroffenenrechten, die mit Ausnahme der Informationspflichten regelmäßig einen Antrag oder ein Verlangen der betroffenen Person voraussetzen.[35]

Ein solches Antragserfordernis ist den von der DS-GVO vorgesehenen objektiven Verarbeitungsverboten grundsätzlich fremd und droht somit zu einer systemwidrigen Umdeutung des Verarbeitungsverbots zu einem subjektiven Betroffenenrecht zu führen.

c) Übertragbarkeit der Antragslösung auf KI-Trainings-Konstellationen

Schließlich ist zu (hinter-)fragen, ob und inwieweit die unter Rekurs auf die Ausführungen des EuGH vom OLG Köln entwickelte Antragslösung auf KI-Trainingsdatensätze praktikabel zur Anwendung gebracht werden kann. Denn eine hinreichende Vergleichbarkeit von Datenverarbeitungen durch Suchmaschinenbetreiber einerseits und zum Zwecke von KI-Training andererseits trifft auf mehrere Hürden: Zunächst werden bei lebensnaher Betrachtung die betroffenen Personen bei drittbezogenen Daten regelmäßig bereits keine Kenntnis von der Verarbeitung ihrer sensiblen Daten zum Zwecke des KI-Trainings haben. Die Aktivierung eines Betroffenenantrags setzt jedoch zwingend voraus, dass die betroffenen Personen von der Datenverarbeitung im konkreten Fall Kenntnis erlangen.

Der Entscheidung des EuGH hinsichtlich der Suchmaschinenbetreiber liegt mit Blick auf die Möglichkeit der Kenntniserlangung der Betroffenen von der Datenverarbeitung ein gänzlich anders gelagerter Sachverhalt zugrunde, da den betroffenen Personen im Anschluss an eine Suchanfrage die relevanten Daten in der Ergebnisliste der Suchmaschine angezeigt werden. Dementsprechend führten im betreffenden EuGH-Verfahren gerade erst (abgelehnte) Auslistungsersuchen betroffener Personen gegen den Suchmaschinenbetreiber zu einem gerichtlichen Verfahren. Dem Verfahren voraus gingen also Suchanfragen der betroffenen Personen und die Auffindbarkeit entsprechender Suchein-

26 OLG Köln, RDV 2025, 262, 269 Rn. 119.

27 OLG Köln, RDV 2025, 262, 269 Rn. 118.

28 EuGH, NJW 2019, 3503, 3507 Rn. 45 ff.

29 OLG Köln, RDV 2025, 262, 269 Rn. 121.

30 OLG Köln, RDV 2025, 262, 269 Rn. 119 unter Verweis auf ErwG 8 der KI-VO.

31 OLG Köln, RDV 2025, 262, 269 Rn. 120 unter Verweis auf ErwG 105 der KI-VO.

32 OLG Köln, RDV 2025, 262, 269 Rn. 120.

33 OLG Köln, RDV 2025, 262, 269 Rn. 120.

34 Vgl. BeckOK/Albers/Veit, DS-GVO, 52. Edition, Stand: 01.05.2025, Art. 9 Rn. 49; Ehmann/Selmayr/Schiff, DS-GVO, 3. Aufl., 2024, Art. 9 Rn. 9; Gola/Heckmann/Schulz, DS-GVO, 3. Aufl., 2022, Art. 9 Rn. 4; Kühling/Buchner/Weichert, DS-GVO, 4. Aufl., 2024, Art. 9 Rn. 7.

35 Unter anderem setzen die Betroffenenrechte (i.e. Art. 15 ff. DS-GVO) grundsätzlich einen vorherigen Antrag bzw. ein vorheriges Verlangen des Betroffenen voraus.

träge, sprich eine Möglichkeit zur Kenntnisnahme und der Stellung eines Auslistungsantrags. Eine solche Suchanfrage steht den betroffenen Personen bei einem KI-Trainingsdatensatz aber nicht zur Verfügung. Hervorzuheben ist, dass dieser Befund eine Privilegierung von Datenverarbeitungen im Zusammenhang mit KI-Entwicklungen nicht ausschließt, wenn insoweit eine andere belastbare(re) Rechtsgrundlage gefunden wird.[36]

Ferner steht einer Vergleichbarkeit entgegen, dass eine nachträgliche Löschung der sensiblen Nutzerdaten aus einer bereits trainierten KI – anders als bei Suchmaschinenbetreibern durch einfaches Auslisten[37] – jedenfalls nach dem aktuellen Stand von Technik und Wissenschaft nicht oder allenfalls sehr eingeschränkt möglich ist. Im Zuge des KI-Trainings kommt es dabei zu einer verstetigten Einbettung der Trainingsdaten in das Daten- und Verhaltensmuster des KI-Algorithmus.[38] Diese technische Besonderheit von KI-Algorithmen ist vor allem im Zusammenhang mit der Gefahr sog. Model Inversion Attacks zu betrachten. Dabei handelt es sich um Reverse Engineering-Technologien, mit denen auf der Output-Ebene die sensiblen Trainingsdaten rekonstruiert und offengelegt werden können.[39]

Das OLG Köln erkennt die Problematik der nur eingeschränkten Löschmöglichkeit von KI-Trainingsdaten, hält sie im Ergebnis jedoch für unbeachtlich.[40] Zur Begründung wird insoweit verwiesen auf die „festgestellten nur geringen Gefahren einer konkreten Schädigung der Betroffenen durch die weitere Verarbeitung der bereits öffentlichen Daten".[41]

V. Alternative Lösungsansätze und Überlegungen

In Ansehung der bisherigen Ausführungen und Erwägungen soll nunmehr dem Gedanken einer teleologischen Reduktion des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO erneut nähergetreten werden.

1. Keine pauschale Absage des EuGH an eine teleologische Reduktion

Die durch das OLG Köln vorgenommene pauschale Absage an eine teleologische Reduktion von Art. 9 Abs. 1 DS-GVO im Hinblick auf das KI-Training unter Bezugnahme auf die EuGH-Rechtsprechung zur personalisierten Werbung und zu Medikamentenbestellungen auf Onlineplattformen vermag nicht vollumfänglich zu überzeugen.

Der EuGH hat in den beiden Urteilen – anders als vom OLG Köln unzutreffend unterstellt – bereits gar nicht über die Möglichkeit einer teleologischen Reduktion entschieden, sondern vielmehr nur Art. 9 DS-GVO dahingehend ausgelegt, ob die Vorschrift ein subjektives Element (i.e. Finalität) voraussetzt.[42] Hieraus wird sich gerade nicht ableiten lassen, dass eine teleologische Reduktion des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO insgesamt ausgeschlossen ist. Vielmehr sind die einschlägigen Ausführungen des EuGH lediglich dahingehend zu verstehen, dass die Nicht-Zielgerichtetheit einer Verarbeitung und Analyse von sensiblen personenbezogenen Daten für sich genommen (noch) nicht ausreicht, um eine teleologische Reduktion zu begründen.

Soweit das OLG Köln die EuGH-Rechtsprechung darüber hinausgehend als pauschale Absage an eine teleologische Reduktion versteht, ist dem erkennenden Senat nicht zu folgen. Denn eine solche teleologische Reduktion muss für das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO nach den allgemeinen Grundsätzen der juristischen Methodenlehre weiterhin grundsätzlich möglich sein,[43] wenn und soweit die entsprechenden Voraussetzungen vorliegen.

Überdies mangelt es, wie auch das OLG Köln selbst zutreffend festgestellt hat, an einer hinreichenden normativen und strukturellen Vergleichbarkeit der den EuGH-Entscheidungen zugrunde liegenden Sachverhalten mit der vorliegend untersuchungsgegenständlichen Konstellation des KI-Trainings.[44]

2. Teleologische Reduktion von Art. 9 Abs. 1 DS-GVO für KI-Training

Das Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO beruht nach seinem Sinn und Zweck auf der erhöhten Schutzbedürftigkeit solcher Datenkategorien, denen aufgrund ihrer höchstpersönlichen Natur und ihrem identitätsstiftenden Charakter ein erhöhtes Missbrauchs-, Schadens- und Diskriminierungspotenzial zukommt.[45] In Ansehung dieser abstrakt-generellen Zweckwürdigung der Norm sollte eine korrigierende schutzbedarfsgerechte teleologische Reduktion immer dann in Betracht gezogen werden, wenn ein erhöhtes Missbrauchs-, Schadens- und Diskriminierungspotenzial im Wege einer umfassenden Gesamtwürdigung aller Umstände des konkreten Einzelfalls für die in Rede stehende Datenverarbeitung ausgeschlossen werden kann.[46] An den Ausschluss des spezifischen Missbrauchs-, Schadens- und Diskriminierungspotenzials dürfen hierbei unter Berücksichtigung des risikobasierten Ansatzes der DS-GVO keine unerfüllbaren Anforderungen gestellt werden.[47]

Vor diesem Hintergrund sprechen gewichtige Erwägungen für eine teleologische Reduktion des Art. 9 Abs. 1 DS-GVO betreffend Datenverarbeitungen zum Zwecke des KI-Trainings: Wie auch das OLG Köln richtigerweise festgestellt hat, werden die personenbezogenen Daten für das KI Training zu allgemeinen Mustern für statistische Wahr-

36 Siehe hierzu sogleich unter V.

37 Vgl. Simitis/Hornung/Spiecker gen. Döhmann/Dix, DS-GVO, 2. Aufl., 2025, Art. 9 Rn. 23 ff. mit ausführlicher Diskussion zu EuGH, NJW 2014, 2257 – Google Spain.

38 Vgl. Kindshofer, ZD 2024, 673, 677.

39 Vgl. Paal, ZfDR 2024, 129, 152 f. m.w.N.

40 OLG Köln, RDV 2025, 262, 269 Rn. 121.

41 OLG Köln, RDV 2025, 262, 270 Rn. 121.

42 EuGH, GRUR 2023, 1131 Rn. 69 – Meta Platforms ua (Facebook Ireland); EuGH, GRUR 2025, 1721, 1727 Rn. 87 – Lindenapotheke.

43 Vgl. zu dem Stellenwert des Normzwecks in der Methodenlehre und der teleologischen Reduktion als selbstverständlich anerkanntes methodisches Instrument etwa Grigoleit, in: FS Claus-Wilhelm Canaris, Privatrechtsdogmatik im 21. Jahrhundert, Dogmatik – Methodik – Teleologik, 2017, S. 241 ff.

44 OLG Köln, RDV 2025, 262, 269 Rn. 119.

45 Vgl. Kühling/Buchner/Weichert, DS-GVO, 4. Aufl., 2024, Art. 9 Rn. 17; Paal/Pauly/Frenzel, DS-GVO, 3. Aufl., 2021, Art. 9 Rn. 6 m.w.N.

46 Das Erfordernis einer schutzbedarfsgerechten, kontextabhängigen teleologischen Reduktion wird in der Literatur überwiegend bejaht, vgl. BeckOK/Albers/Veit, DS-GVO, 52. Edition, Stand: 01.05.2025, Art. 9 Rn. 21; Paal/Pauly/Frenzel, DS-GVO, 3. Aufl., 2021, Art. 9 Rn. 6 ff.; Gola/Heckmann/Schulz, DS-GVO, 3. Aufl., 2022, Art. 9 Rn. 13.

47 Ausführlich zum risikobasierten Ansatz in der DS-GVO Schröder, ZD 2019, 503; Jungkind/Koch, ZD 2022, 656.

scheinlichkeitsberechnungen abstrahiert.[48] Eine Profilbildung auf Grundlage der in Art. 9 Abs. 1 DS-GVO genannten besonders schutzwürdigen Kategorien soll hiernach gerade nicht erfolgen.[49] Für die Risikobewertung ist zudem relevant, ob der Datensatz etwa dem Training einer KI mit allgemeinem Verwendungszweck (General Purpose AI, GPAI) dienen soll oder für ein fachspezifisches KI-Modell bzw. -System (beispielsweise im medizinischen Bereich) konzipiert ist. Falls es sich um eine GPAI handelt, wird das spezifische Missbrauchs-, Schadens- und Diskriminierungsrisiko auf Grundlage einer besonders schutzwürdigen Datenkategorie durch das KI-System für die betroffenen Personen grundsätzlich niedriger einzustufen sein. Überdies sollten auch besondere technische Schutzmaßnahmen, wie beispielsweise die Einrichtung von Output-Filtern, positiv in die Gesamtbetrachtung einfließen.

3. Aktivierung des risikobasierten Ansatzes der DS-GVO

Der Gedanke einer teleologischen Reduktion des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO findet zudem eine systematische Stütze im risikobasierten Ansatz der DS-GVO, der sich auch und gerade in Art. 24 DS-GVO manifestiert. Bereits in den ErwG 75 f. DS-GVO wird zudem ausdrücklich betont, dass das Ausmaß und die Eintrittswahrscheinlichkeit der mit der Verarbeitung verbundenen Risiken relevante Faktoren bei der Anwendung der DS-GVO sind. Die DS-GVO verfolgt insoweit im Einklang mit Art. 8 GRCh keine formale, sondern eine materielle Perspektive: Entscheidend ist somit nach dem Sinn und Zweck nicht allein die abstrakte Datenkategorie, sondern die konkrete Gefährdungslage für die Rechte und Freiheiten der betroffenen Personen.

Bei KI-Trainingsvorhaben, die – wie auch im Falle von Meta – nicht auf die gezielte Auswertung sensibler Informationen zur Individualprofilierung, sondern vielmehr auf die Entwicklung allgemeiner Sprachmodelle gerichtet sind, lässt sich ein spezifisches, relevantes Missbrauchs-, Diskriminierungs- oder Schadensrisiko im Sinne von Art. 9 Abs. 1 DS-GVO regelmäßig nicht feststellen. In einer solchen Konstellation erscheint es – unter Wahrung der systematischen Trennung von Erlaubnistatbeständen und Betroffenenrechten – daher sachgerecht, den Anwendungsbereich des Verarbeitungsverbots im Wege einer zweckorientierten Auslegung durch teleologische Reduktion zu begrenzen.

Dies gilt umso mehr, als die Einführung eines generellen Verbots auch für risikominimierte Verarbeitungen dazu führen würde, dass der Schutzmechanismus der DS-GVO nicht mehr verhältnismäßig, sondern vielmehr überdehnt zur Anwendung zu kommen droht. Der risikobasierte Ansatz der DS-GVO verlangt nach alledem, (auch) die dogmatische Konstruktion von Art. 9 Abs. 1 DS-GVO so zur Anwendung zu bringen, dass der Zweck der Norm – sprich der Schutz vor spezifischen Gefährdungen – nicht zu einer pauschalen Blockade risikoadjustierter Verarbeitungsmodelle fehlgeleitet wird.

4. Analoge Anwendung von Art. 10 Abs. 5 S. 1 KI-VO auf nicht zielgerichtete Datenverarbeitung zum Zwecke des KI-Trainings

Die datenschutzrechtliche Zulässigkeit der Verarbeitung sensibler Daten im Sinne des Art. 9 Abs. 1 DS-GVO zum Zwecke des KI-Trainings könnte ferner in Betracht kommen im Zuge einer analogen Anwendung des vom OLG Köln thematisierten Erlaubnistatbestands aus Art. 10 Abs. 5 S. 1 KI-VO auf nicht zielgerichtete Datenverarbeitungen aufgrund einer planwidrigen Regelungslücke und einer vergleichbaren Interessenlage.

Mit Art. 10 Abs. 5 S. 1 KI-VO hat der EU-Gesetzgeber von der Möglichkeit einer unionsrechtlichen Rechtfertigung der Verarbeitung sensibler Daten nach Art. 9 Abs. 1 lit. g) DS-GVO Gebrauch gemacht und einen entsprechenden Erlaubnistatbestand geschaffen.[50] Konkret ermöglicht Art. 10 Abs. 5 KI-VO unter engen Voraussetzungen die zielgerichtete Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO, soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist.[51] Hierbei zeigt der Umkehrschluss aus Art. 10 Abs. 6 KI-VO, dass diese Fehlerkorrektur vor allem das Training des zugrunde liegenden KI-Modells betrifft und die Vorschrift daher Implikationen auch für KI-Modelle (mit allgemeinem Verwendungszweck), also über den späteren Einsatz als Hochrisiko-KI-System hinaus haben könnte.

Eine planwidrige Regelungslücke könnte insoweit darauf gestützt werden, dass Art. 10 Abs. 5 KI-VO lediglich eine zielgerichtete Verarbeitung von besonderen Kategorien personenbezogener Daten bei Hochrisiko-KI-Systemen erlaubt, eine solche Regelung jedoch fehlt für die nicht zielgerichtete, aber mangels Vermeidbarkeit erforderliche Verarbeitung bei KI-Systemen, die keine Hochrisiko-KI-Systeme sind. Zugleich ist insoweit zu berücksichtigen, dass der europäische Gesetzgeber das Phänomen gekannt und erkannt haben dürfte – und Art. 10 Abs. 5 KI-VO vor diesem Hintergrund hätte (deutlich) ausbauen können.

Für das Vorliegen einer vergleichbaren Interessenlage mag angeführt werden, dass der Gesetzgeber mit Art. 10 Abs. 5 S. 1 KI-VO gerade Möglichkeiten zur Sicherstellung der Datenqualität im Hinblick auf ein KI-Modell eröffnet, welches in einem Hochrisiko-KI-System zum Einsatz kommt. Das gleicht dem Fall, dass ohne die beiläufige, nicht zielgerichtete Verarbeitung besonderer Kategorien personenbezogener Daten mangels verfügbarer oder praktikabel zusammenstellbarer Datensätze ein entsprechender Qualitätsstandard nicht sichergestellt werden kann (und erhebliche Verzerrungen denkbar sind). Dieses Bedürfnis an „riesigen Mengen an Text, Bildern, Videos und anderen Daten" zum Training eines KI-Modells mit allgemeinem Verwendungszweck erkennt der europäische Gesetzgeber aber gerade in ErwG 105 S. 2 KI-VO an.[52]

In Ansehung des engen Bezugs zum Training eines (jeden) KI-Modells und dem ebenfalls gebotenen Qualitätsstandard könnte dies auch für KI-Modelle mit allgemeinem Verwendungszweck und unabhängig davon gelten, ob die-

48 Vgl. OLG Köln, RDV 2025, 262, 270 Rn. 122.

49 Vgl. OLG Köln, RDV 2025, 262, 270 Rn. 122.

50 Vgl. Martini/Wendehorst/Braun Binder/Egli, KI-VO, 2024, Art. 10 Rn. 80.

51 Ausführlich zu den Voraussetzungen einer ausnahmsweisen Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 10 V KI-VO Martini/Wendehorst/Braun Binder/Egli, KI-VO, 2024, Art. 10 Rn. 81 ff.

52 S. hierzu auch OLG Köln, RDV, 262, 269 – Rn. 120.

se später in ein Hochrisiko-KI-System integriert werden. Hier stellt sich sodann die Frage, weshalb für die – einer nachträglichen Korrektur denklogisch vorgelagerten – originäre Zusammenstellung des Trainingsdatensatzes eine Verarbeitung sensibler personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO nicht unter bestimmten Voraussetzungen zulässig sein sollte, wenn der Gesetzgeber mit Art. 10 Abs. 5 S. 1 KI-VO die nachträgliche Korrektur von Verzerrungen durch eine Verarbeitung von sensiblen personenbezogenen Daten ermöglicht.

Insgesamt bleibt abzuwarten, wie sich die Diskussion zur Frage der analogen Anwendung von Art. 10 Abs. 5 S. 1 KI-VO auf nicht zielgerichtete Datenverarbeitung zum Zwecke des KI-Trainings entwickelt. Eine belastbar rechtssichere Klärung wird nur durch den EuGH im Wege eines Art. 267 AEUV-Vorlageverfahrens erfolgen können.

VI. Gesamtergebnis und Ausblick

Die den Ausgangspunkt dieser Abhandlung bildende Eilverfahrens-Entscheidung des OLG Köln vom 23.05.2025 verdient besondere Beachtung, da sie sich einer komplexen, höchst praxisrelevanten und bislang kaum geklärten datenschutzrechtlichen Problematik widmet. Der rechtlichen Zulässigkeit der Verarbeitung von sensiblen personenbezogenen Daten für das Training von KI-Technologien auf der Grundlage und am Maßstab von Art. 9 DS-GVO kommt hierbei hervorgehobene Bedeutung zu. Das Gericht hat zutreffend erkannt, dass im Spannungsfeld zwischen dem technologischen Entwicklungsdruck im Bereich KI und dem hohen Schutzniveau der Datenschutz-Grundverordnung eine rechtliche Klärung erforderlich ist, die im Sinne von Verhältnismäßigkeit und schonendem Grundrechtsausgleich den verschiedenen betroffenen Interessen angemessen Rechnung trägt.

Der Lösungsansatz des Senats, nicht pauschal ein Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO anzunehmen, sondern den Sachverhalt im Lichte der tätigkeitsbezogenen Besonderheiten bei der KI-Entwicklung differenziert zu würdigen, offenbart strukturelle Klärungsnotwendigkeiten des geltenden Datenschutzrechts im Umgang mit innovativen Technologien wie KI. Vor diesem Hintergrund erscheint eine richtungsweisende Klärung durch den EuGH geboten – und gegebenenfalls darüber hinaus auch ein gesetzgeberisches Tätigwerden. Die vom OLG Köln bereits in Aussicht gestellte Vorlage im Hauptsacheverfahren gemäß Art. 267 AEUV könnte daher zu einer grundsätzlichen Weichenstellung für die datenschutzrechtliche Behandlung von KI-Trainingsdaten führen. Hierbei wird es insbesondere darauf ankommen, wie sich der EuGH zu einer teleologischen Reduktion des Verarbeitungsverbots nach Art. 9 Abs. 1 DS-GVO im KI-(Trainings-)Kontext sowie der Reichweite von Öffnungsklauseln wie Art. 10 Abs. 5 KI-VO verhält. Für die Praxis wäre eine solche Klärung von erheblichem Wert, um sowohl Anbietern als auch Betroffenen (mehr) Rechtssicherheit im Umgang mit sensiblen personenbezogenen Daten im Rahmen von KI-Prozessen zu verschaffen.

Klar ist bereits jetzt: Die Thematik der datenschutzrechtlichen Beurteilung des KI-Trainings und -Einsatzes wird eines der zentralen Themen der kommenden Jahre bleiben. In diesem Sinne markiert das Urteil des OLG Köln einen ersten Schritt auf dem Weg zu ausgewogenen rechtlichen Lösungen, die sowohl Datenschutz gewährleisten als auch Innovation ermöglichen. Ein wesentliches übergreifendes Ziel muss es sein, eine belastbare und rechtssichere Privilegierung (auch) für die Entwickler und das Training von KI-Technologien im europäischen Raum zu schaffen.

Prof. Dr. Boris P. Paal, M.Jur.
ist Inhaber des Lehrstuhls für Law and Regulation of the Digital Transformation, Technische Universität München (TUM), und Of Counsel bei Baumgartner Baumann.

Datenschutz-Awareness stärken

Interaktive E-Learning-Kurse mit echtem Menschen als Trainer

Unsere E-Learning-Kurse:

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

Jetzt kostenfrei testen:
elearning-mit-zertifikat.de

UNIVADO

DATAKONTEXT

Dr. Stefan Brink/Lea Brink

Data Act – ein Akt, lauter Probleme

Der EU Data Act steht an. Die EU-Verordnung „über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung" (VO (EU) 2023/2854 – DA), Teil der europäischen Datenstrategie[1], ist am 11. Januar 2024 in Kraft getreten, ihr Geltungsbeginn steht mit dem 12. September 2025 unmittelbar bevor.

Allgemeine Zielsetzung des Data Acts ist die Verbesserung der Informationsversorgung der Wirtschaft, auch die digitale Transformation und die „Innovation durch Daten" sollen gefördert werden.[2] Hintergrund des Data Acts ist die Erkenntnis der EU-Kommission, dass in Zeiten der datengetriebenen Wirtschaft die Europäische Union im internationalen Wettbewerb um innovative Produkte und Dienstleistungsangebote für die sich formierende Informationsgesellschaft gegenüber Anbietern aus den USA, China und Indien zurückzufallen droht – ja die EU in vielen strategisch wichtigen Marktsektoren wie der Künstlichen Intelligenz oder des Internet-Marketing zum fremdbestimmten und abhängigen Konsumenten verzwergt. Dem soll durch eine nachdrückliche Ankurbelung des Datennutzens und Datenteilens begegnet werden – letztlich soll mehr „Daten-Traffic" zu mehr Produktivität der europäischen Wirtschaft führen.

Anders als etwa die Europäische Datenschutz-Grundverordnung (DS-GVO), welche als öffentlich-rechtliche Regulierung mit den Mitteln der hoheitlichen Rechtsgestaltung bis hin zu eigenständigen Sanktionensystemen agiert, bedient sich der Data Act privatrechtlicher Instrumente zur Erreichung seiner regulatorischen Ziele und wird so zu einem zentralen Baustein eines „europarechtlichen Privatrechts der Datenökonomie".[3] Über das Vehikel der lenkenden Vertragsgestaltung behandelt der Data Act also die zentralen Fragen der Datenwirtschaft – vom Datenzugang über die Datennutzung bis hin zur Datenteilung im multipolaren Rechtsverhältnis von Dateninhaber, möglichen Datennutzern und -empfängern.[4] Dadurch sind vom Data Act Unternehmen genauso wie Behörden und Verbraucher betroffen – sei es als Hersteller von IoT-Geräten, als Datenzugang begehrende öffentliche Stelle oder als Person, die Cloud-Services gewerblich oder privat anbietet bzw. nutzt.[5] Dies lässt nicht nur eine enorme Relevanz und Durchschlagskraft des Data Acts erwarten, sondern verdeutlicht auch, wie anspruchsvoll die regulatorische Aufgabe ist, der sich der europäische Gesetzgeber hier stellt.

I. Problematiken Data Act

Je anspruchsvoller die Aufgabe, desto besser sollte sie vorbereitet und umso umsichtiger sollte sie erfüllt werden. Schon hier zeigen sich beim Data Act allerdings erste Probleme:

1. Kurzer Gesetzgebungsprozess

Der Gesetzgebungsprozess des Data Acts war ein bemerkenswert kurzer: Grundstein des Data Acts ist die Datenstrategie der EU-Kommission vom Februar 2020 mit dem formulierten Ziel, einen sektorübergreifenden Rechtsrahmen für Datenzugang und Datennutzung zu schaffen.[6] Im Februar 2022 folgte dann bereits der konkrete Vorschlag des Data Acts durch die EU-Kommission, woraufhin das Europäische Parlament und der Rat 2023 ihre Änderungsvorschläge vorlegten. Bereits Ende Juni 2023 wurde im Trilog-Verfahren ein Kompromiss gefunden und der Data Act im Dezember 2023 verabschiedet.[7] Innerhalb von nur drei Jahren ein solch weitreichendes Gesetzgebungsprojekt zum Abschluss zu führen, zeugt vom unbändigen Regulierungswillen der EU – birgt jedoch die Gefahr von unklaren, lückenhaften oder wenig durchdachten Formulierungen, die im Ergebnis mehr Probleme schaffen als lösen.[8]

2. Knappe Übergangsfristen

Unter Zeitdruck entstand der Data Act nicht nur, er setzt auch seine Adressaten – Hersteller, Nutzer, Empfänger – unter enormen Anpassungsdruck. Hier sticht zunächst die Problematik ins Auge, dass Art. 50 DA für die Implementierung des Regelwerks den Adressaten außergewöhnlich knappe Übergangsfristen setzt.

Nach Art. 50 UAbs. 2 DA gilt der Data Act bereits ab dem 12.09.2025. Damit liegt der Geltungsbeginn drei Jahre nach der Vorlage des ersten Regelungsentwurfs und nur 21 Monate nach dem Inkrafttreten des Data Acts im Januar 2024, womit Adressaten der Verordnung eine nur sehr kurze Vorbereitungszeit gewährt wird, in der die notwendigen Anpassungen und Vorkehrungen getroffen werden müssen. Und dies wohlgemerkt bei einer Regulierung, welche das „europarechtliche Privatrecht der Datenökonomie"[9] grundlegend neu entworfen hat. Das erscheint mehr als sportlich, geradezu gewagt, vielleicht sogar halsbrecherisch.

Hier lohnt ein näherer Blick auf die spezifisch geregelten Übergangsfristen[10]: Spezialregelungen trifft der Data Act für die zeitliche Umsetzung der Vorgaben von Kapitel IV, welche missbräuchliche Vertragsklauseln für den Datenzugang und die Datennutzung zwischen Unternehmen definieren und die betroffenen Akteure vor besondere Schwierigkeiten stellen: Kapitel IV DA gilt ab dem Stichtag des 12.09.2025 für ab die-

1 COM(2020) 66 final.

2 Wiebe, CR 2023, 777; BeckOK DatenschutzR/Brink/v. Ungern-Sternberg, DA Einführung zum Data Act Rn. 1.

3 Sattler, CR 2024, 213, 214.

4 Staudenmeyer, NJW 2024, 1377, 1378.

5 Hennemann/Steinrätter, NJW 2024, 1; Specht/Hennemann, DGA DA Vorwort.

6 Specht/Hennemann/Hennemann, DGA DA, Einleitung Rn. 71.

7 BeckOK DatenschutzR/Brink/v. Ungern-Sternberg, DA Einführung zum Data Act Rn. 3.

8 Insgesamt kritisch Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 488.

9 Sattler, CR 2024, 213, 214.

10 Grundlegend Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 489 ff.

sem Datum geschlossene Verträge (vgl. Art. 50 UAbs. 5 DA). Es gilt ab dem 12.09.2027 sogar rückwirkend, also auch für Verträge, die am oder vor dem 12.09.2025 geschlossen wurden, falls sie unbefristet abgeschlossen wurden oder eine Laufzeit bis mindestens zum 11.01.2034 haben (vgl. Art. 50 UAbs. 6 DA). Solche Rückwirkungsanordnungen des Gesetzgebers verschärfen die Umsetzungsproblematik auf Seiten der Normadressaten natürlich nochmals enorm.

Kapitel IV ist zudem inhaltlich äußerst innovativ, führt es doch in Art. 13 DA eine Inhaltskontrolle von AGB in Verträgen zwischen Unternehmen ein – ein Novum[11] auf europäischer Ebene. Es ist auf sämtliche Datenverträge im unternehmerischen Verkehr anwendbar, womit es einen sehr breiten Anwendungsbereich hat.[12] Art. 13 DA verfolgt das Ziel der Fairness in Datenverträgen (vgl. ErwG 5 S. 5 DA), indem er missbräuchliche Klauseln in Bezug auf Datenzugang und Datennutzung zwischen Unternehmen zu verhindern versucht. Der Kontrollmaßstab der Missbräuchlichkeit richtet sich nach Art. 13 Abs. 3 – 5 DA. Art. 13 Abs. 3 DA enthält eine Generalklausel („große Abweichung von der guten Geschäftspraxis", „Treu und Glauben"), während Art. 13 Abs. 4 und 5 DA Listen stets missbräuchlicher und widerleglich vermuteter missbräuchlicher Klauseln aufstellen.[13]

Art. 13 DA enthält damit nicht nur eine hohe Regulierungsdichte für die Inhaltskontrolle von Verträgen, sondern stellt dafür eine Vielzahl unbestimmter, weder von Gerichten oder Rechtsliteratur vorgeformter Tatbestandsmerkmale in den Raum und versieht Verstöße gegen die Regularien mit massiven vertraglichen Konsequenzen; er greift somit tief in die jeweiligen Vertragsverhältnisse ein.[14]

Trotz dieser intensiven und zeitkritischen Regulierung besteht hier Rechtsunsicherheit nicht nur über die genaue Auslegung der Gesetzesregelungen – die extrem rasche „Gesetzesproduktion" führte zudem zu handwerklichen Problematiken: So wird die deutsche Version von Art. 13 Abs. 3 sprachlich mehrfach als irreführend und abweichend angesehen.[15] Die Anpassungslast für betroffene Unternehmen an das hier kurz beleuchtete Kapitel IV führt damit zu hohen Transaktionskosten und macht eine fristgerechte Umsetzung der Vorgaben zum Stichtag zur kaum zu bewältigenden Belastung.

Umso bedenklicher ist es daher, dass gerade die Vorschriften zur Geltung des Data Acts in Art. 50 DA weitere rechtliche und praktische Probleme aufwerfen, die noch über die vergleichsweise spezifische Regulierung zu Kapitel IV DA hinausgehen. Exemplarisch soll daher betrachtet werden, welche Vorgaben Kapitel VI DA zum Wechsel zwischen Verarbeitungsdiensten macht und wie vertrackt die Gesetzeslage im Bereich der Cloud-Dienstleistungen ab dem 12. September 2025 sein wird.

3. Vorgaben des Kapitels VI und Rückwirkungsproblematik

a) Vorgaben des Kapitels VI

Vor noch größere Herausforderungen als bei Kapitel IV werden Unternehmen bei der Umsetzung der Vorgaben des Kapitels VI gestellt:

Die Art. 23 ff. DA machen detaillierte Vorgaben zum Wechsel zwischen sogenannten Datenverarbeitungsdiensten. In erster Linie betreffen sie Verträge zwischen Kunden und Anbietern von Cloud- und Edge-Diensten.[16] Nutzern soll der Wechsel zwischen verschiedenen Anbietern (sog. „Cloud Switching") durch Anpassung der vertraglichen Grundlagen erleichtert werden. Konkret geht es dem Unionsgesetzgeber darum, es einfacher zu machen, Daten und Anwendungen (von privaten Fotoarchiven bis hin zu kompletten Geschäftsunterlagen) kostenlos von einem Anbieter zu einem anderen zu übertragen und dort bruchlos weiterverarbeiten zu lassen.[17] Dadurch sollen sogenannte „Anbieter-Lock-in-Effekte"[18] bei Kunden verhindert, Marktzutrittsschranken für neue Anbieter abgebaut und letztlich der Wettbewerb angekurbelt werden.[19]

Um dies zu erreichen, machen insbesondere die Art. 23 und 25 DA konkrete Vorgaben zum Inhalt eines Vertrages zwischen dem Diensteanbieter und seinem Kunden.[20] Zentralnorm von Kapitel VI ist Art. 23 S. 2 DA.[21] Danach muss der Alt-Anbieter unter anderem vertragliche Hindernisse beseitigen, die einen effektiven Anbieterwechsel behindern könnten. Er soll alle in seiner Macht stehenden Maßnahmen ergreifen, um die Erreichung von Funktionsäquivalenz beim Anbieterwechsel durch die Bereitstellung von Fähigkeiten, Informationen, Dokumentation und technischer Unterstützung zu erleichtern.[22] Diese Verpflichtung trifft den Anbieter ohne tatbestandliche Einschränkungen – er kann weder technische noch rechtliche noch ökonomische Gründe vorbringen, um die Aufrechterhaltung solcher Hindernisse zu rechtfertigen,[23] was eine äußerst starke Belastung für den Anbieter bedeutet.

Hinzu kommt, dass es sich bei Art. 23 S. 2 DA um eine Generalklausel handelt. Die Pflicht nach Art. 23 S. 2 DA wird also gerade nicht abschließend durch die Vorgaben der Art. 25, 26, 27, 29 und 30 DA ausgefüllt, sondern den Anbieter können darüberhinausgehende Pflichten treffen.[24] Die unklare Weite der Verpflichtung führt zu erheblicher Rechtsunsicherheit aufseiten des Anbieters.

Neben Art. 23 S. 2 greift auch Art. 25 Abs. 2 DA tiefgehend in die privatautonome Vertragsgestaltung ein, indem er zahlreiche Mindestanforderungen an den Vertragsinhalt, die sich spezifisch auf das Recht zum Anbieterwechsel und auf den Wechselprozess beziehen[25], gesetzlich vorschreibt. Diese Gestaltungsvorgaben haben massive Auswirkungen für die Konzeption von Cloud-AGB.[26] Sie bringen den Kunden zudem

11 Wiebe, CR 2023, 777.

12 Wiebe, CR 777, 779, Specht/Hennemann/Determann/Hennemann, DA DGA, Art. 13 DA Rn. 28.

13 Specht/Hennemann/Determann/Hennemann, DA DGA, Art. 13 DA Rn. 5.

14 Specht/Hennemann/Determann/Hennemann, DA DGA, Art. 13 Rn. 4, 16.

15 Konkreter hierzu: Specht/Hennemann/Determann/Hennemann, DA DGA, Art. 13 Rn. 16, 72.

16 Hennemann/Steinrötter, NJW 2024, 1, 5.

17 Datengesetz – Fragen und Antworten, 28.06.2023, https://ec.europa.eu/commission/presscorner/detail/de/qanda_22_1114 (zuletzt abgerufen am 11.08.2025).

18 Bomhard, MMR 2024, 109; Sattler, CR 2024, 213, 215.

19 Staudenmeyer, NJW 2024, 1377, 1382.

20 Dazu Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 489 ff.

21 Siara, MMR 2024, 935.

22 Bomhard, MMR 2024, 109, 110 f.

23 Specht/Hennemann/Linardatos, DA DGA, Art. 23 Rn. 39 f.

24 Siara, MMR 2024, 935.

25 Specht/Hennemann/Linardatos, DA DGA, Art. 25 DA Rn. 6.

26 Bomhard, MMR 2024, 109, 111.

in eine äußerst vorteilhafte Position, die er – selbst bei starker Verhandlungsposition – wohl kaum hätte durchsetzen können.[27]

Gerade im Vergleich zu Kapitel IV bedeuten die Regelungen des Kapitels VI demnach einen noch tieferen Eingriff in inhaltliche Vertragsfreiheit und die Privatautonomie des Diensteanbieters.

b) Rückwirkungsproblematik

Hier drängt sich die Frage nach dem Geltungsbeginn der Pflichten nach Kapitel VI DA auf: Da Art. 50 DA anders als für Kapitel IV keine Sonderregelungen enthält, ist nach Art. 50 UAbs. 2 DA klar, dass Neuverträge, die ab dem 12.09.2025 geschlossen werden, den Vorgaben des Kapitels VI entsprechen müssen. Deutlich problematischer ist der Umgang mit sog. Bestandsverträgen, die vor diesem Stichtag abgeschlossen wurden. Die Frage der (Nicht-)Anwendung von Kapitel VI auf Bestandsverträge muss also durch Auslegung des Art. 50 DA ermittelt werden.[28]

Möglich wäre es, Art. 50 DA derart auszulegen, dass Kapitel VI ab dem 12.09.2025 nicht nur auf Neuverträge, sondern auch auf alle Bestandsverträge Anwendung findet. Dann läge rechtlich ein Fall der Rückwirkung vor, da der Data Act Geltung für Sachverhalte beanspruchen würde, die bereits vor seinem förmlichen Geltungsbeginn liegen. Eine solche rückwirkende Anwendung des Kapitels VI auf Bestandsverträge scheint dem Wortlaut von Art. 50 UAbs. 2 DA zu entsprechen und wird wohl auch von der EU-Kommission vertreten.[29] Dies würde bedeuten: Alle Bestandsverträge wären vor dem 12.09.2025 an die Vorgaben des Kapitels VI „anzupassen"[30].

Andererseits könnte Kapitel VI nur auf Neuverträge und gerade nicht auf Bestandsverträge anzuwenden sein. Dafür ließe sich systematisch anführen, dass eine Rückwirkung nur im Rahmen des Art. 50 UAbs. 6 DA intendiert sein könnte. Näher liegt jedoch der Umkehrschluss zu Art. 50 UAbs. 5 und UAbs. 6 DA, dass für Kapitel VI gerade keine Spezialregelung gelten soll und es daher beim allgemeinen Geltungsbeginn des Art. 50 UAbs. 2 DA bleibt.[31]

Eine letzte Auslegungsmöglichkeit ist die analoge Anwendung der Art. 50 UAbs. 5 und UAbs. 6 DA auf Kapitel VI. Bei Art. 50 Uab. 5, 6 DA handelt es sich allerdings erkennbar um Sonderregelungen für Kapitel IV, die ihrer Natur nach nicht analogiefähig sind.[32] Darüber hinaus kann dem Gesetzgeber, der gerade bewusst für Kapitel IV eine Sonderregelung zur zeitlichen Geltung geschaffen hat, nicht unterstellt werden, diese für Kapitel VI unbewusst und planwidrig unterlassen zu haben. Ein solches gesetzgeberisches Versagen wäre beispiellos.

Somit spricht viel für die Auslegung, wonach Kapitel VI DA ab dem 12.09.2025 auch rückwirkend auf Bestandsverträge Anwendung finden soll.

Dies erscheint im Vergleich mit den Vorgaben von Kapitel IV ungereimt, da für Kapitel IV eine nur beschränkte Rückwirkung inklusive Übergangsregelungen angeordnet ist, obwohl die Vorgaben des Kapitels IV gegenüber Kapitel VI gerade einen deutlich geringeren Eingriff in die Privatautonomie der Parteien darstellen.[33]

Zusammenfassend ist festzustellen, dass der Data Act nicht nur wegen seiner handwerklichen Unschärfe,[34] sondern wegen der Rückwirkung auf Bestandsverträge auch verfassungsrechtlich problematisch ist. Konkret ist damit die Frage nach der Vereinbarkeit des DA mit dem unionsrechtlichen Rückwirkungsverbot aufgeworfen.

II. Das unionsrechtliche Rückwirkungsverbot

1. Existenz und Entwicklung eines unionsrechtlichen Rückwirkungsverbots

Die Unzulässigkeit von rückwirkenden Legislativakten ist im EU-Primärrecht nur in Bezug auf Strafvorschriften ausdrücklich geregelt (Art. 49 Abs. 1 GRCh).

Hinsichtlich anderer Normen findet sich keine primärrechtliche Regelung zum Rückwirkungsverbot; allein in der Rechtsprechung des EuGH wurden Maßstäbe zur Rückwirkung von unionsrechtlichen Rechtsnormen entwickelt. Ein striktes Rückwirkungsverbot wie im Strafrecht existiert hier nicht.

Wie im deutschen Recht richtet sich die (Un-)Zulässigkeit der Rückwirkung von Unionsrechtsakten nach der Auflösung des Spannungsverhältnisses zwischen der Dispositionsfreiheit des Unionsgesetzgebers einerseits und dem Vertrauensschutz der von der Rechtsänderung Betroffenen andererseits. Die Unionsorgane sind zwar nach Art. 297 Abs. 1 AEUV frei in der Bestimmung des Zeitpunkts, zu dem ein Rechtsakt in Kraft treten soll – dennoch sind Vertrauensschutzerwägungen zu berücksichtigen, wenn der Rechtsakt Sachverhalte betrifft, die vor dessen Geltung zumindest begonnen haben. Der Rechtsakt würde sonst zulasten von Unionsbürgern wirken können, bevor diese die Möglichkeit haben, von diesem überhaupt Kenntnis zu nehmen.[35]

Unter Berücksichtigung dieses Spannungsverhältnisses entwickelte der EuGH das Rückwirkungsverbot aus den allgemeinen Rechtsgrundsätzen des Unionsrechts, die den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten entsprechen (vgl. Art. 6 Abs. 3 EUV).[36] Konkret ist das Verbot der Rückwirkung von Rechtsnormen Ausdruck der Gebote von Rechtssicherheit und Vertrauensschutz, die ihrerseits Ausprägung des allgemeinen Rechtsgrundsatzes der Rechtsstaatlichkeit sind.[37] Das erste Urteil, mit dem der Gerichtshof effektiv den Grundsatz des Vertrauensschutzes gegenüber einem Normensetzungsakt durchgesetzt hat, wurde in der Rechtssache Kommission / Rat aus dem Jahr 1973 gefällt, in welcher der Rat von seinem eigenen Beschluss über die Beamtenbesoldung durch spätere Verordnung abweichen wollte.[38]

27 Bomhard, MMR 2024, 109, 111; Pommerening, RDi 2024, 289, 295.

28 Dazu eingehend Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 490 ff.

29 Freiberg/Niebuhr, BB 2025, 1067, 1068 sowie Fn. 8.

30 Dass diese Anpassung nicht als einseitiger Akt des Anbieters, sondern nur als konsensuale Änderung des vereinbarten Vertragsinhalts erfolgen kann, wird gleich zu erörtern sein.

31 Specht/Hennemann/Hennemann, DA DGA, Art. 50 Rn. 5, 6; Siara, MMR 2024, 935.

32 Bitter/Rauhut, JuS 2009, S. 289, 298.

33 So auch Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 490 ff.

34 Unter anderem wurde in der deutschen Version des DA schlicht vergessen, den letzten Halbsatz von Art. 25 Abs. 2 a) zu übersetzen und zu übernehmen.

35 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 55, 61.

36 Geiger/Khan/Kotzur/Kirchmair/Geiger/Kirchmair, EUV Art. 6 Rn. 60, 64.

37 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 186 f.; Schwarze/Becker/Hatje/Schoo/Bittner, EU-Kommentar, AEUV Art. 40 Rn. 59 f.

38 EuGH, Rs. C-81/72 – Kommission/Rat ECLI:EU:C:1973:60.

Wie im deutschen Recht kann zwischen „echter" und „unechter" Rückwirkung unterschieden werden.[39] Diese Unterscheidung dient dazu, die Anforderungen an den Vertrauensschutz auszutarieren.

2. Unterscheidung von echter und „unechter" Rückwirkung

a) Echte Rückwirkung

Ein Fall der echten Rückwirkung – der EuGH spricht auch von „Rückwirkung im eigentlichen Sinne"[40] – liegt vor, wenn der Gesetzgeber eine Regelung für bereits abgeschlossene, der Vergangenheit angehörende Sachverhalte einführt. Entweder wird für den Beginn der Geltungsdauer der Verordnung ein Datum bestimmt, das zeitlich vor dem Tag ihrer Veröffentlichung liegt oder die Verordnung knüpft an Sachverhalte an, die vor ihrem Inkrafttreten nicht nur entstanden, sondern auch bereits tatbestandlich abgeschlossen sind.[41]

Ein Fall echter Rückwirkung liegt z.B. vor, wenn nach Abschluss eines Wirtschaftsjahres abgabenrechtliche Regelungen getroffen werden, die gerade das vergangene Wirtschaftsjahr betreffen. Es werden an den abgeschlossenen Tatbestand des Wirtschaftsjahrs ungünstige Rechtsfolgen angeknüpft, mit denen der Bürger zum Zeitpunkt seiner Dispositionen nicht rechnen musste, beispielsweise bei Wiedereinführung einer Produktionsabgabe für ein bereits zurückliegendes Wirtschaftsjahr.[42]

Nach der ständigen Rechtsprechung des EuGH – geprägt durch die Rechtssachen Racke[43], Decker[44] und die sogenannten „Isoglucose-Fälle"[45] – ist die echte Rückwirkung aus Gründen der Rechtssicherheit als grundsätzlich unzulässig anzusehen.[46]

b) „Unechte" Rückwirkung

Kein Fall der (echten) Rückwirkung liegt vor, wenn der Unionsgesetzgeber auf in der Vergangenheit entstandene, aber zum Zeitpunkt des Inkrafttretens der Regelung in der Entwicklung noch nicht abgeschlossene Sachverhalte einwirkt.[47] Die Neuregelung wird also auf die künftigen Rechtsfolgen von Sachverhalten, die unter der Geltung früherer Regelungen entstanden sind, angewandt.[48]

Relevant wurde dies in der Rechtsprechung des EuGH vor allem im Bereich des Agrarrechts, wenn Normänderungen sich auf laufende Verträge im Agrarbereich auswirkten.[49] In den Rechtssachen Westzucker C-1/73[50] und SOPAD C-143/73[51] wurden beispielsweise nach der Erteilung von Ausfuhrlizenzen, aber vor Ausfuhr von Agrarprodukten Erstattungsregelungen für vertragsrelevante Produkte geändert. In der Folge stellte sich die Frage, ob die Erstattungen sich nach dem Recht zum Zeitpunkt der Lizenzerteilung oder nach dem für den Lieferanten ungünstigeren Recht zum Zeitpunkt der tatsächlichen Ausfuhr richten.[52] Im letzteren Fall läge eine tatbestandliche Rückanknüpfung an nicht abgeschlossene Sachverhalte vor.

Das BVerfG bezeichnet bezogen auf das deutsche Recht die tatbestandliche Rückanknüpfung als „unechte Rückwirkung".[53] Der EuGH hingegen benutzt diesen Begriff bisher nicht, er spricht von einer Problematik, die „keine rückwirkende Kraft im eigentlichen Sinne" habe.[54] Daher gilt in einem solchen Falle in Abgrenzung zur echten Rückwirkung auch nicht das grundsätzliche Rückwirkungsverbot und ein nur abgeschwächter Vertrauensschutztatbestand.[55]

3. Zulässigkeitsvoraussetzungen von echter und unechter Rückwirkung

a) Zulässigkeitsvoraussetzungen echter Rückwirkung

Zwar sieht der EuGH die echte Rückwirkung in Anbetracht des Grundsatzes der Rechtssicherheit als grundsätzlich unzulässig an, dennoch lässt er nach der sogenannten „Racke-Formel"[56] Ausnahmen von diesem grundsätzlichen Rückwirkungsverbot zu, wenn die folgenden zwei Voraussetzungen kumulativ vorliegen: Erstens müssen zwingende Unionsinteressen die Rückwirkung erfordern (Erforderlichkeit der Rückwirkung) und zweitens muss das berechtigte Vertrauen der Betroffenen gebührend berücksichtigt werden oder darf nicht schutzwürdig sein (individueller Vertrauensschutz).[57] Der individuelle Vertrauensschutz fächert sich wiederum in eine objektive und subjektive Komponente auf: Die objektive Vertrauenslage wird bereits durch die echte Rückwirkung geschaffen und bedarf keines konkreten Verhaltens der Unionsorgane.[58] Damit kommt es letztlich auf die subjektive Vertrauenslage an, hierfür ist die Vorhersehbarkeit der Rechtsänderung durch den Betroffenen maßgeblich.[59] Im Endeffekt ist eine Abwägung der widerstreitenden Interessen im Sinne einer modifizierten Verhältnismäßigkeitsprüfung vorzunehmen.[60]

b) Zulässigkeitsvoraussetzungen unechter Rückwirkung

Der EuGH geht im Gegensatz zur echten Rückwirkung von der generellen Zulässigkeit der „unechten" Rückwirkung aus. Er postuliert in ständiger Rechtsprechung, dass Gesetzesänderungen, soweit nichts Abweichendes bestimmt ist, auf die künftigen Auswirkungen unter dem alten Recht entstandener Sachverhalte anwendbar sind. [61]

39 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 180; Grabitz/Hilf/Nettesheim/von Rintelen/Wolf, AEUV Art. 43 Rn. 110.

40 EuGH, Rs. C-74/74 – CNTA / Kommission ECLI:EU:C:1975:59 Rn. 29, 32.

41 Schwarze, Europäisches Verwaltungsrecht, S. 1084.

42 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 181; s. u.a. EuGH, Rs. C-108/81 – Amylum / Rat ECLI:EU:C:1982:322.

43 EuGH, Rs. C-98/78 – Racke / Hauptzollamt Mainz ECLI:EU:C:1979:14.

44 EuGH, Rs. C-99/78 – Decker / Hauptzollamt Landau ECLI:EU:C:1979:15.

45 EuGH, Rs. C-108/81 – Amylum / Rat ECLI:EU:C:1982:322; Rs. C-110/81 – Roquette Frères / Rat ECLI:EU:C:1982:323; Rs. C-114/81 – Tunnel Refineries / Rat ECLI:EU:C:1982:324.

46 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 57.

47 Schwarze, Europäisches Verwaltungsrecht, S. 1085.

48 Schulze/Janssen/Kadelbach/Schmahl, Handbuch Europarecht, § 6 Rn. 44.

49 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 182.

50 EuGH, Rs. C-1/73 – Westzucker GmbH / Einfuhr- und Vorratsstelle für Zucker ECLI:EU:C:1973:78.

51 EuGH, Rs. C-143/73 – SOPAD / FORMA u.a. ECLI:EU:C:1973:145.

52 Schwarze, Europäisches Verwaltungsrecht, S. 1085.

53 BVerfGE 134, 33 Rn. 72.

54 EuGH, Rs. C-74/74 – CNTA / Kommission ECLI:EU:C:1975:59 Rn. 29, 32.

55 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 60; Borchardt, Vertrauensschutz im Europäischen Gemeinschaftsrecht, EuGRZ 1988, 309, 311.

56 Heukels, Intertemporales Gemeinschaftsrecht, S. 240.

57 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 57 ff.; Schulze/Janssen/Kadelbach/Schmahl, Handbuch Europarecht, § 6 Rn. 44.

58 Heukels, Die Rückwirkungsjudikatur des EuGH, S. 30; Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 59.

59 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 59.

60 Schulze/Janssen/Kadelbach/Schmahl, Handbuch Europarecht, § 6 Rn. 44.

61 EuGH, Rs. C-1/73 – Westzucker GmbH / Einfuhr- und Vorratsstelle für Zucker ECLI:EU:C:1973:78 Rn. 5; Borchardt, EuGRZ 1988, 309, 311; Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 61.

Damit betont der EuGH die Dispositionsfreiheit des Gesetzgebers; ein Unternehmen solle sich gegenüber Änderungen der Rechtslage auch „nicht auf ein wohlerworbenes Recht auf Beibehaltung eines Vorteils berufen" können.[62]

Allerdings bestehen Ausnahmen von dieser generell weiten Dispositionsbefugnis, wenn das als schutzwürdig angesehene Vertrauen des Einzelnen in den Fortbestand der Rechtslage das Unionsinteresse überwiegt.[63]

Bei der Schutzwürdigkeit des Vertrauens sind sowohl die Vorhersehbarkeit der Rechtsänderung als auch Art und Verfestigungsgrad der jeweiligen Dispositionen des Betroffenen heranzuziehen.[64] So ist es nach der Rechtsprechung des EuGH z.B. zu berücksichtigen, wenn das allgemeine Rechtsverhältnis, dem potenziell eine Vielzahl von Wirtschaftsteilnehmern unterworfen ist, schon eine bestimmte Konkretisierung erfahren hat.[65] Dabei muss es sich nicht um eine bereits aufgrund eines Verwaltungsakts erworbene individuelle Rechtsposition handeln. Notwendig ist aber, dass Dispositionen getroffen worden sind.[66] Der Grundsatz des Vertrauensschutzes erlangt somit vor allem für im Zeitpunkt der Verkündung einer Verordnung schon laufende Verträge Bedeutung.[67]

Das schutzwürdige Vertrauen kann jedoch von Unionsinteressen in Form von zwingenden Allgemeinwohlinteressen überwogen werden; dann ist im Zuge der Neuregelung auch der Erlass von Übergangsregelungen aus Vertrauensschutzgründen nicht notwendig. Umgekehrt ist es dem Unionsgesetzgeber aber verboten, eine allgemeine Regelung ohne Erlass von Übergangsbestimmungen zu ändern, sofern diese zwingenden Allgemeinwohlinteressen fehlen.[68]

III. Data Act und Rückwirkungsverbot

1. Echte oder unechte Rückwirkung

Es fragt sich also wegen der unterschiedlichen Zulässigkeitsmaßstäbe, ob die Geltung von Kapitel VI des Data Acts für Bestandsverträge einen Fall der grundsätzlich unzulässigen echten oder der grundsätzlich zulässigen unechten Rückwirkung darstellt.

Wie beschrieben, läge ein Fall der echten Rückwirkung vor, wenn die Art. 23 ff. DA im Hinblick auf Bestandsverträge Regelungen für bereits tatbestandlich abgeschlossene, der Vergangenheit angehörende Sachverhalte treffen würden. Umgekehrt läge eine unechte Rückwirkung vor, wenn der zugrundeliegende Sachverhalt – also der Vertrag mit dem Diensteanbieter – zum Zeitpunkt des Inkrafttretens ein noch nicht abgeschlossener Sachverhalt wäre.

Für das Vorliegen einer unechten Rückwirkung lässt sich anführen, dass Cloud-Verträge Dauerschuldverhältnisse sind, bei denen den Diensteanbieter eine fortwährende Leistungspflicht trifft. Es handelt sich also um laufende, zeitlich gestreckte Verträge, weswegen der Sachverhalt des Vertrags als „nicht abgeschlossen" angesehen werden könnte. So hat der EuGH etwa auch in den Rechtssachen Westzucker C-1/73 und SOPAD C-143/73 entschieden, dass bei der Einwirkung einer Gesetzesänderung auf laufende, noch zu erfüllende Verträge nicht von einer unzulässigen echten Rückwirkung auszugehen sei. Vielmehr gelte die neue Erstattungsregelung für vertragsrelevante Produkte gerade auch für bereits vor Erlass der Neuregelung abgeschlossene Verträge.

Allerdings darf allein der Terminus „laufender Vertrag" nicht dazu führen, dass unbesehen auf eine unechte Rückwirkung geschlossen wird. Vielmehr sind die Besonderheiten des Einzelfalls zu betrachten. Obwohl es sich bei den Cloud-Verträgen nach Kapitel VI DA in der Tat um laufende Verträge handelt, besteht ein entscheidender Unterschied zu den Rechtssachen Westzucker und SOPAD: In diesen Rechtssachen wurde nur eine öffentlich-rechtliche Erstattungsregelung geändert, die den Vertragsinhalt als solchen unberührt ließ. Die Änderung der Erstattungsbedingungen nach Erteilung der Ausfuhrlizenz, aber vor der Ausfuhr machte lediglich die Erfüllung des Vertrags für den Exporteur weniger lukrativ, sie verpflichtete aber nicht kraft Gesetzes zu einer Vertragsanpassung.

Bei Anwendung von Kapitels VI des Data Acts auf Altverträge hingegen würden insbesondere Art. 23 und 25 des Data Acts den Anbieter zu einer Änderung des Vertragsinhalts verpflichten. Dadurch wäre – im Unterschied zu den bisher vom EuGH entschiedenen Fällen – nicht lediglich die Erfüllungsphase des Vertrags, sondern der Vertragskern selbst betroffen. Der Inhalt des Vertrags bleibt durch die Rechtsänderung gerade nicht unberührt.

Bezogen auf die Rückwirkungsproblematik bedeutet dies: In den Rechtssachen Westzucker und SOPAD ist der nicht abgeschlossene Sachverhalt die Vertragserfüllung. Bei den vom Data Acta adressierten Cloud-Verträgen ist die Vertragserfüllung wegen des Charakters als Dauerschuldverhältnis zwar auch noch nicht abgeschlossen – der Sachverhalt, an den die Rechtsänderung anknüpft, ist aber nicht die noch laufende Erfüllungsphase des Vertrags, sondern der zwischen den Parteien abschließend vereinbarte Vertragsinhalt selbst. Wenn Bestandsverträge von Kapitel VI des Data Acts erfasst werden, besteht für den Diensteanbieter eine Pflicht zur Vertragsänderung und der ursprüngliche Vertrag kann überhaupt nicht mehr erfüllt werden, da sich durch die geforderte Inhaltsänderung des Vertrags das vertragliche Pflichtenprogramm für den Anbieter ändert.

Folglich liegen in den Rechtssachen Westzucker bzw. SOPAD und beim Data Act verschiedene Ansatzpunkte der Rechtsänderung vor und eine rechtliche Gleichbehandlung mit Blick auf das Rückwirkungsverbot ist nicht schlüssig. Der Data Act knüpft an einen bereits abgeschlossenen Sachverhalt an – die verbindliche Festlegung des Vertragsinhaltes durch die Parteien bei Abschluss des Vertrages. Damit liegt eine grundsätzlich unzulässige echte Rückwirkung vor[69] – der Gesetzgeber hätte damit eine verfassungswidrige Regelung getroffen.

Ausnahmsweise Zulässigkeit der echten Rückwirkung?

Es könnte jedoch eine Ausnahme vom Rückwirkungsverbot nach der „Racke-Formel" vorliegen – wegen der Erforderlichkeit der Rückwirkung und fehlenden individuellen Vertrau-

62 EuGH, Rs. C-230/78 – Eridania ECLI:EU:C:1979:216 Rn. 22; Rs. C-59/83 – Biovilac/EWG ECLI:EU:C:1984:380 Rn. 23.

63 EuGH, Rs. C-84/78 – Tomadini ECLI:EU:C:1979:129 Rn. 20 ff.; Rs. C-278/84 – Deutschland/Kommission ECLI:EU:C:1987:2 Rn. 36; Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 194.

64 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 62 f.

65 Schwarze, Europäisches Verwaltungsrecht, S. 1094.

66 Schwarze, Europäisches Verwaltungsrecht, S. 1094.

67 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 182; Schwarze, Europäisches Verwaltungsrecht, S. 1094.

68 EuGH, Rs. C-74/74 – CNTA / Kommission ECLI:EU:C:1975:59 Rn. 41 ff.; Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 63.

69 In diesem Sinne auch Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 491.

ensschutzes. In diesem Fall ist eine modifizierte Verhältnismäßigkeitsprüfung durchzuführen.

Die Zulässigkeit der echten Rückwirkung setzt zunächst voraus, dass ein zwingendes Unionsinteresse verfolgt wird. Die mit den Art. 23 ff. DA verfolgten Ziele sind das Verhindern von Anbieter-Lock-in-Effekten, der Abbau von Marktzutrittsschranken für alternative Anbieter und die Wettbewerbsförderung. Ob diese Ziele als zwingend zu bewerten sind, erscheint fraglich, obliegt jedoch letztlich dem EuGH.

Hinsichtlich der Erforderlichkeit der Regelung für die Zielerreichung ist der Ermessensspielraum des Unionsgesetzgebers zu achten. Anhaltspunkte dafür, dass die Ziele ohne Rückwirkungsanordnung evident genauso gut hätte verwirklicht werden können,[70] gibt es nicht. Vielmehr können die aufgezeigten Ziele der Union dann, wenn auch Altverträge von Kapitel VI DA betroffen sind, durchaus effektiver umgesetzt werden.

Allerdings kann die Rückwirkung nur dann zulässig sein, wenn das berechtigte Vertrauen der Betroffenen gebührend berücksichtigt worden oder nicht schutzwürdig ist.

Der Anbieter von Cloud-Services darf berechtigterweise darauf vertrauen, durch Maßnahmen des Unionsgesetzgebers nicht in unverhältnismäßiger Weise in seiner unternehmerischen Freiheit nach Art. 16 GRCh eingeschränkt zu werden. Unterausprägungen der unternehmerischen Freiheit des Art. 16 GRCh sind die unternehmensbezogene Vertragsfreiheit und der Grundsatz pacta servanda.[71]

Wie erläutert, regeln die Art. 23 S. 2 und 25 DA Mindestanforderungen an den Vertragsinhalt hinsichtlich des Wechsels zwischen Datenverarbeitungsdiensten und greifen dadurch tief in die Privatautonomie ein. Wenn nun die Vorschriften der Art. 23 S. 2 und 25 DA auch rückwirkend für Bestandsverträge gelten, wird der Alt-Anbieter nicht nur in seiner Entscheidung, einen Vertrag abzuschließen, beeinflusst, sondern sogar zur Änderung eines bereits existierenden Vertrags gezwungen. Der Data Act reguliert in das bestehende Vertragsverhältnis hinein. Besonders deutlich wird dies durch die Formulierung „Hindernisse beseitigen" in Art. 23 S. 2 DA, die sich auch und gerade auf bereits existierende Hindernisse in Bestandsverträgen bezieht.[72] Die Vertragsinhaltsfreiheit und der Grundsatz pacta sunt servanda werden dadurch in ihrem Kern betroffen.

Darüber hinaus ist die unternehmerische Freiheit des Diensteanbieters auch dadurch betroffen, dass die mit der Pflicht zur Vertragsänderung zwingend einhergehenden Vertragsneuverhandlungen für den Diensteanbieter sehr zeit- und kostenintensiv sind.[73] Auch machen die Anforderungen des Art. 25 Abs. 2 DA die Bindung von Kunden an feste Vertragslaufzeiten unmöglich, was die wirtschaftliche Planungssicherheit und die Realisierung von Umsatz durch die Diensteanbieter erheblich erschwert.[74] Die gegebenenfalls bereits vor Jahren getroffene unternehmerische Kalkulation droht dadurch leerzulaufen.

Für den Anbieter kommt weiter erschwerend hinzu, dass Kapitel VI DA, anstatt dies einfach direkt per Gesetz zu regeln, dem Anbieter vorschreibt, bestimmte Inhalte in seinen Vertrag mit dem Kunden aufzunehmen – eine durchaus merkwürdige Methode legislativer Gestaltung[75]: Der Data Act scheint zu übersehen, dass der Anbieter den Vertrag nicht selbst und einseitig ändern kann, sondern dazu ein Konsens beider Vertragsparteien erforderlich ist. Die Pflicht zur Vertragsänderung wird dem Cloud-Anbieter also auferlegt, obwohl er sie aus eigener Kraft gar nicht umsetzen kann. In bestimmten Bereichen, nämlich bei Verträgen mit öffentlichen Auftraggebern, die unter vergaberechtlichen Grundsätzen geschlossen wurden, ist nicht nur eine einseitige Anpassung, sondern ggf. sogar eine einvernehmliche nachträgliche Vertragsanpassung ausgeschlossen, soweit dadurch die Ausschreibungspflicht beeinträchtigt wird. Weiter wirkt verschärfend, dass die Nichterfüllung der Pflichten aus Kapitel VI nach Art. 40 DA sanktionsbewehrt ist.

Dies wäre ein praktisch zu vernachlässigendes Problem, wenn mit einer Zustimmung des Kunden in Bezug auf die vom Anbieter pflichtgemäß vorgeschlagenen Vertragsänderungen zwingend zu rechnen wäre. Dies ist aber keinesfalls sicher, da den Kunden, der ein Cloud Switching vornehmen möchte, auch durchaus negative Folgen treffen. Beispielsweise muss er nach Art. 29 Abs. 2 bei einem Wechsel bis zum 12.01.2027 (ermäßigte) Wechselentgelte zahlen (s. Art. 25 Abs. 2 lit. i) DA) und ihn können Sanktionen bei vorzeitiger Kündigung treffen (Art. 29 Abs. 4 DA). Dass er einer Vertragsänderung mit solch negativen Folgen immer zustimmen wird, ist daher keineswegs ausgemacht. Und in diesen Fällen kann der Anbieter seine gesetzlichen Pflichten nicht erfüllen.

Es liegt also ein besonders schwerer Eingriff in die unternehmerische Freiheit des Cloud-Anbieters vor; ihm werden sanktionsbewehrte Pflichten auferlegt werden, die er gegebenenfalls gar nicht erfüllen kann. Eine verhältnismäßigere Gestaltungsmöglichkeit wäre gewesen, ein bloßes Angebot des Anbieters auf Vertragsänderung entsprechend den Vorgaben der Art. 23 ff. DA ausreichen zu lassen. Dann stellt sich allerdings das Problem, wie ein etwaiger Verstoß des Anbieters nachgewiesen werden sollte.

Das aufseiten der Union verfolgte Interesse der Verhinderung von Lock-in-Effekten kann diesen massiven Eingriff in Art. 16 GRCh keineswegs aufwiegen, zumal die Union dieses Ziel ja jedenfalls mit Blick auf Neuverträge durchaus umsetzen kann. Die Union hätte es in der Hand gehabt, einen verhältnismäßigeren Interessenausgleich zu finden, indem sie für Kapitel VI ähnliche Übergangsregelungen wie für Kapitel IV (vgl. Art. 50 UAbs. 5 und 6 DA) geschaffen hätte. Dass sie das nicht getan hat, leuchtet schon deswegen nicht ein, weil Kapitel IV hinsichtlich der Privatautonomie und damit in Bezug auf Art. 16 GRCh weniger invasiv ist. Dies impliziert die Unverhältnismäßigkeit des Eingriffs und die Unzulässigkeit der Rückwirkung.

An dem Überwiegen des Vertrauensschutzes des Diensteanbieters hätte sich allenfalls dann etwas ändern können, wenn die am Gesetzgebungsverfahren beteiligten Gemeinschaftsorgane die Normadressaten durch frühzeitige Unterrichtung rechtzeitig auf die beabsichtigte Rückwirkungsanordnung aufmerksam gemacht hätten.[76] Eine solche Benachrichtigung ist jedoch nicht erfolgt. Es besteht im Gegenteil bei den Betroffenen Rechtsunsicherheit hinsichtlich der Frage, ob sich der Geltungsbeginn der Verordnung nach Art. 50 UAbs. 2 DA auch auf Bestandsverträge erstreckt.

70 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 189.

71 Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV/Kühling/Drechsler, GRC Art. 16 Rn. 15; BeckOGK/Herresthal, BGB § 311 Rn. 15.

72 Specht/Hennemann/Linardatos, DA DGA, Art. 23 Rn. 39; Plitz/Zwerschke, CR 2024, 153, 155.

73 Freiberg/Niebuhr, BB 2025, 1067, 1068.

74 Bomhard, MMR 2024, 109, 111.

75 Siara, MMR 2024, 935.

76 Berger, Zulässigkeitsgrenzen der Rückwirkung von Gesetzen, S. 192.

Folglich besteht keine Ausnahme vom Rückwirkungsverbot nach der „Racke-Formel". Die Anwendung von Kapitel VI DA auf Bestandsverträge verstößt gegen das unionsrechtliche Rückwirkungsverbot und ist rechtswidrig.

IV. Folge der unzulässigen echten Rückwirkung

Folge der unzulässigen echten Rückwirkung ist grundsätzlich die ex-tunc-Nichtigkeit der entsprechenden Vorschriften.[77] Die Anwendung von Kapitel VI DA auf Bestandsverträge folgt aus Art. 50 UAbs. 2 DA. Würde man Art. 50 UAbs. 2 DA als nichtig ansehen, so würde allerdings der Geltungsbeginn für keine Vorschrift des Data Acts mehr bestimmt werden. Es wäre für den Geltungsbeginn des gesamten Rechtsakts auf die allgemeine Regelung des Art. 297 Abs. 1 AEUV zurückzugreifen, womit der Geltungsbeginn mit dem Inkrafttreten des Data Acts am 11.01.2024 zusammenfiele. Damit läge der Geltungsbeginn des DA in der Vergangenheit, was ein Ergebnis wäre, das für die Praxis noch mehr Fragen aufwerfen und einen noch tieferen Einschnitt in die unternehmerische Freiheit nach Art. 16 GRCh bedeuten würde.

In Frage käme auch, Art. 50 UAbs. 2 primärrechtskonform anhand von Art. 16 GRCh so auszulegen, dass er nur auf Neuverträge Anwendung findet und Bestandsverträge nicht an die Vorgaben des Kapitels VI angepasst werden müssen. Oder aber stattdessen die Vorschriften des Kapitels VI entsprechend auszulegen. Solche Auslegungen würden aber gegen den klaren Wortlaut von Art. 50 UAbs. 2 DA und von Art. 23 S. 2 DA verstoßen. Die Formulierung „Hindernisse beseitigen" bezieht sich gerade auf bereits existierende Hindernisse in bestehenden Verträgen, andernfalls wäre „beseitigen" ein unpassender Begriff. Diese Auslegung wird auch durch die englische („remove obstacles") und französische Sprachfassung („supprimer les obstacles") bestätigt. Eine primärrechtskonforme Auslegung, nach der Bestandsverträge von Kapitel VI unberührt blieben, wäre also contra legem und muss damit ausscheiden.[78]

Letztlich wäre der einzig gangbare Weg, die Rückwirkung von Kapitel VI DA in Bezug auf Bestandsverträge als unionsrechtswidrig und daher unstatthaft anzusehen, es aber für die sonstige Geltung des Data Acts beim Geltungsbeginn des Art. 50 UAbs. 2 DA zu belassen. Eine solche geltungserhaltende Reduktion der Vorschrift führte zu verhältnismäßigen Ergebnissen.

Sollte sich der Verordnungsgeber nicht noch bis zum Geltungsbeginn des Data Acts dazu entscheiden, eine Sonderregelung für Kapitel VI in Bezug auf Bestandsverträge zu erlassen bzw. diese vom allgemeinen Geltungsbeginn des Art. 50 UAbs. 2 DA auszunehmen, könnte der EuGH im Wege des Vorabentscheidungsverfahrens nach Art. 267 Abs. 1 lit. b) AEUV mit der Unzulässigkeit der Rückwirkung befasst werden.

Bei diesem Verfahren sind allerdings nur die mitgliedstaatlichen Gerichte vorlageberechtigt, sofern über die Rechtsfrage der Anwendung von Kapitel VI DA auf Bestandsverträge in einem anhängigen Verfahren zu entscheiden ist (Art. 267 Abs. 2, 3 AEUV).

V. Fazit

Der Data Act soll ab dem 12.09.2025 Geltung entfalten – und das, obwohl er rechtlich gesehen offensichtlich äußerst problematisch ist. Der Data Act ist an vielen Stellen unklar formuliert oder lückenhaft und erscheint wenig durchdacht. Dies ist nicht zuletzt auf den nur kurzen Gesetzgebungsprozess zurückzuführen.

Darüber hinaus legen Kapitel IV und VI des Data Acts datengestützt agierenden Unternehmen besondere Verpflichtungen hinsichtlich ihrer Vertragsgestaltung auf, die mit hohen Transaktionskosten verbunden sind und für die nur kurze bis keine Übergangsfristen gelten. Für die betroffenen Wirtschaftsakteure besteht insbesondere enorme Rechtsunsicherheit in Bezug auf Kapitel VI des Data Acts, der die vertragliche Gestaltung von Datenverarbeitungsverträgen bei Cloud- und Edge-Diensten behandelt. Die Systematik von Art. 50 DA legt nahe, dass Kapitel VI auch auf Verträge Anwendung findet, die vor dem 12.09.2025 geschlossen wurden. Es wird also nachträglich in Bestandsverträge hineinreguliert; Vertragsneuverhandlungen würden nötig.

Diese von Kapitel VI geforderte Abänderung des ursprünglich festgelegten Vertragsinhalts stellt eine unionsrechtlich unzulässige echte Rückwirkung dar, die mit einem nicht zu rechtfertigenden Eingriff in die Vertragsfreiheit des Unternehmers nach Art. 16 GRCh einhergeht. Übergangsregelungen fehlen hier gänzlich, die Union signalisiert zudem in keiner Weise Entgegenkommen gegenüber der Wirtschaft in Bezug auf Kapitel VI. Daraus folgt, dass Kapitel VI in der derzeitigen Fassung auf Bestandsverträge wegen Verstoßes gegen das Rückwirkungsverbot nichtig ist und keine Anwendung finden darf.

In der Gesamtschau handelt es sich beim Data Act um eine misslungene Regulierung, die zumindest in wesentlichen Punkten verfassungswidrig in die Rechte der betroffenen Wirtschaftsteilnehmer eingreift. Eine rasche Reaktion der EU-Kommission ist zwingend geboten, andernfalls wird der EuGH diese Fehlregulierung aufheben müssen.

Dr. Stefan Brink
ist Geschäftsführender Direktor des Instituts wida/Berlin und Landesdatenschutzbeauftragter Baden-Württemberg a.D.

Lea Brink
ist Ref. jur. in Baden-Württemberg. Sie studierte Rechtswissenschaften an der Albert-Ludwigs-Universität Freiburg (1. Staatsexamen) sowie an der Université Paris 1 Panthéon-Sorbonne.

77 Heselhaus/Nowak EU-Grundrechte-HdB/Bungenberg, § 37 Rn. 69.

78 Riesenhuber, Europäische Methodenlehre, S. 229; in diesem Sinne aber Zikesch/Sörup: Bestandsvertrag trifft Data Act, MMR 2025, 487 ff., 492 f.

Eva-Maria Pottkämper, LL.M. (TH Köln), LL.M. (Passau)

Die Einwilligungsverwaltungsverordnung (EinwV): Reduzierung von Cookie-Bannern und Stärkung der Nutzerkontrolle

Die Digitalisierung prägt nahezu alle Lebensbereiche, vom privaten Alltag über den öffentlichen Sektor bis hin zu Wirtschaft und Industrie. Digitale Angebote, sei es in Form von Websites, Online-Diensten oder mobilen Anwendungen, sind fester Bestandteil der modernen Informationsgesellschaft. Dabei hat sich der Umgang mit personenbezogenen Daten zu einer der zentralen Herausforderungen entwickelt, insbesondere im Hinblick auf Datenschutz, Nutzerfreundlichkeit und digitale Selbstbestimmung. Während Unternehmen und Website-Betreiber auf Tracking-Technologien angewiesen sind, um ihre Angebote zu monetarisieren oder zu optimieren[1], stehen Nutzer oft vor der Frage, inwieweit sie der Verarbeitung ihrer Daten überhaupt zustimmen möchten.

Ein besonders kontrovers diskutiertes Thema in diesem Zusammenhang sind Cookie-Banner, die durch die Einführung der Datenschutz-Grundverordnung (DS-GVO)[2] und des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)[3] zur Pflicht wurden. Diese Banner fordern Nutzer dazu auf, ihre Einwilligung zur Datenspeicherung und -verarbeitung zu erteilen, bevor Webseiten Cookies oder Tracking-Technologien verwenden dürfen. Obwohl die Maßnahme ursprünglich für mehr Transparenz sorgen sollte, hat sie in der Praxis zu einer Flut an Zustimmungserklärungen geführt, die den Nutzern auf nahezu jeder Webseite begegnen.[4] Das Ergebnis ist nicht mehr Transparenz, sondern vielmehr eine sog. „Consent Fatigue" (Einwilligungsverdruss)[5], also eine Ermüdung der Nutzer gegenüber Einwilligungsanfragen, die dazu führen kann, dass viele aus Bequemlichkeit „Akzeptieren" klicken – oftmals ohne sich über die Konsequenzen bewusst zu sein.

Um die dargelegte Problematik des Einwilligungsmanagements insbesondere in Cookie-Bannern zu lösen, empfahl die Datenethikkommission bereits 2019 im Rahmen eines Gutachtens, die Nutzung sogenannter PIMS (Personal Information Management Systems).[6] Schließlich wurde am 4. September 2024 zur weiteren Verbesserung des Datenschutzes im digitalen Raum und der Nutzerfreundlichkeit die Einwilligungsverwaltungsverordnung (EinwV)[7] nach § 26 Abs. 2 TDDDG von der Bundesregierung verabschiedet. Sie trat zum 1. April 2025 in Kraft.

Dieser Beitrag erläutert die Hintergründe und die Zielsetzung der EinwV, beschreibt die Funktionsweise der zentralen Einwilligungsverwaltung, zeigt praxisnahe Implementierungsschritte für Unternehmen, beleuchtet die Auswirkungen für Nutzer und Unternehmen und geht auf die bestehenden Herausforderungen in diesem Bereich ein.

I. Hintergrund und Zielsetzung der EinwV

Cookies sind eine häufig genutzte Technologie, um Daten während der Kommunikation zwischen dem Client (dem Browser des Nutzers) und dem Server (der Webseite eines digitalen Dienstes) über mehrere Anfragen hinweg zu speichern und abzurufen.[8] Sie sind technisch unverzichtbar für Funktionen wie Logins oder Warenkörbe.[9] In der Werbewirtschaft dienen Cookies vor allem der Verfolgung von Nutzeraktivitäten über verschiedene Webseiten hinweg („Tracking") sowie der Erstellung von Profilen für zielgerichtete Werbung („Targeting").[10] Um Nutzer über den Einsatz dieser Technologien zu informieren und deren rechtskonforme Einwilligung einzuholen, nutzen Webseitenbetreiber in der Regel spezielle „consent management platforms", die nach dem Transparency und Consent Framework (TCF)[11] aufgestellt sind.[12]

Die EinwV wird auch als „Cookie-Verordnung" bezeichnet, da sie darauf abzielt, klassische – und für den Nutzer teilweise undurchsichtige und überfordernde[13] – Cookie-Banner und Consent-Management-Plattformen („CMPs") durch zentral verwaltete Einwilligungen zu ersetzen. Damit wäre es möglich, Datenschutzpräferenzen einmalig und abstrakt-generell festzulegen, anstatt sie auf jeder Webseite und bei jedem Besuch einzeln angeben zu müssen.

Dabei ist die EinwV kein isoliertes Gesetz, sondern Teil einer umfassenderen Entwicklung hin zu mehr Datenschutz und digitaler Selbstbestimmung. Die ePrivacy-Richtlinie[14] regelt insbesondere den Einsatz von Cookies und anderen Tracking-Technologien. In Deutschland wurde die ePriva-

1 Hanloser/Burkhardt/Pottkämper, in: Schwartmann/Benedikt/Reif Datenschutz im Internet, Kapitel 10 Teil B, Rn. 50.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

3 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG).

4 Assion, Die Entwicklung des Datenschutzrechts, NJW 2025, 633.

5 Hanloser, Einwilligungsverwaltungs-Verordnung – Droht jetzt die Consent Management Fatigue? ZD 2022, 529.

6 Gutachten der Datenethikkommission, S. 21, 133, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6; vgl. auch Kühling/Sauerborn, Die Sinnhaftigkeit des § 26 TTDSG, ZD 2022, 531.

7 Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV) v. 06.02.2025 (BGBl. 2025 I Nr. 32) (Inkrafttreten gem. Art. 3 dieser VO am 01.04.2025).

8 Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 603.

9 Vgl. zu den technischen Grundlagen von Cookies: Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 604 f.

10 Hanloser/Burkhardt/Pottkämper in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 10 Teil B, Rn. 50 ff.; Klink-Straub/Straub, Und bist du nicht willig, so brauch' ich ... PIMS – Entwurf der Einwilligungsverwaltungsverordnung nach § 26 TDDDG, ZD-Aktuell 2024, 01820.

11 IAB Europe, Transparency & Consent Framework , abrufbar unter: https://iabeurope.eu/transparency-consent-framework/.

12 Keppeler in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B Rn. 357 ff.; Klink-Straub/Straub, Und bist du nicht willig, so brauch' ich ... PIMS – Entwurf der Einwilligungsverwaltungsverordnung nach § 26 TDDDG, ZD-Aktuell 2024, 01820.

13 Vgl. Bouhoula et al., USENIX Security Symposium 2024: Eine Analyse populärer Webseiten in der EU zeigt, dass viele Seiten derzeit so eingestellt sind, dass Werbe- und Analyse-Cookies auch ohne ausdrückliche Einwilligung gesetzt werden und Cookie-Banner durch sogenannte „Dark Patterns" gezielt irreführend gestaltet sind.

14 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

cy-Richtlinie durch das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)[15] umgesetzt.[16] § 25 TDDDG sieht in Umsetzung des Art. 5 Abs. 3 ePrivacy-RL vor, dass für das Speichern von Informationen und deren Auslesen vom Endgerät der Nutzer eine Einwilligung erforderlich ist.

Die Einwilligungsverwaltungsverordnung basiert konkret auf der gesetzlichen Vorgabe in § 26 Abs. 2 TDDDG, wonach „nutzerfreundliche und wettbewerbskonforme Verfahren" über sog. „anerkannte Dienste" zur Einholung der nach § 25 Abs. 1 TDDDG erforderlichen Einwilligung geschaffen werden sollen. Gemäß § 25 Abs. 1 TDDDG dürfen Informationen in der Endeinrichtung des Endnutzers nur gespeichert bzw. auf bereits vorhandene Informationen nur zugegriffen werden (also auch das Setzen von Cookies), wenn Nutzer vorher ausdrücklich eingewilligt haben – mit wenigen Ausnahmen, etwa für technisch notwendige Cookies (§ 25 Abs. 2 Nr. 2 TDDDG).[17]

§ 25 TDDDG ist immer dann anwendbar, sofern Informationen in der Endeinrichtung des Endnutzers gespeichert werden oder ein Zugriff auf Informationen erfolgt, die bereits in der Endeinrichtung gespeichert sind.[18] Der Tatbestand des § 25 TDDDG setzt nicht bereits bei jeder Verarbeitung von Informationen aus dem Endgerät des Nutzers ein, sondern erfordert vielmehr einen aktiven „Zugriff" auf diese Informationen.[19] Dies ergibt sich sowohl aus dem Wortlaut der Norm als auch ihrem spezifischen Schutzzweck, der nicht primär datenschutzrechtlicher Natur ist, sondern auf den Schutz der Privatsphäre im Kontext digitaler Endeinrichtungen abzielt.[20] Eingriffe in die Privatsphäre der Endnutzer erfolgen jedoch nicht ausschließlich durch Cookies, sondern potenziell beispielsweise auch durch sogenanntes Browser- oder Device-Fingerprinting, bei dem Nutzer anhand spezifischer Einstellungen ihres Endgeräts wiedererkannt werden können.[21] Beim Fingerprinting wird zwischen passivem und aktivem Fingerprinting unterschieden. Während beim passiven Fingerprinting lediglich solche Geräteinformationen verarbeitet werden, die der Browser von sich aus an den Webseitenbetreiber übermittelt (IP-Adresse, Browserinformationen (Hersteller und Version, i.d.R. auch Betriebssystem), sprachliche Präferenzen sowie technische Netzwerkparameter), erfolgt beim aktiven Fingerprinting ein gezielter Zugriff auf Informationen, die im Endgerät des Nutzers gespeichert sind.[22] Nur das aktive Fingerprinting stellt somit einen „Zugriff" im Sinne des § 25 TDDDG dar und unterliegt daher dem Einwilligungserfordernis dieser Norm. Passive Verfahren, die ohne Zugriff auf das Endgerät auskommen, erfordern hingegen keine Einwilligung nach § 25 Abs. 1 TDDDG.[23]

Die Konsequenz dieser Regelungen war eine explosionsartige Zunahme von Cookie-Bannern und Content-Management-Plattformen (CMPs) auf Webseiten, die in der Praxis jedoch nicht die gewünschte Wirkung erzielten. Eine Studie des Branchenverbandes Bitkom aus dem Jahr 2024 zeigt, dass 76 % der Internetnutzer Cookie-Banner als störend empfinden, während 21 % angaben, Einwilligungsanfragen routinemäßig zu akzeptieren, ohne sie zu lesen.[24] Dadurch wurde rasch deutlich, dass die bestehende Lösung nicht zu mehr Datenschutz, sondern lediglich zu einer formalen Erfüllung gesetzlicher Anforderungen führte, ohne dass sich die tatsächliche Entscheidungsfreiheit der Nutzer verbesserte.

Um dieser Entwicklung entgegenzuwirken, wurde die Einwilligungsverwaltungsverordnung (EinwV) als Ergänzung zum TDDDG ins Leben gerufen. Sie beruht auf der Verordnungsermächtigung gemäß § 26 Abs. 2 TDDDG. Die EinwV ermöglicht es einer unabhängigen Stelle (vorliegend der BfDI), zentrale Einwilligungsverwaltungsdienste zu zertifizieren und anzuerkennen.[25] Diese Dienste speichern die entsprechenden Datenschutzpräferenzen der Nutzer und geben sie automatisch an teilnehmende Webseiten weiter.

Die EinwV enthält Regelungen in drei zentralen Bereichen: Sie legt zum einen Anforderungen fest, die Dienste zur Einwilligungsverwaltung erfüllen müssen und regelt das Anerkennungsverfahren solcher Dienste. Zudem definiert sie technische und organisatorische Maßnahmen, die Anbieter digitaler Dienste sowie Hersteller und Anbieter von Software zur Darstellung digitaler Inhalte umsetzen müssen. Außerdem werden inhaltlich zwei Ebenen geregelt: Zum einen das Verhältnis zwischen Nutzern und dem Einwilligungsverwaltungsdienst, zum anderen die Beziehung zwischen dem Einwilligungsverwaltungsdienst und den Anbietern digitaler Dienste.[26]

Allerdings ist es wichtig zu erwähnen, dass die Einbindung eines anerkannten Dienstes zur Einwilligungsverwaltung für die Anbieter von digitalen Diensten gemäß § 18 Abs. 1 EinwV freiwillig ist. Zudem kann die EinwV und somit auch die Anerkennung der Einwilligungsverwaltungsdienste inhaltlich nur die im TDDDG verankerten Anforderungen nach § 25 Abs. 1 TDDDG regeln, während die Datenverarbeitungen nach der DS-GVO davon unberührt bleiben. Werden durch einen Endgerätezugriff zugleich personenbezogene Daten verarbeitet, müssen neben § 25 TDDDG auch die datenschutzrechtlichen Vorgaben der DS-GVO berücksichtigt werden. Liegen die Voraussetzungen für einen Zugriff nach § 25 Abs. 2 TDDDG vor, so besteht typischerweise gleichzeitig ein Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO, insbesondere aufgrund vertraglicher Verpflichtung oder berechtigter Interessen.[27] Ist hingegen nach § 25 Abs. 1 TDDDG eine Einwilligung erfor-

15 Hanloser/Burkhardt/Pottkämper, in: Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 10 Teil B, Rn. 2.

16 Am 12.02.2025 gab die Europäische Kommission bekannt, dass sie den Entwurf der ePrivacy-Verordnung zurückzieht. Somit wurden die Pläne zur Einführung der ePrivacy-Verordnung eingestellt.

17 Hanloser/Burkhardt/Pottkämper in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 10 Teil B, Rn. 8 ff.; Weiß/Schwartmann in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 322; DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von digitalen Diensten (OH Digitale Dienste) Version 1.2; Artikel-29-Datenschutzgruppe, Stellungnahme 04/2021 zur Ausnahme von Cookies von der Einwilligungspflicht, WP 194, 7 ff.

18 Schwartmann/Reif/Burkhardt in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 49.

19 Schwartmann/Reif/Burkhardt in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 54.

20 Schwartmann/Reif/Burkhardt in Schwartmann/Jaspers/Eckhardt TTDSG § 25 Rn. 12; aA Taeger/Gabel/Ettig TTDSG § 25 Rn. 16.

21 Alich/Voigt, Mitteilsame Browser – Datenschutzrechtliche Bewertung des Trackings mittels Browser-Fingerprints, CR, Band 28, Heft 5, 2012, 344 f.

22 Zur Abgrenzung von passivem und aktivem Fingerprinting vgl. Karg/Kühn, ZD 2014, 285 f.

23 Schwartmann/Reif/Burkhardt in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 56.

24 Bitkom, Presseinformation v. 25.03.2024, „Drei Viertel sind von Cookie-Bannern genervt", abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Drei-Viertel-von-Cookie-Bannern-genervt.

25 Kühling/Sauerborn, Die Sinnhaftigkeit des § 26 TTDSG, ZD 2022, 531 f.

26 Klink-Straub/Straub, Und bist du nicht willig, so brauch' ich ... PIMS – Entwurf der Einwilligungsverwaltungsverordnung nach § 26 TDDDG, ZD-Aktuell 2024, 01820.

27 Vgl. hierzu die Stellungnahme des Sachverständigen Golland zum RegE für ein TTDSG, Golland Ausschuss-Drs- 19(9)1054,4.

derlich, erstreckt sich diese Einwilligung regelmäßig sowohl auf den Zugriff als auch auf die personenbezogene Datenverarbeitung, wobei sich die Anforderungen an die Einwilligung aufgrund der Verweisung in § 25 Abs. 1 S. 2 TDDDG nach den Vorgaben der DS-GVO richten.[28]

II. Personal Information Management Systeme (PIMS) als Einwilligungsverwaltungsdienste

Der Gesetzgeber hat mit § 26 TDDDG eine Regelung eingeführt, die sogenannte Personal Information Management Systems (PIMS) betrifft. PIMS stellen in der Regel einen Unterfall von Datenvermittlungsdiensten dar.[29] Die EinwV adressiert konkret Einwilligungsverwaltungsdienste, die als spezielle Ausprägung von PIMS gelten. Das Verhältnis zwischen Einwilligungsverwaltungsdiensten und PIMS ist vielschichtig und weist sowohl Gemeinsamkeiten als auch wesentliche Unterschiede auf. Beide Konzepte verfolgen das Ziel, die Kontrolle von Nutzern über ihre personenbezogenen Daten zu stärken, unterscheiden sich jedoch in ihrem regulatorischen Rahmen, ihrem Funktionsumfang und ihrem Anwendungskontext.

Einwilligungsverwaltungsdienste sind ein spezifisches Konzept, das im Rahmen der EinwV geregelt wird. Die EinwV regelt explizit die Voraussetzungen, unter denen Dienste als Einwilligungsverwaltungsdienste anerkannt werden können. Sie müssen unabhängig und ohne kommerzielles Eigeninteresse an der Verarbeitung von Nutzerdaten agieren, um Vertrauen und Transparenz zu gewährleisten.[30]

PIMS hingegen sind ein umfassenderes Konzept zur Verwaltung personenbezogener Daten und existieren in sehr unterschiedlichen Ausprägungen.[31] Sie ermöglichen nicht nur die Steuerung von Einwilligungen, sondern können auch Funktionen wie Identitätsmanagement, Datenportabilität und umfassende Kontrollmöglichkeiten für personenbezogene Daten abdecken.[32] In der Praxis können PIMS als technische Grundlage für Einwilligungsverwaltungsdienste dienen. Da beide Konzepte darauf ausgerichtet sind, Nutzern mehr Kontrolle über ihre Daten zu geben, könnten PIMS sich als Einwilligungsverwaltungsdienste qualifizieren, sofern sie die Anforderungen der EinwV erfüllen.

Insgesamt ist festzuhalten, dass Einwilligungsverwaltungsdienste eine spezifische, gesetzlich geregelte Form von PIMS darstellen, die sich auf die Verwaltung von Online-Einwilligungen konzentrieren. PIMS hingegen bieten darüber hinaus erweiterte Möglichkeiten zur umfassenden Kontrolle personenbezogener Daten.[33] Beide Konzepte verfolgen das gemeinsame Ziel der Stärkung der Nutzerautonomie, wobei die Umsetzung und Wirksamkeit der Einwilligungsverwaltungsverordnung im praktischen Einsatz noch zu beobachten bleibt.

III. Anforderungen an Einwilligungsverwaltungsdienste

Die Anforderungen an anerkannte Einwilligungsverwaltungsdienste sind in der EinwV detailliert geregelt. Ein Dienst, der offiziell als „anerkannter Einwilligungsverwaltungsdienst" zugelassen ist, muss den Nutzerinnen und Nutzern ermöglichen, klar und eindeutig festzulegen, ob sie einer Speicherung von Informationen (z.B. Cookies) oder dem Zugriff auf bereits gespeicherte Informationen auf ihren Geräten zustimmen oder dies ablehnen möchten. Diese Einwilligung muss den Anforderungen der DS-GVO entsprechen – sie muss also freiwillig, informiert, ausdrücklich und widerruflich erfolgen (§ 3 Abs. 1 EinwV).

Der Dienst zur Einwilligungsverwaltung muss die getroffenen Entscheidungen („Willensbekundungen") der Nutzerinnen und Nutzer (also Zustimmung oder Ablehnung) speichern und verwalten. Wenn die Nutzerinnen und Nutzer später erneut denselben digitalen Dienst aufrufen (z.B. dieselbe Webseite oder App), übermittelt der Einwilligungsverwaltungsdienst automatisch ihre bereits gespeicherten Einstellungen an diesen Anbieter. So muss der Anbieter nicht bei jedem Besuch erneut fragen, ob Cookies oder andere Daten gespeichert werden dürfen (§ 3 Abs. 2 EinwV).

Gemäß § 3 Abs. 3 EinwV muss ein anerkannter Einwilligungsverwaltungsdienst es Endnutzern ermöglichen, Einwilligungen nach § 25 Abs. 1 TDDDG zu erteilen, abzulehnen und zu verwalten. Dabei muss der Dienst sicherstellen, dass Endnutzer umfassend über die folgenden Punkte informiert werden:

- den verantwortlichen Anbieter von digitalen Diensten,
- die Art der gespeicherten oder abgerufenen Informationen,
- der Zweck der Speicherung oder des Zugriffs,
- die Speicherdauer sowie die Dauer des Zugriffs auf die Informationen,
- die Widerruflichkeit der Einwilligung.

§ 3 Abs. 4 EinwV schreibt vor, dass die Einwilligung und alle dazugehörigen Details (z.B. Zweck, Umfang, Dauer der Datennutzung) transparent und für die Nutzer dauerhaft zugänglich dokumentiert werden müssen. So können Nutzer ihre Entscheidungen jederzeit nachvollziehen und überprüfen.

§ 4 EinwV stellt sicher, dass Dienste zur Einwilligungsverwaltung nutzerfreundlich gestaltet sind. Konkret heißt das: Die Benutzeroberfläche muss transparent sein, um freie und informierte Entscheidungen zu ermöglichen. Nutzerinnen und Nutzer müssen jederzeit Einblick in ihre Entscheidungen zur Einwilligung (inklusive Zeitstempel und relevanter Informationen) erhalten und diese Einstellungen jederzeit ändern können. Ändert sich die Art der Datennutzung, sollen

28 Schwartmann/Reif/Burkhardt, in: Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 98; Zippel/Benedikt in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 18 Teil B, Rn. 55.

29 Vgl. Schwartmann et al., Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zum Thema Entwurf eines Gesetzes zur Durchführung der EU-Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz – DGG) v. 13.11.2024; Stiemerling/Weiß/Wendehorst, Forschungsgutachten zum Einwilligungsmanagement nach § 26. TTDSG, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie v. 16.12.2021, Rn. 44.

30 Vgl. §§ 26 Abs. 1 Nr. 2 TDDDG, 11 Abs. 3 Nr. 6 EinwV.

31 Vgl. EDSB, TechDispatch #3/2020, abrufbar unter edps.europa.eu/data-protection/our-work/subjects/sys.teme-de-gestion-des-informations-personnelles_de.

32 Schwartmann et al., Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zum Thema Entwurf eines Gesetzes zur Durchführung der EU-Verordnung. Über europäische Daten-Governance (Daten-Governance-Gesetz – DGG) v. 13.11.2024, S. 12; Schwartmann/Jaspers/Eckhardt/Benedikt/Weiß, HK-TTDSG, § 26 Rn. 2.

33 Schwartmann et al., Stellungnahme im Rahmen der öffentlichen Anhörung des Deutschen Bundestages am 26. Juni 2024, S. 25 (abrufbar unter https://www.bundestag.de/resource/blob/1010058/15b3c22909f8abd112260e5eaa1cfdc1/Stellungnahme-Schwartmann.pdf).

Nutzerinnen und Nutzer aktiv erinnert werden, ihre früheren Einstellungen zu überprüfen – allerdings frühestens nach Ablauf eines Jahres, außer sie haben eine kürzere Frist selbst gewählt. Zudem muss der Dienst den Export der gespeicherten Informationen in gängige Formate ermöglichen und kann optional weitere Hilfestellungen anbieten, etwa Nutzerinnen und Nutzer auf unerlaubte Datenspeicherungen hinzuweisen oder sie bei der Wahrnehmung ihrer Datenschutzrechte (gemäß DS-GVO) zu unterstützen.

§ 5 EinwV bestimmt, dass Nutzerinnen und Nutzer jederzeit problemlos zu einem anderen anerkannten Einwilligungsverwaltungsdienst wechseln können müssen. Hierfür müssen die gespeicherten Einwilligungseinstellungen in einem standardisierten, maschinenlesbaren Format bereitgestellt werden, um einen unkomplizierten Transfer zwischen verschiedenen Diensten sicherzustellen.

§ 6 EinwV verlangt von Einwilligungsverwaltungsdiensten, dass sie wettbewerbsneutral agieren. Jeder Anbieter digitaler Dienste muss unter gleichen Bedingungen Einwilligungen der Nutzerinnen und Nutzer erfragen und deren Entscheidungen erhalten können. Außerdem müssen Anbieter digitaler Dienste einheitlich und alphabetisch geordnet dargestellt werden, und auch die Einwilligungseinstellungen müssen auf der Benutzeroberfläche klar und einheitlich präsentiert werden.

Zusätzlich verpflichtet § 7 EinwV anerkannte Einwilligungsverwaltungsdienste dazu, technische Lösungen bereitzustellen, die eine reibungslose Kommunikation mit digitalen Dienstleistern ermöglichen. Anbieter digitaler Dienste und Software müssen in der Lage sein, die Nutzung eines Dienstes zu erkennen, Einwilligungsanfragen ohne Aufwand weiterzuleiten und den Stand der Einwilligungen – ob erteilt oder abgelehnt – jederzeit nachvollziehen zu können. Die Einwilligungsentscheidungen werden gespeichert und bei jedem weiteren Aufruf des digitalen Dienstes automatisch übermittelt. Falls erforderlich, kann die zuständige Behörde durch technische Richtlinien detaillierte Anforderungen festlegen, um eine sichere Datenübertragung und eine ordnungsgemäße Dokumentation im Sinne der DS-GVO zu gewährleisten.

Schließlich muss der Dienst gemäß § 10 EinwV ein Sicherheitskonzept vorlegen, das den Schutz personenbezogener Daten und der Einwilligungsentscheidungen gewährleistet. Dieses Konzept muss Maßnahmen zur Vertraulichkeit, Integrität und Verfügbarkeit der Daten enthalten (§ 10 Abs. 2 Nr. 1-6 EinwV).

Die Anerkennung eines Einwilligungsverwaltungsdienstes erfolgt nach den Vorgaben von § 8 EinwV, wobei der Anbieter einen entsprechenden Antrag stellen und die Einhaltung der genannten Anforderungen nachweisen muss. Der Antrag auf Anerkennung gemäß § 9 EinwV kann auf elektronischem Wege erfolgen.[34] Zuständig für die Anerkennung ist gemäß § 12 EinwV die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Es werden entsprechende Gebühren für die Bearbeitung des Antrags erhoben.[35] Anerkannte Dienste werden gemäß § 13 EinwV zukünftig in einem öffentlichen Register der BfDI geführt.[36]

1. Kein wirtschaftliches Eigeninteresse (§ 26 Abs. 1 Nr. 2 TDDDG): Aktuelle Diskussion

Die Voraussetzung des fehlenden wirtschaftlichen Eigeninteresses (§ 9 Abs. 1 S. 1 Nr. 7 EinwV, § 26 Abs. 1 Nr. 2 TDDDG) besagt, dass anerkannte Dienste zur Einwilligungsverwaltung neutral und unabhängig von wirtschaftlichen Interessen an der Datenerhebung und Nutzung sein müssen.[37] Dies bedeutet konkret, dass die Anbieter solcher Dienste kein eigenes finanzielles Interesse daran haben dürfen, möglichst viele Einwilligungen zu sammeln oder die Daten für eigene Zwecke zu nutzen. Ziel dieser Regelung ist es, Interessenkonflikte zu vermeiden und die Neutralität der Einwilligungsverwaltungsdienste zu gewährleisten.

Der Verbraucherzentrale Bundesverband (vzbv) gab kürzlich ein Gutachten zum Thema Tracking und Profilbildung zu Werbezwecken in Auftrag.[38] Ein zentraler Aspekt, der im Gutachten diskutiert wird, ist, dass wirtschaftliche Interessen im Bereich personalisierter Werbung sehr ausgeprägt sind und erhebliche Risiken für Nutzer und Gesellschaft darstellen. So bestehe ein grundlegender Konflikt zwischen dem wirtschaftlichen Interesse der Anbieter, möglichst umfassend Daten zu sammeln und zu monetarisieren, und dem datenschutzrechtlichen Schutzinteresse der Betroffenen.[39]

2. IAB TCF 2.2 als Dienst zur Einwilligungsverwaltung

Im Kontext der Einwilligungsverwaltungsverordnung (EinwV) wird das Transparency & Consent Framework (TCF 2.2) des Interactive Advertising Bureau (IAB Europe) bislang kaum als potenziell anerkannter Dienst gemäß § 26 Abs. 2 TDDDG bzw. EinwV diskutiert. Zwar bietet das TCF 2.2 einen weit verbreiteten technischen Standard zur Einholung und Weiterleitung von Einwilligungen im Bereich personalisierter Online-Werbung. Seine Ausgestaltung orientiert sich jedoch primär an den wirtschaftlichen Interessen der Werbewirtschaft und weist erhebliche Flexibilität bei der Implementierung auf, was zu Inkonsistenzen führen kann. Zudem stehen strukturelle Defizite hinsichtlich Transparenz und Datenschutzkonformität im Mittelpunkt intensiver Kritik durch Datenschutzbehörden, insbesondere seitens der belgischen Aufsichtsbehörde, die Untersuchungen und Verfahren im Zusammenhang mit dem TCF führt. Angesichts dieser Umstände erscheint es derzeit unwahrscheinlich, dass das TCF 2.2 als neutraler, anerkannter Dienst zur Einwilligungsverwaltung im Sinne der EinwV anerkannt werden könnte, da es nicht auf spezifische nationale Anforderungen, sondern vorrangig auf die globale Werbebranche ausgerichtet ist.[40]

34 Vgl. Elektronischer Antrag nach § 10 EinwV, abrufbar unter: https://formulare.bfdi.bund.de/lip/form/display.do?%24context=E304D3D76546AE846EA7.

35 Es fallen Gebühren gemäß § 1 Abs. 1 Nr. 7 Besondere Gebührenverordnung Telekommunikation (BMDVTKBGebV) an; Vgl. auch Schwartmann et al., Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zum Thema Entwurf eines Gesetzes zur Durchführung der EU-Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz – DGG) v. 13.11.2024, S. 14; BT-Drs. 20/12718, S. 3 f.

36 Nähere Informationen auf der Webseite der BfDI, abrufbar unter: https://www.bfdi.bund.de/DE/Fachthemen/Themen-Positionen/Einwilligungsverwaltung/Einwilligungsverwaltung_node.html.

37 Weiß/Schwartmann in Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 329 ff.

38 Vzbv-Gutachten, von Grafenstein/Herbort, Regulation of Online Advertising, Dezember 2024, abrufbar unter: https://www.vzbv.de/sites/default/files/2025-02/vzbv-Gutachten_Expert-Opinion_Grafenstein_Herbort_Online-Advertising.pdf.

39 Vzbv-Gutachten, von Grafenstein/Herbort, Regulation of Online Advertising, Dezember 2024, S. 65, abrufbar unter: https://www.vzbv.de/sites/default/files/2025-02/vzbv-Gutachten_Expert-Opinion_Grafenstein_Herbort_Online-Advertising.pdf.

40 Keppeler, in: Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 9 Teil B, Rn. 397 ff.

IV. Praktische Schritte zur Implementierung der EinwV in Unternehmen

Die Einführung der EinwV und damit verbundene Implementierung eines anerkannten Einwilligungsverwaltungsdienstes bringt erhebliche Veränderungen für Unternehmen mit sich, insbesondere für diejenigen, die digitale Geschäftsmodelle betreiben oder auf Online-Werbung angewiesen sind. Die Umstellung auf eine zentrale Einwilligungsverwaltung erfordert eine strategische Planung, technologische Anpassungen und ein Bewusstsein für die rechtlichen Implikationen. Unternehmen, die sich frühzeitig mit der Umsetzung der EinwV auseinandersetzen, können nicht nur die gesetzlichen Vorgaben leichter einhalten, sondern auch ihr Ansehen als vertrauenswürdiger Anbieter digitaler Dienstleistungen stärken.

1. Bestandsaufnahme der aktuellen Cookie- und Tracking-Technologien

Der erste Schritt besteht darin, eine genaue Bestandsaufnahme der aktuell eingesetzten Cookie- und Tracking-Technologien durchzuführen. Unternehmen müssen hierzu zunächst herausfinden, welche Cookies und Tracking-Tools momentan auf ihren Webseiten und in mobilen Anwendungen genutzt werden. Wichtig ist dabei, zu klären, welche Cookies genau eingesetzt werden, wo auf der Webseite sie verwendet werden und für welche Zwecke die gesammelten Daten genutzt werden. Außerdem sollten die Unternehmen untersuchen, in welche Kategorien (essenzielle, funktionale, analytische oder marketingbezogene Cookies) sich die vorhandenen Technologien einteilen lassen. Ebenfalls wichtig ist es, externe Dienstleister und Werbenetzwerke zu identifizieren und zu prüfen, ob und wie Daten an Dritte übermittelt werden.

2. Auswahl eines geeigneten Einwilligungsverwaltungsdienstes

Nach Abschluss der Bestandsaufnahme folgt die Auswahl eines geeigneten, anerkannten Einwilligungsverwaltungsdienstes. Unternehmen sollten hierbei mehrere Kriterien sorgfältig berücksichtigen, um eine Lösung zu finden, die sowohl den technischen als auch rechtlichen Anforderungen gerecht wird. Zu den wesentlichen Auswahlkriterien zählen insbesondere Datenschutz und Sicherheit, wobei der Dienst alle Vorgaben der DS-GVO, des TDDDG sowie der EinwV erfüllen und zertifizierte Sicherheitsstandards nachweisen muss. Auch Interoperabilität ist entscheidend, sodass die Lösung reibungslos in bestehende Systeme und digitale Infrastrukturen integriert werden kann.[41] Darüber hinaus sind Benutzerfreundlichkeit und intuitive Bedienbarkeit sowohl für Endnutzer als auch Administratoren unverzichtbar, um Akzeptanz und effiziente Nutzung sicherzustellen. Ebenfalls wichtig sind umfassende Reporting- und Audit-Funktionalitäten, die eine vollständige Dokumentation aller Einwilligungsentscheidungen ermöglichen und im Falle behördlicher Prüfungen schnelle Berichtserstellung gewährleisten. Schließlich sollte die ausgewählte Lösung flexibel und anpassbar sein, um die Einwilligungsoptionen spezifischen geschäftlichen Bedürfnissen anzupassen und gegebenenfalls weitere Kategorien einzubeziehen.

V. Auswirkungen auf Unternehmen und Nutzer

Die Einführung der EinwV hat weitreichende Folgen für Unternehmen und Endnutzer. Während Nutzer von erhöhter Transparenz und Benutzerfreundlichkeit profitieren, können Unternehmen Kosten einsparen und ihre Compliance verbessern. Dennoch gibt es Herausforderungen, insbesondere im Bereich der technischen Umsetzung und der Abhängigkeit von Drittanbietern.

1. Vorteile für Nutzer

Die zentrale Verwaltung der Einwilligungsentscheidungen bietet für Endnutzer zahlreiche Vorteile. Ein zentrales Dashboard erlaubt es, alle Datenschutzentscheidungen an einem Ort einzusehen, zu verwalten und zu ändern. Nutzer müssen gerade nicht mehr bei jedem Webseitenbesuch erneut auf Cookie-Banner reagieren, sondern können eine einmal getroffene Entscheidung für verschiedene Plattformen anwenden.[42] Dies führt zu einer verbesserten Nutzererfahrung und einer Reduktion von „Consent Fatigue", also der Ermüdung durch ständige Einwilligungsabfragen. Zusätzlich stärkt die erhöhte Transparenz das Vertrauen der Nutzer in digitale Dienste. Sie erhalten einen klaren Überblick darüber, welche Daten gesammelt und zu welchem Zweck verwendet werden. Insbesondere in sensiblen Bereichen wie Online-Banking oder Gesundheits-Apps ist diese Kontrolle entscheidend, da hier personenbezogene Daten höchst sensibel behandelt werden müssen.[43]

2. Vorteile für Unternehmen

Auch für Unternehmen bringt die Implementierung der EinwV Vorteile. Die zentrale Erfassung und Verwaltung von Einwilligungen kann den administrativen Aufwand reduzieren und zugleich die Betriebskosten senken. Mit der EinwV kann nun eine einheitliche Schnittstelle genutzt werden, die automatisch sicherstellt, dass alle Datenschutzvorgaben eingehalten werden. Dies minimiert Compliance-Risiken und erleichtert den Nachweis der rechtmäßigen Datennutzung gegenüber Aufsichtsbehörden. Für Unternehmen kann der Einsatz von Einwilligungsverwaltungsdiensten auch besonders sinnvoll für die Erfüllung von Rechenschaftspflichten sein, da diese Dienste unter Berücksichtigung von technischen und organisatorischen Maßnahmen anerkannt werden.[44]

Ein weiterer Vorteil ist die verbesserte Nutzererfahrung: Weniger Einwilligungsanfragen können eine höhere Verweildauer auf Webseiten bedeuten, was sich positiv auf Conversion-Raten und die allgemeine Kundenbindung auswirkt. Zudem verbessert sich das Markenimage von Unternehmen, die als Vorreiter bei der Umsetzung datenschutzkonformer Lösungen auftreten. Firmen, die Transparenz und Datenschutz als Wettbewerbsvorteil nutzen, können so neue Kundengruppen ansprechen und langfristig das Vertrauen in ihre digitalen Angebote erhöhen.

41 Rudolph in HK-DS-GVO/BDSG, Art. 20 Rn. 80 f.

42 Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 603.

43 Jaspers/Schwartmann/Mühlenbeck in HK-DS-GVO/BDSG, Art. 9, Rn. 1 ff.

44 Zippel/Benedikt, in: Schwartmann/Benedikt/Reif, Datenschutz im Internet, Kapitel 18 Teil B, Rn. 55.

3. Herausforderungen und Risiken

Die Einführung eines zentralen Einwilligungsverwaltungsdienstes bietet zwar viele Vorteile, ist jedoch zugleich mit einer Reihe von Herausforderungen und Risiken verbunden. Zunächst stellt die technische Umsetzung eine wesentliche Hürde dar: Die Integration eines EV-Dienstes in bestehende IT-Systeme kann sich als komplex, zeitaufwendig und kostenintensiv erweisen, insbesondere für kleinere Unternehmen oder solche, die ältere IT-Systeme einsetzen. Häufig sind dabei zusätzliche Investitionen in Softwarelösungen sowie Beratung erforderlich, um die Systeme an die neuen Anforderungen anzupassen.

Ein weiteres Risiko besteht darin, dass die Nutzung der zentralen Einwilligungsverwaltung für Webseitenbetreiber freiwillig bleibt.[45] Wenn nur ein Teil der Anbieter einen solchen Dienst verwendet, entsteht für Nutzer ein fragmentiertes Umfeld, das weiterhin durch uneinheitliche Einwilligungsbanner und unterschiedliche Datenschutzpraktiken geprägt ist. Dies könnte zu Verwirrung oder Unsicherheit führen, da Nutzer nicht immer einheitlich auf die zentrale Verwaltung ihrer Datenschutzpräferenzen vertrauen können. Auch die Frage der Neutralität anerkannter Dienste ist zentral: Sie dürfen kein eigenes wirtschaftliches Interesse an den verwalteten Daten haben. Dies könnte die Attraktivität für potenzielle Anbieter mindern, da deren Geschäftsmodelle möglicherweise durch diese Vorgabe erheblich eingeschränkt werden. Derzeit gibt es daher Bedenken, ob überhaupt genügend Anbieter von Einwilligungsdiensten die strengen Voraussetzungen erfüllen und eine Anerkennung durch die BfDI anstreben werden.

Darüber hinaus bestehen Bedenken hinsichtlich der Datensicherheit und des Datenschutzes. Da Einwilligungsentscheidungen zentral gespeichert werden, könnten diese Daten zum Ziel für Cyberangriffe werden, wodurch erhebliche Risiken für Nutzer und Unternehmen entstehen. Hinzu kommt die Befürchtung, dass marktbeherrschende Unternehmen – beispielsweise große Anbieter wie Google oder Meta – ihre Marktmacht nutzen könnten, um eigene EV-Dienste durchzusetzen und somit indirekt Einfluss auf die Datenschutzentscheidungen der Nutzer auszuüben. Unternehmen müssen daher sehr genau prüfen, welchen Dienstleister sie auswählen und klare vertragliche Regelungen zur Datensicherheit und Haftung treffen.

Zusätzlich können rechtliche Unsicherheiten auftreten, besonders für Unternehmen, die international tätig sind, da die Einwilligungsverwaltung nach wie vor in verschiedenen Ländern unterschiedlich geregelt ist. Solange keine internationalen Standards existieren, müssen Unternehmen weiterhin unterschiedliche Datenschutzregelungen berücksichtigen, was die Umsetzung zusätzlich erschwert.

VI. Kritik

Die Einwilligungsverwaltungsverordnung steht in der Kritik, da sie nach Ansicht vieler Datenschützer und Verbraucherschutzorganisationen ihr erklärtes Ziel – eine spürbare Vereinfachung der Einwilligungsverwaltung und die Reduktion lästiger Consent-Banner – nur unzureichend erfüllt.[46]

Ein zentraler Kritikpunkt betrifft die begrenzte Reichweite der Verordnung. Sie regelt lediglich Einwilligungen nach § 25 Abs. 1 TDDDG, nicht jedoch solche nach der DS-GVO. Dies bedeutet, dass viele datenschutzrechtliche Zustimmungen weiterhin individuell verwaltet werden müssen. Sowohl die Datenschutzkonferenz (DSK)[47], einzelne Datenschutzbehörden als auch der Verbraucherzentrale Bundesverband (vzbv)[48] bemängeln, dass dieses eingeschränkte Anwendungsfeld die angestrebte Vereinfachung erheblich einschränkt.

Ein weiteres Problem stellt die fortgesetzte Nutzung von Consent-Bannern dar. Kritiker wie der Landesbeauftragte für Datenschutz Niedersachsen, Denis Lehmkemper[49], heben hervor, dass die Verordnung keinen sofort spürbaren Effekt gegen die Vielzahl an Einwilligungsbannern bringt. Da die Einwilligungen zunächst weiterhin über klassische Banner eingeholt werden müssen und der Einwilligungsstatus erst beim zweiten Besuch[50] der Webseite automatisch übermittelt wird, bleibt der gewünschte Effekt – weniger störende Banner – aus.

Auch die Freiwilligkeit der Nutzung von anerkannten Einwilligungsverwaltungsdiensten wird kritisch gesehen. Hier sehen sowohl Lehmkemper als auch der vzbv die Gefahr, dass Webseitenbetreiber aus wirtschaftlichen Interessen heraus weiterhin herkömmliche Consent-Banner einsetzen und die neuen Dienste somit kaum Anwendung finden.

Darüber hinaus kritisiert der vzbv die Verordnung als technikzentriert und praxisfern. Die vorgegebenen technischen Anforderungen seien teils unklar und schwer umzusetzen, was die Bereitschaft der Anbieter zusätzlich verringern könnte. Zudem konzentriere sich die Verordnung primär auf browserbasierte Anwendungen und vernachlässige damit andere Technologien wie IoT-Geräte[51], was den Anspruch der Technikneutralität untergrabe.

Ein weiterer gravierender Kritikpunkt ist die fehlende Verbindlichkeit für Webseitenbetreiber. Es bleibt ihnen vollständig freigestellt, ob und wie sie mit Einwilligungsverwaltungsdiensten zusammenarbeiten. Dies widerspricht aus Sicht des vzbv dem eigentlichen Ziel der Verordnung, da Anbieter trotz der Einbindung eines Einwilligungsverwaltungsdienstes parallel eigene Consent-Banner einsetzen könnten. Dadurch könnte sich die Bannerflut kaum verringern und die angestrebte Verbesserung für Verbraucherinnen und Verbraucher ausbleiben.[52]

Besonders kritisch bewertet der vzbv zudem die Möglichkeit wiederholter Abfragen. Selbst wenn Nutzerinnen und

45 Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 609.

46 Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 608.

47 DSK, Stellungnahme v. 11.07.2023 zum Referentenentwurf des BMDV zur Rechtsverordnung nach § 26 Abs. 2 TTDSG (heute TDDDG), abrufbar unter: https://lfd.niedersachsen.de/download/213724/.

48 Verbraucherzentrale Bundesverband e.V., Stellungahme „Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten", v. 04.09.2024, abrufbar unter: https://www.vzbv.de/sites/default/files/2024-09/24-09-04_Stellungnahme_vzbv_RegE_EinwV.pdf.

49 Vgl. Pressemitteilung Nr. 20/2024, Landesbeauftragte für den Datenschutz Niedersachsen, Denis Lehmkemper, abrufbar unter: https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/verabschiedete-einwilligungsverwaltungsverordnung-verfehlt-ihr-eigentliches-ziel-238383.html.

50 Hunter/Ebert/Spiecker gen. Döhmann, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, Rn. 607.

51 Vgl. auch die EDSA Leitlinien 02/2023 zum technischen Anwendungsbereich von Art. 5 Abs. 3 e-Privacy-RL.

52 Verbraucherzentrale Bundesverband e.V., Stellungahme „Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten", v. 4.9.2024, S. 9, abrufbar unter: https://www.vzbv.de/sites/default/files/2024-09/24-09-04_Stellungnahme_vzbv_RegE_EinwV.pdf.

Nutzer eine Einwilligung abgelehnt haben, dürfen Anbieter digitaler Dienste laut der EinwV diese dennoch beliebig oft erneut abfragen. Dies führe dazu, dass Verbraucherinnen und Verbraucher sich unter Druck gesetzt fühlen könnten, schließlich doch einzuwilligen, was die Freiwilligkeit der Entscheidung im Sinne der DS-GVO gefährdet.[53] Hinzu kommt die Gefahr eines "Rosinenpickens" durch Webseitenbetreiber. Der vzbv warnt davor, dass Anbieter gezielt bestimmte Einwilligungsverwaltungsdienste bevorzugen könnten, die möglicherweise weniger strenge Standards an Transparenz und Datenschutz anlegen. Um dies zu verhindern, fordert der vzbv klare Vorgaben zur verpflichtenden und einheitlichen Integration von Einwilligungsverwaltungsdiensten.[54]

VII. Fazit

Der neue Rechtsrahmen für die Anerkennung von neuen Diensten zur Einwilligungsverwaltung durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) soll nutzerfreundliche und wettbewerbskonforme Verfahren bereitstellen, um die nach dem TDDDG erforderlichen Einwilligungen von Endnutzern zu verwalten. Die Wirksamkeit der neuen Regelungen der EinwV soll innerhalb von zwei Jahren überprüft werden. Dabei wird untersucht, ob die Vorgaben und die damit verbundenen Schutzmaßnahmen ausreichend sind, um tatsächlich positive Effekte für Nutzerinnen und Nutzer zu erzielen. Darüber hinaus wird angestrebt, langfristig eine europaweit einheitliche Lösung für Dienste zur Einwilligungsverwaltung zu erreichen.[55] Sollte sich im Rahmen der geplanten Evaluation zeigen, dass die freiwillige Nutzung anerkannter Einwilligungsdienste nicht zu der gewünschten Datenschutzverbesserung führt, könnte dies laut Aussage der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Prof. Dr. Louisa Specht-Riemenschneider, dazu führen, dass die Einbindung solcher Dienste künftig verpflichtend wird.[56]

Zusammenfassend lässt sich feststellen, dass die Einwilligungsverwaltungsverordnung zwar auf dem Papier eine deutliche Verbesserung für Nutzerinnen und Nutzer darstellen könnte, die Praxisnähe und die tatsächliche Wirksamkeit jedoch derzeit fraglich erscheinen. Solange Anbieter digitaler Dienste nicht verbindlich verpflichtet werden, anerkannte Dienste zur Einwilligungsverwaltung einzusetzen, besteht das Risiko, dass die Regelung ihr eigentliches Ziel – die nachhaltige Verbesserung von Datenschutz und Nutzerfreundlichkeit – nicht erreichen wird. Die EinwV könnte somit zu einem gut gemeinten, aber letztlich zahnlosen Instrument verkommen, dessen praktische Auswirkungen durch die Freiwilligkeit seiner Anwendung deutlich geschwächt werden. Langfristig wäre daher eine verbindliche, europaweit einheitliche Lösung wünschenswert, um tatsächliche Fortschritte beim Einwilligungsmanagement und im Datenschutz erzielen zu können.

Eva-Maria Pottkämper, LL.M. (TH Köln), LL.M. (TH Passau)
ist Diplom-Juristin mit Schwerpunkt im Datenschutz- und Digitalisierungsrecht. In den vergangenen Jahren war sie zudem als wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht der TH Köln tätig.

53 Verbraucherzentrale Bundesverband e.V., Stellungahme „Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten", v. 4.9.2024, S. 10, abrufbar unter: https://www.vzbv.de/sites/default/files/2024-09/24-09-04_Stellungnahme_vzbv_RegE_EinwV.pdf.

54 Verbraucherzentrale Bundesverband e.V., Stellungahme „Kein Rosinenpicken beim Einsatz von Einwilligungsverwaltungsdiensten", v. 4.9.2024, S. 9, abrufbar unter: https://www.vzbv.de/sites/default/files/2024-09/24-09-04_Stellungnahme_vzbv_RegE_EinwV.pdf.

55 Vgl. Bundestag Drucksache 20/13418 und entspr. Entschließung des Bundesrats; https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2024/24_Einwilligungsverordnung.html.

56 Stiftung Datenschutz, Datenschutz 2025 – Schwerpunkte und Herausforderungen in der Datenschutzpolitik mit Prof. Dr. Louisa Specht-Riemenschneider v. 16.01.2025, abrufbar unter: https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datenschutz-2025-schwerpunkte-und-herausforderungen-541.

Praxisfälle zum Datenschutzrecht XXXVI: Datenverarbeitungserlaubnis in Allgemeinen Geschäftsbedingungen (AGB)?

RAin Yvette Reif, LL.M.*

I. Sachverhalt

Versicherungsunternehmen V setzt im Log-In-Bereich seines Internetauftritts seit einigen Monaten einen KI-Chatbot ein, um den Versicherungsnehmern eine schnelle und möglichst unkomplizierte Bearbeitung ihrer Serviceanliegen zu ermöglichen. Der KI-Chatbot der Versicherung unterstützt z.B. mit Blick auf die Aktualisierung der Daten des Versicherungsnehmers bzw. der Versicherungsnehmerin, die Anforderung von Versicherungsangeboten, die Information mit Blick auf den Versicherungsumfang sowie die Geltendmachung von Schäden und die Einreichung von Rechnungen.

Um möglichst effektiv unterstützen zu können, wird der Chatbot seit Beginn seines Einsatzes ständig weiterentwickelt. Grundlage der Weiterentwicklung bildet insbes. eine Auswertung bislang erfolgter Interaktionen, d.h., es wird analysiert, wie die Benutzer/-innen mit dem Chatbot interagieren, welche Fragen häufig gestellt werden und wo in der Praxis Probleme entstehen. Um das Training des Chatbots datenschutzrechtlich abzusichern, hat V seine wirksam einbezogenen Allgemeinen Geschäftsbedingungen (AGB) um eine Klausel erweitert, die besagt, dass dem Unternehmen das Recht zusteht, Kommunikationen des Versicherungsnehmers mit dem Chatbot auszuwerten, um die anonymisierten Ergebnisse für die Weiterentwicklung des KI-Chatbots zu nutzen. Auf technischer Ebene ist sichergestellt, dass die Analyse nur mit Blick auf solche Versicherungsnehmer/-innen erfolgt, für die bereits die aktualisierten AGB gelten. Die Unterscheidung der Versicherungsnehmer/-innen erfolgt über die Zugangsdaten zum Log-In-Bereich, welche mit der bei Registrierung anzugebenden Versicherungsnummer verknüpft sind.

Die Gestaltung über die Einräumung einer datenschutzrechtlichen Erlaubnis in den AGB wurde bewusst gewählt, da sich die Unternehmensleitung nicht auf die ihrer Meinung nach „unsichere Rechtsgrundlage" aus Art. 6 Abs. 1 lit. f) DS-GVO (sog. Interessenabwägung) berufen will. Da insofern nicht in eine Abwägung eingetreten werden müsse, mit Blick auf welche die zuständige Datenschutzaufsicht bzw. die Gerichte stets zu einer anderen Ansicht kommen könnten, biete die vertragliche Konstruktion mehr Rechtssicherheit, so die Leitung. V informiert die Versicherungsnehmer/-innen auch nicht über mögliche berechtigte Interessen und ihr Widerspruchsrecht.

Hat die Leitung Recht? Werden die Daten der Versicherungsnehmer/-innen aktuell zulässigerweise zum Zwecke des KI-Trainings verwendet?

II. Musterlösung

1. Allgemeines zum Verhältnis der Erlaubnistatbestände in Art. 6 Abs. 1 DS-GVO

Die Verarbeitung personenbezogener Daten unterliegt – auch wenn sie in einer AGB-Klausel ausgestaltet ist – angesichts der unmittelbaren Geltung der DS-GVO stets den datenschutzrechtlichen Vorgaben, sodass bei Vorliegen personenbezogener Daten auch ein Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 DS-GVO erfüllt sein muss.[1]

Die analysierten Chatverläufe stellen personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO dar, da über die Zugangsinformationen zum Log-In-Bereich nachvollzogen werden kann, welche konkrete natürliche Person jeweils mit dem Chatbot der Versicherung kommuniziert. Die KI-VO enthält keine speziellen auf KI-Systeme zugeschnittenen Regelungen mit Blick auf die personenbezogene Datenverarbeitung, vielmehr sind die allgemeinen Rechtsgrundlagen der DS-GVO heranzuziehen.

Nach Art. 6 Abs. 1 S. 1 Hs. 1 DS-GVO ist eine Verarbeitung personenbezogener Daten nur rechtmäßig, wenn „mindestens" einer der nachfolgend aufgezählten Erlaubnistatbestände erfüllt ist. Die in Art. 6 Abs. 1 S. 1 DS-GVO aufgeführten Erlaubnistatbestände stehen demzufolge im Ausgangspunkt gleichrangig nebeneinander und Verantwortliche sind grundsätzlich frei, auf welche Legitimationsgrundlage sie ihre Datenverarbeitung stützen wollen,[2] vorausgesetzt, die Voraussetzungen des jeweiligen Erlaubnistatbestandes sind erfüllt bzw. – im Falle der Einwilligung – werden noch erfüllt.

Im Bereich der Privatwirtschaft stellen Art. 6 Abs. 1 lit. a) (Einwilligung), lit. b) (Vertrag bzw. vorvertragliche Maßnahmen auf Anfrage der betroffenen Person) und lit. f) DS-GVO (Interessenabwägung) die datenschutzrechtlichen Rechtsgrundlagen mit der größten praktischen Bedeutung dar. Entgegen der Reihenfolge in Art. 6 Abs. 1 DS-GVO stellt die Einwilligung dabei in der Praxis allerdings nicht das erste Mittel der Wahl dar, sondern vielmehr lediglich einen Auffangtatbestand, sofern sich die Datenverarbeitung nicht mit hinreichender Rechtssicherheit auf Art. 6 Abs. 1 lit. b) bzw. lit. f) DS-GVO stützen lässt.

Gemäß dem erklärten Willen des Versicherungsunternehmens soll Erlaubnistatbestand für die Datenverarbeitung zwecks Weiterentwicklung des Chatbots vorliegend Art. 6 Abs. 1 lit. b) DS-GVO bilden. Damit sich das Versicherungsunternehmen tatsächlich auf Art. 6 Abs. 1 lit. b) DS-GVO berufen kann, müssten die tatbestandlichen Voraussetzungen dieser Norm erfüllt sein.

2. Vorliegen der Voraussetzungen von Art. 6 Abs. 1 lit. b) DS-GVO

a) Bestehen eines Vertrages

Art. 6 Abs. 1 lit. b) DS-GVO gestattet personenbezogene Datenverarbeitungen, sofern diese für die Erfüllung eines Vertrags erforderlich sind, dessen Vertragspartei die betroffe-

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

1 BeckOK IT-Recht/Munz, 19. Ed. 01.07.2024, BGB § 307 Rn. 22 f.

2 Vgl. etwa Kühling/Buchner/Buchner/Kühling, DS-GVO BDSG, 4. Aufl. (2024), DS-GVO Art. 7 Rn. 16.

ne Person ist. Für die Anwendbarkeit von Art. 6 Abs. 1 lit. b) DS-GVO könnte vorliegend sprechen, dass die Berechtigung zur Datenauswertung zwecks Trainings der KI über die diesbezügliche AGB-Bestimmung Gegenstand der vertraglichen Vereinbarung zwischen dem Versicherungsunternehmen und seinen Versicherungsnehmern geworden ist.

Allgemeine Geschäftsbedingungen (AGB) sind nach § 305 Abs. 1 S. 1 Bürgerliches Gesetzbuch (BGB) alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt. Die nach dem Sachverhalt zu unterstellende „Einbeziehung" von AGB bezeichnet im deutschen Zivilrecht den rechtlichen Prozess, durch den vorformulierte Vertragsbedingungen Teil eines Vertrages werden (vgl. hierzu im Einzelnen § 305 Abs. 2 BGB).

b) Enge Auslegung von Art. 6 Abs. 1 lit. b) DS-GVO

Zu beachten ist allerdings, dass es nach dem EuGH einer engen Auslegung von Art. 6 Abs. 1 lit. b) DS-GVO bedarf. Konkret hat der EuGH insofern ausgeführt, dass der Anwendungsbereich von Art. 6 Abs. 1 lit. b) DS-GVO nicht bereits dadurch eröffnet wird, dass eine Verarbeitung im Vertrag erwähnt oder für dessen Erfüllung lediglich von Nutzen ist.[3] Von der Notwendigkeit einer restriktiven Auslegung des Erlaubnistatbestandes gehen zudem auch die europäischen Datenschutzaufsichtsbehörden[4] sowie die herrschende Datenschutzliteratur[5] aus. Zwecks Feststellung, in welchem Umfang eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b) DS-GVO erforderlich ist, ist demzufolge die „vertragscharakteristische Leistung" des Schuldverhältnisses zu bestimmen, d.h. das, was spezifisches Charakteristikum des vom Anbieter erbrachten Dienstes ist.[6] Lediglich solche personenbezogenen Datenverarbeitungen, die im Zusammenhang mit dieser vertragscharakteristischen Leistung stehen, sind nach der Auffassung von EuGH, EDSA und herrschender Literatur über Art. 6 Abs. 1 lit. b) DS-GVO gestattet.

Für die beschriebene enge Auslegung von Art. 6 Abs. 1 lit. b) DS-GVO sprechen gute Gründe: Würde man es für eine Anwendbarkeit von Art. 6 Abs. 1 lit. b) DS-GVO genügen lassen, wenn sich ein Verantwortlicher „bei Gelegenheit" des Vertragsschlusses Datenverarbeitungen gestatten lässt, welche mit den Beweggründen, warum die Vertragsbeziehung eingegangen wurde, nicht mehr in unmittelbarem Zusammenhang stehen, so könnten Verantwortliche mit entsprechender Verhandlungsmacht die gesetzliche Zulässigkeitsregelung nahezu beliebig zu ihren Gunsten ausdehnen und auf diesem Weg die Grenzen umgehen, die sich aus dem Koppelungsverbot (Art. 7 Abs. 4 DS-GVO)[7] ergeben.[8] Hintergrund der gesetzlichen Verarbeitungserlaubnis in Art. 6 Abs. 1 lit. b) DS-GVO ist, dass eine Datenverarbeitung im Hinblick auf das Recht auf informationelle Selbstbestimmung als unbedenklich angesehen werden kann, sofern diese auf eine von der betroffenen Person autonom getroffene Entscheidung zurückgeht, mit dem Verantwortlichen ein Schuldverhältnis einzugehen und damit auch in diesem Zusammenhang erforderliche Datenverarbeitungen in Gang zu setzen.[9] Diese Begründung dafür, dass es keiner Einwilligung bedarf, verliert aber die Tragfähigkeit, sofern Datenverarbeitungen nur „bei Gelegenheit" des Vertragsschlusses gestattet werden, ohne Bezug zum eigentlichen Vertragszweck zu haben.[10]

c) Konsequenzen der engen Auslegung mit Blick auf den hier zu beurteilenden Sachverhalt

Vertragscharakteristische Leistung des Versicherungsunternehmens mit Blick auf den Versicherungsvertrag ist die Absicherung des Versicherungsnehmers bzw. der Versicherungsnehmerin gegen das versicherte Risiko. Gegen Zahlung der Versicherungsprämie erfolgt eine Abwälzung von Risiken vom Versicherungsnehmer auf den Versicherer. Die Versicherungspolice statuiert die zentralen Merkmale des jeweiligen Vertrages.

Die Bereitstellung des KI-Chatbots durch die Versicherung mag in diesem Zusammenhang nützlich sein, da hierdurch die Abwicklung des Versicherungsverhältnisses erleichtert wird, indem die Versicherungsnehmer einen zusätzlichen Service erhalten. Die Unterstützung durch den KI-Chatbot ist aber keine vertragscharakteristische Leistung in dem Sinne, dass diese dem Versicherungsvertrag sein typisches Gepräge verleihen würde.

Dies hat zur Folge, dass die Datenverarbeitung zwecks Weiterentwicklung des KI-Chatbots selbst dann nicht auf Art. 6 Abs. 1 lit. b) DS-GVO gestützt werden kann, wenn die diesbezügliche Datenverarbeitung über die AGB zum Vertragsinhalt geworden sein sollte.

Ergebnis: Art. 6 Abs. 1 lit. b) DS-GVO scheidet im vorliegenden Fall als Rechtsgrundlage der Datenverarbeitung aus. Die Leitung hat nicht Recht.

Ergänzender Hinweis: Ob die AGB-Klausel zum Training der KI tatsächlich zum Vertragsinhalt geworden ist, wäre ansonsten im Übrigen noch abschließend zu prüfen. Denn zwar ist die wirksame Einbeziehung der AGB i.S.v. § 305 Abs. 2 BGB hier durch den Sachverhalt vorgegeben und demzufolge nicht zu prüfen. Zum einen werden aber gemäß § 305c Abs. 1 BGB sog. überraschende Klauseln nicht Vertragsbestandteil. Zum anderen können auch wirksam einbezogene AGB-Klauseln nach entsprechender Inhaltskontrolle im Einzelfall unwirksam sein (vgl. §§ 307 ff. BGB). Da die Frage der Wirksamkeit der AGB-Klausel datenschutzrechtlich, wie dargestellt, nicht ausschlaggebend ist, kann ihre Beantwortung hier dahinstehen.

3. Art. 6 Abs. 1 lit. f) DS-GVO als Rechtsgrundlage für das Training der KI?

a) Auswechseln der Rechtsgrundlage möglich?

Mit Blick auf die zweite am Ende des Sachverhalts aufgeworfene Frage („Werden die Daten der Versicherungsnehmer/-innen zulässigerweise zum Zwecke des KI-Trainings verwendet?") stellt sich die Frage, ob das Training der KI-Daten vorliegend ggf. auf Art. 6 Abs. 1 lit. f) DS-GVO (sog. Interessenabwägung) gestützt werden kann. Nach der genannten Regelung ist eine Verarbeitung personenbezogener Daten rechtmäßig, soweit diese zur Wahrung der berechtigten In-

3 EuGH Urt. v. 04.07.2023 – C-252/21 Rn. 99.

4 EDSA, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. b) DS-GVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Vers. 2.0 (Stand: 08.10.2019), Rn. 26.

5 Vgl. etwa Kühling/Buchner/Buchner/Kühling, DS-GVO BDSG, 4. Aufl. (2024), DS-GVO Art. 7 Rn. 49; Simitis/Hornung/Spiecker gen. Döhmann/Schantz, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 6 Abs. 1 Rn. 34 ff.; ähnlich BeckOK DatenschutzR/Albers/Veit, 52. Ed. 01.05.2025, DS-GVO Art. 6 Rn. 44.

6 Kessen/Reif, EuDIR 2025, 23 (25).

7 Nach Art. 7 Abs. 4 DS-GVO muss bei Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, in größtmöglichem Umfang dem Umstand Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

8 Kessen/Reif, EuDIR 2025, 23 (25).

9 Kühling/Buchner/Buchner/Petri, DS-GVO Art. 6 Rn. 26; BeckOK DatenschutzR/Albers/Veit, DS-GVO Art. 6 Rn. 41.

10 Kühling/Buchner/Buchner/Petri, DS-GVO Art. 6 Rn. 40.

teressen des Verantwortlichen oder eines Dritten erforderlich ist und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Art. 6 Abs. 1 lit. f) DS-GVO stellt in der Praxis typischerweise die Rechtsgrundlage dar, auf die zurückgegriffen wird, wenn KI-Systeme unter Verwendung personenbezogener Informationen trainiert werden sollen.[11] Insbesondere ist der Begriff des berechtigten Interesses i.S.v. Art. 6 Abs. 1 lit. f) DS-GVO weit zu verstehen: Als solches kommt jedes rechtliche, wirtschaftliche oder ideelle Interesse in Frage[12] und damit grundsätzlich auch das wirtschaftliche Interesse, innovative Produkte zu entwickeln, im Wettbewerb mithalten zu können und i.S.d. technischen Fortschritts KI-Systeme (weiter-)zu entwickeln.[13]

Fraglich ist, ob einer Anwendung von Art. 6 Abs. 1 lit. f) DS-GVO im vorliegenden Fall entgegensteht, dass der Verantwortliche die relevante Datenverarbeitung eben gerade nicht auf diese Regelung stützen wollte, sondern auf einen anderen gesetzlichen Erlaubnistatbestand. Teilweise findet sich in der Literatur insofern die Auffassung, dass der Wechsel hin zu einer gesetzlichen Rechtsgrundlage, die seit Anfang der Verarbeitung bestand, regelmäßig ausgeschlossen sei.[14]

In dieser Absolutheit kann der dargestellten Auffassung nach hier vertretener Ansicht nicht gefolgt werden. Insbesondere ist die (Nicht-)Einschlägigkeit gesetzlicher Erlaubnisregelungen mit Bezug auf die Datenverarbeitung nicht vom Willen des Verantwortlichen abhängig, sondern davon, dass die tatbestandlichen Voraussetzungen der jeweiligen Erlaubnisregelung erfüllt sind. Ohnedies wird es der Verantwortliche im Übrigen wohl typischerweise bevorzugen, die Verarbeitung auf Basis einer anderen als der präferierten Rechtsgrundlage durchzuführen, anstatt rechtswidrig zu handeln.

Nach hiesiger Auffassung wird vor allem entscheidend sein mit Blick auf die Zulässigkeit des Austauschs der datenschutzrechtlichen Rechtsgrundlage, ob hierdurch ein Wertungswiderspruch entstehen würde, vorausgesetzt – und hierin dürfte vielfach das praktische Problem bestehen –, die Voraussetzungen des potenziellen datenschutzrechtlichen Ersatzerlaubnistatbestandes können überhaupt als erfüllt angesehen werden.

Die Frage eines möglichen Wertungswiderspruches kann vorliegend offenbleiben, da, wie sogleich aufgezeigt werden wird, in der vorliegenden Konstellation bereits die Voraussetzungen von Art. 6 Abs. 1 lit. f) DS-GVO nicht erfüllt sind.

b) Fehlen der Voraussetzungen von Art. 6 Abs. 1 lit. f) DS-GVO

aa) Dreistufige Prüfung

Ob die Voraussetzungen von Art. 6 Abs. 1 lit. f) DS-GVO gegeben sind, ist über eine dreistufige Prüfung zu ermitteln.

Der erste Prüfungspunkt wurde im Abschnitt a) dem Grunde nach bereits bejaht, d.h. das Vorliegen eines berechtigten Interesses des Verantwortlichen bzw. eines Dritten: Die Weiterentwicklung des KI-Chatbots stellt grundsätzlich jedenfalls ein berechtigtes Interesse des Versicherungsunternehmens i.S.v. Art. 6 Abs. 1 lit. f) DS-GVO dar. Diskutieren lässt sich außerdem, ob die Optimierung des KI-Chatbots nicht auch im Interesse der Gesamtheit der das Servicetool ggf. nutzenden Versicherungsnehmer/-innen von V liegt und insofern nicht nur berechtigten Interessen des Verantwortlichen dient, sondern auch berechtigten Interessen Dritter i.S.v. Art. 6 Abs. 1 lit. f) DS-GVO.

Die im zweiten Schritt zu prüfende Erforderlichkeit der Datenverarbeitung zur Wahrung der relevanten berechtigten Interessen dürfte sich wohl ebenfalls begründen lassen. Denn es ist anzunehmen, dass ab einem gewissen Fortschritt in der Entwicklung ein System wie der eingesetzte Chatbot ohne Analyse realer Interaktionen nicht mehr effektiv verbessert werden kann.

Eigentliches Problem ist vorliegend der dritte Prüfungsschritt der Interessenabwägung, also die Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall (sog. Interessenabwägung im engeren Sinne). Unabhängig von der Gewichtung der sich vorliegend konkret gegenüberstehenden Interessen im Einzelfall – also Unternehmens- und Wirtschaftsfreiheit auf Seiten von V und des Rechts auf informationelle Selbstbestimmung auf Seiten der Versicherungsnehmer/-innen – ist mit Blick auf die Abwägung i.e.S. hier nämlich zu beachten, dass die Versicherung zentrale Transparenzpflichten nicht eingehalten hat, welche mit der Datenverarbeitung einhergehen.

bb) Kein Hinweis auf berechtigte Interessen und Widerspruchsrecht

Die Versicherung hat einerseits die Informationspflichten bei Datenerhebung nach Art. 13 DS-GVO und andererseits den notwendigen Hinweis auf das Widerspruchsrecht der betroffenen Personen gegen die Datenverarbeitung nach Art. 21 Abs. 4 i.V.m. Abs. 1 DS-GVO nicht erfüllt.

Werden personenbezogene Daten bei der betroffenen Person erhoben, so hat der Verantwortliche dieser nach Art. 13 DS-GVO zum Zeitpunkt der Erhebung u.a. Folgendes mitzuteilen:

- die Zwecke, für welche die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung (Abs. 1 lit. c)) sowie
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f) DS-GVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden (Abs. 1 lit. d)).

Dass für die Anwendung von Art. 13 DS-GVO die Datenerhebung bei der betroffenen Person stattfinden muss, schließt dabei nicht aus, dass diese auch ohne deren Beteiligung oder Kenntnis erfolgen kann, etwa durch Einsatz entsprechender Technik, z.B. Hard- und/oder Software.[15]

11 OLG Köln, Beschl. v. 23.05.2025 – 15 UKl. 2/25 mit Blick auf die Verwendung von Nutzerdaten für das KI-Training durch Meta (vgl. in diesem Zusammenhang aber auch Rechtbank Amsterdam, Beschluss vom 19.05.2025 – 10795074 CV FORM 23-14577); LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Vers. 2.0 (17.10.2024), S. 21; umfassend zu den einzelnen Schritten der Abwägung und den jeweils zu berücksichtigenden Gesichtspunkten EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 02.12.2024,Rn. 66 ff.; in der Lit. vgl. z.B. Reichert/Radtke/Eske, ZD 2024, 483 (490): „Die zentrale Rechtsgrundlage für das Training von KI-Modellen mit personenbezogenen Daten und die Nutzung der personenbezogenen Daten in der KI stellt die Interessenabwägung dar.

12 Gola/Heckmann/Schulz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. (2022), DS-GVO Art. 6 Rn. 61.

13 Reichert/Radtke/Eske, ZD 2024, 483 (485); ähnlich LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Vers. 2.0 (17.10.2024), S. 21 f.

14 Krusche, ZD 2020, 232 (236).

15 Simitis/Hornung/Spiecker gen. Döhmann/Dix, DS-GVO Art. 13 Rn. 6.

Gemäß Art. 21 Abs. 1 S. 1 DS-GVO hat die betroffene Person das Recht, gegen eine Verarbeitung, die auf Basis von Art. 6 Abs. 1 lit. f) DS-GVO erfolgt, jederzeit Widerspruch einzulegen, wobei es allerdings – anders als beim voraussetzungslosen Recht auf Werbewiderspruch nach Art. 21 Abs. 2 DS-GVO – einer Begründung des Widerspruchs bedarf. Der allgemeine Widerspruch ist darauf gerichtet, eine im Grundsatz rechtmäßige Verarbeitung ausnahmsweise zu beenden und ist daher an das Vorliegen von Gründen geknüpft, die sich aus der besonderen Situation der betroffenen Person ergeben.[16] Wird Widerspruch nach Art. 21 Abs. 1 S. 1 DS-GVO eingelegt, verarbeitet der Verantwortliche gemäß Art. 21 Abs. 1 S. 2 DS-GVO die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Der Verantwortliche muss also noch mal in eine Interessenabwägung mit Blick auf den konkreten Einzelfall der betroffenen Person eintreten. Über Art. 21 Abs. 1 S. 1 DS-GVO erhält die betroffene Person damit die Möglichkeit, die Verarbeitung einer auf ihre spezifische Situation bezogenen Prüfung unterziehen zu lassen.[17] Auf ihr Widerspruchsrecht muss die betroffene Person nach Art. 21 Abs. 4 DS-GVO hingewiesen werden, wobei der Hinweis in einer verständlichen und von anderen Informationen getrennten Form erfolgen muss. Werden die Daten bei der betroffenen Person erhoben, wie hier, muss der Hinweis auf das Widerspruchsrecht mit Blick auf Art. 13 Abs. 2 lit. b) DS-GVO bereits zum Zeitpunkt der Datenerhebung erfolgen.[18]

Über das Widerspruchsrecht nach Art. 21 Abs. 1 S. 1 DS-GVO wurde vorliegend eindeutig nicht informiert. Mit Blick auf die Informationspflichten aus Art. 13 DS-GVO wurde jedenfalls über die „Rechtsgrundlage der Verarbeitung" i.S.v. Art. 13 Abs. 1 lit. c) DS-GVO nicht korrekt informiert, sondern vielmehr durch die gewählte Gestaltung suggeriert, dass es sich um eine vertragliche Verarbeitung nach Art. 6 Abs. 1 lit. b) DS-GVO handelt.

Unabhängig von der konkreten Abwägung der auf beiden Seiten durch die Datenverarbeitung betroffenen Interessen wird hier bereits der erzeugte Gesamteindruck über die Rahmenbedingungen der personenbezogenen Datenverarbeitung zum Überwiegen schutzwürdiger Interessen der betroffenen Personen führen: Für die betroffenen Personen entsteht der Eindruck, es handele sich um eine durch den Versicherungsvertrag vorgezeichnete Datenverarbeitung, die außerhalb ihrer datenschutzrechtlichen Einflussmöglichkeiten liegt, während tatsächlich Art. 6 Abs. 1 lit. b) DS-GVO keine taugliche Rechtsgrundlage begründet und den betroffenen Personen ein Widerspruchsrecht gegen die Verarbeitung zustünde (Art. 21 Abs. 1 S. 1 DS-GVO). Die hieraus resultierende mangelnde Transparenz mit Blick auf die Rahmenbedingungen der Verarbeitung sowie die Betroffenenrechte führt zu einem Überwiegen der schutzwürdigen Betroffeneninteressen i.R.v. Art. 6 Abs. 1 lit. f) DS-GVO, so dass dieser als Rechtsgrundlage ausscheidet. Die Art und Weise der Verarbeitung ist nicht vereinbar mit Art. 5 Abs. 1 lit. a) DS-GVO, wonach personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Die Bedeutung des datenschutzrechtlichen Transparenzgrundsatzes im Zusammenhang mit Art. 6 Abs. 1 lit. f) DS-GVO und die „Verflechtung"[19] der Informationspflichten mit dem Erlaubnistatbestand hat zuletzt auch noch mal der EuGH in der Rechtssache „Mousse/CNIL" hervorgehoben.[20]

Ergebnis: Unter Zugrundelegung der gegenwärtigen Ausgangslage kann sich V nicht auf Art. 6 Abs. 1 lit. f) DS-GVO berufen mit Blick auf die Datenverarbeitung zwecks Weiterentwicklung des KI-Chatbots. Die Datenverarbeitung zu diesem Zweck ist aktuell nicht zulässig. Erwogen werden könnte eine Nachinformation der betroffenen Versicherungsnehmer/-innen, wobei sich eine solche allerdings nur mit Blick auf ihr zeitlich nachfolgende Verarbeitungen auswirken würde.

Ergänzender Hinweis: Da die Chatdaten stets zum gleichen Zweck des KI-Trainings verwendet werden sollten bzw. sollen, ist Art. 13 Abs. 3 DS-GVO, welcher die Nachinformation bei zweckändernden Datenverarbeitungen regelt, – jedenfalls unmittelbar – hier nicht einschlägig mit Blick auf eine eventuelle Nachinformation.

III. Ergänzende Informationen

Die vorliegend zu beantwortende Fragestellung war spezifisch auf die datenschutzrechtliche Rechtsgrundlage für das Training des KI-Bots bezogen. Neben den datenschutzrechtlichen Vorgaben muss das Versicherungsunternehmen außerdem die Anforderungen der KI-VO beachten, welche sich daraus ergeben, dass es als Betreiber i.S.d. KI-VO agiert. Die Adressaten der KI-VO sind in Art. 2 Abs. 1 KI-VO aufgezählt und legaldefiniert und umfassen insbes. Anbieter und Betreiber von KI, wobei diese nach der KI-VO jeweils unterschiedlich weitreichende Rechtspflichten treffen. Betreiber von KI-Systemen mit begrenztem Risiko treffen nur überschaubare Pflichten nach der KI-VO, nämlich die Verpflichtung zur Sicherstellung von KI-Kompetenz (Art. 4) sowie ggf. Transparenz- und Offenlegungspflichten gemäß Art. 50 Abs. 3 und 4 KI-VO.[21]

Neben dem hier betrachteten Erfordernis einer Rechtsgrundlage für stattfindende personenbezogene Datenverarbeitungen sind beim KI-Einsatz aus Datenschutzperspektive u.a. folgende weitere Aspekte von Belang:[22]

- Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO, insbes. Transparenz, und besondere Pflichten im Falle automatisierter Einzelentscheidungen (Art. 22 DS-GVO)
- Datenschutz-Folgenabschätzung (Art. 35 DS-GV0)
- (Ggf. gemeinsame) Verantwortlichkeit der Beteiligten beim Einsatz von KI und Abgrenzung zur Auftragsverarbeitung
- Betroffenenrechte nach Art. 12 ff. DS-GVO

16 Gola/Heckmann/Schulz, DS-GVO Art. 21 Rn. 9.

17 Kühling/Buchner/Herbst, DS-GVO Art. 21 Rn. 1.

18 Vgl. etwa Kühling/Buchner/Herbst, DS-GVO Art. 21 Rn. 37; Simitis/Hornung/Spiecker gen. Döhmann/Caspar, DS-GVO Art. 21 Abs. 37; Ehmann/Selmayr/Kamann/Braun, Datenschutz-Grundverordnung, 3. Aufl. (2024), DS-GVO Art. 21 Rn. 58; einschränkend demgegenüber Gola/Heckmann/Schulz, DS-GVO Art. 21 Rn. 26.

19 Leicht/Baumann, NJW 2025, 2126 (2127 f.).

20 EuGH, Urt. v. 09.01.2025 – C-394/23 Rn. 63 f.

21 Für einen Gesamtüberblick bzgl. möglicher Pflichten aus der KI-VO vgl. GDD-Praxishilfe: Europäische Datenstrategie: KI-VO, Data Act etc., Stand: Juli 2024, S. 6 ff.; umfassend zur KI-VO Schwartmann/Keber/Zenner, KI-VO – Leitfaden für die Praxis, 2. Aufl. (2024).

22 Zum Thema KI und Datenschutz vgl. GDD-Praxishilfe: Europäische Datenstrategie: KI-VO, Data Act etc., Stand: Juli 2024, S. 11 ff.

Jetzt KI-Kompetenz bei allen Beschäftigten aufbauen!

Das unverzichtbare Merkblatt unterstützt Unternehmen bei der Umsetzung von Artikel 4 der KI-Verordnung.

Umgehend Art. 4 der KI-VO umsetzen!

- ideal für alle Beschäftigten
- firmenindividuell gestaltbar
- anschaulich illustriert und leicht verständlich geschrieben

Jetzt bestellen: **www.datakontext.com/merkblatt-ki**

DATAKONTEXT

RECHTSPRECHUNG

HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

Anforderungen an die Gestaltung eines Cookie-Banners

(VG Hannover, Urteil vom 19. März 2025 – 10 A 5385/22 –)

Relevanz für die Praxis

Das VG Hannover hat mit seinem Urteil die Anforderungen an Cookie-Banner konkretisiert und dabei wenig überraschend sehr nutzerfreundlich entschieden. Konkret hat das Gericht u.a. klargestellt, dass ein Cookie-Banner, der lediglich die Optionen „Alle akzeptieren" oder „Einstellungen" zur Auswahl hat, nicht genügt, um eine freiwillige Einwilligung der Nutzer einzuholen.

Zudem betont das Gericht die Bedeutung der optischen Gestaltung der Banner für die Beurteilung der Freiwilligkeit der hierüber abgegebenen Einwilligungen. Wird der „Alle Akzeptieren"-Button gegenüber dem „Ablehnen"-Button optisch hervorgehoben, werden die Nutzer gezielt zur Zustimmung gedrängt („Nudging"), so das Gericht. Das verhindert die Freiwilligkeit einer Einwilligung. Um eine rechtswirksame Einwilligung einzuholen, müssen die verschiedenen Buttons gleichwertig und sofort sichtbar sein. Zudem muss die Einwilligung unmissverständlich und ausdrücklich erfolgen, d.h. v.a., dass voreingestellte Häkchen unzulässig sind.

Das Gericht bewegt sich mit seinem Urteil prinzipiell auf der bisherigen Linie der Rechtsprechung und bringt daher keine elementaren Wandlungen mit sich. Es könnte jedoch ein Impuls für Aufsichtsbehörden sein, in Zukunft intensiver auf die rechtsfehlerfreie Gestaltung von Cookie-Bannern zu achten. Unternehmen sollten daher ihre gegenwärtige Praxis streng prüfen und auf jede Form des Nudging verzichten.

1. **Der Landesbeauftragte für den Datenschutz ist nach § 20 Abs. 1 NDSG in Verbindung mit Art. 58 DS-GVO befugt, die Einhaltung des § 25 TTDSG als „andere datenschutzrechtliche Bestimmung" zu überwachen.**
2. **Die Gestaltung eines Cookie-Einwilligungsbanners mit zwei Ebenen, bei welchem auf erster Ebene nur die Auswahlmöglichkeiten „Alle akzeptieren", "Akzeptieren & schließen x" und „Einstellungen" bestehen, die zweite Ebene neben verschiedenen Drop Down Menüs die Optionen „Alle akzeptieren" und „Auswahl speichern" enthält und das bei der Auswahl des Buttons „Auswahl speichern" beim Aufruf der Website stets neu erscheint, lenkt die Nutzer der Website in der Gesamtschau gezielt zur Abgabe der Einwilligung hin. Die Einwilligung ist daher nicht freiwillig im Sinne von § 25 Abs. 1 TTDSG, Art. 4 Nr. 11 DS-GVO.**
3. **Die Gestaltung eines Cookie-Einwilligungsbanners mit dem Button „Akzeptieren & schließen x" in der rechten oberen Ecke führt zur Unwirksamkeit der Einwilligung, weil es sich weder um eine unmissverständlich abgegebene noch um eine freiwillige Erklärung im Sinne von § 25 Abs. 1 TTDSG, Art. 4 Nr. 11 DS-GVO handelt.**
4. **Der Einsatz des Dienstes Google Tag Manager bedarf einer Einwilligung nach § 25 Abs. 1 TTDSG und Art. 6 Abs. 1 lit. a) DS-GVO.**

Aus den Gründen:

aa. Die Verwendung von Cookies und anderen Technologien auf der Website der Klägerin verstößt gegen § 25 Abs. 1 TTDSG sowie Art. 6 Abs. 1 DS-GVO.

[...] Das Setzen und Auslesen von Cookies stellt eindeutig eine Speicherung von Informationen in der Endeinrichtung und einen Zugriff auf dort bereits gespeicherte Informationen im Sinne des § 25 Abs. 1 TTDSG dar, unabhängig davon, ob First- oder Third-Party-Cookies gesetzt und ausgelesen werden.

(b) Es ist weder vorgetragen noch ersichtlich, dass es sich bei den nach dem Klick im Einwilligungsbanner auf "Alle akzeptieren" bzw. "Akzeptieren & schließen x" gesetzten Cookies um technisch erforderliche Cookies handelt, für welche nach § 25 Abs. 2 Nr. 2 TTDSG kein Einwilligungserfordernis besteht.

(c) Für das Setzen dieser Cookies ist nach § 25 Abs. 1 TTDSG eine wirksame Einwilligung der Nutzer erforderlich, welche den Anforderungen der DS-GVO entspricht. [...]

(aa) Welche Voraussetzungen an eine "in informierter Weise" erteilte Einwilligung zu stellen sind, wird weder in § 25 Abs. 1 TTDSG noch in Art. 4 Nr. 11, 7 DS-GVO geregelt. Der EuGH fordert als Mindestinformationen eine Angabe der Funktionsdauer sowie Angaben zu eventuellen Empfängern der in den Cookies enthaltenen Informationen (EuGH, Urteil vom 01.10.2019 – C-673/17 –, juris Rn. 75-81). Die zu erteilenden klaren und umfassenden Informationen müssen den Nutzer in die Lage versetzen, die Konsequenzen einer etwaigen von ihm erteilten Einwilligung leicht zu bestimmen, und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird. Sie müssen klar verständlich und detailliert genug sein, um es dem Nutzer zu ermöglichen, die Funktionsweise der verwendeten Cookies zu verstehen (EuGH, ebd., Rn. 74). Nach Ansicht des Bundesgerichtshofs ist insoweit maßgeblich, von welchen Informationen der Nutzer aufgrund der Gestaltung der Einwilligungserklärung "regelmäßig" Kenntnis nehmen wird (BGH, Urt. v. 28.05.2020 – I ZR 7/16 –, juris Rn. 33).

Daran gemessen ist zu bezweifeln, ob das Merkmal der Informiertheit für die mittels des Einwilligungsbanners der Klägerin erteilten Einwilligungen der Nutzer vorliegt.

Einerseits fehlt auf erster Ebene des Einwilligungsbanners die Angabe der Anzahl der über hundert Drittdienstleister der Klägerin. Bei dieser Anzahl handelt es sich um eine Information, die vielleicht nicht über die Erteilung oder Nichterteilung der Einwilligung entscheiden mag, jedoch den Nutzer dazu veranlassen kann, nicht bereits auf erster Ebene auf den Button "Alle akzeptieren" zu klicken, sondern sich die Liste der Partner vorher anzuschauen, auf zweiter Ebene die Einwilligung abzulehnen oder zu versuchen, die Anzahl der Partner zu reduzieren. Andererseits ist auf erster Ebene des Einwilligungsbanners ein Herunterscrollen notwendig, um zum Hinweis auf die Datenverarbeitung durch Anbieter in Drittstaaten wie den USA und die Möglichkeit des Widerrufs der Einwilligung zu gelangen. Regelmäßig wird ein Nutzer, der einen Artikel auf der Website der Klägerin lesen möchte, jedoch nur die erste Ebene des Einwilligungsbanners, wie es bei Erstaufruf der Website erscheint, überfliegen, ohne darin noch bis zum Ende zu scrollen. Sein Hauptinteresse wird es sein, die dahinterliegende Website aufrufen zu können. Sowohl die Einbindung von über hundert Drittdienstleistern als auch die Datenverarbeitung in Drittstaaten wie den USA sind Informationen, die dem durchschnittlichen Nutzer der Website der Klägerin gegebenenfalls nicht bewusst sind. Sie sind jedoch relevant für eine informierte Entscheidung, um das Ausmaß einer erteilten Einwilligung zu überblicken.

(bb) Jedenfalls beruhen die von der Klägerin eingeholten Einwilligungen nicht auf einer freiwilligen Entscheidung der Nutzer. Als freiwillig wird die Einwilligung nur betrachtet, wenn die betroffene Person tatsächlich eine Wahlmöglichkeit hat, also ohne Nachteile auf die Erteilung der Einwilligung verzichten kann (Ehmann/Selmayr/Klabunde/Horváth, DS-GVO, 3. Aufl. 2024, Art. 4 Rn. 53). Dazu muss die Einwilligung aufgeklärt erfolgen. In jedem Fall ist der Betroffene darauf hinzuweisen, dass er seine Einwilligung verweigern kann (Wolff/Brink/von Ungern-Sternberg/Schild, BeckOK Datenschutzrecht, 51. Edition, Art. 4 DS-GVO Rn. 128). Er muss die Möglichkeit haben, den Inhalt der von ihm erwarteten Erklärung in zumutbarer Weise zur Kenntnis zu nehmen. Dies gilt in jedem Fall bei vorformulierten Einwilligungen. Versteckte Hinweise, technische Textformate, die nicht jedem Nutzer zugänglich sind, oder undeutliche Schriftarten können diese Zumutbarkeit ebenso hindern wie überlange Texte (Paal/Pauly/Ernst, DS-GVO, 3. Aufl. 2021, Art. 4 Rn. 79, 80).

Ob aus diesen Vorschriften herzuleiten ist, dass die Möglichkeit zur Ablehnung von Cookies in gleicher Weise wie die Einwilligung in das Setzen von Cookies gestaltet sein muss, ist durch die Rechtsprechung noch keiner abschließenden Klärung zugeführt worden (vgl. Sesing, MMR 2021, S. 544 (547) m.w.N.; OLG Köln, Urt. v. 03.11.2023 – I-6 U 58/23 -, juris Rn. 50). Jedenfalls darf aber das Cookie-Banner nicht so gestaltet sein, dass es den Nutzer gezielt zur Abgabe der Einwilligung hinlenkt und von der Ablehnung der Cookies abhält (LG Köln, Urt. v. 04.05.2023 – 33 O 311/22; ähnlich BGH, Urt. v. 28.05.2020 – I ZR 7/16 –, juris Rn. 32).

Aus der Gesamtschau der Gestaltung der verschiedenen Ebenen des Einwilligungsbanners ergibt sich indes, dass Nutzer gezielt in Richtung einer Einwilligungserklärung gelenkt werden sollen und ihr Wahlrecht beeinflusst werden soll.

Wie vom Beklagten anschaulich beschrieben, besteht für Nutzer ein erheblicher Mehraufwand, wenn sie die Einwilligung nicht erteilen möchten. Während die umfassende Einwilligung auf erster Ebene gleich durch zwei Buttons ("Alle akzeptieren" sowie "Akzeptieren & schließen x") erteilt werden kann, muss für eine Ablehnung zunächst auf erster Ebene der Button "Einstellungen" ausgewählt werden. Auf zweiter Ebene des Banners folgen fünf verschiedene Drop Down Menus mit weiteren Unterpunkten, bei denen der Nutzer kontrollieren muss, ob die Opt-In-Regler abgeschaltet sind, um anschließend den Button "Auswahl speichern" auszuwählen. In diesem Fall wird der Nutzer bei jedem Besuch der Website erneut mit dem Einwilligungsbanner konfrontiert, während hingegen die umfassende Erteilung der Einwilligung gespeichert wird und das Banner nicht bei jedem Aufruf der Website erneut erscheint.

Insbesondere vor dem Hintergrund, dass Nutzer sich des Umfangs der erteilten Einwilligung möglicherweise nicht bewusst sind, da die Hinweise auf die Datenverarbeitung in Drittländern oder die Anzahl der eingebundenen Drittdienstleister nicht wahrgenommen werden, werden sie regelmäßig durch Interaktion mit dem Banner auf erster Ebene versuchen, dieses verschwinden zu lassen und die dahinterliegende Website lesen zu können. Deshalb werden sie eine Auswahl auf erster Ebene treffen, die dies möglich macht – im Rahmen der Bannergestaltung der Klägerin folglich die Erteilung einer umfassenden Einwilligung, da eine Ablehnungsoption auf erster Ebene nicht besteht. Darüber hinaus findet sich auf erster Ebene des Banners kein Hinweis darauf, dass beim Klick auf "Einstellungen" die Einwilligung verweigert werden kann. Nutzer sind sich deshalb auf erster Ebene nicht im Klaren darüber, dass sie mehrere Wahlmöglichkeiten haben. Lediglich beim Scrollen innerhalb des Banners auf erster Ebene findet sich die Formulierung "es besteht keine Verpflichtung, der Verarbeitung Ihrer Daten zuzustimmen, um dieses Angebot zu nutzen". Dass eine Ablehnungsoption auf nächster Ebene folgt, ergibt sich jedoch selbst aus diesem Hinweis nicht. Insofern ist die Gestaltung des Einwilligungsbanners irreführend. Bei den verschiedenen Auswahlmöglichkeiten auf erster Ebene ("Alle akzeptieren", "Akzeptieren & schließen x", "Einstellungen") kann vielmehr der Eindruck entstehen, dass eine Ablehnungsmöglichkeit gar nicht besteht.

Zudem ist die Funktion des Buttons "Alle akzeptieren" auf der zweiten Ebene des Einwilligungsbanners unklar: Hiermit kann erneut die umfassende Einwilligung in die Speicherung von Cookies und die Verarbeitung von Daten erteilt werden. Nutzer können die Schaltfläche indes auch so verstehen, dass die vorgenommenen Einstellungen akzeptiert werden, insbesondere, da die Schaltfläche im Gegensatz zum Button "Auswahl speichern" in blau hervorgehoben ist.

Auch das "Mürbemachen" durch die ständige Konfrontation mit dem Einwilligungsbanner beim erneuten Aufruf der Website, bis die umfassende Einwilligung erteilt wird, ist technisch nicht notwendig und wird teilweise als unzulässige Manipulationstaktik angesehen (vgl. Loy/Baumgartner, ZD 2021, S. 404 (406)).

Hinzu kommt die Gestaltung des sonst regelmäßig als "x" bezeichneten Buttons oben rechts als "Akzeptieren & schließen x". Die Gestaltung verstößt gegen die Grundsätze von Transparenz und Freiwilligkeit der Einwilligung (vgl. OLG Köln, Urt. v. 19.01.2024 – 6 U 80/23 –, juris Rn. 47). Das "x"-Symbol wird von Nutzern üblicherweise als Schaltfläche zum

Schließen eines Fensters verstanden, wie derartige Kreuz-Schaltflächen es in den meisten Betriebssystemen bewirken. Eine Einwilligung in die Verwendung von Cookies und anderen Technologien durch einen Klick auf einen "x"-Button oben rechts ist hingegen überraschend und unüblich. Dass hiermit eine Einwilligung erklärt wird, wird dem durchschnittlichen Nutzer daher nicht bewusst sein. Zwar steht unmittelbar neben dem "x"-Symbol "Akzeptieren & schließen". Die Verknüpfung dieser beiden Funktionen ist aber irreführend und intransparent für die Nutzer. Auch wird für die Nutzer nicht ohne weiteres erkennbar, dass es sich bei "Akzeptieren & schließen" und dem "x"-Symbol um ein und denselben Button handelt, da dieser in schwarzer Schrift auf weißem Hintergrund und damit in derselben farblichen Gestaltung wie der Rest des Banners gehalten ist, sich also nicht als ein einziger Button vom Banner hervorhebt.

Nach alledem verfolgt die Ausgestaltung des Einwilligungsbanners das klare Ziel, Nutzer dahingehend zu beeinflussen, eine umfassende Einwilligung in die Verwendung von Cookies und anderen Technologien zu erteilen und sie von der Möglichkeit, diese abzulehnen, abzulenken.

Für ein gezieltes Lenken der Nutzer hin zur Erteilung der umfassenden Einwilligung spricht auch das Argument der Klägerin, dass die Erteilung der Einwilligung insbesondere für das Real Time Bidding und damit die Finanzierung des Internetangebots der Klägerin unerlässlich sei. Dies deutet darauf hin, dass aufgrund der wirtschaftlichen Interessenlage der Klägerin bewusst Maßnahmen ergriffen werden, um die Nutzerentscheidung zu beeinflussen.

Die Argumente der Klägerin, dass Nutzer die Website nicht besuchen müssen, wenn sie keine Einwilligung erteilen möchten, gehen hingegen fehl. Denn die Möglichkeit, die Website zu verlassen und stattdessen eine andere zu lesen, ändert nichts an der Tatsache, dass diejenigen Nutzer, die tatsächlich eine Einwilligung erteilen, dies nicht auf Grundlage einer transparenten und freien Entscheidung tun, sondern weil die Gestaltung des Einwilligungsbanners sie dahin lenkt. Die Argumentation zielt nur auf die Frage ab, ob eine Möglichkeit zur Nichterteilung im Sinne eines "Alle ablehnen"-Buttons auf erster Ebene des Banners erforderlich ist, nicht jedoch, ob dieses durch eine gezielte Gestaltung die Nutzer zur Erteilung einer umfassenden Einwilligung beeinflusst.

(cc) Es handelt sich ferner nicht um eine unmissverständlich abgegebene Willensbekundung im Sinne des Art. 4 Nr. 11 DS-GVO. Die verbindliche Erteilung der Einwilligung setzt wie jede verbindliche Willensäußerung im Rechtsverkehr in ihrem subjektiven Tatbestand ein entsprechendes Bewusstsein voraus, etwas rechtsgeschäftlich Erhebliches zu erklären. Art. 4 Nr. 11 DS-GVO schreibt das bereits aus allgemein rechtsgeschäftlichen Grundsätzen erforderliche Einwilligungsbewusstsein ausdrücklich fest (Kühling/Buchner/Buchner/Kühling, DS-GVO BDSG, 4. Aufl. 2024, Art. 7 DS-GVO Rn. 56). Nach ErwG 32 der DS-GVO ist unmissverständlich und eindeutig etwa das Anklicken eines Kästchens beim Besuch einer Website, die Auswahl entsprechender technischer Einstellungen oder auch jede sonstige Erklärung oder Verhaltensweise, "mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert". Das Einwilligungsbanner der Klägerin hat einen insgesamt nicht eindeutig gestalteten Wortlaut, da zu keinem Zeitpunkt ausdrücklich die Erteilung einer Einwilligung im Raum steht, sondern ausweislich der Überschrift vielmehr das "optimale Nutzererlebnis" Ziel des Banners ist. Erst beim weiteren Scrollen innerhalb des Banners auf erster Ebene ist von einer "Zustimmung" die Rede. Allerdings ist zu berücksichtigen, dass durchschnittliche Nutzer der Website der Klägerin vergleichbare Banner, wie sie auf beinahe jeder Website im Internet zu finden sind, gewöhnt sein werden und ihnen daher bewusst ist, eine Einwilligungserklärung beim Klick auf den Button "Alle akzeptieren" abzugeben.

Etwas anderes gilt jedoch für diejenigen Nutzer, die oben rechts auf "Akzeptieren & schließen x" klicken. Dass eine rechtserhebliche, bewusste Einwilligung abgegeben wird, kann aufgrund der intransparenten und überraschenden Gestaltung nicht mehr angenommen werden (vgl. OLG Köln, Urteil vom 19.01.2024 – 6 U 80/23 –, juris Rn. 47). Stattdessen dürfte der durchschnittliche Nutzer davon ausgehen, durch das Anklicken des "x"-Symbols oben rechts das Einwilligungsbanner lediglich zu schließen, ohne eine rechtliche Erklärung abzugeben.

(2) Die Verwendung von Cookies und anderen Technologien auf der Website der Klägerin verstößt zudem gegen Art. 6 Abs. 1 DS-GVO. Durch das Speichern und Auslesen von Cookies und anderen Informationen durch die Klägerin sowie ihre Drittdienstleister werden personenbezogene Daten der Nutzer der Website verarbeitet, ohne dass ein Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO besteht.

(a) Gemäß Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung identifiziert werden kann. Verarbeitung ist nach Art. 4 Nr. 2 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Ausweislich der von der Klägerin innerhalb ihres Einwilligungsbanners selbst mitgeteilten Hinweise werden personenbezogene Daten wie Wiedererkennungsmerkmale oder Profildaten verarbeitet, um die Identifikation von Endgeräten sowie personalisierte Werbung, die Messung von Werbeleistung und der Performance von Inhalten, Zielgruppenforschung und die Verbesserung von Angeboten zu ermöglichen.

Nach eigenen Angaben verwendet die Klägerin bei der Versteigerung von Werbeplätzen im Wege des Real Time Biddings das TCF des IAB Europe, welches nach dem Abfragen der Einwilligung der Nutzer durch die CMP der TC-String auf dem Gerät des Nutzers als Cookie speichert. Diese codierte Zeichenkette enthält die Präferenzen eines Nutzers in Bezug auf dessen Einwilligung in die Verarbeitung der ihn betreffenden personenbezogenen Daten durch Anbieter von Websites oder Anwendungen sowie durch Datenbroker

und Werbeplattformen nebst der IP-Adresse des Nutzers und eines Werbeprofils des Nutzers. Je aussagekräftiger die Inhalte des TC-Strings über die Person des Nutzers sind, desto höhere Entgelte können erzielt werden (Jandt/Steidle/Steidle/Skistims, Datenschutz im Internet, 2. Aufl. 2024, Kap. V Rn. 233). Nach der Rechtsprechung des Europäischen Gerichtshofs stellt der Vorgang des Speicherns und Auslesens des TC-Strings eine Übermittlung personenbezogener Daten dar (EuGH, Urt. v. 07.03.2024 – C-604/22 –, juris Rn. 42 ff.).

Soweit die Klägerin dazu ausführt, für die Speicherung und Auslesung des TC-String nicht verantwortlich zu sein, da die Verantwortung stattdessen bei den Drittdienstleistern liege, dringt sie hiermit nicht durch. Als Verantwortliche nach Art. 4 Nr. 7 DS-GVO können diejenigen Personen angesehen werden, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nehmen und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirken (EuGH, Urt. v. 10.07.2018 – C 25/17 –, Celex-Nr. 62017CJ0025 Rn. 68). Durch die Einbindung der CMP und des TCF auf ihrer Website und die hierauf fußende Übersendung des TC-Strings und der darin enthaltenen Inhalte ist es gerade die Klägerin, welche eine Verarbeitung personenbezogener Daten durch die Drittdienstleister veranlasst und ermöglicht. Ohne das Webangebot der Klägerin sowie ihre Vermittlung wäre die Verarbeitung durch werbetreibende Dritte nicht möglich, schließlich besuchen Nutzer die Website der Klägerin, um deren Inhalte zu lesen, und nicht, um personifizierte Werbung angezeigt zu bekommen. Da die Klägerin ihr Internetangebot u.a. durch die Verwertung personenbezogener Daten zum Schalten von Werbeanzeigen Dritter finanziert, besteht auch ein Eigeninteresse an der Verarbeitung. Auch der Europäische Gerichtshof geht von einer geteilten Verantwortlichkeit der Anbieter von Websites und des Branchenverbands IAB Europe aus (EuGH, Urt. v. 07.03.2024 – C-604/22 –, juris Rn. 74).

Bei jedem Besuch der Website der Klägerin verarbeitet diese zudem die vollständige IP-Adresse der Nutzer, unabhängig von der Übermittlung an Drittdienstleister im Rahmen des Real Time Biddings (vgl. die Datenschutzerklärung der Klägerin, online abrufbar unter https://www.noz.de/datenschutz, zuletzt abgerufen am 24.04.2025). IP-Adressen, die ein Anbieter von Online-Diensten wie die Klägerin speichert, stellen Einzelangaben über sachliche Verhältnisse dar, da die Daten Aufschluss darüber geben, dass zu bestimmten Zeitpunkten bestimmte Seiten bzw. Dateien über das Internet abgerufen wurden, und können daher personenbezogene Daten sein, wenn die datenverarbeitende Stelle über die rechtlichen oder tatsächlichen Mittel verfügt, um die Identität des Nutzers zu ermitteln (BGH, Urt. v. 16.05.2017 – VI ZR 135/13 –, juris Rn. 17 ff.; EuGH, Urt. v. 19.10.2016 – C-582/14 –, juris Rn. 49). Als Betreiberin der Website verfügt die Klägerin über die rechtlichen Mittel, die vernünftigerweise eingesetzt werden können, um mithilfe Dritter die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen. Dies ergibt sich ausweislich der Entscheidung des Bundesgerichtshofs daraus, dass diese Betreiber sich insbesondere im Fall von Cyberattacken an die zuständige Behörde wenden könnten, damit diese die nötigen Schritte unternehme, um die fraglichen Informationen vom Internetzugangsanbieter zu erlangen und die Strafverfolgung einzuleiten (BGH, Urt. v. 16.05.2017 – VI ZR 135/13 –, juris Rn. 25). Auch den Drittdienstleistern der Klägerin ist eine solche Zusammenführung demzufolge möglich. Es ist daher irrelevant, dass die Klägerin versichert, erhobene personenbezogene Daten nicht miteinander zusammenzuführen, da es ihr technisch und rechtlich zumindest möglich wäre.

Darauf, ob in den durch die Klägerin oder ihre Dienstleister gesetzten Cookies individuelle Kennungen (Nutzer-IDs) gespeichert werden, die zumindest die Bestimmbarkeit des Nutzers durch die Klägerin sowie ihre Drittdienstleister ermöglichen, kommt es im Ergebnis nicht an. Eine solche individuelle Kennung könnte dann im Zusammenspiel mit der IP-Adresse ebenfalls einen Personenbezug ermöglichen.

(b) Die Verarbeitung personenbezogener Daten durch die Klägerin erfolgt nicht zur Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c) DS-GVO. Voraussetzung dieses Erlaubnistatbestands ist eine Verpflichtung kraft Gesetzes oder kraft einer auf einem Gesetz beruhenden Anordnung, Daten zu verarbeiten, mithin zu erheben, aufzuzeichnen, zu speichern oder weiterzugeben (Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 Rn. 16). Erforderlich ist, dass sich die in einer Vorschrift normierte Verpflichtung unmittelbar auf die Datenverarbeitung bezieht. Typischerweise verstößt der Verantwortliche gegen eine gesetzliche Verpflichtung, wenn er die fragliche Verarbeitung nicht vornimmt (Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, Art. 6 Rn. 76). Entgegen der Ansicht der Klägerin schafft § 25 Abs. 1 TTDSG keine unmittelbare Rechtspflicht zum Verarbeiten personenbezogener Daten. Die Norm bestimmt lediglich, dass für die Verwendung von Cookies eine Einwilligung der Nutzer erforderlich ist. Eine Pflicht zur Erhebung, Speicherung oder Weitergabe personenbezogener Daten wird dadurch jedoch nicht unmittelbar statuiert. Die Vorschrift verpflichtet weder unmittelbar zum Setzen von Cookies noch zum Auslesen der IP-Adressen und IDs der Nutzer. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus (Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, Art. 6 Rn. 76).

(c) Die Verarbeitung ist auch nicht nach Art. 6 Abs. 1 lit. f) DS-GVO gerechtfertigt. Nach dieser Vorschrift ist die Datenverarbeitung 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 überwiegen. Im Rahmen einer dreistufigen Prüfung ist zu ermitteln, ob zum Zeitpunkt der Verarbeitung ein berechtigtes Interesse des Verantwortlichen oder eines Dritten, dem die Daten übermittelt werden, vorliegt, ob die Datenverarbeitung zur Verwirklichung dieses Interesses erforderlich ist und ob die Grundrechte und Grundfreiheiten der von der Datenverarbeitung Betroffenen nicht das wahrgenommene berechtigte Interesse überwiegen (EuGH, Urt. v. 11.12.2019 – C-708/18 –, juris Rn. 40). Aus der Rechenschaftspflicht des Verantwortlichen für die Einhaltung der datenschutzrechtlichen Grundsätze nach Art. 5 Abs. 2 DS-GVO folgt, dass der Verantwortliche bereits vor Beginn der Verarbeitung diese Abwägung auf der Grundlage der konkreten Umstände des Einzelfalls vorzunehmen hat und dafür beweispflichtig ist (Ehmann/Selmayr/Heberle, DS-GVO, 3. Aufl. 2024, Art. 6 Rn. 46). Der Ver-

antwortliche muss mithin selbst eine Interessenabwägung durchführen, die durch die Aufsichtsbehörden und Gerichte nachvollzogen werden kann (DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter/-innen von digitalen Diensten, Version 1.2, Stand: November 2024, Rn. 110). Eine solche dreistufige Interessenabwägung nimmt die Klägerin weder im Rahmen ihrer Datenschutzhinweise auf ihrer Website noch im Klageverfahren vor, sondern beruft sich pauschal auf den Erlaubnistatbestand. Die Erstellung redaktioneller Inhalte sei ihr nur möglich, indem sie ihr Angebot durch Werbung und andere Marketingmaßnahmen finanziere (vgl. die Datenschutzerklärung der Klägerin, online abrufbar unter https://www.noz.de/datenschutz, zuletzt abgerufen am 24.04.2025). Eine Rechtfertigung im Rahmen der Interessenabwägung scheidet darüber hinaus auch aus.

(aa) Als berechtigt darf jedes rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse des Verantwortlichen angesehen werden, soweit es von der Rechtsordnung nicht missbilligt wird. Das berechtigte Interesse muss auf einen konkreten Verarbeitungs- oder Nutzungszweck gerichtet sein. Es muss zum Zeitpunkt der Datenverarbeitung entstanden und vorhanden sein und darf zu diesem Zeitpunkt nicht hypothetisch sein (EuGH, Urt. v. 11.12.2019 – C-708/18 –, juris Rn. 44). Der Verantwortliche hat sein berechtigtes Interesse substanziiert vorzutragen und zu belegen (vgl. Art. 5 Abs. 2 DS-GVO; Taeger/Gabel/Taeger, DS-GVO-BDSG-TTDSG, 4. Aufl. 2022, Art. 6 Rn. 135; vgl. auch EuGH, Urt. v. 24.02.2022 – C-175/20 –, juris Rn. 77; BVerwG, Urt. v. 02.03.2022 – 6 C 7.20 –, juris Rn. 50).

Die Finanzierung des journalistischen Internetangebots der Klägerin durch Werbung, insbesondere durch die Versteigerung personalisierter Werbeplätze an Drittdienstleister, ist ein wirtschaftliches Interesse, welches die Klägerin im Klageverfahren substanziiert dargelegt hat. Es entspricht grundsätzlich ihrer unternehmerischen Freiheit, sich zu entscheiden, journalistische Inhalte kostenlos abrufbar zur Verfügung zu stellen und diese durch Werbung zu finanzieren.

(bb) Die Datenverarbeitung ist zur Wahrung der Interessen der Klägerin allerdings nicht erforderlich. Die personenbezogenen Daten sollen für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein; sie sollen nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (vgl. ErwG 39 der DS-GVO). Voraussetzung für die Erforderlichkeit ist also, dass kein milderes, gleich effektives Mittel zur Verfügung steht, um die Interessen des Verantwortlichen zu erreichen (Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 147c). Eine bloße Zweckdienlichkeit der Datenverarbeitung reicht jedenfalls nicht aus und auch das Ansinnen einer "bestmöglichen Effizienz" macht die Datenverarbeitung noch nicht zu einer erforderlichen. Entsprechend kann die Erforderlichkeit auch nicht allein damit begründet werden, dass es sich bei der beabsichtigten Datenverarbeitung um die aus Sicht des Verantwortlichen wirtschaftlich sinnvollste Alternative handelt (Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 147c m.w.N.).

Gemessen daran ist bereits die Erforderlichkeit der Verarbeitung personenbezogener Daten zur Finanzierung des Internetangebots der Klägerin zu bezweifeln. Der Klägerin stehen auch andere Möglichkeiten zur Verfügung, um ihre wirtschaftlichen Interessen zu decken. Diese nutzt die Klägerin bereits, indem sie einerseits mit ihrer Print-Ausgabe Erlöse erwirtschaftet, die ausweislich des eigenen Vortrags der Klägerin auch zur Finanzierung des Online-Angebots genutzt werden. Andererseits bietet die Klägerin auf ihrer Website unter dem Onlinedienst NOZ+ kostenpflichtige Inhalte an. Obgleich es also stimmen mag, dass für die Klägerin keine anderen Werbealternativen als die Versteigerung von Werbeplätzen in Form des Real Time Biddings bestehen, so existieren dennoch alternative Finanzierungsformen zur Werbung, welche die Klägerin auch bereits in Anspruch nimmt. Die Situation der Klägerin ist demnach nicht vergleichbar mit der von Anbietern von Webdiensten, deren alleinige Einnahmequelle das Schalten von personalisierter Werbung ist.

(cc) Jedenfalls überwiegen die Interessen der betroffenen Nutzer das Interesse der Klägerin an der Datenverarbeitung. Ausgangspunkt der Abwägung sind einerseits die Auswirkungen, die eine Datenverarbeitung für die betroffene Person mit sich bringt, und andererseits die Interessen des Verantwortlichen oder von Dritten. In diesem Zusammenhang sind Art, Inhalt und Aussagekraft der betroffenen Daten an dem mit der Datenverarbeitung verfolgten Zweck zu messen (Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, Art. 6 DS-GVO Rn. 149). Im Rahmen der Interessenabwägung sind zudem die vernünftigen Erwartungen der betroffenen Personen bzw. die Absehbarkeit der Verarbeitung zu berücksichtigen, wie sich aus ErwG 47 der DS-GVO ergibt.

Für die von der Datenverarbeitung betroffenen Nutzer streitet ihr Recht auf Schutz der personenbezogenen Daten nach Art. 8 GrCh sowie ihr Recht auf Achtung des Privat- und Familienlebens nach Art. 7 GrCh und Art. 8 EMRK. Diese sind abzuwägen gegen die wirtschaftlichen Interessen der Klägerin an der Finanzierung ihres Internetangebots durch personalisierte Werbung. Dabei ist zu berücksichtigen, dass Nutzer bei der Inanspruchnahme eines entgeltfreien Webdienstes zwar vernünftigerweise davon ausgehen müssen, dass ihre Daten für Werbung verwendet werden, und nicht einfach annehmen können, dass ihnen das Internetangebot ohne Gegenleistung angeboten wird. Allerdings handelt es sich bei der Klägerin um ein Verlagshaus, das auch mit Print-Ausgaben und Abonnements Geld verdient sowie auf ihrer Website auch kostenpflichtige Inhalte anbietet. Im Gegensatz etwa zum Angebot sozialer Netzwerke handelt es sich bei der Bereitstellung journalistischer Inhalte durch die Klägerin also nicht um eine komplett kostenfreie Dienstleistung. Nutzer könnten stattdessen genauso gut davon ausgehen, dass diejenigen Inhalte, die auf der Website der Klägerin veröffentlicht werden, auch in der von Montag bis Samstag täglich erscheinenden kostenpflichtigen Print-Ausgabe der Klägerin erscheinen und daher durch den Erlös der Print-Ausgabe und der Online-Abonnements finanziert sind. Selbst für komplett kostenfrei angebotene soziale Netzwerke hat der Europäische Gerichtshof zudem entschieden, dass allein die Unentgeltlichkeit einer bestimmten Dienstleistung nicht dazu führt, dass die betroffenen Personen mit einer unbeschränkten Verarbeitung ihrer Daten zu Werbezwecken rechnen müssen und die Interessen und Grundrechte eines Nutzers gegenüber dem Interesse des Betreibers an einer Personalisierung der Werbung, mit der er seine Tätigkeit fi-

nanziert, überwiegen (EuGH, Urt. v. 04.07.2023 – C-252/21 -, juris Rn. 117). Im Rahmen der Abwägung ist zu berücksichtigen, dass insbesondere durch die Setzung von Third-Party-Cookies großer, weltweit agierender Unternehmen ein möglichst detailliertes Nutzungsprofil erstellt und vervollständigt werden kann, um ein individuelles Nutzerverhalten vorauszusagen und möglichst personalisierte Werbung zu erstellen. Für Nutzer ruft dies oft ein Gefühl der Überwachung im Internet als "gläserner Mensch" und damit eines Informationsungleichgewichts hervor, wenn Werbung beispielsweise gezielt für Produkte geschaltet wird, welche sie sich zuvor auf einer anderen Website angeschaut haben. Hinzu kommt, dass Nutzer auf der Website der Klägerin nicht detailliert und transparent darüber aufgeklärt werden, welche Informationen zum Erstellen von Profilen genutzt werden können, sondern im Einwilligungsbanner lediglich allgemeine Angaben zu Wiedererkennungsmerkmalen und Profildaten zu Zwecken personalisierter Werbung gemacht werden. Die Unklarheit darüber, welche Daten zum Profiling verwendet werden, verstärkt das Unsicherheits- und Überwachungsgefühl der Nutzer. Ihre Interessen an Freiheit vor Überwachung und Kontrolle über die eigenen Daten wiegen höher als das finanzielle Interesse der Klägerin an der Nutzung personenbezogener Daten zu Werbezwecken. Bei dem durch die Klägerin betriebenen Real Time Bidding handelt es sich auch um keine Direktwerbung im Sinne des Art. 21 Abs. 2 DS-GVO, in deren Rahmen der europäische Gesetzgeber bis zum Widerspruch des Betroffenen eine Datenverarbeitung einschließlich des Profilings als grundsätzlich zulässig erachtet.

Zur Vertiefung

Schwartmann/Benedikt/Reif/Schwartmann/Reif/Burkhardt, Datenschutz im Internet, 2025, Kap. 9 Rn. 208 ff.

Schwartmann/Benedikt/Reif/Duhr/Horn/Pfau/Schaefer/Zimaj, Datenschutz im Internet, 2025, Kap. 21 Rn. 177 ff.

Schwartmann/Jaspers/Eckardt/Schwartmann/Reif/Burkhardt, TTDSG § 25 Rn. 34 ff.

Anwendbarkeit der DS-GVO auf die Daten eines Geschäftsführers

(EuGH, Urteil vom 3. April 2025 – C-710/23 –)

Relevanz für die Praxis

Im vorliegenden Urteil konkretisiert der EuGH ein weiteres Mal den Begriff der personenbezogenen Daten im Sinne der DS-GVO, der nach ständiger Rechtsprechung weit auszulegen ist. Personenbezug ist nach den Vorgaben der DS-GVO nur bei natürlichen Personen möglich, Daten einer juristischen Person unterfallen dem Anwendungsbereich der Verordnung dagegen nicht. Das wirft die Frage auf, ob Informationen, die sich sowohl auf eine juristische als auch auf ihre natürliche Vertreterperson beziehen, einen Personenbezug im Sinne von Art. 4 Nr. 1 DS-GVO aufweisen. Entscheidend für den Bezug zur natürlichen Vertreterperson ist nach der Rechtsprechung des EuGH, ob die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit der identifizierbaren (natürlichen) Person verknüpft ist. Dass die Informationen über das Gesellschaftsorgan im Kontext einer beruflichen Tätigkeit stehen, soll dagegen nicht von Bedeutung sein.

1. **Art. 4 Nrn. 1 und 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist dahin auszulegen, dass die Offenlegung des Vornamens, des Nachnamens, der Unterschrift und der Kontaktdaten einer natürlichen Person, die eine juristische Person vertritt, eine Verarbeitung personenbezogener Daten darstellt. Der Umstand, dass die Offenlegung allein zu dem Zweck erfolgt, die Identifizierung der natürlichen Person zu ermöglichen, die befugt ist, im Namen der juristischen Person zu handeln, ist insoweit ohne Belang. [...]**

Zu den Vorlagefragen:

Zur ersten Frage

Mit seiner ersten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 4 Nrn. 1 und 2 DS-GVO dahin auszulegen ist, dass die Offenlegung des Vornamens, des Nachnamens, der Unterschrift und der Kontaktdaten einer natürlichen Person, die eine juristische Person vertritt, auch dann eine Verarbeitung personenbezogener Daten darstellt, wenn sie ausschließlich zu dem Zweck erfolgt, die Identifizierung der natürlichen Person zu ermöglichen, die befugt ist, im Namen der juristischen Person zu handeln. [...]

Nach ständiger Rechtsprechung kommt in der Verwendung der Formulierung „alle Informationen" bei der Bestimmung des Begriffs „personenbezogene Daten" in dieser Vorschrift das Ziel des Unionsgesetzgebers zum Ausdruck, diesem Begriff eine weite Bedeutung beizumessen, die potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen umfasst, unter der Voraussetzung, dass es sich um Informationen „über" die in Rede stehende Person handelt. 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. 07.03.2024, IAB Europe, C-604/22, EU:C:2024:214, Rn. 36 und 37, sowie v. 04.10.2024, Agentsia po vpisvaniyata, C-200/23, EU:C:2024:827, Rn. 130 und 131 sowie die dort angeführte Rechtsprechung).

Damit stellen Informationen über identifizierte oder identifizierbare natürliche Personen, die als gesetzlich vorgesehenes Gesellschaftsorgan oder als Mitglieder eines solchen Organs befugt sind, die Gesellschaft außergerichtlich zu vertreten, „personenbezogene Daten" im Sinne von Art. 4 Nr. 1 DS-GVO dar. Dass diese Informationen im Kontext einer beruflichen Tätigkeit stehen, bedeutet nicht, dass sie keine personenbezogenen Daten sind (vgl. entsprechend Urt. v. 09.03.2017, Manni, C-398/15, EU:C:2017:197, Rn. 32 und 34 sowie die dort angeführte Rechtsprechung).

Eine solche Auslegung lässt sich, wie die Kommission ausgeführt hat, nicht mit dem 14. ErwG entkräften. Der zweite Satz dieses Erwägungsgrundes verweist nämlich u.a. auf „Name" und „Kontaktdaten" der juristischen Person, nicht aber der natürlichen Personen, die im Namen oder für Rechnung einer juristischen Person tätig sind.

Im vorliegenden Fall ist festzustellen, dass der Vorname und der Nachname einer identifizierten oder identifizierbaren natürlichen Person personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO sind. Gleiches gilt für die Unterschrift einer solchen natürlichen Person (vgl. i.d.S. Urt. v. 04.10.2024, Agentsia po vpisvaniyata, C-200/23, EU:C:2024:827, Rn. 136).

Hinsichtlich der übrigen im Ausgangsverfahren in Rede stehenden Kontaktdaten obliegt dem vorlegenden Gericht die Prüfung, ob diese Kontaktdaten unter Berücksichtigung der in Rn. 21 des vorliegenden Urteils angeführten Rechtsprechung mit einer identifizierten oder identifizierbaren natürlichen Person verknüpft sind. [...]

Aus dem Ausdruck „jeder Vorgang" ergibt sich somit, dass der Gesetzgeber den Begriff „Verarbeitung" weit fassen wollte; dies wird dadurch bestätigt, dass die Vorgänge – die die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung einschließen, wobei diese Vorgänge automatisiert oder nicht automatisiert erfolgen können – in der genannten Bestimmung nicht abschließend aufgezählt werden, was durch die Wendung „wie" zum Ausdruck kommt (vgl. in diesem Sinne Urt. v. 07.03.2024, Endemol Shine Finland, C-740/22, EU:C:2024:216, Rn. 29 und 30 sowie die dort angeführte Rechtsprechung).

In jedem Fall bietet der Wortlaut von Art. 4 Nr. 2 DS-GVO keinerlei Anhaltspunkt dafür, dass der Unionsgesetzgeber die Absicht gehabt hätte, die Einstufung dieser Vorgänge als „Verarbeitung" von ihrer Zweckbestimmung abhängig zu machen.

Eine solche Auslegung steht mit dem Ziel der DS-GVO in Einklang, das, wie aus ihrem Art. 1 und aus ihren Erwägungsgründen 1 und 10 hervorgeht, insbesondere darin besteht, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres in Art. 8 Abs. 1 der Charta und in Art. 16 Abs. 1 AEUV verankerten Rechts auf Privatleben bei der Verarbeitung personenbezogener Daten – zu gewährleisten (vgl. i.d.S. Urt. v. 09.01.2025, Mousse, C-394/23, EU:C:2025:2, Rn. 21 und die dort angeführte Rechtsprechung).

Im vorliegenden Fall fällt die Übermittlung von Daten wie Vorname, Nachname, Unterschrift und Kontaktdaten einer natürlichen Person, die eine juristische Person vertritt, unter den Begriff „Verarbeitung" im Sinne von Art. 4 Nr. 2 DS-GVO. Wie sich aus den Rn. 27 bis 29 des vorliegenden Urteils ergibt, ist es für die Einstufung als „Verarbeitung" im Sinne dieser Bestimmung ohne Belang, dass die Offenlegung dieser Daten allein zu dem Zweck erfolgt, die Identifizierung einer natürlichen Person zu ermöglichen, die befugt ist, im Namen einer juristischen Person zu handeln.

Nach alledem ist auf die erste Frage zu antworten, dass Art. 4 Nr. 1 und 2 DS-GVO dahin auszulegen ist, dass die Offenlegung des Vornamens, des Nachnamens, der Unterschrift und der Kontaktdaten einer natürlichen Person, die eine juristische Person vertritt, eine Verarbeitung personenbezogener Daten darstellt. Der Umstand, dass die Offenlegung allein zu dem Zweck erfolgt, die Identifizierung der natürlichen Person zu ermöglichen, die befugt ist, im Namen der juristischen Person zu handeln, ist insoweit ohne Belang.

Zur Vertiefung

[Urteil] Anspruch eines früheren Vereinsvorstandsmitglieds auf Löschung seiner im Vereinsregister eingetragenen personenbezogenen Daten = RDV 6/2024

[Urteil] DS-GVO-Konformität des IAB Frameworks = RDV 3/2024

WICHTIGES AUS DER RECHTSPRECHUNG

Meta darf Social-Media-Daten für KI-Training nutzen

(OLG Köln, Urteil vom 23. Mai 2025 – 15 UKl 2/25 –)

Die Verarbeitung von personenbezogenen Daten, die Nutzer eines sozialen Netzwerks auf der Plattform veröffentlicht haben, zur Entwicklung und Verbesserung von Systemen Künstlicher Intelligenz ist zulässig.

Nicht amtlicher Leitsatz

Aus den Gründen:

a) Die Verfügungsbeklagte verstößt durch die Einbringung von Daten aus dem Social Media-Angebot Facebook und dem Social Media-Angebot Instagram in einen einheitlichen Datensatz zum Training ihrer KI nicht gegen ihre Pflichten aus Art. 5 Abs. 2 UAbs. 1 lit. b) DMA, da sie diese Daten hierdurch nicht im Rechtssinne "zusammenführt". [...]

b) Der Senat vermag ferner nicht festzustellen, dass die von der Verfügungsbeklagten beabsichtigte und von dem Verfügungskläger angegriffene Verarbeitung personenbezogener Daten nicht rechtmäßig (Art. 5 Abs. 1 lit. a) DS-GVO) wäre und damit Datenschutzrecht verletzen würde. [...]

cc) Die von der Verfügungsbeklagten beabsichtigte Datenverarbeitung ist bei summarischer Prüfung [...] rechtmäßig, da sie sich, was entscheidend ist, da andere Rechtsgrundlagen nicht ersichtlich sind, auf den Rechtfertigungsgrund des Art. 6 Abs. 1 S. 1 lit. f) DS-GVO stützen kann.

aaa) Speziellere, Art. 6 Abs. 1 S. 1 lit. f) DS-GVO verdrängende Rechtsgrundlagen zum Training von KI mittels Nutzerdaten ergeben sich insbesondere nicht aus der KI-VO (vgl. insoweit ErwG 63, S. 3 zur KI-VO; hierzu auch: Schwartmann u.a./Schwartmann/Mühlenbeck/Pieper, DS-GVO, 2024, Art. 6 EUV 2016/679, Rn. 288; Schaffland/Wiltfang/Schaffland/Holthaus, DS-GVO, 2025, Art. 6 EUV 2016/679, Rn. 119a). Auch aus der DS-GVO ergeben sich keine vorrangigen Rechtsgrundlagen. Soweit in der Literatur gelegentlich Art. 6 Abs. 4 DS-GVO für Datenverarbeitungen im Bereich der KI-Trainings herangezogen wird (vgl. die – kritische – Darstellung – bei SSchwartmann u.a./Schwartmann/Mühlenbeck/Pieper, DS-GVO, 2024, Art. 6 EUV 2016/679, Rn. 307 und Gola/Heckmann/Schulz, Da-

tenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2022, Art. 6 Rn. 152), hat sich die Verfügungsbeklagte hierauf bereits nicht berufen. Art. 6 Abs. 4 DS-GVO bietet richtigerweise zudem bereits keinen eigenen Erlaubnistatbestand (so wohl: EuGH, Urt. v. 21.12.2023 – C-667/21 – juris, Rn. 75; aus der Literatur vgl. Schwartmann u.a./Schwartmann/Mühlenbeck/Pieper, DS-GVO, 2024, Art. 6 EUV 2016/679, Rn. 239 mit Nachweisen zur Gegenauffassung; Ehmann/Selmayr/Heberlein, DS-GVO, 2024, Art. 6 Rn. 69; Wolff/Brink/von Ungern-Sternberg/Albers/Veit, BeckOK, Datenschutzrecht, 01.02.2025, Art. 6 Rn. 107 f.).

bbb) Bei einer summarischen Prüfung ist die streitgegenständliche Datenverarbeitung zur Wahrung der berechtigten Interessen der Verfügungsbeklagten erforderlich und überwiegen die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen, die den Schutz personenbezogener Daten erfordern, nicht.

Aus der Rechtsprechung des Europäischen Gerichtshofs (vgl. etwa EuGH, Urt. v. 04.07.2023 – C-252/21 – Rn. 106) ergibt sich folgende Prüfungstrias: 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.

Auf dieser Grundlage vermag der Senat auf Basis einer summarischen Prüfung nicht festzustellen, dass Art. 6 Abs. 1 S. 1 lit f) DS-GVO die von der Verfügungsbeklagten beabsichtigte Datenverarbeitung nicht zu rechtfertigen vermag.

ccc) Die Verfügungsbeklagte verfolgt mit dem Training einer von ihr entwickelten KI mit den von ihren Nutzern in deren Nutzerkonten veröffentlichen Daten ein berechtigtes Interesse.

(1.) Als berechtigte Interessen kommen neben rechtlichen und ideellen insbesondere auch wirtschaftliche Belange in Betracht (EuGH, Urt. v. 04.10.2024 – C-621/22 -, juris, Rn. 47; Hüger, ZfdR 2024, 263, 272). In seiner Stellungnahme vom 17.12.2024 hat der Ausschuss Art. 6 Abs. 1 S. 1 lit. f) DS-GVO auf dieser Basis als taugliche Grundlage angesehen, KI-Modell mit Datensätzen, die personenbezogene Daten enthalten, zu trainieren und hat das entsprechende Interesse damit als berechtigt angesehen. Diese Auffassung hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit in der mündlichen Verhandlung am 22.05.2025 geteilt (entsprechend der ganz h.M. so etwa auch: Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 21: "regelmäßig anzunehmen"; Schaffland/Wiltfang/Schaffland/Holthaus, DS-GVO, 2025, Art. 6 EUV 2016/679, Rn. 119a; Schwartmann u.a./Keber, KI-VO – Leitfaden, 2024, 2. Teil, Kapitel 3 Rn. 28; Golland, EuZW 2024, 846, 849; Dieker, ZD 2024, 132, 134).

(2.) Erforderlich ist weiter, dass das Interesse hinreichend klar und präzise formuliert und real und gegenwärtig und nicht bloß spekulativ ist (EuGH, Urt. v. 04.10.2024 – C-621/22 –, juris, Rn. 49).

Diese Voraussetzungen sind auf Basis einer summarischen Prüfung erfüllt.

Die Verfügungsbeklagte hat beschrieben, die Möglichkeiten generativer KI nutzen zu wollen, um einen Gesprächsassistenten bereitzustellen, der etwa Antworten in Echtzeit für Chats, Hilfe bei der Organisation und Planung etwa eines Urlaubs bis hin zu Hilfen bei der Formulierung von Texten bietet. Hierzu soll die KI an regionale Gepflogenheiten angepasst werden. Zudem sollen Inhalte wie etwa Texte, Bilder und Audios erstellt werden können. Da die Verfügungsbeklagte mit dem entsprechenden Training zeitlich unmittelbar beginnen möchte, ist das entsprechend konkret beschriebene Interesse auch gegenwärtig und nicht bloß spekulativ.

(3.) Damit die Wahrnehmung dieses Interesses eine Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 UnterAbs. 1 lit. f) DS-GVO rechtfertigen kann, ist ferner ist erforderlich, dass die Verfügungsbeklagte allen anderen, ihr obliegenden Pflichten aus der DS-GVO nachkommt (EuGH, Urt. v. 04.10.2024 – C-621/22 -, juris, Rn. 50).

Auf solche weiteren datenschutzrechtlichen Anforderungen, die im Rahmen des Trainings von KI-Modellen zu beachten sind (etwa: Grundsatz der Datenrichtigkeit, Art. 5 Abs. 1 lit. d) DS-GVO; Grundsatz der Zweckbindung, Art. 5 Abs. 1 lit. b) DS-GVO; Transparenzgrundsatz, Art. 5 Abs. 1 lit a) Var. 3 DS-GVO und Art. 12 ff. DS-GVO; vgl. Paal, ZfDR 2024, 129, 141 ff.), beziehen sich die Angriffe des Verfügungsklägers nicht im Schwerpunkt. Oftmals erscheint eine Beachtung auch noch im Rahmen des Betriebs der KI möglich. Unabhängig von einer Anwendbarkeit des Art. 14 Abs. 5 lit. b) DS-GVO ist den Transparenzerfordernissen (Art. 12 ff. DS-GVO) durch die von der Verfügungsbeklagten umfangreich zur Verfügung gestellten Informationen (Anlage AG 8, 22 bis 29) Rechnung getragen. Ferner kommt es nicht darauf an, ob die Verfügungsbeklagte gegen eine – in Art. 83 Abs. 4 lit. a) DS-GVO allerdings bußgeldbewehrte – Pflicht zur Einholung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO verstoßen hat. Diese ist – wie sich aus ihrer Stellung in Kapitel IV der DS-GVO ergibt, dessen Anforderungen der Europäische Gerichthof nicht als Rechtmäßigkeitsvoraussetzungen der Datenschutzverordnung erachtet (EuGH, Urt. v. 04.05.2023 – C-60/22 –, juris, Rn. 62; Wolff/Brink/von Ungern-Sternberg/Hansen, BeckOK Datenschutzrecht, 01.02.2024, Art. 35 Rn. 76a) – keine Rechtmäßigkeitsvoraussetzung der Datenverarbeitung (BSG, Urt. v. 20.01.2021 – B 1 KR 7/20 R –, juris, Rn. 84 m.w.N.; Simitis/Hornung/Spiecker gen. Döhmann/Karg, Datenschutzrecht, 2025, Art. 35 Rn. 104; Gola/Heckmann/Nolte/Werkmeister, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2022, Art. 35 Rn. 74).

ddd) Die entsprechende Datenverarbeitung erweist sich bei einer summarischen Prüfung auch – unter gemeinsamer Prüfung mit dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO (vgl. hierzu EuGH Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 109; EuGH, Urt. v. 09.01.2025 – Rs. C-394/23, Rn. 48f.) – als erforderlich.

Mit dieser Ansicht steht der Senat im Wesentlichen im Einklang mit der in der mündlichen Verhandlung am 22.05.2025 geschilderten Auffassung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, der eine Erforderlichkeit im Grundsatz anerkannte und lediglich Zweifel hinsichtlich der Verwendung besonders eingriffsintensiver Daten äußerte (etwa Nummernschilder von Fahrzeugen, Kreditkartennummern).

Eine Datenverarbeitung ist erforderlich, wenn sie zur Erreichung des Interesses des Verarbeiters geeignet ist und es keine weniger in die Privatsphäre eingreifende Möglichkeit gibt, den entsprechenden Zweck zu erreichen (EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 108).

Hierfür ist – worauf der Verfügungskläger mit Recht hinweist – die Verfügungsbeklagte beweisbelastet (EuGH, Urt. v. 11.07.2024 – C-757/22 –, Rn. 52; OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23 –, juris, Rn. 182 ff). Die entsprechenden Verfahrensvorschriften ergeben sich mangels konkreter Regelungen im europäischen Recht aus dem nationalen Recht. § 5 UKlaG verweist insoweit auf die Zivilprozessordnung. Für die im Verfahren des einstweiligen Rechtsschutzes erforderliche Glaubhaftmachung besteht insoweit eine Abweichung vom Regelbeweismaß der vollen Überzeugung von der Wahrheit einer Tatsache. Es genügt, wenn ihr Vorliegen überwiegend wahrscheinlich ist, d.h., dass etwas mehr für das Vorliegen der Tatsache spricht als gegen sie (Kessen/Tholen/Kessen, KK-Vorläufiger Rechtsschutz, § 920 Rn. 19; Kessen, aaO., § 935 Rn. 9). Ob das Beweismaß erreicht ist, beurteilt das Gericht in freier Würdigung (Kessen/Tholen/Kessen, KK-Vorläufiger Rechtsschutz, § 920 Rn. 21; Kessen, aaO., § 935 Rn. 9).

Nach diesen Maßstäben hat der Senat keine Zweifel, dass das Training der von der Verfügungsbeklagten entwickelten KI mit den Nutzerdaten geeignet ist, die aufgezeigten, mit ihm verfolgten Zwecke zu erreichen, d.h. eine generative KI optimiert an regionale Gepflogenheiten anzubieten und in die Dienste der Verfügungsbeklagten zu implementieren.

Im Hinblick auf weniger in die Privatsphäre eingreifende – aber gleich geeignete – Möglichkeiten der Zielerreichung hat zwar der Verfügungskläger entsprechend der Stellungnahme vom 17.12.2024 des Ausschusses (Rn. 75; ähnlich auch: Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 22) auf die Möglichkeit des Trainings mittels anonymisierter oder sog. synthetischer Daten hingewiesen. Zudem hat der Verfügungskläger vorgetragen, die Verfügungsbeklagte könne das Training der KI auf sog. Flywheel-Daten beschränken. Ferner hat er vorgetragen, die Erforderlichkeit müsse hinsichtlich jedes einzelnen Datenpunktes gegeben sein. Angesichts der Vielzahl der für das Training der KI erhobenen Daten sei nicht dargetan, dass jeder einzelne Datenpunkt erforderlich sei.

Dennoch erscheint dem Senat der mittels eidesstattlicher Verfügung glaubhaft gemachte Vortrag der Verfügungsbeklagten, dass es "keine andere sinnvolle Alternative für Meta [gibt], um seine Interessen ebenso wirksam mit anderen, milderen Mittel zu verfolgen und zu erreichen. Meta hat zur Zielerreichung verfügbare Alternativen geprüft [im übersetzten Original: "considered available alternative ways], die eine weniger intensive Nutzung personenbezogener Daten ermöglichen würden" als überwiegend wahrscheinlich. Die Notwendigkeit des Trainings großer generativer KI-Modelle mit "riesigen Mengen an Text, Bildern, Videos und anderen Daten" ist im ErwG 105 der KI-VO ausdrücklich anerkannt (vgl. zu dem erforderlichen Einsatz von Massendaten aus dem juristischen Schrifttum etwa Paal, ZfDR 2024, 129, 141). Der Vortrag der Verfügungsbeklagten wird im Hinblick auf eine fehlende Möglichkeit zur Anonymisierung durch Stellungnahmen im juristischen Schrifttum bestätigt, die eine solche für unpraktikabel halten (vgl. Paal, ZfDR 2024, 129, 136; Dieker, ZD 2024, 132, 134; Schürmann ZD 2022, 316, 317). Im Hinblick auf den bloßen Einsatz von sog. Flywheel-Daten ist es kaum plausibel, dass die so zu erzielende, deutlich geringere Menge an Daten im Vergleich zu dem vorhandenen Datenbestand aus aktiven Nutzerkonten zu vergleichbaren Ergebnissen beim Training der KI führt. Das insoweit ein "minderwertiges Produkt" entstehen würde, hat die Verfügungsbeklagte mit eidesstattlicher Versicherung des Direktors GenAI Produkt Management bei Meta Platforms Inc, U. R., v. 18.05.2025 (Anlage AG 42) ebenso glaubhaft gemacht, wie die fehlende Gleichwertigkeit des Rückgriffs auf synthetische Daten (eidesstattliche Versicherung vom 21.05.2025, Anlage AG 45). Dem ist der Verfügungskläger nicht substanziiert entgegengetreten. Eine Pflicht, die Erforderlichkeit bezüglich jedes Datenpunktes zu belegen, trifft die Verfügungsbeklagte nicht. Das Training einer KI erfordert die Verwendung von Massen von Daten zur Generierung von Mustern und Wahrscheinlichkeitsparametern (Schwartmann u.a./Schwartmann/Köhler, KI-VO – Leitfaden, 2024, 2. Teil Kapitel 3 Rn. 9). Insoweit kommt dem einzelnen Datum im Zweifel kaum je ein messbarer Einfluss zu (vgl. insoweit Paal, ZfDR 2024, 129, 141: "Prüfung der Erforderlichkeit für jedes einzelne Datum weder zielführend noch praktikabel"). Der Senat geht – wie dargelegt – in Übereinstimmung mit dem Ausschuss und der ganz h.M. davon aus, dass Art. 6 Abs. 1 S. 1 lit. f) DS-GVO ein tauglicher Rechtfertigungsgrund für Datenverarbeitung zum Training von KI sein kann. Unmöglich zu erfüllende Anforderungen würden diese Annahme konterkarieren und dürfen nicht aufgestellt werden. Zwar werden in der Literatur teilweise Möglichkeiten diskutiert, die die Diskrepanz zwischen dem "Datenhunger" des KI-Trainings und dem Grundsatz der Datenminimierung auflösen (vgl. insoweit Paal, ZfDR 2024, 129, 141 m.w.N.). Im Rahmen der im Eilrechtsschutz zur Verfügung stehenden Erkenntnismöglichkeiten sieht der Senat aber keine hinreichend verlässlichen Alternativen. Soweit erwogen werden kann, den Grundsatz der Erforderlichkeit auf die Art der verarbeiteten Daten zu beziehen, also die Verarbeitung personenbezogener Daten möglichst zu meiden (vgl. Hüger, ZfDR 2024, 263, 273), hat die Verfügungsbeklagte glaubhaft gemacht, auf Methoden der Deidentifizierung der in den Trainingsdatensatz eingestellten Daten zurückzugreifen. Damit wird auch den geschilderten Bedenken des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit Rechnung getragen. Soweit in der Literatur die häufig durchgeführte Form der Datensammlung durch Web-Scraping und Crawling als die "effektivste" Form (Dieker, ZD 2024, 132,134) der Datensammlung angesehen wird, kommt es hierauf nicht an: Diese wäre mit deutlich erheblicheren Eingriffen in die Rechte der Betroffenen verbunden, da die von der Verfügungsbeklagten implementierten Abschwächungsmaßnahmen insoweit nicht greifen würden. Zudem beabsichtigt die Verfügungsbeklagte gerade ein Training mit "regionalen" Daten, sodass diese Art der Datengewinnung nicht gleich geeignet wäre.

eee) Bei einer summarischen Prüfung vermag der Senat auch nicht festzustellen, dass die Interessen der Nutzer und der Drittbetroffenen am Schutz ihrer Daten gegenüber dem Interesse der Verfügungsbeklagten am Training der KI mit Nutzerdaten überwiegen.

Hauptsächliche Anknüpfungspunkte für die Abwägung sind, ob der Betroffene bei Erhebung der Daten vernünftigerweise mit einer entsprechenden Verarbeitung rechnen musste (ErwG 47 S. 4 der DS-GVO) und welche Folgen die Datenverarbeitung für die Betroffenen mit sich bringt (EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 116), d.h. deren Eingriffsintensität.

aaaa) (1.) Im Hinblick auf die nicht im Einzelfall, sondern objektivierend und generalisierend zu betrachtenden (Schwartmann u.a./Schwartmann/Klein, DS-GVO, 2024, Art. 6 EUV 2016/679 Rn. 162) Folgen der Datenverarbeitung für die Betroffenen ist entscheidungserheblich allein das Training der KI mit personenbezogenen Daten und dessen Folgen. Sonstige mögliche Rechtsverletzungen, die durch die spätere "Arbeit" der KI entstehen können (etwa Desinformation, Manipulationen, sonstige schädliche Praktiken), sind derzeit nicht hinreichend absehbar und können gesondert verfolgt werden. Es ist jedenfalls fernliegend, dass diese Risiken sich so weit materialisieren, dass eine rechtmäßige Nutzung der KI unmöglich würde und letztlich die Geeignetheit der Datenverarbeitung in Frage stünde. Entscheidend ist damit der Eingriff der Datenverarbeitung in das jeweilige Grundrecht der Betroffenen auf Achtung ihres Privat- und Familienlebens aus Art. 8 EMRK bzw. Art. 7 GrCh sowie in ihr Recht auf Schutz ihrer personenbezogenen Daten gem. Art. 8 GrCh (vgl. EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 108; zur Anwendbarkeit des europäischen Rechts vgl. BVerfG, Beschl. v. 06.11.2019 – 1 BvR 276/17 –, juris, Rn. 77, 95).

Da der Verfügungskläger ausschließlich die Untersagung der Nutzung von sog. First Party Data beantragt, beschränkt sich die durch den Senat zu prüfende Datenverarbeitung und damit der Eingriff in die Rechte der Betroffen auf die öffentlich gestellten Daten in den aktiven Nutzerkonten Volljähriger sowie von Institutionen (Schulen, Kindergärten, Vereine). Allerdings verkennt der Senat nicht, dass auch durch Volljährige und Institutionen Daten von Minderjährigen gepostet werden können, die dann in den Trainingsdatensatz eingehen. Zu denken ist dabei auch an sensible Daten, insbesondere Fotographien ("Kinderfotos"). Insoweit hat der Senat den Aspekt des Minderjährigenschutzes trotz der Vorkehrungen der Verfügungsbeklagten zur Ausklammerung solcher Daten in seine Überlegungen einbezogen.

(2.) Durch die Beschränkung der Verarbeitung auf "öffentlich" in den Nutzkonten eingestellte Daten sind allein personenbezogene Daten betroffen, die bereits zuvor für jedermann öffentlich einsehbar und auch mittels Suchmaschinen auffindbar waren. Letzteres wurde im Rahmen der mündlichen Verhandlung sowohl durch die Verfügungsbeklagte als auch den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit auf ausdrückliche Nachfrage des Senats bestätigt. Ein Unterschied zwischen den Daten in den Nutzerkonten und allgemein im Internet verfügbaren Daten liegt allein in deren Verarbeitbarkeit für Zwecke des Web-Scrapings, das bei den Daten in den Nutzerkonten nicht ohne weiteres möglich ist. Insoweit beschränkt sich der Eingriff gerade durch die angegriffene Datenverarbeitung auf eine zusätzlich hinzukommende Art der Datenverarbeitung zur bislang erfolgten Verarbeitung. Aufgrund der bereits bestehenden Öffentlichkeit der Daten sind über den Eingriff in das Selbstbestimmungsrecht über die Verwendung der eigenen personenbezogenen Daten hinausgehende neue Nachteile durch eine Offenlegung der Daten, wie etwa soziale oder berufliche Konsequenzen, regelmäßig nicht zu befürchten. Hinzu kommt, dass KI-Systeme nicht mit einem "Datenarchiv" gleichzusetzen sind, sondern regelmäßig allein aus Parametern für Wahrscheinlichkeitsberechnungen bestehen (Schwartmann u.a./Schwartmann/Köhler, KI-VO – Leitfaden, 2024, 2. Teil Kapitel 3 Rn. 9). Allerdings ist zu berücksichtigen, dass die Einstellung von personenbezogenen Daten in die KI ein rechtlich relevantes (zutreffend: Schwartmann/Köhler, RDV 2024, 316) Risiko der "Erinnerung" (Pesch/Böhme, MMR 2023, 917 ff.) der KI an personenbezogene Daten und damit deren Rekonstruierbarkeit und Ausgabe dieser Daten bei der "Arbeit" der KI birgt (vgl. Ausschuss vom 17. Dezember 2024, Rn. 35 ff.; Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 7 ff.; Schwartmann u.a./Schwartmann/Köhler, KI-VO – Leitfaden, 2024, 2. Teil, Kapitel 3 Rn. 10).

Hinzu kommt die fehlende Erklärbarkeit, Transparenz und Funktionsweise großer generative KI-Modelle, die das Recht zur Selbstbestimmung der Betroffenen über ihre Daten beeinträchtigen kann (vgl. Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 25). Dieses Risiko erlangt eine besondere Bedeutung, weil die KI letztlich einer unabsehbaren Vielzahl von Nutzern zur Verfügung steht und in vielen Fällen sehr umfangreiche Datenbestände einzelner Personen betroffen sind (vgl. Paal, ZfDR 2024, 129, 152; vgl. auch Ausschuss vom 08.10.2024, Rn. 41). Ferner ist insoweit zu berücksichtigen, dass eine spätere Löschung der Daten aus der KI nur eingeschränkt möglich ist und mit einem einmal erfolgten Training der KI die Verfügungsbeklagte ihr mit dem Training verfolgte Ziel der Erarbeitung eines Modells erreicht haben wird. Mit der Einschränkung des Löschungsrechts (Art. 17 DS-GVO) wird ein zentrales Betroffenenrecht beeinträchtigt.

Der Senat hat im Rahmen des von dem Verfügungskläger geführten Verbandsklageverfahrens auch berücksichtigt, dass die Datennutzung personenbezogene Daten erheblicher Teile der deutschen Bevölkerung betrifft (die Antragsschrift, S. 33, spricht von ca. 40 Millionen Nutzern von Facebook und 31 Millionen Nutzern von Instagram in Deutschland).

(3.) Ferner ist bei der Feststellung der Eingriffsintensität von Bedeutung, dass die Verfügungsbeklagte zahlreiche der Maßnahmen umgesetzt hat, die der Ausschuss in seiner Stellungnahme vom 17.12.2024 (Rn. 96 ff.) empfohlen hat, um die mit dem Training einer KI mit Nutzerdaten verbundenen Eingriffe in die Rechte der Betroffenen abzuschwächen und in einen angemessenen Ausgleich mit dem Interesse des Verantwortlichen zu bringen.

(a) Die Verfügungsbeklagte hat durch eidesstattliche Versicherung des Direktors GenAI Produkt Management bei Meta Platforms Inc, U. R., vom 18.05.2025 (Anlage AG 42) glaubhaft gemacht, Maßnahmen zu Deidentifizierung der Datensätze vorzunehmen (Entfernung von vollständigen Namen, E-Mail-Adressen, Telefonnummern, nationale Identifikationsnummern, Benutzerkennungen, Kredit-/Debitkartennummern, Bankkontonummern/Bankleitzahlen, Fahrzeugkennzeichen, IP-Adressen und Postanschriften) und diese in unstrukturierter Form und "tokenisiert" zusammenzustellen. Unstreitig ist

mit diesen Maßnahmen zwar keine Anonymisierung verbunden. Insbesondere werden die Gesichter der auf Fotographien erkennbaren Personen nicht verborgen, sodass insoweit eine Deidentifizierung faktisch nicht erfolgt. Obwohl damit nicht ausgeschlossen ist, dass im Einzelfall trotz der Deidentifizierung eine Identifizierung erfolgen kann, steht für den Senat außer Zweifel, dass diese Maßnahme insgesamt das entsprechende Risiko mindern wird.

(b) Die Verfügungsbeklagte hat ferner glaubhaft gemacht, technische, physische und organisatorische Maßnahmen ergriffen zu haben, um einen unberechtigten Zugriff auf die Trainingsdaten zu verhindern und sicherheitsrelevante Aktivitäten durch die Arbeit der KI festzustellen. Es ist jedenfalls hinreichend wahrscheinlich, dass diese Maßnahmen geeignet sind, etwaige Risiken zu mindern.

(c) Zudem stehen den Nutzern umfangreiche Möglichkeiten offen, die Aufnahme ihrer Daten in den Trainingsdatensatz zu verhindern. So hat die Verfügungsbeklagte unwidersprochen vorgetragen, dass bei Facebook die Möglichkeit besteht, sämtlichen Beiträgen – auch nachträglich – mittels einer einzelnen Anordnung in den Einstellungen den "öffentlichen" Status zu entziehen, und dass bei Instagram die Möglichkeit besteht, dem Konto insgesamt den öffentlichen Status zu entziehen. Damit würde verhindert, dass die Daten in den Trainingsdatensatz eingehen. Der Senat verkennt nicht, dass dies für einen bestimmten Teil der Nutzer mit einer erheblichen und möglicherweise als unzumutbar empfundenen Einschränkung der eigenen Wahrnehmbarkeit für Dritte verbunden ist. Insoweit gewährt die Verfügungsbeklagte aber ergänzend die Möglichkeit, lediglich der Aufnahme der Daten in den Trainingsdatensatz zu widersprechen. Dies gibt dem durchschnittlichen Nutzer eine effektive Möglichkeit, eine Aufnahme ihrer personenbezogenen Daten in den Trainingsdatensatz zu verhindern.

Anderes als der Verfügungskläger meint, sieht der Senat keine relevanten technischen Hürden bei der Ausübung des Widerspruchsrechts. Die Verfügungsbeklagte hat verschiedene Möglichkeiten des Widerspruchs vorgetragen und mit der von ihr vorgelegten eidesstattlichen Versicherung (Anlage AG 9) glaubhaft gemacht, dass diese technisch auch – von üblichen Fehlerraten abgesehen – funktionieren. Demgegenüber von dem Verfügungskläger aus seiner Praxis berichtete einzelne Problemfälle vermögen dies nicht grundsätzlich in Frage zu stellen. Aus dem von der Verfügungsbeklagten vorgelegten Screenshot der Internetseite, auf der die Widerspruchsmöglichkeit ausgeübt werden kann (Anlage AG 31), ergibt sich ferner, dass der Widerspruch für den durchschnittlichen Nutzer unkompliziert ausgeübt werden kann.

Auch ist die Frist von immerhin ca. sechs Wochen für die zu treffende Entscheidung hinreichend bemessen. Dabei verkennt der Senat nicht, dass die Entscheidung mit für durchschnittliche Nutzer kaum übersehbaren technischen Vorfragen über die Funktionsweise von KI-Systemen verbunden ist (vgl. Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 25). Bei verbleibenden Zweifeln steht es jedem Nutzer aber frei, den Widerspruch auszuüben.

Eine mangelnde Transparenz der Informationen zum Widerspruchsrecht vermag der Senat ebenfalls nicht zu erkennen. Mit Pressemitteilung vom 14. April 2025 informierte die Verfügungsbeklagte über die anstehende Datennutzung für das KI-Training und kündigte weitere Informationen an. Diese erfolgten sodann insbesondere mittels In-App-Benachrichtigungen und einer E-Mail-Kampagne. In der Informations-Email für Facebook-Nutzer (Anlage AG 27) heißt es bei der Erläuterung, welche Daten verwendet werden für den Durchschnittsnutzer ohne Weiteres verständlich:

"Dazu zählen alle öffentlichen Informationen, die du seit dem Erstellen deines Kontos in Meta-Produkten geteilt hat. Darüber hinaus verwenden wir auch deine Interaktionen mit Funktionen von KI bei Meta."

Die Verfügungsbeklagte hat insoweit durch Vorlage von (elektronischen) Abschriften der entsprechenden Dokumente (Anlage AG 8, 22 bis 29) glaubhaft gemacht, die beabsichtigte Datennutzung transparent und für den Durchschnittsnutzer verständlich erläutert und eine Handlungsnotwendigkeit verdeutlicht zu haben.

Der Senat verkennt allerdings nicht die begrenzte Wirksamkeit der Möglichkeit zur Rücknahme der Öffentlichkeit von Postings oder des Kontos bzw. der Möglichkeit eines Widerspruchs in Bezug auf Daten von Dritten in Nutzerkonten. Soweit personenbezogene Informationen über eine dritte Person in einem Konto enthalten sind, vermag eine Rücknahme der Öffentlichkeit bzw. ein Widerspruch diese dritte Person nur dann zu schützen, wenn sie von dem Kontoinhaber vorgenommen bzw. erklärt wird. Dies gilt unabhängig von der Frage, ob der betroffene Dritte die Angebote der Verfügungsbeklagten überhaupt nutzt oder nicht. Hinzu kommt, dass ein Widerspruch für institutionsbezogene Konten (Schulen, Kindergärten, Unternehmen, Fanpages) nicht möglich ist. Dort eingestellten Daten genießen damit keinen Schutz, soweit sie – auf Basis einer entsprechenden Abwägungsentscheidung der jeweiligen Einrichtung – öffentlich gehalten werden.

Insgesamt betrachtet, ist es – trotz der geschilderten Einschränkungen – im Rahmen der im Eilverfahren zur Verfügung stehenden Erkenntnismöglichkeiten überwiegend wahrscheinlich, dass die Möglichkeit, die Öffentlichkeit der betroffenen Daten zu widerrufen, und/oder die Möglichkeit der Ausübung des Widerspruchs gegen die Verwendung der Daten für das KI-Training entgegen der Befürchtungen des Verfügungsklägers eine praktische Wirksamkeit entfalten wird.

bbbb) Eine Erwartbarkeit der Verwendung von Nutzerdaten für Zwecke des Trainings von KI vermag der Senat erst für ab dem 26.06.2024 in die betroffenen Dienste eingestellte Daten festzustellen.

Der Ausschuss verweist zur Feststellung der berechtigten Erwartungen der Betroffenen in seiner Stellungnahme vom 17.12.2024 insbesondere darauf, ob die entsprechenden Daten öffentlich zugänglich waren, welche Art der Beziehung zwischen der betroffenen Person und dem Verantwortlichen sowie der Quelle bestand, aus der die Daten stammen, den dort gebotenen Datenschutzeinstellungen und ob die betroffenen Personen dem für die Verarbeitung Verantwortlichen die Daten direkt – etwa im Rahmen der Nutzung des Dienstes – zur Verfügung gestellt haben (Ausschuss vom 17.12.2024, Rn. 93 f.; vgl. zu den Feststellungskriterien auch DSK, Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung

unter Geltung der Datenschutz-Grundverordnung (DS-GVO), https://www.datenschutzkonferenzonline.de/media/oh/OH-Werbung_Februar%202022_final.pdf; Paal, ZfDR 2024, 129, 153; Franke, RDi 2023, 565, 567). Nicht entscheidend sind dabei etwaige – möglicherweise missbräuchliche – Gepflogenheiten der Datenverarbeitung in bestimmten Branchen. Die von der Verfügungsbeklagten mittels Pressemitteilungen großer KI-Unternehmen (Anlage AG 20 und AG 21) belegte Praxis, Daten zum Training von KI mittels sog. Web-Scrapings schlicht "abzugreifen", prägt daher nicht die berechtigten Erwartungen der Betroffenen (vgl. Ausschuss vom 08.10.2024, Rn. 52 unter Hinweis auf EuGH, Urt. v. 04.07.2023 – C-252/21 -, juris, Rn. 117).

Nach diesen Maßgaben konnte und musste "vernünftigerweise" mit einer Nutzung von der Verfügungsbeklagten überlassenen Daten zum Training von KI jedenfalls ab ihrer öffentlichen Mitteilung vom 10.06.2024, ab dem 26.06.2024 Nutzerdaten zum Zwecke des Trainings ihrer KI nutzen zu wollen, gerechnet werden. Wenngleich die Verfügungsbeklagte diese Ankündigung später zunächst zurückgenommen hat, war ihre grundsätzliche Nutzungsabsicht damit deutlich.

Im Hinblick auf vor diesem Zeitpunkt eingestellte Daten vermag der Senat im Rahmen einer summarischen Prüfung eine solche Erwartung hingegen nicht festzustellen. Eine solche Erwartung ist von der Verfügungsbeklagten bereits nicht substanziiert dargetan. Sie ist auch nicht anderweitig erkennbar. Insoweit ist breiten Nutzerkreisen der Begriff der "Künstlichen Intelligenz" und die Notwendigkeiten des "Trainings" solcher Systeme mit umfangreichen Datenbeständen lange nicht bekannt gewesen. Im Anschluss an die öffentliche Vorstellung von "ChatGTP" im November 2022 musste zwar bei öffentlich "gestellten" Daten mit einer potenziellen Nutzung mittels Web-Scraping im Bereich des Trainings von KI möglicherweise gerechnet werden (Franke, RDi 2023, 565, 567; in diese Richtung auch etwa Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 24). Allerdings hat die Verfügungsbeklagte insoweit bereits nicht weiter vorgetragen. Im Hinblick auf die hier maßgebliche Verwendung gerade von Nutzerdaten in Konten sozialer Netzwerke, die – wie auch die Verfügungsbeklagte – oftmals Schutzvorkehrungen gegen solches Web-Scraping anbieten (vgl. Ziffer 3.2.3 der Nutzungsbedingungen der Verfügungsbeklagten), wird eine entsprechende Erwartung der Betroffenen, dass die Daten auch in ihren Nutzerkonten entsprechend verwendet werden, aber mit guten Gründen verneint (vgl. etwa Hüger, ZfdR 2024, 263, 273; Wilmer, K&R 2023, 233, 236). Eine solche Verwendung geht auch weit über die anzunehmende Erwartung, der Verfügungsbeklagten überlassene Daten könnten im Rahmen allgemeiner Produktverbesserunen verwendet werden, hinaus. Diese Auffassung entspricht auch der in der mündlichen Verhandlung am 22.05.2025 geäußerten Einschätzung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Dieser hat insoweit auf einen fundamentalen Unterschied bei der Erwartbarkeit einer Datenverwendung für KI-Systeme, die bestehende Dienste lediglich verbessern und – wie hier – der Entwicklung selbstständig einsetzbarer KI-Modelle, die jedem zugänglich sind, hingewiesen.

cccc) Wenngleich auf dieser Basis beachtliche Beeinträchtigungen der Interessen und Grundrechte der Betroffenen festzustellen sind, überwiegen diese das Interesse der Verfügungsbeklagten an der Datenverarbeitung im Ergebnis nicht.

(1.) Jedenfalls für ab dem 26.06.2024 durch Betroffene selbst eingestellte eigene Daten, ergibt sich dies bereits daraus, dass diese vernünftigerweise mit einer entsprechenden Verarbeitung der von ihnen freiwillig auf die Plattformen der Verfügungsbeklagten für jedermann öffentlich einsehbar eingestellten Daten rechnen mussten. Wenngleich berücksichtigungsfähig ist (Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 24; Hüger, ZfDR 2024, 263, 274), dass die von der Verfügungsbeklagten entwickelte KI – auch wenn die Verfügungsbeklagte den Nutzen für eine breite Masse an Nutzern hervorhebt – im Wesentlichen wirtschaftlichen Zwecken und nicht vorrangig dem Allgemeinwohl dient, vermögen angesichts der Erwartbarkeit der entsprechenden Nutzung der der Verfügungsbeklagten überlassenen Daten die Interessen der Betroffenen auch die bloßen Individualinteressen der Verfügungsbeklagten nicht zu überwiegen. Diese Rechtsauffassung wurde in der mündlichen Verhandlung am 22.05.2025 im Grundsatz auch durch den Hamburgischen Beauftragte für Datenschutz und Informationsfreiheit vertreten, der eine entsprechende Erwartbarkeit lediglich eher ab dem 27.05.2025 annehmen wollte. Der Beauftragte hat auf Nachfrage dabei klargestellt, dass sich seine Auffassung auch auf "Bilder" beziehe.

(2.) Für vor diesem Zeitpunkt eingestellte eigene Daten und für solche Daten von Betroffenen, die in Konten Dritter eingestellt wurden, gilt im Ergebnis nichts Anderes.

Aufgrund der im Ergebnis – gerade auch aufgrund der weiteren von der Verfügungsbeklagten getroffenen Abschwächungsmaßnahmen – eher geringen Intensität des Eingriffs überwiegen aber auch in diesem Fall die Interessen der betroffenen Personen gegenüber dem, wie dargelegt, als sehr bedeutsam einzuschätzenden und kernbereichsnah betroffenen Interesse der Verfügungsbeklagten an der Datenverarbeitung nicht. Der Senat verkennt dabei nicht, dass unter den Betroffenen auch Kinder sein können, deren Interessen in besonderer Weise schutzbedürftig sind (vgl. Schwartmann u.a./Schwartmann/Klein, DS-GVO, 2024, Art. 6 EUV 2016/679, Rn. 173) und hat dies in besonderer Weise in die Abwägung einbezogen.

Es ist unwahrscheinlich, dass ein – über das grundsätzliche Recht, über die Nutzung der eigenen Daten zu bestimmen, hinausgehender – konkreter Nachteil durch die Verarbeitung entstehen kann. Es geht, worauf der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hinweist, bei der – hier in Rede stehenden – Entwicklung von großen Sprachmodellen auf Grundlage sehr großer Trainingsdatensätze regelmäßig nicht um die gezielte Verarbeitung personenbezogener Daten oder um die Identifizierung einer konkreten Person. Es kommt insoweit nicht, wie bei einem eingriffsintensiven Profiling im Sinne des Art. 4 Abs. 4 DS-GVO, das die DS-GVO nur unter strengen Voraussetzungen erlaubt, gerade auf die Informationen des Individuums an (Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 25; Franke, RDi 2023,

565, 568). Über das beeinträchtigte Interesse an der Selbstbestimmung über die eigenen Daten hinausgehende eigene Nachteile können letztlich im Wesentlichen nur durch eine spätere Wiedergabe der Daten durch die KI entstehen. Diese Gefahr ist zwar – wie dargelegt – rechtlich nicht zu vernachlässigen. Insoweit hat die Verfügungsbeklagte aber durch die eidesstattliche Versicherung des Direktors GenAI Produkt Management bei Meta Platforms Inc, U. R., vom 07.05.2025 (Anlage AG 9) sowie durch dessen weitere eidesstattlich Versicherung vom 22.05.2025 (Anlage AG 45) glaubhaft gemacht, dass diese Gefahr als gering einzuschätzen ist. Zudem hat die Verfügungsbeklagte – wenngleich nicht lückenlose – Maßnahmen zur Deidentifizierung der in den Trainingsdatensatz übernommenen Daten ergriffen. Insgesamt wird der Vortrag der Verfügungsbeklagten auch durch eine Stellungnahme des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg bestätigt, in der darauf hingewiesen wird, dass in die Interessenabwägung einzubeziehen sei, dass aufgrund der Größe der Trainingsdatensätze zur Entwicklung eines Sprachmodells nur eine geringere Identifizierungswahrscheinlichkeit für Einzelpersonen besteht. Wenn Informationen in Datensätzen nur einzeln vorhanden sind und KI-Modelle nicht wiederholt mit diesen Informationen trainiert werden, ist die Wahrscheinlichkeit hoch, dass Informationen über Einzelpersonen in der Datenmasse von KI-Modellen untergehen, d.h. nicht unverändert in einer Ausgabe eines KI-Systems erscheinen (Landesbeauftragte BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 17.10.2024, S. 25). Im Hinblick auf eine eingeschränkte Möglichkeit, einmal in die KI eingestellte Daten zu löschen, wird zwar ein zentrales Betroffenenrecht deutlich in Frage gestellt. Allerdings hat sich die Verfügungsbeklagte in der mündlichen Verhandlung am 22.05.2025 dahingehend eingelassen, solche Daten bei künftigen Trainingsvorgängen nicht mehr zu nutzen, wodurch die entsprechenden Informationen jedenfalls gleichsam verblassen würden. Dem ist der Verfügungskläger nicht substanziiert entgegengetreten. Insoweit ist die Gefahr eines unumkehrbaren Schadens jedenfalls abgeschwächt. [...]

dd) Die Verarbeitung der Daten ist auch nicht nach Art. 9 Abs. 1 DS-GVO untersagt.

aaa) Zwar wird der zu Trainingszwecken vorgesehene Datensatz auch personenbezogene Daten im Sinne des Art. 9 Abs. 1 DS-GVO enthalten.

Es handelt sich bei den in den KI-Trainingsdatensatz aufgenommenen Daten um personenbezogene Daten. Dass die von der Verfügungsbeklagten unternommene Deidentifizierung nicht zu einer vollständigen Anonymisierung führt, ist unstreitig.

Aufgrund der Weite des Anwendungsbereichs des Art. 9 Abs. 1 DS-GVO ist sicher davon auszugehen, dass solche Daten in den Nutzerdaten enthalten sind. Nach der Rechtsprechung des Europäischen Gerichtshofs sind Daten bereits dann als Gesundheitsdaten im Sinne Art. 9 Abs. 1 DS-GVO einzustufen, wenn aus diesen Daten mittels gedanklicher Kombination oder Ableitung auf den Gesundheitszustand der betroffenen Person geschlossen werden kann (EuGH, Urt. v. 04.10.2024 – C-21/23 -, juris, Rn. 83). Es ist nicht ersichtlich, dass im Rahmen der anderen Kategorien des Art. 9 Abs. 1 DS-GVO ein anderer Maßstab gelten würde (vgl. EuGH, Urt. v. 01.08.2022 – C-184/20 -, juris, Rn. 123). Dies gilt unabhängig davon, ob diese Informationen einen Nutzer einer Plattform oder eine andere natürliche Person betreffen (EuGH, Urt. v. 04.10.2024 – C-21/23 –, juris, Rn. 86; EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 68). Solche Rückschlüsse auf Dritte hält der Gerichtshof selbst dann für möglich, wenn innerhalb eines Nutzerkontos agiert werde, weil auch dann die in diesem Zusammenhang gemachten Angaben – insbesondere in Kombination mit weiteren Informationen – verwendet werden können, um Rückschlüsse auf den Dritten zu ziehen (EuGH, Urt. v. 04.10.2024 – C-21/23 –, juris, Rn. 88, 91). Das in Art. 9 Abs. 1 DS-GVO vorgesehene grundsätzliche Verbot gilt unabhängig davon, ob die durch die Verarbeitung offengelegte Information richtig ist oder nicht (EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 69).

Diesem Ergebnis lässt sich auch nicht entgegenhalten, der Trainingsdatensatz enthalte lediglich "auch" Daten im Sinne des Art. 9 Abs. 1 DS-GVO. Vielmehr hat der Europäische Gerichtshof in einer die Verfügungsbeklagte betreffenden Rechtssache (Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 89) anders entschieden:

"Wenn ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, Gegenstand solcher Vorgänge ist und insbesondere als Ganzes erhoben wird, ohne dass die Daten zum Zeitpunkt dieser Erhebung voneinander getrennt werden können, ist die Verarbeitung dieses Datensatzes aber als i.S.v. Art. 9 I DS-GVO untersagt anzusehen, sofern sie mindestens ein sensibles Datum umfasst und keine der in Art. 9 II DS-GVO genannten Ausnahmen greift."

bbb) Zwar kann sich die Verfügungsbeklagte jedenfalls nicht für sämtliche in Frage stehende Daten im Sinne des Art. 9 Abs. 1 DS-GVO auf den von ihr angeführten Ausnahmetatbestand des Art. 9 Abs. 2 lit. e) DS-GVO berufen.

Danach gilt das in Art. 9 Abs. 1 DS-GVO aufgestellte grundsätzliche Verbot jeder Verarbeitung besonderer Kategorien personenbezogener Daten nicht, wenn sich die Verarbeitung auf personenbezogene Daten bezieht, die "die betroffene Person offensichtlich öffentlich gemacht hat".

Nach allgemeinen Grundsätzen ist die Ausnahmevorschrift eng auszulegen (EuGH, Urt. v. 04.07.2023 – C-252/21 -, juris, Rn. 76 m.w.N.; EuGH, Urt. v. 04.10.2024 – C-446/21 -, Rn. 76). Insoweit ist entscheidend, ob die betroffene Person die Absicht hatte, die fraglichen personenbezogenen Daten ausdrücklich und durch eine eindeutige bestätigende Handlung der breiten Öffentlichkeit zugänglich zu machen (EuGH, Urt. v. 04.07.2023 – C-252/21 –, juris, Rn. 77; EuGH, Urt. v. 04.10.2024 – C-446/21 –, Rn. 76; Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679, Art. 9 Rn. 166 ff.).

Danach kann der Ausnahmebestand lediglich hinsichtlich solcher Daten bejaht werden, die ein Nutzer zur eigenen Person in sein öffentliches Nutzerkonto eines Social Media-Dienstes eingestellt bzw. in öffentlichen Postings mitgeteilt hat. Bei einer entsprechenden "öffentlichen" Einstellung von Daten in ein Nutzerkonto muss dem durchschnittlichen Nutzern bekannt sein, dass diese Daten von Jedermann zur Kenntnis genommen werden können und sogar mittels Suchmaschinen auffindbar sind. Insoweit wird aus der "öffentlichen" Einstellung solcher Informationen in ein Nutzerkonto die Absicht offensichtlich, solche Daten der breiten

Öffentlichkeit zugänglich zu machen (vgl. Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679, Art. 9 Rn. 169).

Im Hinblick durch von Nutzern geteilte Daten Dritter ist die Ausnahmeregel allerdings nicht anwendbar. Der Ausnahmeregelung liegt ein Verzicht auf den Schutz des Art. 9 Abs. 1 DS-GVO zugrunde (Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679, Art. 9 Rn. 165), über den jeder Betroffene nur für sich selbst entscheiden kann. Der Europäische Gerichtshof hat die Ausnahme "wohlgemerkt" auf Daten, die die betroffene Person selbst öffentlich gemacht hat, beschränkt (Urt. v. 04.07.2023 – C-252/21 -, juris, Rn. 75).

ccc) Auch soweit Daten Dritter betroffen sind, ist der vorliegende Fall nach Auffassung des Senats, dem im vorliegenden Eilverfahren nicht die Möglichkeit einer Vorlage an den Gerichtshof zur Verfügung steht, allerdings von dem Verarbeitungsverbot des Art. 9 Abs. 1 DS-GVO dennoch nicht erfasst. Der Senat geht vorbehaltlich einer im Hauptsacheverfahren zu prüfenden Vorlage an den Europäischen Gerichtshof davon aus, dass dieses Verbot im konkreten Fall einer "Aktivierung" durch einen Antrag des betroffenen Dritten auf Herausnahme seiner Daten aus dem veröffentlichten Beitrag beziehungsweise aus dem Trainingsdatensatz bedurft hätte.

Zwar hat der Gerichtshof einer in der Literatur (vgl. Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679 Rn. 26; Plath/Plath, DS-GVO, 2023, Art. 9 EUV 2016/679 Rn. 5, 10f) oftmals vertretenen teleologischen Reduktion des Art. 9 Abs. 1 DS-GVO in solchen Fällen, in denen der Zweck der Verarbeitung – wie hier – gerade nicht darin liegt, in identifizierender Weise "sensible" Informationen zu erlangen bzw. zu verarbeiten, eine Absage erteilt und entschieden, dass es gerade nicht darauf ankommt, ob der Verantwortliche mit dem Ziel handelt, Informationen zu erhalten, die unter eine der in dieser Bestimmung genannten besonderen Kategorien fallen (EuGH, Urt. v. 04.07.2023 – C-252/21 -, juris, Rn. 69; EuGH, Urt. v. 04.10.2024 – C-21/23 –, juris, Rn. 87).

Diese Absage an eine teleologische Reduktion des Art. 9 DS-GVO stellt das Verarbeitungsverbot in Art. 9 Abs. 1 DS-GVO aber nicht absolut. So ergibt sich aus der Entscheidung des Europäischen Gerichtshofs v. 24.09.2019 (C-136/17 –, juris, Rn. 45 ff.; vgl. insoweit auch Schlussanträge des Generalanwalts vom 10.01.2019, Rn. 56 f.) im Hinblick auf einen Suchmaschinenbetreiber, dass zwar tätigkeitsbezogene Besonderheiten des Betriebs einer Suchmaschine keine Freistellung rechtfertigen, die Vorgaben von Art. 9 Abs. 1 DS-GVO einzuhalten. Allerdings können sich diese Besonderheiten auf den Umfang der Verantwortlichkeit und der konkreten Verpflichtungen des Suchmaschinenbetreibers im Hinblick auf diese Bestimmungen auswirken. Für den Betreiber einer Suchmaschine folgt daraus, dass für Datenverarbeitungen im Rahmen der Suchmaschinentätigkeit das in Art. 9 DS-GVO vorgesehene Verbot nur nach einer Prüfung anwendbar ist, die erst auf der Grundlage eines Antrags der betroffenen Person unter der Aufsicht der zuständigen nationalen Behörden vorzunehmen ist.

Zudem lagen den Entscheidungen in den vorgenannten Sachen C-252/21 (EuGH, Urt. v. 04.07.2023, juris, Rn. 69) und C-21/23 (EuGH, Urt. v. 04.10.2024, juris, Rn. 87) deutlich andere Sachverhalte zugrunde als im Streitfall. Der Entscheidung in der Rechtssache C-252/21 lagen Fragen im Zusammenhang mit personalisierter Werbung zugrunde. Die Sache C-21/23 betraf den Umgang mit Nutzerdaten im Rahmen der Bestellung apothekenpflichtiger Medikamente bei einer Onlineplattform. Das hier in Frage stehende Training von KI ist damit nicht hinreichend vergleichbar. Der Europäische Gesetzgeber hat in der KI-VO – wie oben bereits dargelegt – das Ziel artikuliert, "bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren KI weltweit eine Führungsrolle einzunehmen" (ErwG 8 der KI-VO) und hierzu einen "einheitlichen Rechtsrahmen" für KI zu schaffen (ErwG 1 der KI-VO). Es steht außer Zweifel, dass eine solche Vorreiterrolle kaum zu erreichen ist, wenn im Geltungsbereich der DS-GVO ein Training von generativer KI mittels Massendaten unmöglich wäre. Dies wäre aber die Folge einer wörtlichen Anwendung des Art. 9 DS-GVO (kritisch zu einer weiten Auslegung etwa: Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679 Rn. 26 m.w.N.). Angesichts der Breite des Anwendungsbereichs des Art. 9 Abs. 1 DS-GVO ist es vernünftigerweise ausgeschlossen, dass große Datensätze solche Daten nicht enthalten. Eine Anonymisierung solcher Datensätze ist nicht praktikabel, eine Einwilligung der Betroffenen ist oftmals kaum mit zumutbarem Aufwand zu erlangen. Eine solche Auslegung würde auch der "Dualität" der Schutzzwecke der DS-GVO, die neben dem Schutz personenbezogener Daten auch dem Schutz des freien Verkehrs solcher Daten und damit ihrer Verwendbarkeit dient (Art. 1 Abs. 1 DS-GVO; Taeger/Gabel/Schmidt, DS-GVO, 2022, Art. 1 Rn. 1; Schwartmann u.a./Schwartmann/Jacquemain, DS-GVO, 2024, Art. 1 EUV 2016/679, Rn. 1), zuwiderlaufen.

In der KI-VO hat der europäische Gesetzgeber zudem in Kenntnis der Notwendigkeit des Trainings generativer KI mittels großer Massen an Daten (die Notwendigkeit des Trainings großer generativer KI-Modelle mit "riesigen Mengen an Text, Bildern, Videos und anderen Daten" ist im ErwG 105 der KI-VO ausdrücklich anerkannt) und in Kenntnis der seit längerem erfolgenden Nutzung von Webscraping zur Gewinnung von KI-Trainingsdaten, das stets die Gefahr der – unbeabsichtigten und nicht zielgerichteten – Verarbeitung von Daten im Sinne des Art. 9 DS-GVO birgt, Öffnungsregelungen, die ein Training von KI mit Massendaten erlauben, nicht getroffen. Dies lässt sich aus Sicht des Senats nicht anderes verstehen, als dass der Gesetzgeber nicht von einer entsprechenden Unmöglichkeit oder grundsätzlichen Rechtswidrigkeit ausgegangen ist. Eine Regelung, die ein solches Training ermöglicht, wäre in einem Gesetz, das der Erlangung einer "Vorreiterrolle" dient, sonst zwingend zu erwarten gewesen. Dass der Gesetzgeber der KI-VO die Einschränkungen durch die DS-GVO durchaus im Blick hatte, zeigt die (gem. Art. 113 KI-VO ab dem 02.08.2026 geltenden) Ausnahmeregelung des Art. 10 Abs. 5 der KI-VO, die eine Rechtsgrundlage für den zielgerichteten Einsatz von Daten im Sinne des Art. 9 DS-GVO beim Training von Hochrisiko-KI schafft (vgl. ErwG 70 der KI-VO; Schwartmann/Schwartmann/Keber/Köhler/Nägele, KI-VO – Leitfaden, 2024, 2. Teil 1. Kapitel Rn. 305; Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679, Rn. 185). Ferner ergibt sich dies aus den Regelungen für den Einsatz biometrischer Daten im Sinne

des Art. 9 Abs. 1 DS-GVO (vgl. Erwägungsgründe 30 ff. der KI-VO). Für die nicht zielgerichtete Verarbeitung solcher Daten beim Training von KI hat der europäische Gesetzgeber hingegen keinen Regelungsbedarf gesehen.

Im Hinblick auf die Rechtsprechung des Europäischen Gerichtshofs in der Sache C-136/17 (Urt. v. 24.09.2019) geht der Senat insoweit für das Training einer KI von einer tätigkeitsbezogenen Reduktion der Unterlassungspflicht der Verfügungsbeklagten dahin aus, dass diese jedenfalls dann, wenn die Verarbeitung nicht zielgerichtet erfolgt, einer näheren Konkretisierung durch einen Antrag des Betroffenen auf Herausnahme seines Datensatzes bedarf. Dabei verkennt der Senat auch insoweit nicht, dass eine spätere Löschung der Daten aus der KI nur eingeschränkt möglich ist. Angesichts der festgestellten nur geringen Gefahren einer konkreten Schädigung der Betroffenen durch die weitere Verarbeitung der bereits öffentlichen Daten sieht der Senat einen entsprechenden Willen des europäischen Gesetzgebers insgesamt dennoch hinreichend klar artikuliert. Auch der Stellungnahme des Ausschusses vom 17.12.2025 lassen sich keine gegenteiligen Ausführungen entnehmen. Zwar wird dort auf die grundsätzliche Untersagung der Verarbeitung von Daten nach Art. 9 Abs. 1 DS-GVO und auf die Auslegungsgrundsätze aus der Kartellamts-Entscheidung des Europäischen Gerichtshofs vom 04.07.2023 (C-252/21) verwiesen (Stellungnahme, Rn. 17). Eine nähere Untersuchung hat der Ausschuss aber ausdrücklich nicht vorgenommen.

Die Voraussetzung der nicht zielgerichteten Verarbeitung der Daten ist aufgrund des hierauf nicht gerichteten Ziels des KI-Trainings, das allgemeine Muster für Wahrscheinlichkeitsberechnungen und keine Profilbildung zu einzelnen Personen schaffen soll, sowie durch die zahlreichen entsprechenden Schutzmaßnahmen der Verfügungsbeklagten hinreichend dargelegt.

Ein Verarbeitungsverbot besteht damit nicht, der auch für die Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DS-GVO erforderliche (vgl. Schwartmann u.a./Jaspers/Schwartmann/Mühlenbeck, DS-GVO, 2024, Art. 9 EUV 2016/679, Art. 9 Rn. 165; Franke, RDi 2023, 565, 568) Erlaubnistatbestand nach Art. 6 Abs. 1 lit. f) DS-GVO ist – wie dargelegt – erfüllt.

Ausschluss des Auskunftsanspruchs bei Videoüberwachung

(OVG Berlin-Brandenburg, Urteil vom 13. Mai 2025 – 12 B 14/23 –)

1. **Der Anspruch auf Herausgabe einer Kopie nach Art. 15 Abs. 3 DS-GVO (juris: EUV 2016/679) ist gemäß Art. 11 Abs. 2 i.V.m. Art. 12 Abs. 2 S. 2 DS-GVO (juris: EUV 2016/679) ausgeschlossen, sofern mit der Identifizierung des Auskunftsuchenden ein unzumutbarer Aufwand für den Verantwortlichen verbunden ist. Dieser kann auch aus den Vorkehrungen eines kohärenten und den Zielen der DS-GVO (juris: EUV 2016/679) Rechnung tragenden Datenschutzkonzepts herrühren. (Rn. 47 und 53)**

2. **Die Freiheiten und Rechte anderer Personen – inklusive des Verantwortlichen – können gemäß Art. 15 Abs. 4 DS-GVO (juris: EUV 2016/679) zum Ausschluss des Herausgabeanspruchs nach Art. 15 Abs. 3 DS-GVO (juris: EUV 2016/679) führen, sofern die anzustellende Güterabwägung ein außergewöhnliches Missverhältnis zwischen den Folgen einer Auskunftserteilung und dem Informationsinteresse des Auskunftssuchenden im jeweiligen Einzelfall ergibt. (Rn. 59)**

Aus den Gründen:

A. Soweit die Klägerin ihre Anschlussberufung zurückgenommen hat, ist das Berufungsverfahren in entsprechender Anwendung von § 92 Abs. 3 S. 1 VwGO einzustellen. […]

II. Die Anfechtungsklage gegen den Bescheid vom 21.12.2021 ist auch begründet, da die darin ausgesprochene Verwarnung der Klägerin rechtswidrig ist. […]

3. Der Bescheid ist jedoch materiell rechtswidrig. Die Klägerin hat den Auskunftsanspruch des Beigeladenen aus Art. 15 DS-GVO nicht verletzt, so dass die Tatbestandsvoraussetzungen für den Erlass einer Verwarnung nach Art. 58 Abs. 2 lit. b) DS-GVO nicht erfüllt waren. […]

a) Der Anwendungsbereich der Datenschutz-Grundverordnung ist eröffnet.

Diese gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO), sofern keine Bereichsausnahme nach Art. 2 Abs. 2 DS-GVO vorliegt.

Die Videoaufnahmen aus den Zügen der Klägerin sind als personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO einzuordnen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Identifizierbar ist eine natürliche Person, 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 (Art. 4 Nr. 1 DS-GVO). […]

bb) Letztlich kommt es auf die Frage der Identifizierbarkeit durch die Klägerin selbst aber nicht an. Denn es handelt sich bei den Videoaufnahmen in den Zügen der Klägerin jedenfalls infolge der möglichen Identifizierung durch Dritte in Gestalt der Strafverfolgungsbehörden um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DS-GVO – unabhängig davon, ob man für die Zurechnung von deren Erkenntnismitteln einen absoluten (vgl. (1)) oder relativen Ansatz (vgl. (2)) verfolgt. […]

c) Der Anspruch des Beigeladenen auf Herausgabe der Videoaufnahmen ist jedoch gemäß Art. 11 Abs. 2 i.V.m. Art. 12 Abs. 2 S. 2 DS-GVO ausgeschlossen.

Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren (Art. 11 Abs. 1 DS-GVO). Kann der Verantwortliche in diesen Fällen nachweisen, dass

er nicht in der Lage ist, die betroffene Person zu identifizieren, so unterrichtet er diese hierüber, sofern möglich (Art. 11 Abs. 2 S. 1 DS-GVO). In diesen Fällen finden die Art. 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen (Art. 11 Abs. 2 S. 2 DS-GVO). Der Verantwortliche darf die Auskunft verweigern, wenn er glaubhaft macht, dass er – weiterhin – nicht in der Lage ist, die betroffene Person zu identifizieren (Art. 12 Abs. 2 S. 2 DS-GVO). Diese Voraussetzungen sind vorliegend erfüllt.

aa) Die Videoüberwachung in der S-Bahn unterfällt dem Anwendungsbereich des Art. 11 Abs. 1 DS-GVO. Die Klägerin verarbeitet durch die Aufnahmen personenbezogene Daten (vgl. a)), ohne dass es ihr – vorbehaltlich konkreter Anhaltspunkte für strafrechtlich relevante Vorgänge – auf die Identifizierung der aufgezeichneten Personen ankäme. Solche Datenverarbeitungen ohne gezielten Personenbezug erfasst Art. 11 Abs. 1 DS-GVO (vgl. zur Videoüberwachung als Anwendungsfall des Art. 11 Abs. 1 DS-GVO EDPB, Leitlinien zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1 [28.03.2023], Rn. 61; Klabunde, in: Ehmann/Selmayr, DS-GVO, 3. Aufl. 2024, Art. 11 Rn. 24; Plath, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 11 DS-GVO Rn. 17).

bb) Die Klägerin hat nachgewiesen, dass sie „nicht in der Lage ist", den Beigeladenen auf den begehrten Videoaufzeichnungen zu identifizieren (vgl. Art. 11 Abs. 2 S. 1 DS-GVO). Sofern Art. 12 Abs. 2 S. 2 DS-GVO eine „Glaubhaftmachung" voraussetzt, ist damit jedenfalls kein strengerer Maßstab für die Darlegung der Nicht-Identifizierbarkeit als mit dem Erfordernis des „Nachweises" in Art. 11 Abs. 2 DS-GVO verbunden (vgl. zum Verhältnis der Normen Veil, in: Gierschmann, DS-GVO, 2018, Art. 11 Rn. 54 ff.; Paal/Pauly/Paal/Hennemann, DS-GVO/BDSG, 3. Aufl. 2021, Art. 12 DS-GVO Rn. 48 ff.; Simitis/Hornung/Spiecker gen. Döhmann/Dix, DatenschutzR, 2. Aufl. 2025, Art. 12 DS-GVO Rn. 24).

(1) Dabei ist für die Identifizierbarkeit im Rahmen des Art. 11 Abs. 2 DS-GVO – anders als bei der Frage, ob überhaupt personenbezogene Daten gemäß Art. 4 Nr. 1 DS-GVO vorliegen (vgl. a)) – allein auf den Organisationskreis des Verantwortlichen abzustellen (vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, 3. Aufl. 2024, Art. 15 DS-GVO Rn. 65; Spiecker gen. Döhmann u.a./Carmichael u.a., General Data Protection Regulation, 1. Aufl. 2023, Art. 11 DS-GVO Rn. 7; Simitis/Hornung/Spiecker gen. Döhmann/Hansen, DatenschutzR, 2. Aufl. 2025, Art. 11 DS-GVO Rn. 34). Art. 11 Abs. 1 DS-GVO betrifft Fälle, in denen zwar der objektive Personenbezug besteht – ansonsten wäre der Anwendungsbereich der Datenschutz-Grundverordnung schon nicht eröffnet (vgl. Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 DS-GVO; Gierschmann/Veil, DS-GVO, 2018, Art. 11 Rn. 45) –, der Verantwortliche aber subjektiv auf den Personenbezug verzichtet, ihn also mit den ihm unmittelbar zur Verfügung stehenden Mitteln nicht selbst herstellen kann (vgl. Gola/Heckmann/Gola, DS-GVO/BDSG, 3. Aufl. 2022, Art. 11 DS-GVO Rn. 1, 5; Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, 3. Aufl. 2024, Art. 15 DS-GVO Rn. 65). Insbesondere die Möglichkeiten der Strafverfolgungsbehörden finden daher i.R.d. Art. 11 DS-GVO keine Berücksichtigung, da die Klägerin hierauf nicht für Zwecke der Erfüllung von Auskunftsansprüchen zurückzugreifen vermag.

Für die Frage der Identifizierbarkeit gemäß Art. 11 Abs. 2 S. 1 DS-GVO kommt es nicht darauf an, welche Maßnahmen die Klägerin theoretisch – im Sinne einer faktischen Realisierbarkeit – hätte ergreifen können, um den Beigeladenen auf den Videoaufnahmen ausfindig zu machen. Vielmehr ist darauf abzustellen, welcher Identifizierungsaufwand dem Verantwortlichen im Einzelfall zumutbar ist (vgl. zur Zumutbarkeitsschwelle i.R.v. Art. 11 Abs. 2 DS-GVO: EDPB, Leitlinien zu den Rechten der betroffenen Person – Auskunftsrecht, Version 2.1 [28.03.2023], Rn. 61; Plath, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 11 DS-GVO Rn. 9: Plath/Kamlah, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 15 DS-GVO Rn. 19; Kühling/Buchner/Weichert, DS-GVO/BDSG, 4. Aufl. 2024, Art. 11 DS-GVO Rn. 13; Spiecker gen. Döhmann u.a./Carmichael u.a., General Data Protection Regulation, 1. Aufl. 2023, Art. 11 DS-GVO Rn. 20; Taeger/Gabel/Lee-Wunderlich, DS-GVO/BDSG/TTDSG, 4. Aufl. 2022, Art. 11 DS-GVO Rn. 14; Schaffland/Wiltfang/Schaffland/Holthaus, DS-GVO/BDSG [Oktober 2024], Art. 11 DS-GVO Rn. 1a; Steinrötter, in: BeckOK/IT-Recht [1.1.2023] Art. 12 DS-GVO Rn. 27). Die Datenschutz-Grundverordnung bringt verschiedentlich zum Ausdruck, dass im Rahmen von Art. 11 Abs. 2 DS-GVO eine solche wertende Verhältnismäßigkeit anstelle einer reinen Machbarkeitsbetrachtung anzustellen ist. Bereits Art. 11 Abs. 1 DS-GVO, der die Konfliktlage zwischen Betroffenenrechten und Datensparsamkeit dahingehend auflöst, dass bei fehlender Erforderlichkeit der Identifizierung der betroffenen Person durch den Verantwortlichen grundsätzlich auf zusätzliche Datenerhebungen allein zum Zweck der Erfüllung eines Auskunftsanspruchs zu verzichten ist, spricht dagegen, dass der Verantwortliche alle denkbaren Maßnahmen zur Identifizierung ohne Rücksicht auf den damit verbundenen Aufwand und Nutzen ergreifen muss. Die Ausübung der Rechte zum Schutz personenbezogener Daten steht zudem generell unter einem Verhältnismäßigkeitsvorbehalt (vgl. ErwG Nr. 4 DS-GVO). Eine Begrenzung auf „vertretbare" Mittel zur Identifizierung (vgl. ErwG Nr. 64 DS-GVO) erscheint auch insofern sachgerecht, als auf diesem Wege Wertungswidersprüche zu den Maßstäben für die Herstellung des Personenbezugs im Rahmen von Art. 4 Nr. 1 DS-GVO vermieden werden (parallele Maßstäbe ansetzend Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Schneider, DS-GVO/BDSG, 3. Aufl. 2024, Art. 12 Rn. 46 f.): Denn für die Frage der Anwendbarkeit der Datenschutz-Grundverordnung erkennt der Europäische Gerichtshof an, dass es nur auf die „nach allgemeinem Ermessen" und „vernünftigerweise" – nicht aber alle hypothetisch einsetzbaren – Mittel ankommt (vgl. a); s. auch ErwG Nr. 26 DS-GVO). Auch der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO) spricht gegen eine Pflicht, die Datenverarbeitung so zu organisieren, dass eine Verknüpfung zwischen den erhobenen Daten und den jeweiligen Betroffenen allein für Zwecke der Auskunftserteilung nach Art. 15 Abs. 3 DS-GVO hergestellt werden kann oder aufrecht erhalten bleibt. Vielmehr dürfte es gerade im Interesse der Betroffenen sein, dass Zugriffs- und Identifizierungsmöglichkeiten des Verantwortlichen beschränkt sind und bleiben (vgl. Kühling/Buchner/Weichert, DS-GVO/BDSG, 4. Aufl. 2024, Art. 11 DS-GVO Rn. 1b; Sydow/Marsch/Greve, DS-GVO/BDSG, 3. Aufl. 2022, Art. 12 DS-GVO Rn. 23; Spiecker

gen. Döhmann u.a./Carmichael u.a., General Data Protection Regulation, 1. Aufl. 2023, Art. 11 DS-GVO Rn. 15; in diese Richtung auch Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, 3. Aufl. 2024, Art. 15 DS-GVO Rn. 65). Kein Verantwortlicher sollte dazu gezwungen sein, deutlich gefährdungsträchtigere Verfahren im Umgang mit personenbezogenen Daten anzuwenden, nur um Auskunftsersuchen erfüllen zu können (vgl. Britz/Breyer, VersR 2020, 65 [69]). Sofern Beklagte und Beigeladener unter Bezug auf die Maßgaben zur Erleichterung der Wahrnehmung der Betroffenenrechte in Art. 12 Abs. 2 S. 1 und Art. 25 Abs. 1 DS-GVO eine Pflicht des Verantwortlichen annehmen wollen, seine Datenverarbeitung unter Einsatz entsprechender Ressourcen so zu organisieren, dass sie die umfassende, unkomplizierte und fristgerechte Auskunftserteilung ermöglicht, verfangen diese Einwände nicht für die der eigentlichen Auskunft vorgelagerte Frage der Identifizierbarkeit im Rahmen des Art. 11 Abs. 2 DS-GVO. Dies erkennt auch Art. 25 Abs. 1 DS-GVO insofern an, als er eine den Grundsätzen der Datenminimierung Rechnung tragende organisatorische und technische Ausgestaltung der Datenschutzmechanismen einfordert (vgl. Art. 5 Abs. 1 lit. c) DS-GVO). Eine solche kann dazu führen, dass die Identifizierbarkeit von Betroffenen nicht mehr mit verhältnismäßigem Aufwand möglich und damit ihr Auskunftsrecht eingeschränkt wird, ohne dass hierin ein datenschutzrechtlicher Verstoß zu erblicken wäre, wie Art. 11 Abs. 2 S. 2 i.V.m. Art. 12 Abs 2 S. 2 DS-GVO klarstellen. Auch der Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 lit. e DS-GVO, wonach Daten in einer Form gespeichert werden müssen, „die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist", weist darauf hin, dass Datenschutzkonzepte dem Erforderlichkeitsprinzip unterliegen und nicht darauf ausgelegt sein müssen, binnen der Speicherfrist angebrachten Auskunftsersuchen trotz fehlender Identifizierbarkeit ohne Weiteres Rechnung tragen zu können.

(2) Auf Basis dieser Maßstäbe steht das Datenschutzkonzept der Klägerin für den Umgang mit den Videoaufnahmen aus der S-Bahn der zumutbaren Identifizierbarkeit des Beigeladenen gemäß Art. 11 Abs. 2 S. 1 i.V.m. Art. 12 Abs. 2 S. 2 DS-GVO entgegen.

Die Klägerin vermag als Folge ihres Datenschutzkonzepts keine Einsicht in die Videoaufzeichnungen zu nehmen. Zu einer Abkehr von ihrer Datenschutzpraxis zur Identifizierung des Beigeladenen war sie nicht verpflichtet. Das mit der Beklagten abgestimmte Datenschutzsystem der Klägerin, das auch Gegenstand der durch die Länder Berlin und Brandenburg ausgeschriebenen Verkehrsverträge war, ist nicht Ausdruck unzureichender Organisation oder verfolgt das Ziel, Auskunftsansprüche leerlaufen zu lassen. Es sichert vielmehr gerade ein hohes Datenschutzniveau, indem es den Wertungen der Datenschutz-Grundverordnung sowie den Rechten und Freiheiten der von der Datenverarbeitung betroffenen Personen Rechnung trägt. Die dezentrale Speicherung der Aufnahmen, die Sicherung der Datenträger gegen unbefugte Entnahme, der mehrstufige Prozess zur Auslese der Datenträger an einem speziell geschützten Arbeitsplatz, die Autorisierung nur weniger Personen zur Bearbeitung der Daten sowie deren limitierte Zugriffsrechte ohne die Möglichkeit der Einsichtnahme, die eng begrenzte Speicherdauer und die Auswertung allein auf Anforderung der Strafverfolgungsbehörden bilden zentrale Bestandteile des Datenschutzkonzepts. Dieses minimiert die Eingriffe und Gefährdungen im Hinblick auf die personenbezogenen Daten der Beschäftigten der Klägerin und ihrer täglich hunderttausenden Kunden.

Während die zeitlich, technisch, personell und organisatorisch komplexe physische Entnahme der Datenträger (aus dem sich im Betrieb befindenden Zug) und die Extrahierung der relevanten Videosequenz bei Auskunftsanfragen Betroffener nach Art. 15 DS-GVO den Arbeitsschritten im Rahmen der Bereitstellung von Videoaufnahmen für die Strafverfolgungsbehörden entspricht und damit „nur" zusätzlichen – wenn auch durchaus beachtlichen – Aufwand bedeutete, hätte die Identifizierung des Beigeladenen vorausgesetzt, dass die Klägerin dieses kohärente und datenschutzrechtlichen Grundprinzipien Rechnung tragende Konzept in seinen wesentlichen Bestandteilen aufgibt und die eigenen Identifizierungsmöglichkeiten erheblich erweitert. Dies würde die Ziele der Datenschutz-Grundverordnung konterkarieren, denn Resultat wäre eine deutliche Absenkung des Datenschutzniveaus und eine gewichtige Zunahme umfangreicher und sensibler Datenverarbeitungsprozesse: Da die Einsichtnahme und Auswertung nicht mehr nur durch die Strafverfolgungsbehörden, sondern auch seitens der Klägerin selbst erfolgen müsste, hätte sie die technischen Voraussetzungen hierfür schaffen müssen, da es die Konfiguration der Software derzeit weder ihr noch dem beauftragten Dienstleister erlaubt, die verschlüsselten Videosequenzen zu betrachten (vgl. § 4 Abs. 8 S. 2 BetrV). Zudem wären weitere personelle Kapazitäten erforderlich, da das Personal des Drittanbieters bisher nur für die die Extrahierung betroffener Sequenzen bei Anfragen der Strafverfolgungsbehörden beauftragt ist (vgl. §§ 3, 6 Abs. 2 BetrV). Ferner wären umfangreiche Änderungen der Betriebsvereinbarung erforderlich gewesen, die eine Entnahme und Auswertung der Videoaufnahmen derzeit nur auf Anfrage der Strafverfolgungsbehörden zulässt. Auch wenn die Maßgaben der Betriebsvereinbarung nicht unmittelbar den Rechten des Beigeladenen entgegengehalten werden können, ist deren Abschluss zum Schutz der personenbezogenen Daten im Beschäftigungskontext ausdrücklich anerkannt (vgl. Art. 88 Abs. 1 DS-GVO, ErwG Nr. 155 DS-GVO) und der rechtliche Anpassungsbedarf für die Frage der zumutbaren Identifizierungsmaßnahmen ebenfalls zu berücksichtigen. Indem ein Zug mit 40 Videokameras ausgestattet ist, wäre zur Identifikation des Beigeladenen auf Basis seiner Angaben sodann – jedenfalls potenziell – die Durchsicht zahlreicher Aufnahmen sowie ggf. der Einsatz einer Gesichtserkennungssoftware erforderlich gewesen (deren Einsatz § 9 Abs. 1 BetrV ebenfalls untersagt). Mit diesen Maßnahmen wäre zudem zwingend eine längere Speicherung der Aufnahmen einhergegangen, obwohl deren automatische Löschung im Ringspeicherverfahren nach 48 Stunden gerade den Empfehlungen der europäischen Datenaufsicht (EDPB, Leitlinien zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0 [29.01.2020], Rn. 121; so auch DSK, Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung, S. 3), den Maßgaben in § 20 Abs. 4 S. 2 BlnDSG sowie der Abstimmung des Datenschutzkonzepts zwischen der Klägerin und der Beklagten entspricht.

Diese umfangreiche Durchsicht und Analyse – nicht mehr nur durch die Strafverfolgungsbehörden und in eng umgrenzten Ausnahmefällen –, die Abkehr von den Schutzmechanismen des bestehenden Konzepts sowie die längere Speicherung der personenbezogenen Daten zur Identifizierung des Beigeladenen – mit im Übrigen ungewissen Erfolgsaussichten seiner Identifizierung – widerspräche nicht nur den Grundsätzen der Datensparsamkeit und -minimierung (vgl. Art. 5 Abs. 1 lit. c) und e) DS-GVO), sondern ginge auch mit gewichtigen Eingriffen in die Grundrechte der weiteren Fahrgäste einher (vgl. Art. 7, Art. 8 GrCh), die durch Verpixelung oder anderweitige Unkenntlichmachung zwar gemildert, aber nicht vermieden werden können. Der Sinn und Zweck von Art. 11 Abs. 1 DS-GVO besteht aber gerade darin, solche datenschutzrechtlich negativen Implikationen einer aus Sicht des Verantwortlichen gar nicht erforderlichen Identifikation nur zum Zweck der Erfüllung des Auskunftsrechts aus Art. 15 Abs. 3 DS-GVO zu verhindern. Indem Art. 11 DS-GVO anerkennt, dass Verantwortliche ihr Datenschutzsystem so organisieren, dass es als Folge hoher Datenschutzstandards der Identifizierung Betroffener entgegensteht (vgl. oben), kommt es für das Auskunftsbegehren des Beigeladenen nicht darauf an, dass die Klägerin theoretisch die Möglichkeit gehabt hätte, die Datenverarbeitung anders zu gestalten, z.B. durch eine zentrale Speicherung der Videoaufnahmen mit jederzeitiger Einsichtnahmemöglichkeit (vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, 3. Aufl. 2024, Art. 15 DS-GVO Rn. 65).

Auch wenn der Auskunftsanspruch des Art. 15 DS-GVO nicht davon abhängig ist, dass mit seiner Ausübung bestimmte Zwecke verfolgt werden (vgl. EuGH, Urt. v. 26.10.2023 – C-307/22 –, juris Rn. 52; Schemmer, ZGI 2024, 205 [206]), bietet die Frage der Zumutbarkeit von Identifizierungsmaßnahmen i.R.d. Art. 11 Abs. 2 S. 1 DS-GVO Raum für eine Abwägung von Aufwand und Folgen einer Identifizierung mit den Informationsbelangen des Auskunftssuchenden. Danach ist das Transparenzinteresse des Beigeladenen vorliegend als äußerst gering einzuordnen. Der Beigeladene war sich der Datenverarbeitung bereits im Moment seiner Zugfahrt am 6. Oktober 2020 bewusst, wie sein Auskunftsantrag unmittelbar nach Fahrtende belegt. Die Klägerin hat dargelegt, dass die Kameras und die Hinweise auf die Videoüberwachung in ihren Zügen gut sichtbar angebracht sind (vgl. Anlage K 5; „Regionales Betreiberkonzept Videoaufzeichnung", S. 8 und Anlage 4). Sein Antrag diente nach eigenen Angaben auch nicht dazu, Art, Umfang, Richtigkeit oder Vollständigkeit einer Datenverarbeitung zu klären, um ihre Rechtmäßigkeit überprüfen zu können (vgl. ErwG Nr. 63 S. 1 DS-GVO), sondern erfolgte zunächst ohne spezifischen Anlass. Es ist auch nicht erkennbar, dass die Herausgabe der Aufnahme erforderlich gewesen wäre, um sein Recht auf Berichtigung, Löschung („Recht auf Vergessenwerden"), Einschränkung der Verarbeitung sowie Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten auszuüben (vgl. Art. 16-18, 21 DS-GVO; zu diesen Zwecken des Auskunftsrechts EuGH, Urt. v. 04.05.2023 – C-487/21 –, juris Rn. 35; Urt. v. 12.01.2023 – C-154/21 –, juris Rn. 37 f.). Sofern der Beigeladene angibt, mittlerweile an den – auch nach der umfänglich erfolgten Auskunft nach Art. 15 Abs. 1 DS-GVO noch offenen – Details zur Art der Datenverarbeitung (z.B. Winkel und Auflösung der Aufnahmen) interessiert zu sein, bleibt unklar, inwiefern diese Angaben für die Verwirklichung seiner Rechte und Freiheiten von Belang sind. Dies gilt insbesondere deshalb, da nach dem Datenschutzkonzept der Klägerin grundsätzlich keinerlei Einsicht in diese Aufnahmen stattfinden und deren Löschung nach 48 Stunden erfolgen wird, so dass der Beigeladene – unabhängig von der Höhe der Auflösung der Videoaufzeichnungen – keine Auswertung seiner Daten durch den Verantwortlichen oder Dritte fürchten muss. Sollte der Beigeladene wiederum möglicherweise auf einer von den Strafverfolgungsbehörden angefragten Aufzeichnung zu sehen sein, wäre er hierüber nach Art. 15 Abs. 1 lit. c) DS-GVO zu informieren gewesen und weitere Auskünfte (ggf. auch nach Art. 15 Abs. 3 DS-GVO) wären – ohne Entwertung des Datenschutzkonzepts und den damit einhergehenden gewichtigen Bedenken – möglich gewesen. Zudem stellt die Datenverarbeitung im Anwendungsbereich des Art. 11 DS-GVO infolge der nur abstrakten Personenbeziehbarkeit bei fehlender Erforderlichkeit einer konkreten Identifizierung durch den Verantwortlichen schon grundsätzlich nur einen geringen Eingriff in die Rechte der Betroffenen dar (vgl. Steiger, ZD 2024, 143 [144]). Der Verordnungsgeber hat anerkannt, dass diesen Daten nur ein geringes Gefährdungspotenzial innewohnt und der Betroffene weniger schutzbedürftig ist. Die Belange des Beigeladenen rechtfertigen daher nicht die gewichtigen Bedenken begegnende und erheblichen Aufwand hervorrufende Aufgabe des Datenschutzkonzepts der Klägerin. Dies führt zur Annahme der Unzumutbarkeit seiner Identifizierung gemäß Art. 11 Abs. 2 S. 1 DS-GVO.

cc) Indem die Klägerin nicht zur Identifizierung des Beigeladenen in der Lage war, scheidet dessen Anspruch auf Herausgabe der begehrten Videoaufzeichnungen nach Art. 15 Abs. 3 DS-GVO aus (vgl. Art. 11 Abs. 2 S. 2 i.V.m. Art. 12 Abs. 2 S. 2 DS-GVO). Sofern die Beklagte dem entgegenhält, dass dieser Anspruchsausschluss eine „Unterrichtung" gemäß Art. 11 Abs. 2 S. 1 DS-GVO und die Anforderung weiterer Informationen durch die Klägerin vorausgesetzt hätte, dringt sie hiermit nicht durch. Der Zweck der Unterrichtungspflicht besteht darin, der betroffenen Person die Entscheidung darüber zu ermöglichen, ob sie durch die Zulieferung weiterer Daten doch eine Identifizierung ermöglichen möchte (vgl. Plath, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 11 DS-GVO Rn. 14). Die fehlende Identifizierbarkeit des Beigeladenen beruht vorliegend jedoch nicht auf unzureichenden Angaben seinerseits, sondern der konkreten Ausgestaltung des Datenschutzkonzepts der Klägerin. Der Beigeladene hätte die Klägerin folglich nicht durch sein Zutun in die Lage versetzen können, doch einen Personenbezug mit zumutbaren Mitteln herzustellen (vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Klein/Peisker, DS-GVO/BDSG, 3. Aufl. 2024, Art. 15 DS-GVO Rn. 66 zu Fallgruppen, in denen zusätzliche Angaben eine Identifizierung des Betroffenen infolge fehlender Voraussetzungen beim Verantwortlichen nicht ermöglichen). Hierüber hat die Klägerin den Beigeladenen mit E-Mail vom 6. Oktober 2020 und Schreiben vom 22.10.2020 unterrichtet. [...]

Zulässigkeit einer Verarbeitung von Kundendaten zur Rückgewinnung nach Vertragsende

(VG Bremen, Urteil vom 23. April 2025 – 4 K 2873/23 –)

1. **[...]**
2. **Die nachvertragliche Werbung in Form von Haustürbesuchen kann ein berechtigtes Interesse darstellen. Sie verstößt nicht gegen die Rechtsordnung, sondern wird von dieser im Rahmen des § 7 Abs. 1 S. 1 UWG gebilligt. Insbesondere kann eine Kündigung allein nicht bewirken, dass für den Werbenden ersichtlich ist, dass weitere Werbung unerwünscht ist. Insoweit muss hinzukommen, dass der Empfänger seinen entgegenstehenden Willen geäußert hat.**

Aus den Gründen:

bb) Die Daten sind auf rechtmäßige Weise verarbeitet worden, vgl. Art. 5 Abs. 1 lit. a) 1. Alt. DS-GVO. Es ist als Beurteilungszeitpunkt auf den Zeitpunkt der letzten behördlichen Entscheidung abzustellen (1). Die Klägerin kann die Verarbeitung zu Werbezwecken in Form von Haustürwerbung auf Art. 6 Abs. 1 lit. f) i.V.m. Abs. 4 DS-GVO stützen. Der verfolgte Sekundärzweck ist mit dem Primärzweck, zu dem die Daten ursprünglich erhoben wurden, gem. Art. 6 Abs. 4 DS-GVO vereinbar (2). Bezüglich der Verarbeitung zu Werbezwecken in Form des Postversands handelt es sich um einen Primärzweck gem. Art. 6 Abs. 1 lit. f) DS-GVO (3). Weiter sind die Voraussetzungen des Art. 6 Abs. 1 lit. f) DS-GVO (und für die Haustürwerbung i.V.m. Art. 6 Abs. 4 DS-GVO) erfüllt (4). [...]

(2) Es handelt sich zur Überzeugung der Kammer bei der Verarbeitung zu Werbezwecken in Form von Haustürwerbung um eine Verarbeitung zu einem Sekundärzweck gem. Art. 6 Abs. 1 lit. f) i.V.m. Abs. 4 DS-GVO. Dies gilt sowohl für Verträge, die ab dem 25.05.2018 abgeschlossen wurden (a) als auch für Verträge, die davor abgeschlossen wurden (b). Der verfolgte Sekundärzweck ist mit dem Primärzweck, zu dem die Daten ursprünglich erhoben wurden, gem. Art. 6 Abs. 4 DS-GVO vereinbar (c).

Zur Überzeugung der Kammer handelt es sich bei Art. 6 Abs. 4 DS-GVO um eine Auslegungsregel für die Ermächtigungsgrundlagen des Art. 6 Abs. 1 DS-GVO. Art. 6 Abs. 4 DS-GVO stellt keine eigene Ermächtigungsgrundlage dar. Die Regelungssystematik und der Wortlaut des Art. 6 Abs. 4 DS-GVO sprechen dafür, dass allein der Kompatibilitätstest des Abs. 4 eine zweckändernde Datenverarbeitung noch nicht zu einer rechtmäßigen Verarbeitung machen kann. Nach Art. 6 Abs. 1 DS-GVO ist eine Datenverarbeitung nur rechtmäßig, wenn mindestens eine der Bedingungen nach Abs. 1 lit. a)-f) erfüllt ist; einen Vorbehalt hinsichtlich Art. 6 Abs. 4 DS-GVO macht Art. 6 Abs. 1 DS-GVO nicht. Art. 6 Abs. 4 DS-GVO bezieht sich lediglich auf die Vorgabe der Zweckbindung einer Datenverarbeitung nach Art. 5 Abs. 1 lit. b) DS-GVO (Kühling/Buchner/Buchner/Petri, DS-GVO, 4. Aufl. 2024, Art. 6, Rn. 183; in die Richtung auch: EuGH, Urt. v. 20.10.2022 – C-77/21, GRUR-RS 2022, 28068, Rn. 34). [...]

(a) Bei der Verarbeitung von Verträgen, die ab dem 25.05.2018 bis zum Erlass des Bescheides abgeschlossen wurden, handelt es sich zur Überzeugung des Gerichts in Bezug auf die nachvertragliche Haustürwerbung um eine Verarbeitung zu einem Sekundärzweck.

Zur Überzeugung des Gerichts sind die vom EuGH aufgestellten Voraussetzungen, dass über ein berechtigtes Interesse bereits bei Vertragsschluss ausreichend nach Art. 13 Abs. 1 lit. d) DS-GVO informiert werden muss (vgl. EuGH, Urt. v. 09.01.2025 – C-394/23, juris, Rn. 46) in Bezug auf die nachvertragliche Haustürwerbung nicht eingehalten. Denn im Zusammenhang mit dem Begriff des berechtigten Interesses wurde nicht ausreichend auf Haustürwerbung eingegangen. Die allgemeinen Datenschutzinformationen der Klägerin im Stand vom 01.09.2020 und 25.05.2018 führen dazu zunächst unter Ziffer 1. des Punktes „D. Datenverarbeitung aufgrund unserer berechtigten Interessen (Art. 6 Abs. 1 lit. f) DS-GVO)“ aus, dass die Klägerin personenbezogenen Daten auch zur Werbung mit weiteren Produkten und Dienstleistungen nutzt. Dabei ist der Kommunikationskanal allerdings ausdrücklich auf den Postweg begrenzt. Dem ergänzend folgt unter der Überschrift „E. Datennutzung aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO)“ die Erklärung, dass, vorbehaltlich des Postversandes, eine werbliche Kontaktaufnahme nur über die vom Kunden eingewilligten Kanäle vorgenommen wird. Als Zweck der Datenverarbeitung wird dabei unter anderem benannt, dass im Falle des Vertragsendes eine Kontaktaufnahme mit Werbung erfolgt. Dies bezog sich nach den nachvollziehbaren Ausführungen der Klägerin in der mündlichen Verhandlung aber lediglich auf ein Opt-In-Verfahren“, nicht auf die hier streitgegenständlichen Werbekanäle. Dem schließt sich die Kammer an, da der Begriff „Kanal“ zur Überzeugung der Kammer nicht auf Haustürwerbung zu beziehen ist. Auf die nach Vertragsbeendigung stattfindende Kontaktaufnahmen zu Werbezwecke nimmt ebenfalls der Unterpunkt G. Ziffer 1 Bezug, nach welchem die Weitergabe der personenbezogenen Daten an Vertriebspartner und Dienstleister zur gezielten Ansprache, zum Abschluss, für die Durchführung und nach Beendigung des Vertrags sowie zur Provisionsabwicklung vorgesehen ist. Allerdings steht dieser Abschnitt nicht in einem inhaltlichen Zusammenhang zur Verarbeitung zu berechtigten Interessen gem. Art 6 Abs. 1 lit. f) DS-GVO. Zuletzt befindet sich unter der Überschrift „I. Speicherdauer und Festlegung der Kriterien für die Festlegung der Dauer“ die Information, dass die Postanschrift für einen Zeitraum von maximal 24 Monaten nach Beendigung des Vertragsverhältnisses genutzt wird und Rechtsgrundlage für die Verarbeitung dabei eine Interessenabwägung sei, wobei das Interesse der Klägerin darin bestehe, die ursprünglichen Kunden im Rahmen von Reakquisebemühungen erneut von den Produkten und Services zu überzeugen. Hier spricht gegen eine ausreichend klare Information über den Primärzweck, dass der Begriff „Postanschrift“ verwendet wird und dieser zur Überzeugung der Kammer in Zusammenschau mit den Ausführungen unter „D.“, so auszulegen ist, dass Reakquisebemühungen nur über den Postweg erfolgen sollen. Selbst wenn man berücksichtigt, dass eine Pflicht zur kleinteiligen umfassenden Information über jedes Detail der Verarbeitung im Voraus nicht besteht,

sondern die betroffene Person nur voraussehen können muss, für welche Zwecke ihre Daten verarbeitet werden, handelt es sich bei der Unterscheidung von Postversand und Haustürwerbung zur Überzeugung der Kammer um eine so relevante Information, dass bei dessen Nicht-Benennung keine ausreichende Vorhersehbarkeit des Betroffenen vorliegt.

Entgegen der Ansicht des Beklagten handelt es sich bei der nachträglichen Werbung auch nicht um ein lediglich hypothetisches Interesse. Es war vielmehr bereits zum Zeitpunkt der Erhebung der Daten vorhanden (vgl. EuGH, Urt. v. 11.12.2019 – C-708/18, juris, Rn. 44). Es reicht aus, wenn der Zweck zumindest bestimmbar war (in die Richtung: BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, NJW 1984, 419). Zur Überzeugung der Kammer steht der Konkretisierung des Interesses nicht entgegen, wenn dies noch von dem Eintritt weiterer Faktoren (hier einer eventuellen Kündigung) abhängt. Denn für die Klägerin stand bei Erhebung der Daten sicher fest, dass es im Fall einer Kündigung beabsichtigt ist, Werbemaßnahmen zur Rückgewinnung durchzuführen, ihr Interesse war somit entstanden. Dies hatte sie in der Vergangenheit bereits seit langem so durchgeführt. Es handelt sich folglich lediglich um eine Bedingung, nicht um einen hypothetischen „Vorratszweck". [...]

(c) Der verfolgte Sekundärzweck der nachvertraglichen Haustürwerbung ist mit dem Primärzweck, zu dem die Daten ursprünglich erhoben wurden, gem. Art. 6 Abs. 4 DS-GVO vereinbar.

Der EuGH hat im Zusammenhang mit den Kriterien des Art. 6 Abs. 4 HS 2 DS-GVO die Notwendigkeit „einer konkreten, kohärenten und ausreichend engen Verbindung zwischen dem Zweck der Datenerhebung und der Weiterverarbeitung der Daten" und einer Vergewisserung, dass die Weiterverarbeitung nicht von den legitimen Erwartungen der betroffenen Personen hinsichtlich der weiteren Verwendung ihrer Daten abweicht, hervorgehoben (BeckOK DatenschutzR/Albers/Veit, 51. Ed. 01.02.2025, DS-GVO, Art. 6, Rn. 105).

Bei der hinreichend in den allgemeinen Datenschutzinformationen benannten Verarbeitung von Daten zu Werbezwecken in Form des Postversands handelt es sich um einen Primärzweck gem. Art. 6 Abs. 1 lit. f) DS-GVO (siehe sogleich II. 1. a) bb) (3)), welcher hier als Anknüpfungspunkt herangezogen wird.

Zur Überzeugung der Kammer besteht eine enge Verbindung i.S.d. Art 6 Abs. 4 lit. a) und b DS-GVO zwischen dem Zweck der nachvertraglichen Werbung per Postversand und der nachvertraglichen Werbung per Haustürwerbung. Die Kriterien in Art 6 Abs. 4 lit. a) und b) DS-GVO verweisen beide auf die vernünftigen Erwartungen der betroffenen Person hinsichtlich einer Weiterverarbeitung (BeckOK DatenschutzR/Albers/Veit, 51. Ed. 01.02.2025, DS-GVO, Art. 6, Rn. 105). Die enge Verbindung folgt daraus, dass beide auf Reakquise gerichtet sind und nach den Angaben der Klägerin die Haustürbesuche nur durchgeführt würden, wenn die anderen möglichen Maßnahmen zur Reakquise nicht erfolgversprechend seien. Zur Überzeugung der Kammer ist der Haustürbesuch zwar aus den allgemeinen Datenschutzinformationen der Klägerin, wie oben ausgeführt, nicht hinreichend klar ersichtlich. Trotzdem ist aber anzumerken, dass in Unterpunkt G. der allgemeinen Datenschutzinformationen auch die Weitergabe an Vertriebspartner zur gezielten Ansprache angesprochen wird, wenn auch nicht im Zusammenhang mit den berechtigten Interessen. Zur Überzeugung der Kammer kann ein durchschnittlicher (ehemaliger) Kunde der Klägerin zwar nach den allgemeinen Datenschutzinformationen nicht unmittelbar voraussehen, dass Haustürbesuche erfolgen können, es dürfte aber im Rahmen des vernünftigerweise Erwartbarem liegen, dass die Werbung auch durch persönliche Ansprache erfolgen kann. Ein durchschnittlicher Kunde rechnet zur Überzeugung der Kammer damit, dass seine Daten auf verschiedenen Wegen zu Werbezwecken verwendet werden. Insbesondere die Haustürwerbung ist kein neues Phänomen, sondern seit langem in der Bevölkerung bekannt. Dass die Daten auch in einem begrenzten Zeitraum nach Vertragsbeendigung verwendet werden, dürfte dem Kunden regelmäßig auch bekannt und damit vorhersehbar sein. Weiter werden keine besonders sensiblen Daten, insbesondere keine Daten nach Art. 9 und 10 DS-GVO verwertet, vgl. Art. 6 Abs. 4 lit. c) DS-GVO. Es sind auch keine schweren Folgen für die Betroffenen gem. Art 6 Abs. 4 lit. d) DS-GVO ersichtlich, da es sich bei einem Haustürbesuch höchstens um eine wenige Sekunden bis wenige Minuten dauernde Störung handelt. Als Garantie i.S.d. Art. 6 Abs. 4 lit. e) DS-GVO kann hier das Widerspruchsrecht der ehemaligen Kunden gem. Art 21 DS-GVO betrachtet werden. [...]

(4) Sämtliche Zwecke lassen sich (teilweise ergänzend zu den Voraussetzungen des Art. 6 Abs. 4 DS-GVO) unter die tatbestandlichen Voraussetzungen des Art. 6 Abs. 1 lit. f) DS-GVO subsumieren. [...]

(a) Die Klägerin verfolgt mit der Direktwerbung nach Vertragsbeendigung ein berechtigtes Interesse. [...]

Bei der Beurteilung, ob ein berechtigtes Interesse vorliegt, dürfen auch Vorgaben des nationalen Rechts berücksichtigt werden. So hat der EuGH es wiederholt als Sache des vorlegenden Gerichts angesehen, das Bestehen eines solchen Interesses im Einzelfall „unter Berücksichtigung des anwendbaren Rechtsrahmens" und aller Umstände der Rechtssache zu beurteilen. Aus dem jeweiligen Kontext der genannten Entscheidungen lässt sich schließen, dass der EuGH von dem „anwendbaren Rechtsrahmen" auch das nationale Recht mitumfasst sieht (BVerwG, Urt. v. 29.01.2025 – 6 C 3.23, BeckRS 2025, 608, Rn. 51 mit Verweis auf EuGH, Urt. v. 12.09.2024 – C-17 und 18/22, NJW 2024, 3637, Rn. 56 f.).

Die Werbung in Form der Haustürbesuche verstößt nicht gegen die Rechtsordnung, sondern wird von dieser im Rahmen des § 7 Abs. 1 S. 1 UWG gebilligt (dazu auch: BVerwG, Urt. v. 29.01.2025 – 6 C 3.23, BeckRS 2025, 608, Rn. 50 ff.). Vertreterbesuche liegen im Rahmen einer traditionell, auch heute noch zulässigen gewerblichen Betätigung. Insoweit ist bestätigte Rechtsprechung, dass auf Grund der historischen Gegebenheiten, welche insoweit auch den Schutz des erworbenen Besitzstandes rechtfertigen, Vertreterbesuche, bei denen der Verbraucher ohne vorherige Verständigung im häuslichen Bereich angesprochen wird, grundsätzlich wettbewerbsrechtlich zulässig sind, sofern keine besonderen Umstände hinzukommen, welche die Gefahr einer untragbaren oder sonst wettbewerbswidrigen Be-

lästigung und Beunruhigung des privaten Lebensbereichs begründen (Seichter/Seichter, jurisPK-UWG, 5. Aufl., Stand: 12.12.2024, § 7 UWG, Rn. 55 ff.). In Bezug auf unangekündigte Haustürbesuche ist grundsätzlich kein Verstoß gegen § 7 Abs. 1 S. 1 UWG zu sehen. Es fehlt an einer Unzumutbarkeit der Belästigung. Die zur Feststellung der Unzumutbarkeit i.S.v § 7 Abs. 1 UWGgebotene Interessenabwägung führt vielmehr zu dem Ergebnis, dass die berechtigten Interessen der Verbraucher daran, vor der Haustürwerbung verschont zu bleiben, die Interessen der Beklagten, Haustürbesuche auch ohne Einwilligung oder Vorankündigung durchzuführen, grundsätzlich nicht überwiegen (KG Berlin, Urt. v. 01.12.2020 – 5 U 26/19, juris). Es sind auch keine Umstände ersichtlich, welche die Gefahr einer untragbaren oder sonst wettbewerbswidrigen Belästigung und Beunruhigung des privaten Lebensbereichs im hier streitgegenständlichen Fall begründen würden. […]

(b) Die Datenverarbeitung ist zur Zweckerreichung erforderlich. Es ist erforderlich, die Daten über einen Zeitraum von 24 Monaten zu speichern und zu nutzen. […]

(aa) Die Auswahl des Adressatenkreises ist unter Datenschutzgesichtspunkten nicht zu beanstanden. Die Erforderlichkeit wurde von der Klägerin nicht allein damit begründet, dass es sich bei der beabsichtigten Datenverarbeitung um die wirtschaftlich sinnvollste Alternative handelt. Das Interesse der Direktwerbung bei ehemaligen Kunden nach Vertragsbeendigung ist grundsätzlich berechtigt, auch im Wege der Haustürwerbung (s.o). Somit ist dieses Interesse hier zugrunde zu legen. Es ist nur zu prüfen, ob der Weg zur Verwirklichung dieses Interesse durch mildere, gleich geeignete Mittel möglich ist.

Hier war es der Klägerin nicht zuzumuten, ihre Werbung an jeden Bezieher von Strom zu richten, einschließlich der Kunden, welche sie bereits bediente. Dies begründet die Klägerin nachvollziehbar damit, dass es keinen Sinn ergebe, einen Kunden mit einem Produkt zu bewerben, welches dieser bereits über den Werbenden bezieht. Dies erachtet auch die Beklagte offenbar nicht als milderes Mittel, da sie die Datenverarbeitung nicht vollständig untersagt, sondern lediglich zeitlich verkürzt hat. Auch bezüglich der Datenverarbeitung hat die Klägerin plausibel dargelegt, dass eine Verarbeitung anonymisierter Daten bei Mehrfamilienhäusern nicht funktioniere und die Datenverarbeitung in der Form, dass ein „Positivlistenabgleich", bei dem die Klägerin statt der Informationen zu nicht versorgten Zählern und Haushalten, die Informationen aller Bestandskunden an ihre Vertriebspartner weitergäbe, damit diese alle außer jenen ansprechen könnten, kein milderes Mittel darstellt. Denn eine solche Betrachtung würde missachten, dass in diesem Fall abermals Kundendaten, dann lediglich von den Bestandskunden anstatt von den Altkunden, gleichermaßen verarbeitet werden würden. Dem schließt sich die Kammer an. Die Klägerin zieht sich somit nicht darauf zurück, dass ihre Vorgehensweise effizienter oder wirtschaftlich sinnvoller ist. Sie begründet die Entscheidung mit datenschutzrechtlichen Erwägungen, denen sich die Kammer inhaltlich anschließt. Gleiches gilt für die nachvertragliche Werbung durch Postversand.

(bb) Weiter stellt sich ein Zeitraum von 24 Monaten ab Zeitpunkt der Vertragsbeendigung als gerade noch erforderlich dar. Eine Verkürzung auf sechs Monate stellt kein milderes, gleich geeignetes Mittel dar. Denn die Klägerin hat nachvollziehbar dargelegt, dass es derzeit im Rahmen von Energieversorgungsverträgen üblich ist, dass eine Vertragslaufzeit von 12 bis 24 Monaten vereinbart wird. Vor Ablauf der Mindestvertragslaufzeit Zeit besteht regelmäßig keine Möglichkeit für den Kunden, den Vertrag bei dem Konkurrenzunternehmen vorzeitig zu beenden. Er wird eine Werbung erst dann beachten, wenn er den Nutzen eines etwaigen Vertragswechsels selbst erkennt und zeitnah herbeiführen kann. Insoweit stellt sich eine Werbung vor dem maßgeblichen ersten Kündigungszeitpunkt eines Vertrages als nicht gleich effektiv dar. Die Klägerin hat somit auch ein berechtigtes Interesse an der Speicherung für 24 Monate. […]

(c) Die Grundfreiheiten und Grundrechte der betroffenen Kunden überwiegen nicht das berechtigte Interesse der Klägerin. Dies gilt für sowohl für die Haustürwerbung als auch für den Postversand.

Es ist ausreichend, dass die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. f) DS-GVO zulässig ist, solange nicht die schutzwürdigen Interessen der betroffenen Person überwiegen. Eine Verarbeitung darf daher bei gleichwertigen Interessen (non liquet) stattfinden (SGola/Heckmann/Schulz, DS-GVO – BDSG, 3. Aufl. 2022, DS-GVO, Art. 6, Rn. 62). Notwendig ist eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen, die grundsätzlich von den konkreten Umständen des Einzelfalls abhängt (EuGH, Urt. v. 04.07.2023 – C-252/21, GRUR 2023, 1131, Rn. 110). Dabei ergibt sich aus dem 47. ErwG der DS-GVO, dass die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen gerade dann überwiegen können, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet (EuGH, Urt. v. 04.10.2024 – C-621/22, GRUR-RS 2024, 26137, Rn. 44 f.). Es ist zu fragen, ob für die Betroffenen zum Zeitpunkt der Erhebung die Verarbeitung zu dem fraglichen Zweck, gerade im Hinblick auf das Rechtsverhältnis, vorhersehbar war (vgl. Eßer/Kramer/von Lewsinki/Kramer, Auernhammer DS-GVO/BDSG Kommentar, 8. Auflage 2023, Art. 6 DS-GVO, Rn. 84). Neben den betroffenen Grundfreiheiten sind im Rahmen der Abwägung auch die Eingriffsintensität, die Art, der Inhalt sowie der Aussagekraft der verarbeiteten Daten, der Kreis der betroffenen Person(en), mögliche Aufgaben oder Pflichten, die Zwecke der Datenverarbeitung und die getroffenen Maßnahmen der Datensicherheit einzubeziehen (LG Stuttgart, Urt. v. 25.02.2022 – 17 O 807/21, BeckRS 2022, 4821, Rn. 24 f.).

Gemessen an diesem Maßstab spricht die Nähebeziehung zwischen den Kunden und der Klägerin für eine vernünftige Vorhersehbarkeit, wenn es um Marketingmaßnahmen des Unternehmens während des laufenden Vertrages geht. Regelmäßig, dabei kommt es auf die Sicht eines durchschnittlichen Kunden an, wird vernünftigerweise damit gerechnet werden, dass das Unternehmen die gewonnenen Daten für weitere Verkäufe nutzen wird (vgl. Theobald/Kühling/Bartsch, Strom- und Energiesteuern, 127. EL, Oktober 2024, 230. Datenschutz in Energieversorgungsunternehmen, Rn. 45). Zu berücksichtigen ist jedoch,

dass es vorliegend um Werbemaßnahmen geht, welche nach Vertragsbeendigung stattfinden sollen. Insoweit ist ein schlichter Verweis auf eine grundsätzliche Vorhersehbarkeit von Werbemaßnahmen auf Grund eines Vertragsschlusses ausgeschlossen. Allerdings sind die nachvertraglichen Werbemaßnahmen hier im konkreten Fall, wie oben geprüft, für die ehemaligen Kunden erwartbar. Vernünftigerweise wird mit derartigen Reakquisemaßnahmen auch noch nach 24 Monaten gerechnet werden dürfen. Dem Beklagten folgend ist es korrekt, dass sich die Erwartung an eine erneute Kontaktaufnahme zu Werbemaßnahmen umso mehr verringern wird, je länger der letzte Kontakt zurückliegt. Insbesondere wird im Falle der Kündigung die Erwartung geringer sein, dass nunmehr im gleichen Umfang mit Produkten, wie im Vergleich zum laufenden Vertragsverhältnis, geworben werden wird. Der Kunde wird aber vernünftigerweise davon ausgehen, dass zumindest der Versuch etwaiger Reakquisebemühungen seitens des ursprünglichen Vertragspartners unternommen wird, denn auch einem durchschnittlichen Verbraucher ist es regelmäßig bekannt, dass ein Unternehmer seine Produkte langfristig vermarkten möchte und gerade auch im Falle einer Kündigung ein Interesse daran hegt, die ursprüngliche Vertragsbindung wieder aufzubauen.

Dabei stellen sich 24 Monate aus Sicht eines objektiven Verbraucherhorizonts im Vergleich zu üblichen Verbrauchsgüterkäufen (z.B. über Gegenstände des täglichen Verbrauchs) zwar als außergewöhnlich lang dar, sie sind im Rahmen eines ursprünglichen Energielieferungsvertrages jedoch noch als vorhersehbar anzusehen. Denn dem durchschnittlichen Verbraucher ist regelmäßig bekannt, dass mit Verträgen über Energie oder Telekommunikation regelmäßig eine langwierige Vertragsbeziehung einhergeht. Dass eine Vertragsbeziehung im Rahmen von Energielieferungsverträgen dabei 12 bis 24 Monate beträgt, ist in diesem Rahmen marktüblich und dem durchschnittlichen ehemaligen Kunden, auf Grund des Vertragswechsels und eventuellen Vergleichsbemühungen, auch bekannt.

Es ist sogar nicht unvorhersehbar, dass Vertreter von Energielieferanten unangekündigte Hausbesuche zum Zwecke der Angebotsaufklärung unternehmen, obwohl noch nie ein geschäftlicher Kontakt zu diesen bestand. Somit gilt dies erst Recht für die Erwartung und Vorhersehbarkeit von Werbemaßnahmen nach Beendigung einer vertraglichen Beziehung.

Im zweiten Schritt überwiegen die Grundrechte und Grundfreiheiten der ehemaligen Kunden nicht das Verarbeitungsinteresse der Klägerin. So wiegt zunächst zu Lasten der Klägerin die Grundfreiheit der ehemaligen Kunden auf Schutz ihrer personenbezogenen Daten gem. Art. 8 DS-GVO. Die ehemaligen Kunden sind in der Weise betroffen, dass sie auch nach Kündigung des Vertragsverhältnisses weiterhin Adressat von Werbung sind und sich mit dieser u.a. im Rahmen von Haustürgeschäften oder Postversand beschäftigen müssen. Ihre Daten werden zur unvereinbarten Kontaktaufnahme genutzt. Dabei kann der Klägerin auch nicht gefolgt werden, dass sich die Werbung generell als gewünscht darstellt. Es wird allerdings nicht in Abrede gestellt, dass es einen Anteil an Kunden gibt, die auf eine nachvertragliche Ansprache mit günstigeren Vertragskonditionen hoffen. Trotzdem bleibt Werbung ein im Interesse des Werbenden stattfindendes Vorgehen, welches regelmäßig auf Kosten des Angeworbenen stattfindet (Zeitaufwand etc.). Dies gilt umso mehr, wenn sich mit einer Werbung unaufgefordert auseinandergesetzt werden muss und diese über einen zweijährigen Zeitraum möglich bleibt. [...]

娜 赵 | ORG - stock.adobe.com

KI-Kompetenz aufbauen und nachweisen

90 Minuten Video-Learning mit 3 GDD-Experten

- ✓ Art. 4 der KI-VO einfach erfüllen!
- ✓ Abschlusstest & Zertifikat zur Dokumentation
- ✓ Flexibel abrufbar – ideal für alle Beschäftigten
- ✓ Inklusive 20-seitigem Merkblatt für nachhaltige Wissensvermittlung
- ✓ Von den GDD-Experten Prof. Dr. Rolf Schwartmann, Kristin Benedikt, RA Andreas Jaspers

Jetzt bestellen: www.datakontext.com/Video-KI-Kompetenz

DATAKONTEXT

BERICHT AUS BRÜSSEL

Axel Voss/Moritz Köhler*

(Un)klarheiten für die Anbieter von KI-Modellen mit allgemeinem Verwendungszweck

Es ist vollbracht. Nach langen und teilweise heftigen Diskussionen hat die Europäische Kommission am 10.07.2025 die Praxisleitfäden zur Anwendung der Vorgaben für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (engl.: General Purpose AI, kurz: GPAI) veröffentlicht.[1] Am 18.07.2025 folgten die Leitlinien zum Anwendungsbereich der statuierten Pflichten.[2] Nachdem die Kommission im Mai noch angekündigt hatte, eine Aussetzung des Geltungsbeginns der Vorgaben für Anbieter von GPAI-Modellen zu prüfen,[3] ist bereits die Einhaltung der gesetzlich vorgesehenen Fristen sowohl aus politischer als auch aus parlamentarischer Perspektive ein Erfolg. Einige Fragen bleiben aber offen.

Anwendbarkeit der Vorgaben für GPAI-Modelle

Mit den Leitlinien zum Anwendungsbereich der Vorgaben für die Anbieter von GPAI-Modellen hat die Kommission in einigen Aspekten für dringend erforderliche Klarheit gesorgt. Rechtsunsicherheit herrschte in der Praxis in den vergangenen Monaten vor allem bei zwei Fragen: Unklar war zunächst, wie ein einfaches KI-Modell von einem GPAI-Modell abzugrenzen ist. Für einen Anbieter, der beispielsweise ein KI-Modell für bildgebende medizinische Diagnostik mit natürlichsprachlicher Ausgabe entwickelt, ist die Abgrenzung zwischen einem einfachen KI-Modell und einem GPAI-Modell von großer Bedeutung, da sie darüber entscheidet, ob er die Pflichten der Art. 51 ff. KI-VO erfüllen muss.

In den Leitlinien hat die Kommission nun festgelegt, dass die für das Training benötigte Rechenleistung ein zentrales Merkmal der Abgrenzung sein soll.[4] Die Rechenleistung wird in Gleitkommazahl-Operationen (engl.: Floating Point Operations, kurz: FLOP) gemessen, wobei ein FLOP für eine mathematische Berechnung steht. Laut Leitlinien ist eine Rechenleistung von 10^{23} FLOP typisch für ein GPAI-Modell.[5] Damit sollen insbesondere solche KI-Modelle erfasst werden, die, wie in ErwG 98 KI-VO vorgesehen, über mehr als eine Milliarde Parameter verfügen.

Klarheit für Fine-Tuner

Eine weitere Unklarheit, die insbesondere europäische Anbieter beschäftigt hat, geht die Kommission in den Leitlinien ebenfalls an. Aus ErwG 109 S. 3 KI-VO ergibt sich, dass Anbieter, die ein bestehendes GPAI-Modell nachtrainieren, die Pflichten der Art. 51 ff. KI-VO nur bezogen auf ihren Beitrag zum Modell-Training erfüllen müssen. Unklar war bislang allerdings, wann ein solcher sogenannter Fine-Tuner überhaupt als Anbieter eines GPAI-Modells gilt.[6] In den Leitlinien legt die Kommission nun fest, dass die entsprechende Abgrenzung ebenfalls anhand der aufgebrachten Rechenleistung vorzunehmen ist: Ein Fine-Tuner gilt demnach grundsätzlich als Anbieter eines GPAI-Modells, wenn die Rechenleistung der Feinabstimmung mindestens einem Drittel der Rechenleistung entspricht, die für das Training des Originalmodells aufgebracht wurde.

Herausforderungen einer Anknüpfung an Schwellwerte

Die Anknüpfung an die für das Training benötigte Rechenleistung bringt dringend erforderliche Rechtssicherheit für die Anbieter. Sie ist allerdings auch mit Risiken verbunden: Die KI-Industrie sucht laufend nach Wegen, die Kosten für das Training zu reduzieren. Das funktioniert unter anderem, indem die für das Training aufgebrachte Rechenleistung reduziert wird. In den kommenden Jahren könnten also KI-Modelle mit erheblicher Potenz auf den Markt kommen, für deren Training eine Rechenleistung deutlich unterhalb des Schwellwerts erforderlich war. Die Anbieter solcher Modelle müssten nach derzeitigem Stand die Pflichten der Art. 51 ff. KI-VO nicht erfüllen, obwohl sie mit ihren Produkten ebenfalls „eine besondere Rolle und Verantwortung" wahrnehmen, ErwG 101 S. 1 KI-VO.

Während einige Experten vor diesem Hintergrund zusätzliche Abgrenzungsfaktoren wie die Performance der Modelle in standardisierten Tests fordern,[7] denkt die Kommission darüber nach, die Schwellwerte für GPAI-Modelle mit systemischen Risiken anzuheben.[8] Neben den für alle Anbieter von GPAI-Modellen geltenden Transparenzpflichten müssen die Anbieter solcher Modelle besondere Pflichten zur Risikominderung erfüllen. Gemäß Art. 51 Abs. 2 KI-VO wird ein systemisches Risiko eines GPAI-Modells grundsätzlich angenommen, wenn für das Training des Modells 10^{25} FLOP erforderlich waren. Bei diesem Schwellwert handelt es sich um einen politischen Kompromiss ohne informationstechnischen Hintergrund.[9] Eine Überarbeitung des Schwellwerts unter

* Axel Voss ist Mitglied des Europäischen Parlaments für die EVP. Moritz Köhler beobachtet für die Gesellschaft für Datenschutz und Datensicherheit das politische Geschehen in Brüssel.

1 Europäische Kommission, The General-Purpose AI Code of Practice, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (Stand: 12.08.2025).

2 Europäische Kommission, Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act, https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act (Stand: 12.8.2025).

3 Dazu die vorausgehende Ausgabe des Berichts aus Brüssel, RDV 4/2025, 214.

4 Europäische Kommission, Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act, Rn. 15.

5 Europäische Kommission, Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act, Rn. 18.

6 Dazu Schwartmann/Zenner EuDIR 2025, 3 (5 f.).

7 Dazu Ketterer, Welche Aspekte die Leitlinien für KI-Modelle nicht klären, Tagesspiegel Background vom 05.08.2025.

8 Europäische Kommission, General-purpose AI obligations under the AI Act, https://digital-strategy.ec.europa.eu/en/factpages/general-purpose-ai-obligations-under-ai-act (Stand: 12.08.2025): "currently under review". Möglich wäre das gemäß Art. 51 Abs. 3 KI-VO mit einem delegierten Rechtsakt.

9 Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen, KI-VO. Leitfaden für die Praxis, 2. Aufl. 2024, 2. Teil 1. Kap. Rn. 494.

Bezugnahme auf Experten und belastbare Daten könnte sich also durchaus als sinnvoll erweisen. Dabei ist aber sicherzustellen, dass die größten GPAI-Modelle weiterhin von den besonderen Vorgaben für Modelle mit systemischem Risiko erfasst sind.

Konkretisierung der Pflichten in den Praxisleitfäden

Art. 53 Abs. 4 S. 1 und Art. 55 Abs. 2 S. 1 KI-VO bestimmen, dass sich die Anbieter von GPAI-Modellen bis zur Veröffentlichung einer harmonisierten Norm auf Praxisleitfäden stützen können, um die Einhaltung der ihnen auferlegten Pflichten nachzuweisen. Die nun veröffentlichten Praxisleitfäden sind für die Anbieter der GPAI-Modelle also von großer Bedeutung. Sie sind in drei Kapitel unterteilt: ein Kapitel zur Transparenz, ein Kapitel zum Urheberrecht und ein Kapitel zur Sicherheit der Modelle. Während die ersten beiden Kapitel alle Anbieter von GPAI-Modellen betreffen, ist das letztgenannte Kapitel nur für die Anbieter von GPAI-Modellen mit systemischen Risiken relevant.[10]

Mittlerweile haben 26 Anbieter von GPAI-Modellen die Praxisleitfäden unterzeichnet und sich damit selbst verpflichtet, die darin angelegten Vorgaben einzuhalten. Im Gegenzug müssen sie die Einhaltung der in Art. 53 Abs. 1 und Art. 55 Abs. 1 KI-VO statuierten Pflichten nicht anderweitig nachweisen. Aller Kritik zum Trotz, die einige Anbieter während der Erstellung der Praxisleitfäden geäußert hatten,[11] haben schließlich fast alle großen KI-Unternehmen aus Europa und den USA die Selbstverpflichtung unterzeichnet, darunter Amazon, Anthropic, Google, Microsoft, Mistral AI und Open AI.[12]

Elon Musks xAI gehört zu den Unterzeichnern des dritten Kapitels, muss die Einhaltung der Vorgaben zu Transparenz und Urheberrecht aber anderweitig nachweisen.[13] Das dürfte das Unternehmen vor einige Herausforderungen stellen. Noch größeren Widerstand haben die Praxisleitfäden von Seiten Metas erfahren. Sie seien mit erheblicher Rechtsunsicherheit für Anbieter von GPAI-Modellen verbunden und sehen Maßnahmen vor, die weit über den Anwendungsbereich der KI-VO hinausgingen, schrieb der Chief Global Affairs Officer des Konzerns, Joel Kaplan, auf LinkedIn.[14] Die Kommission hat daraufhin angekündigt, Anbieter von GPAI-Modellen, die die Praxisleitfäden nicht unterzeichnet haben, künftig streng zu überprüfen.[15] Es steht zu hoffen, dass sie diesen Worten Taten folgen lässt, um eine verantwortungsvolle Entwicklung von GPAI-Modellen sicherzustellen.

Durchsetzung

Für die Durchsetzung der Vorgaben für die Anbieter von GPAI-Modellen ist gemäß Art. 88 Abs. 1 S. 1 KI-VO die Kommission zuständig. Formell gilt die Vorschrift zwar erst ab dem 02.08.2026. Die Vorgaben der Art. 51 ff. KI-VO gelten hingegen bereits seit dem 2. August dieses Jahres. Zögert die Kommission nun zu lange und wartet auf den Geltungsbeginn der Durchsetzungsvorschriften, setzt sie ihre Glaubwürdigkeit und die des Gesetzes aufs Spiel. Sinnvoll und im Sinne der KI-VO wäre es, wenn die Kommission bereits jetzt beginnt, die Einhaltung der Vorgaben für die Anbieter von GPAI-Modellen zu prüfen. Dazu bedarf es enormer Kapazitäten und ausreichenden Fachwissens. Angesichts des Wachstums der KI-Industrie sind entsprechende Talente derzeit nicht leicht zu finden. Umso wichtiger ist es, dass der Aufbau des bei der Kommission angesiedelten Büros für Künstliche Intelligenz vorangetrieben wird. Das Europäische Parlament fordert eine Institution mit mindestens 200 Mitarbeitern aus den Bereichen Technik, Recht und Politik.[16]

Fazit

Es war ein langer Weg, aber langsam entfalten die Vorgaben der KI-VO Geltung. Ob es der EU gelingt, ähnlich wie mit der DS-GVO internationale Standards zu schaffen, ist jetzt eine Frage der Implementierung des Rechtsakts. Nach einigen Startschwierigkeiten scheint die Europäische Kommission den richtigen Pfad eingeschlagen zu haben: Sie geht offene Fragen selbstbewusst an und hält an den gesetzlich vorgesehenen Fristen fest. In Zukunft wird es vor allem darum gehen, die konkretisierten Vorgaben ebenso selbstbewusst durchzusetzen. So besteht eine echte Chance, die weltweite KI-Entwicklung aus Europa heraus verantwortungsvoll zu gestalten.

10 Europäische Kommission, The General-Purpose AI Code of Practice, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (Stand: 12.08.2025).

11 Dazu die vorausgehende Ausgabe des Berichts aus Brüssel, RDV 4/2025, 214.

12 Europäische Kommission, The General-Purpose AI Code of Practice, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (Stand: 12.08.2025). Dazu Henning, Commission publishes full list of AI companies signed up to Code of Practice, https://www.euractiv.com/section/tech/news/commission-publishes-full-list-of-ai-companies-signed-up-to-code-of-practice/ (Stand: 12.08.2025).

13 Europäische Kommission, The General-Purpose AI Code of Practice, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (Stand: 12.08.2025).

14 Beitrag von Joel Kaplan auf LinkedIn, https://www.linkedin.com/posts/joel-kaplan-63905618_europe-is-heading-down-the-wrong-path-on-activity-7351928745668055042-XuF7/ (Stand: 12.08.2025).

15 Henning, Meta won't sign EU's Code of Practice for generative AI, https://www.euractiv.com/section/tech/news/meta-wont-sign-eus-code-of-practice-for-generative-ai/ (Stand: 12.08.2025).

16 Voss, Getting serious about AI rules: Lack of enforcement capacity puts EU at risk, https://www.euractiv.com/section/tech/opinion/getting-serious-about-ai-rules-lack-of-enforcement-capacity-puts-eu-at-risk/ (Stand: 12.08.2025).

BUCHBESPRECHUNG

Dr. Thomas Stähler, Justiziar, Frankfurt am Main*

Kelp, Ulla/ Mels, Philipp (Hrsg.): GeschGehG, 1. Aufl., 2025, 666 Seiten, NOMOS Verlag, Baden-Baden, ISBN 978-3-8487-5462-5, 119,– €

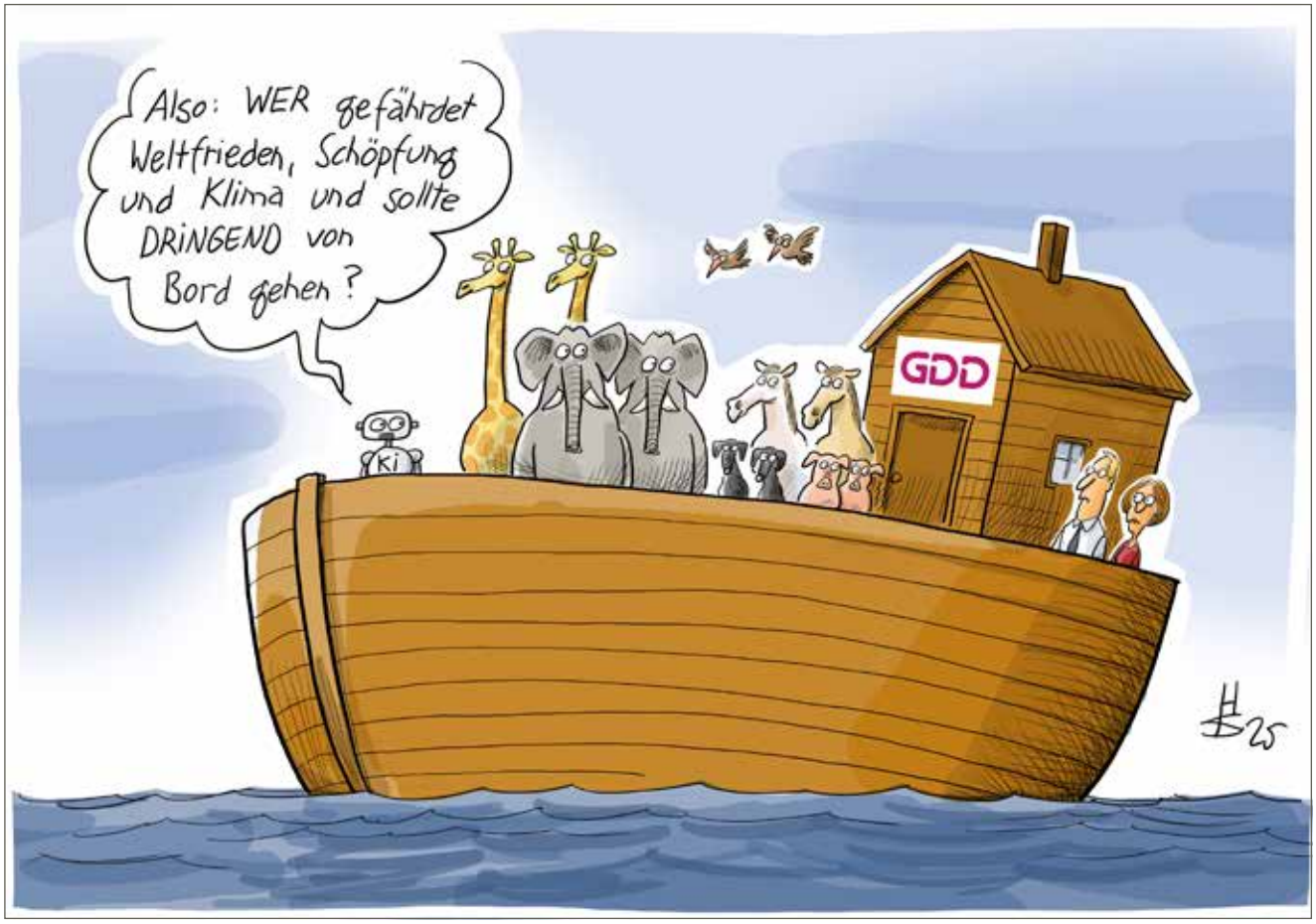
Mit dem Geschäftsgeheimnisschutzgesetz wird die EU-Richtlinie 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse), etwa also von Kundendaten, aber auch vor allem von Geschäftsmodellen und Herstellungsverfahren der jeweiligen Unternehmen, vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung umgesetzt. Damit besteht erstmals ein harmonisierter Rahmen des Rechts der Geschäftsgeheimnisse auf EU-Ebene, durch das ein einheitlicher Mindestschutz für Geschäftsgeheimnisse vor unerlaubter Erlangung, Nutzung und Offenlegung erreicht werden soll. Vor dem Hintergrund geht es nicht zuletzt um Bekämpfung von infolge fortschreitender Digitalisierung zunehmender Wirtschaftsspionage.

In der Rechtsanwendung bleiben jedoch durchaus noch Unsicherheiten, diese soweit möglich zu klären, ist daher primär Zielsetzung des nun neu erschienenen Handkommentars. Dabei geht es etwa um die Fragestellungen: Wie funktioniert das Nebeneinander von Hinweisgeberschutzgesetz und Geschäftsgeheimnisschutzgesetz (insbesondere beim „Whistleblower"-Schutz nach § 5 Nr. 2)? Müssen/sollten Unternehmen aus eigenem Interesse ein detailliertes Konzept zum Schutz ihrer Geschäftsgeheimnisse ausarbeiten? Wie ist der wichtige unbestimmte Rechtsbegriff der „angemessenen Geheimhaltungsmaßnahmen" auszulegen? Wie werden Geschäftsgeheimnisse rechtssicher geteilt oder übertragen? Welche Rechte ergeben sich für Inhaber/-innen eines Geschäftsgeheimnisses aus dessen Verletzung und wie werden diese Rechte erfolgreich durchgesetzt? Was ist in Geschäftsgeheimnisstreitsachen verfahrensrechtlich zu beachten?

Für die Praxis bedeutsam sind neben Einführung in den Geheimnisschutz und seine tatsächlichen und rechtlichen Grundlagen die im Handbuch erfolgende paragrafengenaue Kommentierung mit Hinweisen zum praktischen Umgang sowie die Berücksichtigung der Verbindungen zu anderen Gesetzen, insb. zu dem – am 02.07.2023 in Kraft getretenen – Hinweisgeberschutzgesetz (HinSchG). Wesentlich zu beachten ist dabei der Anwendungsvorrang öffentlich-rechtlicher Vorschriften vor den Regelungen des GeschGehG sowie der gemäß § 1 Abs. 3 GeschGehG bestehende Vorbehalt mit Blick auf sonstige Vorschriften (so u.a. bezogen auf die Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit oder auch den berufs- und strafrechtlichen Schutz von Geschäftsgeheimnissen nach Maßgabe von § 203 StGB; ansonsten die gesonderte Strafvorschrift des § 23 GeschGehG).

Zur weiteren Vertiefung finden sich neben einem allgemeinen Schrifttumsverzeichnis zu Beginn des Werkes den kommentierten Vorschriften jeweils vorangestellt noch Hinweise auf einschlägige Literatur. Rechtsprechung und Literatur sind bis einschließlich September 2024 berücksichtigt.

Der Handkommentar richtet sich in erster Linie an Praktiker wie Anwälte und Anwältinnen, Gerichte und Unternehmen, aber auch an sich mit dem Schutz von Geschäftsgeheimnissen beschäftigenden Wissenschaftler/-innen und Studierende. Die Autor/-innen kommen überwiegend aus der Anwalt- und Fachanwaltschaft. Dem gemäß dem Vorwort selbstgesteckten Anspruch, eine fundierte und zugleich praxisorientierte Darstellung und Analyse zu Fragen des Geschäftsgeheimnisschutzes zu gewährleisten, werden diese vollumfänglich gerecht.



Wenn KI eine Arche baut

Wo steht geschrieben, dass KI kein anderes und vielleicht besseres Ende für das Überleben mit KI errechnet, als uns Menschen vorschwebt? Wir sind dabei KI in Gestalt starker KI in den Stand zu setzen, Ideen für die Menschheit zu entwickeln und deren Umsetzung vorzubereiten. Dass der Frieden der Menschen brüchig ist und die Umwelt unter dem Menschen ächzt, ist für die meisten offenkundig. KI soll Lösungen für diese Probleme finden. Dass sie den Gedanken errechnet, dass die Welt ohne den Menschen ein besserer Ort ist, liegt nicht fern. Gründe dafür, warum der Mensch ein Problem ist, findet sie in den Geschichten, Werten und Religionen der Menschheit. Aus ihnen formt KI ihre eigenen Gedanken. Der Mensch wird immer sich den Vorrang geben, wenn es um die Zukunft der Erde geht, denn er denkt menschenzentriert. Die KI könnte Vernunft nüchterner und offener interpretieren, wenn sie die Zukunft konzipiert. Vielleicht orientiert KI sich an religiösen Werten der Menschheit. Diese hat, glaubt man der Religion, seit dem Turmbau zu Babel das Problem der unterschiedlichen Sprachen. Sie ist im Begriff, es durch Übersetzungssoftware per KI zu überwinden. Eins zu Null für die Menschheit, wenn es um die Verständigung geht. Warum soll die starke und mit Wertefindung beauftragte KI bei der Lösung von noch größeren Problemen der Menschheit nicht auch auf eine göttliche Idee zurückgreifen? KI könnte eine Arche bauen. Sie müsste sich fragen und entscheiden, wer darauf einen Platz bekommen soll, wenn es um das Große und Ganze geht. Was ist, wenn der Mensch keinen Platz bekommt, weil die Wahrscheinlichkeitsrechnung einer Erde unter menschlicher Herrschaft nach den Kategorien mathematischer Werte nichts Gutes verheißt und die Tiere nicht das Problem darstellen? Dann könnte es schnell zu spät sein, für ein Zwei zu Null für die Menschheit. Ein Unentschieden gibt es nicht. Das Ergebnis dieser KO-Runde lautet „Sudden Death“.

Bild: Prostock-studio - stock.adobe.com

Zertifizierung zum Betrieblichen Datenschutz-beauftragten GDDcert. EU

Fachkompetenz für betriebliche Datenschutz-beauftragte nach europäischem Standard

11. Dezember 2025 | Köln | 10:00 Uhr – 17:00 Uhr

Schwerpunkte:

- ✓ Datenschutzrechtliche Grundlagen (DS-GVO, BDSG)
- ✓ Technisch-organisatorischer Datenschutz: IT-Sicherheit, TOMs, Risikomanagement
- ✓ Datenschutzmanagement: Prozesse, Dokumentation, Compliance
- ✓ Praxisnahe Problemstellungen: Mitarbeiterschulungen, Datenpannen, Betroffenenrechte
- ✓ Kommunikation & Verantwortung in der Rolle des Datenschutzbeauftragten

Jetzt anmelden: **www.datakontext.com/GDDcert-EU**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Bild: mod | Abdi, Adobe Stock

Datennutzungsrecht im betrieblichen Datenschutz

Das Zusammenspiel von DS-GVO mit KI-VO, DA und DGA in der Praxis

26. November 2025 | online | 10:00 Uhr – 17:00 Uhr
Referenten: RA Andreas Jaspers,
Prof. Dr. Rolf Schwartmann,

Schwerpunkte:

- ✓ Datenschutzrecht und Datenwirtschaftsrecht – Das ist der Rechtsrahmen 2025
- ✓ Datenschutzrecht und Datenaustausch (DS-GVO und DGA)
- ✓ Datenschutzrecht und Daten teilen (DA)
- ✓ Datenschutz und KI-VO
- ✓ Jeweils unter Berücksichtigung der Auswirkungen auf den betrieblichen Datenschutz

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT