HZ219194 · ISSN 0178-8930 · www.rdv-online.com
42. Jahrgang **Oktober 5/2026**
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. Dr. Frauke Rostalski
Rebekka Weiß
Steffen Weiß
Prof. Dr. Christiane Wendehorst
Kai Zenner

Redaktion
Lucia Burkhardt

AUFSÄTZE

GERWING/HEMMER/RODERBURG: Staatsmodernisierung in Nordrhein-Westfalen

NINK: Cybersicherheitsregulierung nach NIS-2: Chance oder bürokratische Überforderung?

SCHWARTMANN/BURKHARDT: Transparenz beim KI-Einsatz im politischen Kontext

KURZBEITRÄGE

LEHMKEMPER/DEHNERT: Innovationsförderung durch Einrichtung von KI-Reallaboren bei den Landesdatenschutzbehörden

REIF/ZHOU: Praxisfälle zum Datenschutzrecht XLII: Informationspflichten bei der Videoüberwachung

KEBER/LIST: Die „Stuttgarter Impulse zur Modernisierung des Datenschutzes" Eckpunkte aus Sicht der Aufsichtspraxis

BURKHARDT/SCHWARTMANN/ZIEGENHORN: Die Änderung der KI-Verordnung durch den Digital-Omnibus

RECHTSPRECHUNG

BAG: Kein Anspruch auf Kopie eines Compliance-Abschlussberichts

ARBG: Keine Haushaltsausnahme für die kollegiale WhatsApp-Chatgruppe

EUGH: Auch der erste Auskunftsantrag kann exzessiv sein

BGH: Fehlgeleitete Bewerbungsnachricht als Schaden

BGH: Zulässigkeit der SCHUFA-Einmeldung bestrittener Forderungen und Folgenbeseitigung durch Widerruf (LS)

OLG: Lauterkeitsrechtliche Haftung für unzutreffende Facharztangaben des eigenen KI-Chatbots

DATA AGENDA PODCAST

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

Hybrid: Online & in Köln

50. DAFTA

12.–13. November 2026

45. RDV-Forum

11. November 2026

Künstliche Intelligenz – Werkzeug oder Partner? Herausforderungen für den Datenschutz!

Jetzt anmelden: **www.dafta.de**

Mit freundlicher Unterstützung von:

GDD Gesellschaft für Datenschutz und Datensicherheit e.V. · DAV · caralegal · dastra · DATAKONTEXT

EDITORIAL 231

VERANSTALTUNGEN 232

AUFSÄTZE

Jennifer GERWING/Dr. iur Harald HEMMER/
Dr. iur Dominik RODERBURG
Staatsmodernisierung in Nordrhein-Westfalen 233

Dr. Judith NINK
Cybersicherheitsregulierung nach NIS-2: Chance oder bürokratische Überforderung? 242

Prof. Dr. Rolf SCHWARTMANN/Lucia BURKHARDT
Transparenz beim KI-Einsatz im politischen Kontext 246

KURZBEITRÄGE

Denis LEHMKEMPER/Dr. Henning DEHNERT
Innovationsförderung durch Einrichtung von KI-Reallaboren bei den Landesdatenschutzbehörden 251

RAin Yvette REIF/RA Dr. Johannes ZHOU
Praxisfälle zum Datenschutzrecht XLII: Informationspflichten bei der Videoüberwachung 254

Prof. Dr. Tobias KEBER/Tobias LIST
Die „Stuttgarter Impulse zur Modernisierung des Datenschutzes" Eckpunkte aus Sicht der Aufsichtspraxis 260

Lucia BURKHARDT/Prof. Dr. Rolf SCHWARTMANN/
Dr. Gero ZIEGENHORN
Die Änderung der KI-Verordnung durch den Digital-Omnibus 264

RECHTSPRECHUNG

HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

Kein Anspruch auf Kopie eines Compliance-Abschlussberichts
(BAG, Urt. v. 16.4.2026) 272

Keine Haushaltsausnahme für die kollegiale WhatsApp-Chatgruppe
(ArbG Siegburg, Urt. v. 22.5.2026) 274

WICHTIGES AUS DER RECHTSPRECHUNG

Auch der erste Auskunftsantrag kann exzessiv sein
(EuGH, Urt. v. 19.3.2026) 277

Fehlgeleitete Bewerbungsnachricht als Schaden
(BGH, Urt. v. 23.6.2026) 282

Zulässigkeit der SCHUFA-Einmeldung bestrittener Forderungen und Folgenbeseitigung durch Widerruf (LS)
(BGH, Urt. v. 12.5.2026) 284

Lauterkeitsrechtliche Haftung für unzutreffende Facharztangaben des eigenen KI-Chatbots
(OLG Hamm, Urt. v. 12.5.2026) 285

Die Datenkopie muss nicht maschinenlesbar sein
(OLG Brandenburg, Beschl. v. 15.4.2026) 289

KI-Nachschärfung von Luftbildaufnahmen begründet keinen intensiveren Grundrechtseingriff (LS)
(OVG NRW, Beschl. v. 22.6.2026) 291

Angemessener Untersuchungsumfang einer Datenschutzbeschwerde durch die Aufsichtsbehörde (LS)
(VG Düsseldorf, Urt. v. 22.6.2026) 291

Vervielfältigung geschützter Musikwerke beim Training und im Modell eines KI-Musikgenerators (LS)
(LG München I, Endurt. v. 31.7.2026) 291

Exzessiver erster Auskunftsantrag nach Brillen Rottler (LS)
(AG Arnsberg, Urt. v. 1.7.2026) 291

BERICHT AUS BRÜSSEL

Axel VOSS/Lucia BURKHARDT
Anonymisierung, neu vermessen 293

BUCHBESPRECHUNG

Prof. Dr. Rolf SCHWARTMANN
Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz 295

SCHWAKURAI'S SCHLEPPNETZ 296

HERAUSGEGEBEN VON

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

Andreas Jaspers, Rechtsanwalt, Bonn

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

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

EHRENHERAUSGEBER

Prof. Peter Gola

IN KOOPERATION MIT

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

PRAXISBEIRAT

Dr. Peter Allgayer, Richter am Bundesgerichtshof

Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg

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

Paula Cipierre, ada Learning GmbH, Düsseldorf

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

Dr. Jens Eckhardt, Rechtsanwalt, Düsseldorf

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

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

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

Markus Hartmann, Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Köln

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

Prof. Dr. Herwig Hofmann, Universität Luxemburg

Dr. Marek Jansen, Google Deutschland, Köln

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

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

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

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

Thomas Müthlein, DMC Datenschutz Management & Consulting, Köln

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

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

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

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

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

Maria Christina Rost, Landesbeauftragte für den Datenschutz Sachsen-Anhalt

Prof. Dr. Dr. Frauke Rostalski, Universität zu Köln

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

Steffen Weiß, LL.M., Rechtsanwalt, Hamburg

Prof. Dr. Christiane Wendehorst, Universität Wien

Kai Zenner, Digitalreferent im Europäischen Parlament

Redaktion
Lucia Burkhardt
(Verantwortlich für den Rechtsprechungsteil)

Redaktionsbüro
Christina Kopp | Serena Roller
Anschrift Redaktion/-Büro
DATAKONTEXT GmbH
Augustinusstr. 11A | 50226 Frechen-Königsdorf
Telefon: +49 228 969675-00
RDV-Redaktion@datakontext.com

Erscheinungsweise
6 x jährlich

Bezugspreise

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

MwSt. im Preis enthalten, jeweils inkl. Versandkosten

Vertrieb/Produktsicherheit
Stefan Waldeisen | Tel.: +49 2234 98949-0
stefan.waldeisen@datakontext.com
www.datakontext.com/produktsicherheit

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: Stefan Waldeisen, 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.

EDITORIAL

RDV
Recht der Datenverarbeitung

Smarte Brillen in bunten Farben für Datenschutz

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Aktuell verbreiten sich „Smart Glasses", intelligente Brillen, wobei man sich fragen kann, inwieweit smart eben nicht nur ein Synonym für clever ist, sondern auch für halbseiden. Meta hat eine Brille auf den Markt gebracht, in der sich Mikrofone und Kameras verstecken. Apple arbeitet an Ohrstöpseln, die sich für Film- und Tonaufnahmen eignen. Derartige Produkte sind keine Kommunikationsdienste wie Instagram, sondern Produkte, mit denen sich Social-Media-Angebote mit Videos und Bildern fluten kann. Man kann sich damit als sehbehinderter Mensch von der smarten Brille aber auch die Umwelt erklären lassen. Das ist zweifellos ein Gewinn. Keine Technologie ist nur gut oder nur böse. Wenn sie in Produkten versteckt ist, verleitet sie Menschen allerdings in unterschiedlicher Weise zu Missbrauch. Deshalb geht es nicht darum, eine bestimmte Technologie zu verbieten, sondern darum, Produkte zu regulieren. Um Menschen zu schützen. Das Datenschutzrecht setzt beim Schutz personenbezogener Daten an. Bilder und Tonaufnahmen von Menschen dürfen nur dann verbreitet werden, wenn das Gesetz es gestattet. Weder ein Mitbürger noch ein Polizist darf Daten Dritter einfach nutzen und gar verbreiten. Andere Gesetze schützen nicht vor Datenmissbrauch, sondern es geht ihnen um das Produkt selbst. Bei Smart Glasses ist der springende Punkt, ob man sie sicher erkennt. So will es ein Gesetz, das Herstellung und Vertrieb von Produkten verbietet, wenn diese verdeckt Mikrofone und Kameras enthalten, mit denen man andere heimlich ablichten oder abhören kann. Das ist etwa bei einer schwarzen Sonnenbrille der Fall, wenn man je nach Lichtverhältnissen und Entfernung nicht erkennen kann, ob sie gerade filmt oder Gespräche aufzeichnet. Sie signalisiert das mit einem weißen Licht, das man aber je nach Entfernung, Blickwinkel und Lichtverhältnissen nicht sieht.

Was spricht dagegen, für Produkte wie spionagetaugliche Brillen eindeutige Produktvorgaben zu machen? Etwa so: Fassungen smarter Brille müssen rot, die Brillengläser müssen gelb sein. Dann weiß jeder, dem sich ein Brillenträger nähert, dass er besser vorsichtig sein sollte. Damit man erkennen kann, wann die Kamera der Brille aktiv ist, müssen vier deutlich sichtbare Dioden an den Bügeln und an der Vorderseite des Gestells für die Dauer der Aufnahme grün leuchten. Damit fällt man auf? Natürlich, genau darum geht es. Bei Produkten, die Menschen gefährden, geht es nicht primär um unauffälliges, cooles Produktdesign, das Missbrauch leicht macht. Es geht um Funktionalität mit Rücksicht auf den Schutz der Mitmenschen. Dazu dienen Signalfarben. Wenn Datengiganten Vertrauen aufbauen wollen, dann wären solche transparenten und klaren Signale ein Weg dazu.

Termine	Thema	Ort	Kontakt
3.11.2026	Löschen nach DS-GVO	Online	GDD e.V./DATAKONTEXT
4.11.2026	Konzerndatenschutz	Online	GDD e.V./DATAKONTEXT
6.11.2026	Datenschutz und IT-Sicherheit in der Cloud – Risiken minimieren, Chancen nutzen	Online	GDD e.V./DATAKONTEXT
9.-10.11.2026	Datenschutz-Management nach der DS-GVO – Teil 3	Online	GDD e.V./DATAKONTEXT
11.-13.11.2026	45. RDV-Forum und 50. DAFTA	Köln	GDD e.V./DATAKONTEXT
12.11.2026	Unbegrenzte Mobilität – Cloud, Apps & KI datenschutzkonform einsetzbar?	Online	GDD e.V./DATAKONTEXT
17.-18.11.2026	Ausbildung zum/zur Datenschutzkoordinator/in	Online	GDD e.V./DATAKONTEXT
19.11.2026	Eigenes Datenschutz-Lab aufbauen	Online	GDD e.V./DATAKONTEXT
23.-25.11.2026	Fortbildung und Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
25.11.2026	Basiswissen IT-Sicherheit für Datenschutzbeauftragte & -Manager	Online	GDD e.V./DATAKONTEXT
26.11.2026	Prüfung zum/zur Datenschutzkoordinator/in	Online	GDD e.V./DATAKONTEXT
30.11.-8.12.2026	Einführung in den Datenschutz für die Privatwirtschaft - Teil 1	Online	GDD e.V./DATAKONTEXT
30.11.2026	Microsoft 365 und Copilot: technische und rechtliche Fallstricke	Online	GDD e.V./DATAKONTEXT
1.12.2026	Datenschutz-Repetitorium zum GDDcert. EU: Vorbereitung auf die GDDcert. EU-Prüfung	Köln	GDD e.V./DATAKONTEXT
2.12.2026	Künstliche Intelligenz und Datenschutz: Rechtssicherer Einsatz mit der KI-Verordnung	Online	GDD e.V./DATAKONTEXT
7.12.2026	Datenschutz-Folgenabschätzung	Online	GDD e.V./DATAKONTEXT
9.12.2026	Prompting für Datenschützer – KI-Werkzeuge rechtssicher und effizient einsetzen	Online	GDD e.V./DATAKONTEXT
16.12.2026	Datenschutz im Internet	Online	GDD e.V./DATAKONTEXT
17.12.2026	Zertifizierung zum Betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V./DATAKONTEXT
20.1.2027	Unbegrenzte Mobilität – Cloud, Apps & KI datenschutzkonform einsetzbar?	Online	GDD e.V./DATAKONTEXT

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

AUFSÄTZE

Jennifer Gerwing/Dr. iur Harald Hemmer/Dr. iur Dominik Roderburg

Staatsmodernisierung in Nordrhein-Westfalen

Entwurf eines Fünften Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Gesetz für KI-Reallabore in NRW (GKI NRW)

Die laufende Legislaturperiode in Nordrhein-Westfalen steht auch im Zeichen der Staatsmodernisierung. Insbesondere das Jahr 2026 wird – vorbehaltlich der noch ausstehenden parlamentarischen Beschlussfassungen – grundlegende legislatorische Veränderungen bringen.

Hierzu gehört insbesondere auch der Entwurf eines Gesetzes für KI-Reallabore in NRW. Die Landesregierung hat den Gesetzentwurf am 10.6.2026 beschlossen. Gegenwärtig wertet die Landesregierung die Ergebnisse der Verbändeanhörung aus. Dieser Auswertung soll mit dem vorliegenden Beitrag nicht wertend vorgegriffen werden. Vielmehr sollen die Maßnahmen der Staatsmodernisierung in Nordrhein-Westfalen aus dem laufenden Jahr mit einem Schwerpunkt auf den Entwurf des Gesetzes für KI-Reallabore in NRW dargestellt und transparent gemacht werden.

I. Jüngste Entwicklungen der Staatsmodernisierung in Nordrhein-Westfalen

Staatsmodernisierung ist notwendig, um das Fundament des Staates, das in dem Vertrauen der Bürgerinnen und Bürger in die Handlungs- und Leistungsfähigkeit seiner Institutionen liegt, zu erhalten.[1]

Für die weitere Betrachtung ist zunächst zwischen zwei Ebenen zu unterscheiden: Die der Organisation staatlicher Aufgabenwahrnehmung einerseits und die der Ausgestaltung staatlicher Entscheidungs- und Umsetzungsprozesse andererseits.

Auf der Ebene der Staatsorganisation geht es insbesondere um die Zuordnung von Zuständigkeiten. Es ist eine Binse, dass die gegenwärtig oftmals bestehende Vielzahl nebeneinander bestehender Zuständigkeiten im Rahmen ein und derselben Entscheidung eine Verantwortungszuordnung erschwert.[2] Dies widerspricht aber dem Wesen der Demokratie, das auch darin besteht, verantwortliche Akteurinnen und Akteure haftbar machen zu können – sei es politisch in Wahlen, sei es juristisch vor Gericht.

Die zweite Ebene betrifft die konkrete Ausgestaltung staatlicher Entscheidungs- und Umsetzungsprozesse. Hierzu gehören insbesondere die Entbürokratisierung, die Beschleunigung von Verfahren und deren Digitalisierung. Die Notwendigkeit von Reformen ist in Deutschland inzwischen unstreitig. Es besteht insoweit „grundsätzlich kein Erkenntnisproblem“[3], sondern ungelöste Fragen der Umsetzung in einem komplexen Mehrebenensystem, in dem das überwiegende Potenzial von Entbürokratisierung im Unions- und Bundesrecht liegt, jedenfalls gesehen wird. Dies entbindet allerdings nicht die Länder, die ihnen gegebenen Handlungsmöglichkeiten auszuschöpfen. In vielen Bereichen dürfte es dabei mehr um ein „Umsteuern“[4] als lediglich um punktuelle Änderungen gehen.

Auf diese zweite Ebene der Staatsmodernisierung konzentriert sich der vorliegende Beitrag. Blickt man dabei auf die Entwicklungen in Nordrhein-Westfalen in diesem Jahr, standen Maßnahmen zur Umsetzung der Föderalen Modernisierungsagenda, beschlossen von den Regierungschefinnen und Regierungschefs der Länder und dem Bundeskanzler am 5.12.2025, im Vordergrund. Mit dem Zweiten Entlastungs- und Beschleunigungspaket hat das Landeskabinett daneben spezifische landesrechtliche Maßnahmen der Staatsmodernisierung beschlossen. Hinzu kamen weitere Schritte zur Umsetzung des Pakts für Planungs- und Genehmigungs- und Umsetzungsbeschleunigung (gleichfalls fußend auf einem Beschluss der Ministerpräsidentenkonferenz mit dem Bundeskanzler) sowie des Ersten Beschleunigungs- und Entlastungspakets.

1. Das Zweite Entlastungs- und Beschleunigungspaket

Mit dem im Februar 2026 beschlossenen Zweiten Entlastungs- und Beschleunigungspaket wurden über 30 landesspezifische Maßnahmen der Staatsmodernisierung beschlossen. So wurde etwa im Rahmen des Landesplanungsgesetzes die Resilienz von Raumordnungsplänen gegen juristische Anfechtungen gestärkt und die weitere Beschleunigung des Planverfahrens ermöglicht. Ferner wurden Maßnahmen zur Beschleunigung von Verfahren im Zusammenhang mit der klimagerechten Transformation der Wirtschaft sowie Erleichterungen für Großraum- und Schwertransporte beschlossen.

1 Wildberger, Rede bei der Veranstaltung „Staatsmodernisierung mit Wirkung“ in der Berlin-Brandenburgischen Akademie der Wissenschaften am 8.6.2026 in Berlin, https://bmds.bund.de/aktuelles/reden/detail/rede-bei-der-veranstaltung-staatsmodernisierung-mit-wirkung.

2 Wildberger, Rede bei der Veranstaltung „Staatsmodernisierung mit Wirkung“ in der Berlin-Brandenburgischen Akademie der Wissenschaften am 8.6.2026 in Berlin, https://bmds.bund.de/aktuelles/reden/detail/rede-bei-der-veranstaltung-staatsmodernisierung-mit-wirkung.

3 Liminski/Roderburg, EuDIR 2026. 161.

4 Liminski/Roderburg, EuDIR 2026. 161.

2. Umsetzung der Föderalen Modernisierungsagenda

a) Gegenstand der Föderalen Modernisierungsagenda

Die Föderale Modernisierungsagenda wird politisch als „letzter noch glaubhafter Versuch eines Umsteuerns“[5] gesehen. Eine knappe Zusammenfassung der insgesamt 237 Maßnahmen findet sich in der Antwort der Landesregierung zum Umsetzungsstand der Föderalen Modernisierungsagenda.[6] Die Darstellung der einzelnen Maßnahmen in der Agenda unterscheidet sich von vorherigen Maßnahmenpaketen wie etwa dem Pakt für Planungs-, Genehmigungs- und Umsetzungsbeschleunigung, durch eine teilweise erhebliche Detailtiefe.[7]

b) Umsetzung in Nordrhein-Westfalen

Die Umsetzung der Föderalen Modernisierungsagenda wird – unter Wahrung des Ressortprinzips – zentral durch die Staatskanzlei gesteuert.[8] Erklärtes Ziel ist es, strukturelle Veränderungen zu erreichen.[9]

Die Umsetzung fußt bislang insbesondere auf fünf Gesetzentwürfen zur Entlastung von Bürgern und Wirtschaft in NRW sowie mehreren Kabinettbeschlüssen, mit denen das Binnenrecht der Landesregierung angepasst wird.

Eine „Strukturveränderung“[10] wird mit dem Konzept einer „Beweislastumkehr für Bürokratie“ bewirkt. Danach soll nicht mehr derjenige in der Rechtfertigungslast sein, der beabsichtigt, bestehende bürokratische Anforderungen abzuschaffen, sondern derjenige, der daran festhalten möchte.[11] Diesen Ansatz setzen das Berichts- und Dokumentationspflichtenaussetzungsgesetz sowie das Gesetz zur Aufhebung von Schriftformerfordernissen um. Strukturell angegangen wird auch die Problematik von „routinemäßigen“ regierungsinternen Evaluationspflichten von Rechtsverordnungen. Hier setzt die Landesregierung künftig auf eine anlassbezogene Umsetzung. Eine weitere strukturelle Änderung liegt darin, auf Instrumente zur regulatorischen Vereinfachung zu setzen: Dies geschieht durch das Gesetz zur Erprobung der Verwaltungsvereinfachung in Kommunen in Nordrhein-Westfalen sowie das Gesetz für KI-Reallabore in Nordrhein-Westfalen. Mit einem Gesetz zur Gewährleistung und Vereinfachung des Gemeingebrauchs soll einer Entwicklung entgegengewirkt werden, dass Kommunen die kostenfreie Bereitstellung von kommunalen Einrichtungen unter Haftungsgesichtspunkten zunehmend in Frage stellen. Mit zwei Kabinettbeschlüssen zum Thema „bessere Rechtsetzungen“, sollen die Strukturen des regierungsinternen Verfahrens zur Erstellung von Gesetzentwürfen vereinfacht, transparenter, praxisnäher und vor allem bürokratieärmer ausgestaltet werden.

aa) Umsetzung des Konzepts der Beweislastumkehr

(1.) Aussetzung und Abschaffung von Berichts- und Dokumentationspflichten

Mit dem Entwurf eines Zweiten Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Aussetzung von Berichts- und Dokumentationspflichten zu Lasten der Wirtschaft in Nordrhein-Westfalen[12] soll jede landesrechtliche Berichts- und Dokumentationspflicht, deren Fortbestand nicht durch eine Rechtsverordnung ausdrücklich angeordnet wird, zum 1.1.2027 zunächst ausgesetzt werden und zum 1.1.2028 ganz entfallen. Über diese Rechtsverordnung beschließt die Regierung als Kollegium, somit als Ganzes. Die zeitliche Staffelung ermöglicht einen temporär begrenzten Reparaturmechanismus falls sich erweisen sollte, dass einzelne Pflichten weiterhin erforderlich sind, aber nicht in die Rechtsverordnung aufgenommen wurden.

Auch neu beschlossene Berichtspflichten müssen in die Rechtsverordnung aufgenommen werden. Damit entsteht eine tagesaktuelle Übersicht über die geltenden landesrechtlichen Berichtspflichten für Unternehmen.

Der Umfang dieser Rechtsverordnung wird damit zum Lackmustest des Erfolgs des Konzepts.

Vergleichbare Ansätze werden inzwischen auch auf Bundesebene und in anderen Ländern verfolgt. Der Bund – auf dessen Ebene (neben der Europäischen Union) die ganz überwiegende Mehrzahl von Berichtspflichten zu verorten ist – überlässt allerdings den einzelnen Ressorts die Entscheidung über die Inhalte der Rechtsverordnung.[13]

(2.) Aufhebung von Schriftformerfordernissen

Einen vergleichbaren Regelungsansatz verfolgt der Entwurf eines Dritten Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Aufhebung von Schriftformerfordernissen in Nordrhein-Westfalen[14].

Danach sollen zum 1.1.2027 sämtliche landesrechtliche Schriftformerfordernisse durch die Verwendung eines elektronischen Dokuments ersetzt werden können, soweit dies nicht in eine Rechtsverordnung der Landesregierung ausdrücklich ausgeschlossen wird.

Neu eingeführte Schriftformerfordernisse sollen ebenfalls in dieser Rechtsverordnung aufgenommen werden, sodass eine tagesaktuelle Liste der in Nordrhein-Westfalen geltenden Schriftformerfordernisse entsteht.

Entscheidend für den Erfolg, wird auch hier der Umfang der „Erhaltungs-Rechtsverordnung“ sein.

(3.) Erlasse als Bürokratietreiber

Einen nicht zu unterschätzenden Schwerpunkt legen das Zweite Gesetz zur Entlastung von Bürgern und Wirtschaft in NRW – Aussetzung von Berichts- und Dokumentationspflichten zu Lasten der Wirtschaft in Nordrhein-Westfalen sowie das Dritte Gesetz zur Entlastung von Bürgern und Wirtschaft in NRW – Aufhebung von Schriftformerfordernissen in Nordrhein-Westfalen auf Erlasse, die gleichfalls in den Geltungsbereich einbezogen werden.

Erlasse stellen ein zentrales Instrument der Exekutive dar, um den Vollzug von Gesetzen zu konkretisieren und zu ver-

5 Liminski/Roderburg, EuDIR 2026. 161.

6 LT-Drs. 18/19048, S. 4.

7 Liminski/Roderburg, EuDIR 2026. 161.

8 Liminski/Roderburg, EuDIR 2026. 161.

9 Liminski/Roderburg, EuDIR 2026. 161

10 Liminski/Roderburg, EuDIR 2026. 161.

11 Liminski/Roderburg, EuDIR 2026. 161.

12 LT-Drs. 18/20445.

13 Https://www.tagesschau.de/koalitionsausschuss-ergebnisse-102.pdf: „Wir werden ein Berichtsentlastungsgesetz verabschieden, durch das gesetzliche Berichtspflichten gegenüber staatlichen Stellen pauschal aufgehoben werden. Aufrechterhalten bleiben nur Pflichten, deren besondere Erforderlichkeit im Rahmen der Gesetzgebung zum Berichtsentlastungsgesetz seitens des jeweiligen Ministeriums explizit begründet wird (Beweislastumkehr) oder die mit entsprechender Begründung in Rechtsverordnungen des jeweils zuständigen Bundesministeriums als weiter geltend bestimmt werden. Das Gesetz sieht hierfür eine entsprechende Verordnungsermächtigung vor.“

14 LT-Drs. 18/20446.

einheitlichen. Gleichwohl können sie – abhängig von ihrer Ausgestaltung – zu Bürokratietreibern werden. Die Ursachen hierfür liegen vor allem in einer überschießenden Detailtiefe, die über das gesetzlich Erforderliche hinausgeht und zusätzliche Prüf-, Dokumentations- oder Verfahrenspflichten erzeugt. Vielfältig geschieht dies aus dem Antrieb, Regelungen praktikabel zu gestalten. Mitunter entsteht dieser Effekt aus einer Logik der Absicherung der Verwaltung: Um Rechtsfehler, Beanstandungen oder Haftungsrisiken zu vermeiden, werden Erlasse vorsorglich besonders umfassend formuliert.

Um diese Effekte zu reduzieren, sind verschiedene Lösungsmöglichkeiten erforderlich. Zukunftsgewandt zählt hierzu ein systematischer Goldplating Check[15]. Bezogen auf den Bestand erscheint es sinnvoll, die dargestellte Beweislastumkehr auch auf diesen Regelungstyp auszudehnen.

(4.) Verfahrensstand beider Gesetze

Beide Gesetzentwürfe wurden am 15.7.2026 in erster Lesung beim Landtag beraten und an den Hauptausschuss überwiesen. Eine gemeinsame Sachverständigenanhörung ist für den 15.9.2026 vorgesehen.[16]

bb) Umstellung bestimmter Evaluationspflichten auf ein anlassbezogenes System

Mit der Einfügung des § 23a in die Neufassung der Geschäftsordnung der Landesregierung wurde ein Moratorium im Hinblick auf Pflichten zur Evaluation von Rechtsverordnungen geschaffen. Die in Rechtsverordnungen vorgesehenen Pflichten der Ressorts zur Evaluation der jeweiligen Rechtsverordnung und der Bericht hierüber gegenüber der Landesregierung wird während des Moratoriums vollständig durch die Möglichkeit der Landesregierung ersetzt, entsprechende Berichte bei den Ressorts aus konkretem Anlass anzufordern. Die Änderung ist bereits in Kraft.

cc) Gewährleistung und Vereinfachung des Gemeingebrauchs

Der Entwurf eines Vierten Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Gesetz zur Gewährleistung und Vereinfachung des Gemeingebrauchs[17] soll es den Kommunen erleichtern, kommunale Einrichtungen für die Bürgerinnen und Bürger kostenfrei zur Verfügung zu stellen.

Vorgesehen ist eine Regelung in Gemeindeordnung und Kreisordnung, wonach die kostenfreie, freiwillige Nutzung kommunaler Einrichtungen grundsätzlich auf eigene Gefahr erfolgt. Nach der Gesetzesbegründung bleiben bestehende Verkehrssicherungspflichten unberührt; zugleich soll deren Umfang perspektivisch auf ein angemessenes Mindestmaß begrenzt werden.

Die nach § 35 Gemeinsame Geschäftsordnung für die Ministerien des Landes Nordrhein-Westfalen (GGO) vor der Einbringung in den Landtag vorgesehene Verbändeanhörung wurde durchgeführt.

dd) Maßnahmen zur „besseren Rechtsetzung"

Mit zwei Kabinettbeschlüssen vom 10.6.2026 hat die Landesregierung ein Maßnahmenpaket zur Verbesserung der Rechtsetzung in Nordrhein-Westfalen geschnürt. Ziel ist es, Qualität und Transparenz von Gesetzgebungsverfahren zu erhöhen.

Zur Verbesserung der Transparenz beitragen soll etwa die Veröffentlichung der im Rahmen von Verbändeanhörungen abgegebenen Stellungnahmen auf dem Portal „Beteiligung.NRW". Hinzu kommt die Prüfung, ob die Umstellung von Genehmigungs- in Anzeigeverfahren möglich ist oder Genehmigungsfiktionen eingesetzt werden können. Ergänzend soll ein One-in-one-out-Mechanismus zunächst testweise Anwendung finden. Eine Qualitätssteigerung soll u.a. durch einen ausdifferenzierteren Bürokratieabbau- und Digitalcheck sowie die verpflichtende Prüfung, ob bei neuen Gesetzen und Rechtsverordnungen Experimentierklauseln sinnvoll sind, erreicht werden.

ee) Regulatorische Vereinfachungen durch Reallabore

(1.) Erprobung der Verwaltungsvereinfachung in Kommunen

Mit dem Entwurf eines Ersten Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Erprobung der Verwaltungsvereinfachung in Kommunen in Nordrhein-Westfalen[18] – soll eine für bis zu vier Jahre befristete Freistellung von einzelnen Landesnormen beantragt werden können, um landesrechtliche Regelungen passgenau an den Verhältnissen vor Ort ausrichten zu können. Neben den Kommunen sind auch die kommunalen Spitzenverbände und der Landkreistag Nordrhein-Westfalen unter bestimmten Voraussetzungen antragsberechtigt.

Die Voraussetzungen für eine solche Freistellung sind vergleichsweise weit gefasst. Erforderlich ist lediglich, dass weder Unions-, Bundes- oder Landesrecht noch Rechte Dritter entgegenstehen. Eine Ausklammerung des materiellen Rechts enthält der Entwurf – anders als etwa das Bundeserprobungsgesetz – nicht. Hier zeigt sich ein unterschiedlicher Ansatz von Bund und Ländern. Während in einigen Ländern auch materielle Abweichungen im Rahmen von Erprobungsregelungen für verfassungsrechtlich zulässig gehalten werden, schätzt der Bund dies aktuell anders ein.

Über den Antrag soll die Landesregierung innerhalb von drei Monaten entscheiden. Liegen die gesetzlichen Voraussetzungen vor, soll der Antrag nur abgelehnt werden, wenn eine nicht anders abwendbare Gefahr für Leib und Leben von Menschen besteht oder überwiegende Belange des Gemeinwohls entgegenstehen.

Die Freistellung wirkt dabei für die antragstellende Kommune. Hat sich allerdings die antragstellende kommunale Körperschaft um die Ausrichtung der Olympischen und Paralympischen Spiele beworben, gilt die ihr erteilte Genehmigung auch für alle anderen kommunalen Körperschaften, die sich um die Ausrichtung der Olympischen und Paralympischen Spiele beworben haben, soweit ein Zusammenhang mit der Bewerbung oder Ausrichtung besteht.

15 Goldplating bezeichnet die Übererfüllung von EU oder Bundesrecht durch nationale oder untergesetzliche Vorgaben. Erlasse sind ein zentraler Mechanismus, über den Goldplating entsteht, weil sie häufig zusätzliche Anforderungen formulieren, die nicht zwingend aus der übergeordneten Norm folgen, aber im Vollzug verbindlich wirken. Dadurch entsteht eine „Regulierung zweiter Ordnung", die den gesetzgeberischen Willen übersteigt und den Vollzug unnötig belastet.

16 Https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMPT18-127.html; https://www.landtag.nrw.de/home/der-landtag/tagesordnungen/WP18/1800/E18-1842.html.

17 LT-Vorlage 18/5264.

18 LT-Drs. 18/20444.

Das Instrument dient nicht allein dazu, regulatorische Erleichterungen zu schaffen. Vielmehr geht es, worauf die Gesetzesbegründung ausdrücklich hinweist, auch um das regulatorische Lernen. So heißt es dort: „Ohne dass es einer ausdrücklichen gesetzlichen Regelung bedarf, wird das jeweils fachlich zuständige Ministerium die allgemeine Übertragbarkeit des Ergebnisses der Erprobung neuer Formen der Aufgabenerledigung auf die anderen Kommunen des Landes prüfen."[19]

Im Hinblick auf das „Gesetz zur Verbesserung der Rahmenbedingungen für die Erprobung von Innovationen in Reallaboren und zur Förderung des regulatorischen Lernens" des Bundes[20] enthält das Gesetz eine Öffnungsklausel. Sollte Bundesrecht künftig in einer Regelung eine Abweichung von Bundesrecht zulassen und insoweit in einem Verfahren zur Beantragung einer entsprechenden Abweichung eine einheitliche Antragstellung auf Grundlage vergleichbarer Landesgesetze zulassen, enthält das Erste Entlastungsgesetz bereits die landesrechtlichen Verfahrensregelungen.

Auch dieser Gesetzentwurf wurde am 15.7.2026 in erster Lesung beim Landtag beraten und an den Hauptausschuss überwiesen. Eine gemeinsame Sachverständigenanhörung mit den beiden anderen Entlastungsgesetzen ist für den 15.9.2026 vorgesehen.[21]

(2.) Gesetz für KI-Reallabore in Nordrhein-Westfalen

Der Entwurf eines Fünften Gesetzes zur Entlastung von Bürgern und Wirtschaft in NRW – Gesetz für KI-Reallabore in NRW[22] wird die landesrechtlichen Voraussetzungen für die Einrichtung und Durchführung von KI-Reallabore in NRW schaffen. Auch mit diesem Gesetz sollen die Möglichkeiten der regulatorischen Vereinfachung durch die Nutzung von Experimentierklauseln und Reallaboren nutzbar gemacht werden.

Der Entwurf unterscheidet sich von den weiteren Maßnahmen in den ersten drei Entlastungsgesetzen. Während die zuvor dargestellten Entlastungsgesetze vor allem auf den Abbau bestehender bürokratischer Anforderungen in Verwaltungsverfahren zielen, legt das Gesetz für KI-Reallabore einen etwas anderen Fokus: Es soll die Bedingungen, unter denen neue Technologien entwickelt und regulatorisch erprobt werden können, verbessern, insbesondere die Transformation von Forschungsprojekten in konkrete Vorhaben erleichtern.

Auch KI-Reallabore dienen nicht allein einer möglichen Reduzierung regulatorischer Belastungen. Daneben sollen sie die dabei gewonnen Erkenntnisse für eine Weiterentwicklung des Rechts nutzbar machen („regulatorisches Lernen"), Art. 57 Abs. 9 lit. d) KI-Verordnung.

II. Der Entwurf eines Gesetzes für KI-Reallabore in NRW

1. Entwurfstext

Art. 1
KI- Reallabor-Marktüberwachungsbehördengesetz NRW (KIMüG NRW)

§ 1
Anwendungsbereich

(1) Dieses Gesetz dient der Durchführung und Ergänzung der Verordnung (EU) 2024/1689 vom 13.6.2024 (ABl. L, 2024/1689, 12.7.2024;2024/90802, 9.10.2025), im Folgenden KI-Verordnung, sowie des Gesetzes zur Durchführung der Verordnung über Künstliche Intelligenz (KI-MIG). Es regelt die zuständige Marktüberwachungsbehörde gemäß Art. 70 Abs. 1 S. 1 der KI-Verordnung, die Einrichtung und den Betrieb von KI-Reallaboren im Sinne des Art. 57 der KI-Verordnung sowie die hierfür zuständige Behörde.

(2) Es gelten die Begriffsbestimmungen der KI-Verordnung.

§ 2
Zuständige Reallabor-Marktüberwachungsbehörde

(1) Das für Wirtschaft zuständige Ressort ist die zuständige KI-Reallabor-Marktüberwachungsbehörde für Künstliche Intelligenz-Reallabore in Nordrhein-Westfalen (im Folgenden: KI-Reallabor-Marktüberwachungsbehörde).

(2) Das für Wirtschaft zuständige Ressort nimmt die Aufgaben nach diesem Gesetz im Rahmen einer organisatorisch eigenständigen Einheit wahr. Die Einheit führt die Bezeichnung „KI-Marktüberwachungsstelle".

(3) Für sektorspezifische Bereiche sind die jeweils zuständigen KI-Reallabor-Marktüberwachungsbehörden einzubinden (Anhang 3 der KI-Verordnung). Die Landesmarktüberwachungsbehörden werden zur Mitwirkung verpflichtet.

(4) Die KI-Reallabor-Marktüberwachungsbehörde ist mit ausreichend qualifiziertem Personal auszustatten, das über Fachkenntnisse in den Bereichen Künstliche Intelligenz, Marktüberwachungsrecht und Datenschutz verfügt. Zudem ist die Unabhängigkeit der KI-Reallabor-Marktüberwachungsbehörde sicherzustellen.

§ 3
Aufgaben

(1) Die KI-Reallabor-Marktüberwachungsbehörde nimmt die Aufgaben einer Marktüberwachungsbehörde nach Maßgabe der KI-Verordnung wahr für KI-Systeme, die in einem KI-Reallabor nach Art. 57 der KI-Verordnung entwickelt, trainiert, validiert oder getestet werden. Hierzu gehören:

1. die Einrichtung des KI-Reallabors,
2. der Betrieb des KI-Reallabors,
3. Warnungs- und Informationspflichten
4. Beratung und Unterstützung.

(2) Die Behörde ist zuständige KI-Reallabor-Marktüberwachungsbehörde im Sinne des Art. 74 Abs. 1 der KI-Verordnung für KI-Systeme, die im Rahmen eines KI-Reallabors in Nordrhein-Westfalen erprobt werden.

(3) Die Behörde überwacht die Einhaltung der Vorschriften der KI-Verordnung durch Anbieter und Betreiber von KI-Systemen im KI-Reallabor.

(4) Die Behörde kooperiert mit anderen Marktüberwachungsbehörden des Bundes und der Länder, mit dem Europäischen Amt für Künstliche Intelligenz, mit notifizierten Stellen sowie mit den Datenschutzaufsichtsbehörden.

19 LT-Drs. 18/20444, S. 20.

20 BT-Drs. 21/218.

21 Https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMPT18-127.html; https://www.landtag.nrw.de/home/der-landtag/tagesordnungen/WP18/1800/E18-1842.html.

22 LT-Vorlage 18/5264.

§ 4
Datenschutzbeauftragte oder Datenschutzbeauftragter für KI-Reallabore

(1) Die Landesregierung benennt den oder die Datenschutzbeauftragte für KI-Reallabore. Dabei soll der Aspekt der Vermeidung zusätzlicher Bürokratie berücksichtigt werden. Die Ausstattung und Finanzierung entspricht den Anforderungen des Art. 52 Abs. 4 der Verordnung (EU) 2016/679 vom 27.4.2016 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35), im Folgenden Datenschutz-Grundverordnung. Das Nähere regelt eine Rechtsverordnung der Landesregierung.

(2) Die Datenschutzbeauftragte oder der Datenschutzbeauftragte für KI-Reallabore ist zuständige Aufsichtsbehörde im Sinne von Art. 51 der Verordnung (EU) 2016/679 für die Überwachung der Einhaltung der Datenschutzvorschriften bei der Verarbeitung personenbezogener Daten in KI-Reallaboren im Sinne von Art. 57 der KI-Verordnung und tritt damit an die Stelle der oder der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen (LDI).

(3) Die oder der Datenschutzbeauftragte für KI-Reallabore wird an allen wesentlichen Entscheidungen der KI- Reallabor-Marktüberwachungsbehörde beteiligt, die Datenschutzaspekte berühren. Sie oder er ist berechtigt, an den Sitzungen der KI- Reallabor-Marktüberwachungsbehörde mit beratender Stimme teilzunehmen. Die oder der Datenschutzbeauftragte für KI-Reallabore hat insbesondere folgende Aufgaben:

1. Beratung der KI- Reallabor-Marktüberwachungsbehörde in allen Datenschutzfragen im Zusammenhang mit KI-Reallaboren,
2. Prüfung der Vereinbarkeit von KI-Systemen und Testvorhaben mit den datenschutzrechtlichen Vorschriften,
3. Unterstützung bei der Anwendung des Art. 59 der KI-Verordnung,
4. Zusammenarbeit mit den Datenschutzaufsichtsbehörden des Bundes und der Länder,
5. Erstellung von Stellungnahmen und Empfehlungen zur datenschutzkonformen Gestaltung von KI-Reallaboren oder
6. jährliche Erstellung eines Tätigkeitsberichts zur Vorlage an die Landesregierung und den Landtag.

Die oder der Datenschutzbeauftragte kann sich mit anderen für die Datenschutzaufsicht bei KI-Reallaboren zuständigen Stellen, auch in anderen Mitgliedstaaten, austauschen, um eine einheitliche Anwendung der Datenschutzvorschriften zu fördern.

(4) Die oder der Datenschutzbeauftragte für KI-Reallabore ist befugt:

1. von den Betreibern der KI-Reallabore sowie den Teilnehmern an den KI-Reallaboren alle für die Aufgabenerfüllung erforderlichen Informationen zu verlangen (Betreiber und Teilnehmer sind verpflichtet, diese Auskünfte zu erteilen und Einsicht zu gewähren),
2. Einsicht in alle Unterlagen, Akten und Aufzeichnungen zu nehmen, die die Verarbeitung personenbezogener Daten in KI-Reallaboren betreffen,
3. an allen Sitzungen und Besprechungen teilzunehmen, die datenschutzrechtliche Aspekte bei der Einrichtung und dem Betrieb von KI-Reallaboren betreffen oder
4. Empfehlungen zur Verbesserung des Datenschutzes in KI-Reallaboren auszusprechen.

(5) Die oder der Datenschutzbeauftragte für KI-Reallabore muss über besondere Fachkenntnisse und praktische Erfahrungen im Zusammenhang mit KI-Systemen sowie im Datenschutzrecht, insbesondere in der Anwendung der Verordnung (EU) 2016/679 auf KI-Systeme verfügen.

§ 5
Zusammenarbeit mit privaten Betreibern von KI-Reallaboren

(1) Die KI-Reallabor-Marktüberwachungsbehörde kann private Betreiber von KI-Reallaboren mit der Durchführung von Aufgaben nach diesem Gesetz betrauen.

(2) Die Betrauung erfolgt durch öffentlich-rechtlichen Vertrag. Der Vertrag muss insbesondere Regelungen enthalten über:

1. den Umfang der übertragenen Aufgaben,
2. die Befugnisse und Pflichten des privaten Betreibers,
3. die Aufsicht und Weisungsbefugnis der KI-Reallabor-Marktüberwachungsbehörde,
4. die Berichtspflichten des privaten Betreibers,
5. die Datenschutzbestimmungen unter Einbeziehung der Datenschutzbeauftragten oder des Datenschutzbeauftragten für KI-Reallabore gemäß § 4 und
6. die Haftung.

(3) Der private Betreiber unterliegt der Aufsicht der KI- Reallabor-Marktüberwachungsbehörde. Er ist verpflichtet, deren Weisungen nachzukommen.

(4) Die KI-Reallabor-Marktüberwachungsbehörde kann sich jederzeit durch Beauftragte davon überzeugen, dass der private Betreiber die übertragenen Aufgaben ordnungsgemäß erfüllt.

§ 6
Bewerbungsverfahren und Auswahlkriterien

(1) Die Auswahl der Teilnehmer am KI-Reallabor erfolgt durch eine Auswahlkommission, die aus Vertretern der Marktüberwachungsstelle, der Datenschutzbeauftragten oder dem Datenschutzbeauftragten für KI-Reallabore und dem Betreiber des KI-Reallabors besteht. Die Marktüberwachungsstelle entscheidet über die Zulassung. Die Auswahl an den KI-Reallaboren erfolgt auf der Grundlage der folgenden Kriterien:

1. Innovationsgrad,
2. Relevanz für den Markt,
3. Konformitätspotenzial,
4. Risikominimierung,
5. Datenschutzverträglichkeit,
6. Unternehmensgröße,
7. Ressourcen und Kompetenz und
8. Zusammenarbeit

(2) Die Auswahlkriterien sind in ihrer Gesamtheit zu gewichten. Die vorrangige Berücksichtigung von kleinen und mittleren Unternehmen nach Art. 62 Abs. 1 lit. a) der KI-Verordnung ist bei der Gewichtung maßgeblich zu berücksichtigen. Bei im Übrigen gleichwertigen Eignungen ist einer Antragstellerin oder einem Antragsteller, die oder der ein kleines oder mittleres Unternehmen im Sinne von Art. 2 Nummer 23 der KI-Verordnung ist, der Vorrang zu geben.

(3) Die Bewerbung um die Teilnahme an einem KI-Reallabor erfolgt schriftlich oder elektronisch gegenüber der KI-

Reallabor-Marktüberwachungsbehörde. Es ist das von der KI-Reallabor-Marktüberwachungsbehörde zur Verfügung gestellte Antragsformular zu verwenden. Der Antrag muss folgende Informationen enthalten:

1. Angaben zum Antragsteller, wie Name, Rechtsform, Sitz und Unternehmensgröße,
2. Beschreibung des KI-Systems und des geplanten Anwendungsfalls,
3. Darlegung der Erfüllung der Auswahlkriterien nach Abs. 1,
4. Zeitplan für die Entwicklung, das Training, das Testen und die Validierung des KI-Systems,
5. Angaben zu den geplanten Ressourcen und zur Zusammenarbeit mit lokalen Partnern,
6. Konzept zur Datenschutzverträglichkeit und
7. Nachweis über die Möglichkeit zur regelmäßigen physischen Präsenz am Projektstandort.

(5) Die Auswahlkommission entscheidet über den Antrag innerhalb von drei Monaten nach Eingang der vollständigen Unterlagen. Die Frist kann einmal um bis zu zwei Monate verlängert werden, wenn dies zur Prüfung des Antrags erforderlich ist.

(6) Die Entscheidung über die Teilnahme ist der Antragstellerin oder dem Antragsteller schriftlich oder elektronisch mitzuteilen und zu begründen. Bei Ablehnung ist die Antragstellerin oder der Antragsteller auf die Möglichkeit der erneuten Antragstellung hinzuweisen.

(7) Die Teilnahme an einem KI-Reallabor wird für einen begrenzten Zeitraum, in der Regel von bis zu zwei Jahren, gewährt. Eine Verlängerung ist möglich, wenn dies zur Erreichung der Ziele des KI-Reallabors erforderlich ist und die Voraussetzungen für die Teilnahme weiterhin vorliegen.

(8) Der KI-Reallaborbetreiber führt ein öffentlich zugängliches Verzeichnis der Teilnehmer an den KI-Reallaboren. Das Verzeichnis enthält die Namen der Antragsteller, eine Kurzbeschreibung der Projekte und die Dauer der Teilnahme.

§ 7
Befugnisse

(1) Die KI-Reallabor-Marktüberwachungsbehörde und die von ihr beauftragten Personen haben die Befugnisse gemäß Art. 14 Abs. 4 und 5 der Verordnung (EU) 2019/1020 vom 20.6.2019 (ABl. L 169 vom 25.6.20219, S. 1; L, 2024/90589, 1.10.2024), die zuletzt durch Verordnung vom 11.4.2024 (ABl. L, 2024/1252, 3.5.2024) geändert worden ist (§ 7 des Marktüberwachungsgesetzes vom 9.6.2021 (BGBl. I S. 1723). Die Befugnisse bestehen auch gegenüber privaten Betreibern von KI-Reallaboren.

(2) Die Befugnisse nach Art. 14 Abs. 4 lit. e) der Verordnung (EU) 2019/1020 bestehen zu den üblichen Betriebs- und Geschäftszeiten, außerhalb der dort genannten Zeiten nur zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung. Das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 des Grundgesetzes) wird insoweit eingeschränkt.

(3) Die KI-Reallabor-Marktüberwachungsbehörde kann bei den Wirtschaftsakteuren für KI-Systeme im Sinne der KI-Verordnung Proben der betreffenden Systeme entnehmen, Muster verlangen und die für ihre Aufgabenerfüllung erforderlichen Unterlagen und Informationen anfordern (§ 7 des Marküberwachungsgesetzes).

(4) Die Behörde kann im Rahmen der geltenden Gesetze zum Zwecke der Risikobewertung und der Identifikation gefährlicher KI-Systeme öffentlich zugängliche Informationen ohne Personenbezug auf Online-Schnittstellen automatisiert sammeln und analysieren (§ 7 des Marküberwachungsgesetzes).

(5) Die KI-Reallabor-Marktüberwachungsbehörde koordiniert die Zusammenarbeit mit anderen Marktüberwachungsbehörden, soweit diese für die Durchsetzung der KI-Verordnung zuständig sind. Sie kann andere Marktüberwachungsbehörden zur Mitwirkung anweisen, soweit dies zur wirksamen Durchsetzung der KI-Verordnung erforderlich ist. Die Anweisungsbefugnis umfasst insbesondere die:

1. Anordnung, Untersuchungen an KI-Systemen durchzuführen, die in einem KI-Reallabor entwickelt, trainiert, getestet oder validiert werden;
2. Anordnung, die Konformität eines KI-Systems mit den Anforderungen der KI-Verordnung zu prüfen, insbesondere mit den Art. 57, 59 und 60 der KI-Verordnung;
3. Anordnung, an gemeinsamen Untersuchungen von KI-Systemen in KI-Reallaboren teilzunehmen oder
4. Anordnung, an gemeinsamen Bewertungen der Wirksamkeit von Schutzvorkehrungen in KI-Reallaboren teilzunehmen.

§ 8
Überwachung des KI-Reallabors

(1) Die KI-Reallabor-Marktüberwachungsbehörde überwacht den Betrieb des KI-Reallabors, um sicherzustellen, dass die Erprobung von KI-Systemen unter Einhaltung der Vorschriften der KI-Verordnung und der datenschutzrechtlichen Bestimmungen erfolgt.

(2) Sie kann insbesondere:

1. die Zulassung von Teilnehmern am KI-Reallabor genehmigen oder versagen,
2. die Einhaltung der Voraussetzungen für die Teilnahme überwachen,
3. Maßnahmen zur Sicherstellung der Konformität anordnen,
4. bei Verstößen gegen die KI-Verordnung die Zusammenarbeit mit der Datenschutzbeauftragten oder dem Datenschutzbeauftragten gemäß § 4 veranlassen oder
5. bei Verstößen gegen die KI-Verordnung geeignete Maßnahmen ergreifen.

(3) Die Überwachung erfolgt unter Berücksichtigung der in Art. 58 der KI-Verordnung festgelegten Grundsätze, insbesondere der Vorrangigkeit des Zugangs für kleine und mittlere Unternehmen.

(4) Bei Entscheidungen, die die Verwendung personenbezogener Daten betreffen, ist die Datenschutzbeauftragte oder der Datenschutzbeauftragte für KI-Reallabore gemäß § 4 zwingend zu beteiligen.

(5) Eine Überwachung der oder des Datenschutzbeauftragten für KI-Reallabore erfolgt nicht; ausgenommen ist die Überwachung durch den Landesrechnungshof, soweit nicht die Unabhängigkeit der oder des Datenschutzbeauftragten für KI-Reallabore beeinträchtigt wird.

§ 9
Zusammenarbeit und Informationsaustausch

(1) Die KI-Reallabor-Marktüberwachungsbehörde arbeitet mit anderen zuständigen Behörden auf Landes-, Bundes- und Unionsebene zusammen.

(2) Sie unterrichtet die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin im Sinne des § 17 des Marküberwachungsgesetzes über Maßnahmen nach Art. 16 Abs. 5 der Verordnung (EU) 2019/1020.

(3) Die Behörde wirkt im Deutschen Marktüberwachungsforum mit (§ 13 des Marküberwachungsgesetzes).

(4) Die Zusammenarbeit mit den Datenschutzaufsichtsbehörden erfolgt unter Beteiligung der Datenschutzbeauftragten oder des Datenschutzbeauftragten für KI-Reallabore gemäß § 4.

§ 10
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Art. 2
Änderung des Landesorganisationsgesetzes

Das Landesorganisationsgesetz des Landes Nordrhein-Westfalen vom 10.7.1962 (GV. NRW. S. 213), das zuletzt durch Art. 3 des Gesetzes vom 10.7.2025 (GV. NRW. S. 646) geändert worden ist, wird wie folgt geändert:

Nach § 9 wird der folgende § 9a eingefügt:

„§ 9a
KI-Reallabor-Marktüberwachungsstelle

(1) Im für Wirtschaft zuständigen Ministerium wird die KI-Reallabor-Marktüberwachungsstelle als organisatorisch eigenständige Einheit zur Wahrnehmung der Aufgaben nach dem KI-Reallabor-Marktüberwachungsbehördengesetz NRW vom [einsetzen:

Ausfertigungsdatum und Fundstelle dieses Gesetzes] eingerichtet.

(2) Die KI-Reallabor-Marktüberwachungsstelle untersteht der Fachaufsicht des für Wirtschaft zuständigen Ministeriums.

Art. 3
Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

2. Erläuterungen

Gemäß Art. 5 Nr. 55 KI-VO ist ein „KI-Reallabor" ein kontrollierter Rahmen, der von einer zuständigen Behörde geschaffen wird und (zukünftige) Anbieter oder Anbieterinnen von KI-Systemen nach einem Plan für das Reallabor einen begrenzten Zeitraum und unter regulatorischer Aufsicht nutzen können, um ein innovatives KI-System zu entwickeln, zu trainieren, zu validieren und – gegebenenfalls unter Realbedingungen – zu testen.

Art. 57 KI-VO verpflichtet jeden Mitgliedstaat dazu, bis zum 2.8.2026, mindestens ein KI-Reallabor auf nationaler Ebene einzurichten; durch die EU-Omnibus-Verordnung wurde diese Frist bis August 2027 verlängert.

Die Einrichtung und der Betrieb von KI-Reallaboren muss gemäß Art. 57 Abs. 1 i.V.m. Art. 70 KI-VO durch die zuständige nationale Behörde erfolgen; dies muss gemäß Art. 3 Nr. 48 eine notifizierende Behörde oder eine Marktüberwachungsbehörde sein.

Auf Bundesebene dient das deutsche KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG), das am 29.7.2026 in Kraft getreten ist, der nationalen Durchführung der KI-VO. Das Gesetz konzentriert sich auf die institutionellen und verfahrensrechtlichen Grundlagen der KI-Überwachung in Deutschland. Die Bundesnetzagentur (BNetzA) fungiert als zentrale Marktüberwachungsbehörde und nationale Anlaufstelle. Sektorspezifische Aufsichten bleiben bestehen; so überwacht beispielsweise die BaFin KI-Systeme im Finanzsektor. Bei der BNetzA wird das Koordinierungs- und Kompetenzzentrum (KoKIVO) eingerichtet, um die Zusammenarbeit der Behörden zu bündeln. Die BNetzA wird auch ein KI-Reallabor einrichten. Auf die Teilnahme an dem Labor können sich Betreiberinnen und Betreiber von KI-Systemen bewerben, um Unterstützung bezüglich der rechtskonformen Ausgestaltung ihres KI-Systems zu erhalten.

Das Instrument der KI-Reallabore wird als ein zentrales Innovationsinstrument gesehen, auch um eine angemessene Anwendung der DS-GVO zu erreichen. Da eine Anonymisierung von Daten in Zeiten von „Big Data" kaum zu erreichen ist[23], unterliegt das Training von KI nahezu stets der DS-GVO. Die entsprechenden Anforderungen sind oftmals unerfüllbar, das KI-Training damit erheblich erschwert[24]. Auf die hieraus folgende zwingende Notwendigkeit solche Labore für die medizinische Forschung hat etwa der diesjährige Träger des Krebspreises Professor Felix Sahm öffentlich hingewiesen und sich einem breit getragenen Appell, die Einrichtung solcher Labore auch für die Länder zu ermöglichen, angeschlossen.[25] Mit verfasst wurde dieser Appell, der sich auch auf Zugangsmöglichkeiten privater Akteurinnen und Akteure zu solchen Laboren bezieht auch durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, Professor Tobias Keber.[26]

Um die Gratwanderung landesrechtlicher Regelungsmöglichkeiten zwischen EU- und Bundesrecht erfolgreich zu bestehen, hat Nordrhein-Westfalen den Expertenrat „KI und Staatsmodernisierung" eingerichtet, dem Professor Rolf Schwartmann vorsitzt und u.a. Professor Felix Sahm sowie die Co-Autoren dieses Beitrags angehören.[27] Im Juni 2026 hat die Landesregierung Nordrhein-Westfalens die Einbringung eines Gesetzes für KI-Reallabore in NRW in die Verbändeanhörung beschlossen.[28]

Nordrhein-Westfalen als wichtiger Wirtschaftsstandort Deutschlands und als Zentrum der KI-Forschung und -entwicklung hat ein besonderes Interesse daran, die Innovationskraft im Bereich künstlicher Intelligenz zu stärken und gleichzeitig einen hohen Schutzstandard für Grundrechte, insbesondere den Datenschutz, zu gewährleisten.

23 Vgl. OLG Köln, vom 23.5.2025 – I-15 UKl 2/25-, juris, Rn. 73.

24 Vgl. Roderburg, RDV Sonderheft/2025, 15, auch zu den Folgen für die Innovationsfähigkeit.

25 Grzeszick/Keber/Krings/Roderburg/Sahm/Schwartmann/Voss/Zenner, FAZ 27.4.2026, S. 19.

26 Grzeszick/Keber/Krings/Roderburg/Sahm/Schwartmann/Voss/Zenner, FAZ 27.4.2026, S. 19.

27 Liminski/Roderburg, EuDIR 2026. 161, 162.

28 Https://www.land.nrw/pressemitteilung/landesregierung-beschliesst-weitere-entlastungen-zur-modernisierung-des-staates.

Die Entscheidung der Landesregierung, als erstes Bundesland ein solches Spezialgesetz vorzulegen, folgt einer klaren wirtschafts-, innovations- und rechtspolitischen Strategie:

Start-ups und Großunternehmen wandern in Jurisdiktionen ab, die laxere Datenschutz- und Haftungsregeln bieten (z.B. USA). NRW will hier ein Gegengewicht setzen. Das Land zeigt, dass europäische Werte (DS-GVO, AI Act) und Innovationsgeschwindigkeit kein Widerspruch sein müssen, wenn man die rechtlichen Spielräume intelligent nutzt.

Durch das Inkrafttreten der KI-VO entsteht auf nationaler Ebene ein akuter Umsetzungsbedarf. NRW nutzt die Gunst der Stunde, um durch ein schnelles Handeln rechtssichere Erprobungsräume zu generieren.

Die Entwicklung von KI-Systemen und das Training von KI-Modellen erfordert den Zugriff auf enorme, hochwertige Datenmengen. In Europa ist die Verarbeitung personenbezogener Daten streng durch die DS-GVO reglementiert. Dies erschwert vor allem das Training von KI-Modellen nachhaltig.

Die KI-VO sieht in Art. 59 vor, dass rechtmäßig für andere Zwecke erhobene personenbezogene Daten im KI-Reallabor für die Zwecke der Entwicklung, des Trainings und des Testens bestimmter KI-Systeme im Reallabor verarbeitet werden, können, wenn die dort normierten Bedingungen erfüllt sind. Vor allem muss das KI-System zur Wahrung eines erheblichen öffentlichen Interesses entwickelt werden. Dazu zählen:

- öffentliche Sicherheit und öffentliche Gesundheit, einschließlich Erkennung, Diagnose, Verhütung, Bekämpfung und Behandlung von Krankheiten sowie Verbesserung von Gesundheitsversorgungssystemen;
- hohes Umweltschutzniveau und Verbesserung der Umweltqualität, Schutz der biologischen Vielfalt, Schutz gegen Umweltverschmutzung, Maßnahmen für den grünen Wandel sowie Klimaschutz und Anpassung an den Klimawandel;
- nachhaltige Energie;
- Sicherheit und Widerstandsfähigkeit von Verkehrssystemen und Mobilität, kritischen Infrastrukturen und Netzen;
- Effizienz und Qualität der öffentlichen Verwaltung und öffentlicher Dienste.

Auf Bundesebene ist noch nicht final entschieden, wie die in Art. 59 normierte, für die KI-Entwicklung essenzielle, Möglichkeit genutzt werden kann. In Nordrhein-Westfalen soll ein KI-Reallabor mit entsprechender Infrastruktur geschaffen werden, in dem diese durch die KI-VO eröffnete begrenzte „Modifizierung" der DS-GVO zum datengestützten Training von KI-Systemen ermöglicht werden.

NRW befürchtet, dass durch die Zuständigkeit der BNetzA ein „Flaschenhals" entsteht, der die Länder – vor allem mit Blick auf die begrenzten BNetzA-Kapazitäten – bei der Einrichtung eigener KI-Reallabore handlungsunfähig machen könnte. Daher hält NRW es für erforderlich, einen ländereigenen Ansatz zur Einrichtung von KI-Reallaboren zu verfolgen.

Die EU-Verordnung sieht zwar vor, dass auch auf regionaler und lokaler Ebene weitere Reallabore betrieben werden dürfen. Es ist aber nicht ausgeschlossen, dass Art. 57 Abs. 2 der KI-Verordnung so gelesen wird, dass dies nur „zuständige [nationale] Behörden" dürfen. Zwar findet sich im Abs. 2 keine Bezugnahme auf „zuständige Behörden". Aufgrund des Zusammenhangs zu Abs. 1, der diese Bezugnahme ausdrücklich enthält, liegt eine solche Auslegung aber sehr nahe. Zudem wäre sonst europarechtlich völlig offen, wer die regionalen oder lokalen Labore einrichten darf. Zuständige nationale Behörden sind u.a. die sog. Marktüberwachungsbehörden (Art. 3 Nr. 48). Wer dies im nationalen Recht ist, regelt § 2 des KI-MIG. Insoweit lautet § 2 Abs. 6: „Für die Fälle, in denen öffentliche Stellen der Länder im Sinne des § 2 Abs. 2 und 3 des Bundesdatenschutzgesetzes […], KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden, obliegt die Marktüberwachung den nach Landesrecht zuständigen Behörden." Daraus lässt sich mit großer Sicherheit schlussfolgern, dass jede Behörde im Sinne des § 2 Abs. KI-MIG ein solches Reallabor einrichten darf.

Final gesichert ist eine solche Auslegung indessen nicht. § 2 Abs. 6 wurde ausweislich der Gesetzesbegründung auch in Abänderung des Referentenentwurfs nicht eingeführt, um KI-Reallabore zu ermöglichen, sondern aus kompetenzrechtlichen Gründen:[29] „Grund hierfür ist, dass öffentliche Stellen der Länder wegen der Eigenstaatlichkeit der Länder nicht durch eine Bundesbehörde beaufsichtigt werden dürfen." Insbesondere auch auf Betreiben von NRW hat der Bundesrat daher mit großer Mehrheit einen Antrag mit ganz konkreten Gesetzesänderungen beschlossen, die für Rechtssicherheit sorgen würden.[30] In seiner Gegenäußerung[31] erkennt die Bundesregierung zwar das geschilderte Anliegen der Länder an, solche Labore einzurichten, lehnt dessen rechtstechnische Umsetzung aber ab, ohne das hier geschilderte Problem zu adressieren. Damit verbleibt es bei der geschilderten Unsicherheit. Wie bei vielen Projekten der Staatsmodernisierung bewegt der Gesetzgeber sich im rechtlichen Neuland, sodass eine nicht vollständige Sicherheit abwägend hinzunehmen ist.[32]

Auch für das regionale KI-Reallabor muss also eine zuständige Marktüberwachungsbehörde bestehen, die das KI-Reallabor überwacht und es muss sichergestellt sein, dass – bei diesen sensiblen, datenschutzrelevanten Vorhaben, eine enge Zusammenarbeit mit der zuständigen Datenschutzaufsicht erfolgt. Das KIMüG NRW schafft diese – bisher fehlenden – Strukturen in Nordrhein-Westfalen.

Gem. § 2 KIMüG NRW entsteht im für Wirtschaft zuständigen Ressort die zuständige Stelle für KI-Reallabor-Marktüberwachung für Künstliche Intelligenz-Reallabore in Nordrhein-Westfalen. Diese Stelle wird dafür zuständig sein, das KI-Reallabor einzurichten, zu betreiben, Warnungs- und Informationspflichten nachzukommen, sowie zu beraten und zu informieren (vgl. § 3 KIMüG NRW).

Zudem soll es eine oder einen spezifische/n Datenschutzbeauftragte/n für KI-Reallabore geben, der eng mit der Marktaufsichtsbehörde zusammenarbeitet und bei der oder dem spezifisches Know-How im Hinblick auf Systeme Künstlicher Intelligenz und Datenschutz gebündelt werden. Ob diese

29 BT- Drs. 21/4594, S. 51.

30 Ziff. 2 der BR-Drs. 97/26 (B).

31 BT-Drs. 21/5143.

32 Vgl. zu diesem Aspekt der Staatsmodernisierung: Liminski/Roderburg, EuDIR 2026. 161, 162.

Aufgabe am besten durch die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW) oder durch eine andere geeignete Stelle ausgeübt werden sollte, wird mittels der Rückmeldungen zur Verbändeanhörung ausgewertet.

Gemäß § 5 KIMüG NRW kann die KI-Reallabor-Marktüberwachungsbehörde private Betreiberinnen und Betreiber von KI-Reallaboren mit der Durchführung von Aufgaben nach diesem Gesetz betrauen. Auch hier sollen nach Vorstellung des Gesetzgebers keine neuen Strukturen geschaffen werden; vielmehr existieren in Nordrhein-Westfalen bereits eine Vielzahl geeigneter Initiativen und Vorhaben, die in Betracht kämen. Es ist wichtig, dass die Fäden nun zusammengeführt werden und ein zentrales KI-Reallabor in Nordrhein-Westfalen entsteht, auf das die Entwicklerinnen und Entwickler von KI-Systemen zugreifen können.

Hierfür müssen sie sich – wie in § 6 KIMüG NRW dargestellt – auf die Mitwirkung im KI-Reallabor bewerben. Entscheidend für den Zutritt sind Kriterien wie: Innovationsgrad, Relevanz für den Markt, Konformitätspotenzial, Risikominimierung, Datenschutzverträglichkeit, Unternehmensgröße (denn KMU und Start-ups haben prioritären Zugang), Ressourcen und Kompetenz sowie Zusammenarbeit.

Die Zusammenarbeit und der Informationsaustausch mit anderen zuständigen Behörden auf Landes-, Bundes- und Unionsebene wird in § 9 KIMüG NRW normiert.

Auf diese Weise gliedert sich das NRW-KI-Reallabor in die europäischen Strukturen ein und es ist ein effektives Zusammenspiel zwischen den unterschiedlichen Behörden sichergestellt.

3. Abgrenzung KI-Reallabor von KI-Reallabor nach KI-VO

Herkömmliche Experimentierräume, wie sie beispielsweise die Bundes- und Landesregierungen im Zuge von Bürokratieabbaugesetzen etablieren, bewegen sich im Rahmen nationaler Kompetenzen. Sie gewähren Erleichterungen oder zeitlich begrenzte Ausnahmen von nationalen (Verwaltungs-) Vorschriften, können aber das zwingende Unionsrecht – insbesondere das strenge Regime der DS-GVO – nicht modifizieren oder suspendieren.

Ein KI-Reallabor nach der KI-VO ist ein europarechtlich institutionalisiertes Instrument, das im gesamten EU-Binnenmarkt Anerkennung genießt. Werden KI-Systeme in einem solchen staatlich eingerichteten Reallabor entwickelt und erfolgreich getestet, kann dies ein wesentlicher Schritt zur Beschleunigung der Erlangung der Marktzulassung sein: Gemäß Art. 57 Abs. 7 erhalten (zukünftige) Anbieterinnen oder Anbieter eines KI-Systems von der zuständigen Behörde einen schriftlichen Nachweis sowie einen Abschlussbericht. Die Unterlagen erhalten Informationen über die im Reallabor durchgeführten Tätigkeiten, deren Ergebnisse und die gewonnenen Erkenntnisse. Die Anbieterinnen und Anbieter können diese Unterlagen nutzen, um im Rahmen des Konformitätsbewertungsverfahrens oder einschlägiger Marktüberwachungstätigkeiten nachzuweisen, dass sie dieser Verordnung nachkommen. Im Hinblick auf eine Beschleunigung der Konformitätsbewertungsverfahren werden die Unterlagen in angemessenem Maße positiv gewertet.

Das KIMüG NRW greift gezielt auf die unionsrechtliche Ermächtigung des Art. 59 KI-VO zurück. Diese Norm fungiert als datenschutzrechtlicher Game Changer: Sie erlaubt es den Mitgliedstaaten unter strikten Voraussetzungen, den sonst rigiden Zweckwechsel von Daten ausnahmsweise zu durchbrechen. Das KIMüG NRW operationalisiert diese europarechtlichen Optionen, indem es konkretisiert, wie und wann personenbezogene Daten, die ursprünglich für andere Zwecke erhoben wurden, im Rahmen des Reallabors für das Training von KI-Modellen verarbeitet werden dürfen. Erst durch den Rückgriff auf Art. 59 KI-VO erlangt das Landesgesetz die Kompetenz, die Brücke zwischen Datenschutz und technologischer Innovation unionsrechtskonform zu schlagen.

Jennifer Gerwing
ist Referentin für das Recht der digitalen Wirtschaft im Referat 514 „Justiziariat" im Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen.

Dr. iur Harald Hemmer
ist Leiter der Zentralabteilung der Staatskanzlei NRW, damit zuständig für Verfahren Landesgesetzgesetzgebung sowie – in einer eigenständigen Gruppe verortet – die Prozesse der Staatsmodernisierung, der Verwaltungsmodernisierung und des Bürokratieabbaus.

Dr. iur Dominik Roderburg
ist Richter am Oberlandesgericht Köln, derzeit abgeordnet als Leiter des Referats Z A 2 „Staatsmodernisierung" an die Staatskanzlei NRW, wissenschaftlicher Mitarbeiter am Bundesverfassungsgericht bei Bundesverfassungsrichterin Dr. Sibylle Kessal-Wulf von 2016 bis 2018, Rechtsanwalt, Fachanwalt für Steuerrecht und Steuerberater bis 2012.

Dr. Judith Nink

Cybersicherheitsregulierung nach NIS-2: Chance oder bürokratische Überforderung?

Die Umsetzung der NIS-2-Richtlinie durch das BSIG bringt für betroffene Einrichtungen eine Vielzahl neuer Pflichten mit sich, die in der Praxis teilweise als erheblicher bürokratischer Aufwand wahrgenommen werden. Der Beitrag untersucht, ob diese Pflichten tatsächlich eine unnötige Belastung darstellen oder vielmehr einen wesentlichen Beitrag zur Erhöhung der Cyberresilienz leisten. Ausgehend von der zunehmenden Bedrohungslage und den erheblichen wirtschaftlichen und gesellschaftlichen Schäden durch Cyberangriffe werden Pflichten in den Kontext der beabsichtigten Regulierungsziele gesetzt. Dabei zeigt sich, dass die Pflichten untereinander eng miteinander verzahnt sind und auf die Ziele der NIS-2-Richtlinie einzahlen. Der Beitrag kommt zu dem Ergebnis, dass die NIS-2-Vorgaben trotz des mit ihrer Umsetzung verbundenen Aufwands nicht als bloße Bürokratie verstanden werden sollten. Vielmehr bilden sie einen wesentlichen Bestandteil einer resilienten Sicherheitsarchitektur für Gesellschaft und Wirtschaft und können gerade für die betroffenen Unternehmen einen wichtigen Beitrag zur Vermeidung existenzbedrohender Schäden leisten.

I. Einleitung

Knapp ein Jahr nach dem Inkrafttreten des NIS-2-Umsetzungsgesetzes[1] am 6.12.2025 ist ein guter Zeitpunkt für einen genaueren Blick, ob und inwieweit die damit verbundenen Pflichten für betroffene Einrichtungen geeignet sind, die beabsichtigten Ziele zu erreichen oder diese nur bürokratisch belasten.

Besonders wichtige Einrichtungen sollen durch die Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („NIS-2-Richtlinie" (RL (EU) 2022/2555))[2] resilienter gegen Cyberangriffe werden und dadurch Cyberangriffe verhindert, Angreifer abgeschreckt und die Reaktionsfähigkeiten auf Angriffe verbessert werden.[3] Herzstück der Regulierung zur Erreichung der Ziele sind dabei die Risikomanagementmaßnahmen, die betroffene Einrichtungen umsetzen müssen, § 30 BSIG (II. 1.), flankiert u.a. durch ein fristengebundenes gestuftes Melderegime für erhebliche Sicherheitsvorfälle, § 32 BSIG (II. 2.), die Pflicht zur Registrierung beim BSI, §§ 33, 34 BSG (II. 3.), sowie der expliziten Verpflichtung der Leitungsebene, §§ 38, 43 BSIG (II. 4.). Betroffene Einrichtungen müssen zudem die Einhaltung ihrer Pflichten dokumentieren, §§ 30 Abs. 1 S. 3 BSIG, und nachweisen, § 39 BSIG (für Betreiber kritischer Anlagen), § 61 Abs. 3 BSIG (besonders wichtige Einrichtungen auf Anordnung), § 62 i.V.m. § 61 Abs. 3 BSIG (wichtige Einrichtungen anlassbezogen auf Anordnung).

Gerade die Fristen des Melderegimes, die Registrierungspflicht sowie die Dokumentations- und Nachweispflichten werden durch die Wirtschaft als Bürokratie und teils unnötiger Aufwand empfunden.[4] Hinzu kommt, dass IT- und Cybersicherheit in der Vergangenheit in der rechtlichen Regulatorik ein stiefmütterliches Dasein geführt haben. Daher haben zum Beispiel viele Informationssicherheitsbeauftragte in der Vergangenheit häufig um ihr Mandat im Unternehmen und eine direkte Berichtslinie in die Leitung kämpfen müssen. Die in den letzten Jahren durch die EU verabschiedeten Rechtsakte zur Cybersicherheit (siehe I. 2.) haben dies binnen kurzer Zeit komplett verändert. Cybersicherheit ist nun auch in rechtlichen Fokus geraten und das direkt mit einer Fülle an Gesetzen, die zahlreiche Pflichten mit sich bringen. Das kann Unternehmen verständlicherweise vor Herausforderungen stellen und auch zu Überforderung und Ärger über (vermeintliche) Bürokratie führen.

Tatsächlich ist Regulierung aber erforderlich, um Gesellschaft und Wirtschaft zu schützen. Die Bedrohungslage ist extrem gewachsen, Angriffe werden immer mehr und erfolgreicher und die wirtschaftlichen und gesellschaftlichen Schäden sind gravierend (I. 1.). Die breite Masse der Unternehmen hat sich ohne Regulierung in der Vergangenheit nicht ausreichend abgesichert. Insofern dienen die Pflichten aus der NIS-2-Richtlinie auch dem Selbstschutz der betroffenen Unternehmen. Betrachtet man die Pflichten im Kontext des jeweiligen Sinns und Zwecks, wird deutlich, dass diese miteinander verzahnt und keineswegs bloße Bürokratie sind (II.).

1. Die Bedrohungslage und Schäden

Die Cybersicherheitslage ist seit vielen Jahren angespannt und bleibt es auf hohem Niveau.[5] Insbesondere die Anzahl der Bedrohungen sowie der erfolgreichen Angriffe[6] nimmt zu. Viele Unternehmen haben aber immer noch starken Nachholbedarf bei der Implementierung von (Cyber-) Sicherheitsschutzmaßnahmen.[7] Kritisch ist die zunehmende Bedeutung

1 BGBl. 2025 I Nr. 301 vom 5.12.2025.

2 RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) Nr. 910/2014 und der RL (EU) 2018/1972 sowie zur Aufhebung der RL (EU) 2016/1148, ABl. L 333, 80 v. 27.12.2022.

3 Https://digital-strategy.ec.europa.eu/en/factpages/cybersecurity.

4 S. z.B. DIHK, Stellungnahme zur NIS2-Umsetzung, 30.9.2025, abrufbar unter: https://www.dihk.de/de/newsroom/dihk-zur-nis2-umsetzung-mehr-klarheit-weniger-buerokratie-starke-cybersicherheitsstrukturen-157466.

5 BSI, Die Lage der IT-Sicherheit in Deutschland 2025, abrufbar unter: https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/. Im Rahmen einer Bitkom Studie gaben insgesamt 97 % der befragten Unternehmen im Jahr 2025 an, innerhalb der letzten zwölf Monate von Diebstahl, Industriespionage oder Sabotage betroffen oder vermutlich betroffen gewesen zu sein. Davon betrafen 73 % der Angriffe digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen, Bitkom Wirtschaftsschutz 2025, S. 10 f., abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

6 TÜV, Cybersicherheit in deutschen Unternehmen, Cybersecurity Studie 2025, S. 17.

7 Bspw. haben nur 6 von 10 Unternehmen einen Notfallplan: Bitkom Wirtschaftsschutz 2025, S. 29, abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

KI-gestützter Angriffe,[8] die nicht nur die Zahl der Täter erhöht, sondern auch die Effektivität und die Geschwindigkeit. Gleichzeitig setzen bislang nur wenige Unternehmen selbst Künstliche Intelligenz zur Abwehr von Cyberangriffen ein.[9]

Die jüngsten Cyberangriffe auf Wasserwerke (kritische Infrastrukturen) in mehreren US-Bundesstaaten zeigen, dass es immer wieder bereits an den elementaren Grundlagen der IT-Sicherheit fehlt. Betroffen waren über 100 Wasserwerke, alle mit der gleichen Ursache:[10] Die Wasserwerke haben ihre Steuergeräte ungeschützt ins Internet gestellt. Die Angreifer verschafften sich über das Internet Fernzugriff auf ungeschützte Steuerungen, änderten danach IP-Adressen und Passwörter, mit der Konsequenz, dass die Techniker vor Ort keine Überwachungs- und Steuerungsfähigkeiten mehr hatten. Dies wiederum hatte Druckabfälle – mit dem Risiko, dass unbehandeltes Grundwasser in das Rohrnetz einsickern kann – im Leitungsnetz und Überflutungen zur Folge. Die gesellschaftliche Dimension dieser Angriffe ist offensichtlich.

Dass es häufig bereits an den elementarsten Grundlagen der IT-Sicherheit fehlt, bestätigen auch jüngste Messungen des BSI. Danach haben nur 1,8% der deutschen Webseiten eine der niedrigschwelligsten IT-Sicherheitsmaßnahmen überhaupt, nämlich die Textdatei security.txt,[11] implementiert.[12] Laut der BITKOM Studie Wirtschaftsschutz verfügen 59% der befragten Unternehmen über ein Notfallmanagement, 41% haben keine Präventionsmaßnahmen ergriffen.[13] Nach der TÜV Cybersecurity Studie 2025 testen nur knapp ¼ aller befragten Unternehmen den Ernstfall.[14] Hier zeigt sich bereits ein starkes Gefälle. Selbst wenn man positiv davon ausgehen wollte, dass der Wert im Median aller deutschen Unternehmen in der Mitte liegt, ist das Ergebnis desaströs: Ohne Notfallmanagement dürfte es, z.B. im Falle einer Verschlüsselung der Systeme durch einen Ransomwareangriff,[15] sehr schwer werden, schnell wieder operational zu werden. Je länger die Wiederherstellung der Operationalität dauert, desto größer ist das Risiko, dass betroffene Unternehmen die Attacke wirtschaftlich nicht durchstehen werden. Auch die wirtschaftlichen Folgen für Deutschland können je nach Menge und/oder Kritikalität der betroffenen Unternehmen gravierend sein.

Betrachtet man die wirtschaftlichen Schäden von Cyberangriffen ergibt sich ein besorgniserregendes Bild.[16] Laut einer Studie der PWC wurden in den Jahren 2022-2025 neun von zehn der befragten Unternehmen (in Deutschland 262) Opfer eines Cyberangriffs. Dabei lagen die Schäden bei 47 % der betroffenen Unternehmen bei bis zu 1 Mio. US-Dollar, bei 16 % zwischen 1 und 10 Mio. US-Dollar und bei 11 % bei mehr als 10 Mio. US-Dollar.

Ein verbreiteter Irrglaube, insbesondere bei kleinen und mittleren Unternehmen (KMU) ist, zu denken, man sei zu klein und/oder zu uninteressant für Angreifer.[17] Das ist nicht der Fall. Angreifer schauen vor allem, wo sie leicht Zugriff erhalten können. Gerade KMU werden „meist nicht zielgerichtet zum Opfer, sondern werden von großflächig und automatisiert durchgeführten Angriffen getroffen".[18] Im Jahr 2025 richteten sich bspw. rund 80 % der angezeigten Angriffe, zum Beispiel mit Ransomware, gegen KMU.[19]

2. NIS-2 im Kontext europäischer Cybersicherheitsregulierung

Die NIS-2-Richtlinie sollte stets im Kontext der europäischen Cybersicherheitsstrategie[20] betrachtet werden, die das Ziel hat, der angespannten Bedrohungslage Resilienz entgegenzusetzen und dadurch gesellschaftliche und wirtschaftliche Folgen abzuwenden oder zumindest in Grenzen zu halten. Die NIS-2-Richtlinie ist dabei ein Baustein aus dem europäischen Cybersicherheits-Rechtsrahmen. Dieser umfasst:

1. den Cyber Resilience Act (CRA, (EU) 2024/2847), der als digitaler Zwilling der NIS-2-Richtlinie die Sicherheit bei Produkten mit digitalen Elementen regelt,
2. die NIS-2-Richtlinie,
3. den Digital Operational Resilience Act (DORA, (EU) 2022/2054), der als lex specialis zur NIS-2-Richtlinie die Cybersicherheit und operationale Resilienz im Finanzsektor regelt, sowie
4. den Cyber Solidarity Act ((EU) 2025/38), der die Zusammenarbeit der Mitgliedstaaten im Bereich der Cybersicherheit reguliert.

Übergeordnet steht der Cyber Security Act ((EU) 2019/881), der mit Definitionen, Regelungen zur ENISA und Zertifizierungen grundlegende Regelungen im Bereich der Cybersicherheit enthält. Im AI-Act (2024/1689) finden sich zudem Cybersicherheitsvorschriften für Hochrisiko-KI-Systeme und die im KRITISDachG umgesetzte CER-Richtlinie (2022/2557) regelt die physische Sicherheit bei kritischen Infrastrukturen. Letztere ist lex specialis zur NIS-2-Richtlinie.

Die NIS-2-Richtlinie schützt Netz- und Informationssysteme sowie die Verfügbarkeit, Integrität und Vertraulichkeit der von ihnen verarbeiteten Daten und Dienste, Art. 21 Abs. 1 NIS-2-RL/§ 30 Abs. 1 BSIG.

8 Bitkom Wirtschaftsschutz 2025, S. 27, abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

9 Im Jahr 2025 waren es unter den vom Bitkom befragten Unternehmen nur 4 von 10, Bitkom Wirtschaftsschutz 2025, S. 26, abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

10 Details: Krempl, Cyberangriffe auf Wasserwerke in mehreren US-Bundesstaaten, 2.8.2026, abrufbar unter: https://www.heise.de/news/FBI-und-US-Umweltbehoerde-warnen-Cyberangriffe-auf-US-Wasserwerke-haeufen-sich-11394614.html.

11 Webseitenbetreiber müssen nur einen konkreten Kontakt sowie das Ablaufdatum verpflichtend angeben. Darüber hinaus muss die Datei über den Pfad /.well-known/security.txt erreichbar sein. Damit sind bereits die wichtigsten Kriterien zu Umsetzung der security.txt erfüllt, Anleitung abrufbar unter: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_149.html.

12 BSI, Pressemitteilung v. 6.8.2026, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2026/260806_security_txt.html.

13 Bitkom Wirtschaftsschutz 2025, S. 29, abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

14 TÜV, Cybersicherheit in deutschen Unternehmen, Cybersecurity Studie 2025, S. 32.

15 Ransomware zählt nach wie vor zu den gefährlichsten Angriffsarten, da die Schadwirkungen mit direkten Datenverlust, Produktionsausfällen, Reputationsschäden und hohen Wiederherstellungskosten am gravierendsten sind: Bitkom Wirtschaftsschutz 2025, S. 20, abrufbar unter: https://www.bitkom.org/GGTSPU-5537757d40cc219a-90368-6056301-qztvTCCG4BXyDWeO-LOD/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf.

16 PWC, Global Digital Trust Insights 2026 für Deutschland, abrufbar unter: https://www.pwc.de/de/cyber-security/digital-trust-insights.html.

17 S. auch BMWE, Cybersicherheit im Mittelstand, abrufbar unter: https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Dossier/cybersicherheit.html zu Handwerksbetrieben.

18 BSI, Kleine- und Mittlere Unternehmen, abrufbar unter: https://www.bsi.bund.de/dok/KMU.

19 BSI, Die Lage der IT-Sicherheit in Deutschland 2025, abrufbar unter: https://medien.bsi.bund.de/lagebericht/de/vorworte-und-fazit/.

20 Https://digital-strategy.ec.europa.eu/en/policies/cybersecurity.

II. Die Pflichten im Detail

Betroffene Unternehmen haben im Wesentlichen die folgenden Pflichten:

1. Sie müssen einen Katalog an Risikomanagementmaßnahmen umsetzen. Der Katalog stellt ein Minimum an Maßnahmen dar, die jede Einrichtung umsetzen muss. Die Intensität der Maßnahmen orientiert sich aber am Risiko der jeweiligen Einrichtung, § 30 BSIG.
2. Sie müssen einen Prozess für die Meldung erheblicher Sicherheitsvorfälle nach einem dreistufigen Melderegime implementieren, § 32 BSIG.
3. Geschäftsleitungen müssen sich und ihre Mitarbeitenden ausreichend im Bereich der Cybersicherheit fortbilden und schulen, denn sie tragen die Verantwortung für die Implementierung der Risikomanagementmaßnahmen, § 38 BSIG.
4. Betroffene Einrichtungen müssen sich beim BSI registrieren, §§ 33, 34 BSIG.

Damit einher gehen Dokumentations- sowie (teils auf Anforderung) Nachweispflichten der betroffenen Einrichtungen.

1. Risikomanagementmaßnahmen

Die Risikomanagementmaßnahmen dienen dem Ziel, das Ausmaß von Sicherheitsvorfällen, die jede Einrichtung früher oder später treffen könnten – soweit möglich –, beherrschbar zu halten.[21] § 30 BSIG ist, wie auch die Vorlage in Art. 21 NIS-2-RL, technikneutral formuliert und basiert auf einem risikobasierten Ansatz.

a) Die Maßnahmen im Einzelnen

Nach § 30 Abs. 2 S. 2 BSIG müssen die Maßnahmen mindestens folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Geht man die Liste sorgfältig durch, handelt es sich hierbei um nichts anderes als grundlegende Maßnahmen der IT-Sicherheit sowie wichtige Konzepte und Prozesse, die essenziell für eine Basisabsicherung sind. Betrachtet man die Bedrohungslage und die Schadensrisiken (s. I. 1.), ist die Umsetzung auch aus wirtschaftlicher Perspektive unerlässlich. Die Einhaltung gesetzlicher Pflichten, insbesondere im Bereich des Risikomanagements, ist häufig sogar eine Obliegenheit für den Abschluss von Cyberversicherungen.[22] Viele Unternehmen starten auch nicht bei null. ISMS, ISO/IEC-27001-Zertifizierungen oder Datenschutzprozesse können bereits wichtige Bausteine liefern.[23] Die Dokumentationspflichten nach § 30 Abs. 1 S. 3 BSIG dienen dabei zum einen der Nachvollziehbarkeit, was genau implementiert wurde und sind damit Voraussetzung für eine ordnungsgemäße Überwachung. Zum anderen können sie auch dem Nachweis gegenüber Aufsichtsbehörden für die Erfüllung der Pflichten aus dem BSIG dienen. Die Implementierung der angemessenen Risikomanagementmaßnahmen ist daher ein Baustein zum wirtschaftlichen Überleben von Unternehmen und eine Art Versicherung.

b) Der risikobasierte Ansatz

Die durch jede betroffene Einrichtung verpflichtend zu implementierenden Risikomanagementmaßnahmen können je Einrichtungsart hinsichtlich Ausgestaltung, Tiefe und Intensität ihrer Umsetzung variieren. Maßgeblich sind nach § 30 Abs. 1 S. 2 BSIG Risikoexposition, Unternehmensgröße, Umsetzungskosten sowie die Eintrittswahrscheinlichkeit und Schwere möglicher Vorfälle einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen. Haben Einrichtungen eine höhere Risikoexposition oder sind sie von systemischer Bedeutung müssen sie ein entsprechend höheres Schutzniveau gewährleisten.[24] So ist sichergestellt, dass Einrichtungen nicht überfordert werden.[25] Flankiert wird der risikobasierte Ansatz durch den gefahrenübergreifenden Ansatz in § 30 Abs. 1 S. 1 BSIG, der den Blick auf relevante Risiken reduziert. Zusammen sichern sie ein verhältnismäßiges und kohärentes Sicherheitsniveau,[26] das mit Augenmaß elementare Maßnahmen der Cybersicherheit von betroffenen Einrichtungen verlangt.

2. Meldepflichten

§ 32 BSIG verpflichtet betroffene Einrichtungen, dem BSI nach einem dreistufigen Melderegime erhebliche Sicherheitsvorfälle, § 2 Nr. 11 i.V.m. Nr. 40 BSIG, zu melden. Der Gesetzgeber knüpft die drei Meldungsstufen an unterschiedlich kurze Fristen und verlangt dabei einen unterschiedlichen Detailgrad (vom Verdacht bis zur Abschlussmeldung).[27]

21 Nink, ZfPC 2025, 58 (64).

22 SWK-Digitale Sicherheit/Nink, 42 Rn. 34.

23 Ausf. Grochala/Nink, EuDiR 2026, i.E.

24 Grochala/Nink, EuDiR 2026, i.E.

25 SWK-Digitale Sicherheit/Zaudig, 32 Rn. 21.

26 Ausf. warum der risikobasierte Ansatz sinnvoll und richtig ist: Grochala/Nink, EuDiR 2026, i.E.

27 Details s. auch SWK-Digitale Sicherheit/Rothkegel, 37 Rn. 50 ff.

Meldepflichten, insbesondere die kurzen Fristen, werden teils als Bürokratie empfunden. Tatsächlich sind sie aber ein Grundpfeiler der mit der NIS-2-Richtlinie beabsichtigten Ziele, Cyberangriffe zu verhindern und die Reaktionsfähigkeiten auf Angriffe zu verbessern. Die Meldungen ermöglichen es dem BSI, Vorfälle zu sammeln, auszuwerten und miteinander in Beziehung zu setzen, um bspw. erkennen zu können, ob eine bestimmte Schwachstelle, Schadsoftware oder Angriffsmethode gleichzeitig mehrere Organisationen oder Branchen betrifft. Mit diesen Informationen kann das BSI zum einen ein Lagebild zur Sicherheit in der Informationstechnik erstellen, zum anderen kann es aber vor allem andere betroffene Organisationen informieren, warnen und relevante Informationen weitergeben. Denn Angriffe auf eine bestimmte Organisation können Erkenntnisse liefern, die dabei helfen, ähnliche Angriffe auf andere Organisationen zu verhindern.

Die Meldepflicht hat damit sowohl eine gesellschaftliche als auch wirtschaftliche Dimension. Denn wenn Angriffe auf andere Organisationen verhindert werden, bleiben die Schäden gesamtpolitisch überschaubar. Damit Warnungen auch rechtzeitig erfolgen können, muss das BSI selbstverständlich auch frühestmöglich einbezogen werden, so dass die kurzen Fristen sinnvoll und notwendig sind.

3. Registrierung

Nach § 33 Abs. 1 BSIG sind betroffene Einrichtungen innerhalb von drei Monaten verpflichtet, sich beim BSI zu registrieren und bestimmte Angaben, wie Informationen zur Einrichtung und zu ihren Tätigkeitsbereichen, zu übermitteln. Die Registrierung schafft damit zunächst Transparenz darüber, wer überhaupt reguliert ist. Das wiederum ist essenziell, damit das BSI betroffene Einrichtungen erreichen und ihnen bspw. Warnungen und Informationen zu erheblichen Sicherheitsvorfällen übermitteln kann. Die Registrierungspflicht ist daher zum einen Voraussetzung für die effektive Wahrnehmung der staatlichen Cyberabwehraufgaben und zum anderen notwendig, um die Ziele, Cyberangriffe zu verhindern und die Reaktionsfähigkeiten auf Angriffe zu verbessern, überhaupt erreichen zu können.

4. Geschäftsleitungen

§ 38 Abs. 1 BSIG verpflichtet die Geschäftsleitung, § 2 Nr. 13 BSIG, betroffener Einrichtungen, die Risikomanagementmaßnahmen aus § 30 BSIG umzusetzen und deren Umsetzung zu überwachen. Um dieser Pflicht in ausreichendem Maße gerecht zu werden, flankiert der Gesetzgeber die Umsetzungs- und Überwachungsverantwortung mit der Pflicht, „regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können“, § 38 Abs. 3 BSIG.

Selbstverständlich können Geschäftsleitungen die Umsetzung der Risikomanagementmaßnahmen delegieren, sie müssen aber die allgemeinen Anforderungen an Auswahl und Kontrolle beachten.[28] Nicht delegierbar ist die Schulungspflicht. Denn andernfalls kann die Geschäftsleitung ihren Überwachungspflichten aus § 38 Abs. 1 BSIG nicht nachkommen. Zudem sind die Kenntnisse auch erforderlich, um ausreichend Ressourcen und Mittel in eine angemessene Implementierung von Cybersicherheit zu allokieren. Die Schulungspflicht kann sogar als Schutz für die Geschäftsleitung betrachtet werden. Denn kommt die Geschäftsleitung ihren Pflichten nicht nach, haftet sie ihrer Organisation gegenüber persönlich für etwaige Schäden nach den allgemeinen Vorschriften, § 38 Abs. 2 BSIG i.V.m. § 91 AktG/§ 43 GmbHG, dh unter Anwendung der Business Judgement Rule.[29]

Cybersicherheit zur Chef- und Chefinnensache zu machen, ist ein wichtiger Hebel, um Einrichtungen tatsächlich cyberresilienter zu machen. Denn ohne ausreichende Unterstützung auf höchster Ebene, besteht das Risiko, dass Cybersicherheit nicht ernst (genug) genommen wird und die Einrichtung nicht die erforderlichen Ressourcen und Mittel bereitstellt.

III. Fazit

Die im BSIG umgesetzten Pflichten aus der NIS-2-Richtlinie sind keine bloße Bürokratie und auch nicht auf Überforderung der Einrichtungen angelegt, sondern sinnvolle aufeinander abgestimmte Pflichten, mit dem Ziel Deutschland gesellschaftlich und wirtschaftlich cyberresilienter zu machen. Für viele Unternehmen bedeutet dies verständlicherweise Aufwand, der gerade bei KMU auch neuer Aufwand sein wird. Dieser Aufwand ist aber notwendig, um die Wirtschaft und Gesellschaft nicht zu belasten und/oder nachhaltig zu schädigen. Für Unternehmen selbst kann die Umsetzung den Unterschied zwischen weiterem Bestehen und wirtschaftlichen Ruin bedeuten.

Um die Erfüllung einfacherer zu machen, stellt das BSI zahlreiche Hilfestellungen zur Verfügung, schafft Awareness und unterstützt die Wirtschaft.[30] Die Hilfestellungen werden fortlaufend aktualisiert und ergänzt. Wer nicht weiß, wo er beginnen soll, sollte mit einem Notfallplan starten (und diesen auch testen), damit er Fall eines erfolgreichen Angriffs noch handlungsfähig ist und weiß, wen er wie erreichen kann.[31]

Dr. Judith Nink
ist Fachbereichsleiterin Cybersicherheit bei Unternehmen im BSI, Bonn.

28 Nink, Das neue IT-Sicherheitsrecht, § 6 Rn. 4; SWK-Digitale Sicherheit/Zaudig 41 Rn. 4 ff.

29 Ausf. Nink, Das neue IT-Sicherheitsrecht, § 6 Rn. 5; SWK-Digitale Sicherheit/Zaudig 41 Rn. 24; Hornung/Schallbruch, IT-SicherheitsR-Hdb/Thalhofer § 16 Rn. 9 ff.

30 Https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/regulierte-wirtschaft_node.html.

31 Tipps zur Risikoanalyse: https://www.bsi.bund.de/dok/nis-2-risikoanalyse.

Prof. Dr. Schwartmann/Lucia Burkhardt

Transparenz beim KI-Einsatz im politischen Kontext

KI generierte Inhalte sind auch in der Politik an der Tagesordnung. Das gilt für die Unterstützung bei der Erstellung von Texten als auch bei der Erstellung von Bildern. Der Einsatz der Technik ist ebenso zeitgemäß wie lebensnah. Dennoch birgt er insbesondere in Wahlkämpfen besondere Risiken in politischer und rechtlicher Hinsicht. Der Beitrag zeigt sie auf und erläutert die rechtlich erforderlichen Transparenzanforderungen nach der KI-Verordnung. Die Frage nach einem transparenten Umgang mit KI-generierten Texten stellt sich jedoch auch dann, wenn die Transparenzpflicht der KI-VO nicht greift. Rechtliche Pflichten markieren lediglich eine Untergrenze. Gerade politische Akteure sollten sich daher fragen, ob sie den Einsatz von KI im Lichte ihrer besonderen Verantwortung für die öffentliche Meinungsbildung auch ohne Rechtspflicht offenlegen. Vieles spricht dafür, einen grundsätzlichen, aber aussagekräftigen Transparenzhinweis auch dann zu geben, wenn die Inhalte nicht vollständig KI-generiert sind oder einer menschlichen Kontrolle unterlagen. Das ist für jeden konkreten Fall zu prüfen.

I. Kennzeichnung und Transparenz schaffen Vertrauen

Seit dem 2.8.2026 gilt die Kennzeichnungspflicht für KI-generierte oder modifizierte Inhalte aus der KI-VO. Die KI-VO sieht in Art. 50 einen Mindeststandard der Transparenzpflicht vor. Kurz nachdem das Gesetz Wirkung entfaltete schlug Anthropic eine Lösung zur Markierung von Texten vor. Der Anbieter von Claude will Texte, die durch seine Systeme generiert werden, zukünftig mit einem für den Menschen unsichtbaren Wasserzeichen versehen. Versteckt ist das Zeichen in der Wortwahl. Der Mechanismus dahinter ist vereinfacht dargestellt folgender: Der Algorithmus wird so modifiziert, dass die KI bei zwei gleich wahrscheinlichen Wörtern (Wahl zwischen Option A und B) immer Option A wählt. Dieses Schema kann nachträglich ausgelesen werden. Unklar ist nach aktuellem Stand wie zuverlässig die Kennzeichnung wirkt und, das ist ein zentraler Kritikpunkt, wer Zugang zu seiner Entschlüsselung erhält. Anthropic hat angekündigt, einen Schnittstellenzugang zu einem „Scanner" anzubieten. Kostenlos wird der wahrscheinlich nicht sein. Hier zeichnet sich also ein neues Geschäftsmodell für die großen KI-Anbieter ab. Davon mag man halten, was man möchte, jedenfalls muss sich jeder, der mit KI arbeitet, nun umso mehr die Frage stellen, in welchem Umfang er die Arbeit mit KI offenlegt. Tatsächlich kann es unterhalb der Schwelle der gesetzlichen Mindestanforderungen angeraten sein, KI-generierten Output kenntlich zu machen. Nicht zuletzt deshalb, weil Staat und Gesellschaft zu einem selbstbewussten Umgang mit KI finden müssen. Alle nutzen KI, aber keiner darf es wissen ist keine gute Lösung, auch wenn das häufig die Realität abbilden mag. „KI-Scham" ist ebenso fehl am Platz wie das Verbergen des Einsatzes, wenn man sich im Rahmen des Rechts für den Einsatz entscheidet.

In der Sache geht es bei Art. 50 KI-VO um drei Dinge. Er bestimmt in seinen ersten beiden Absätzen Pflichten für Entwickler von KI-Systemen. Schon auf Systemebene muss sichergestellt werden, dass die generierten Outputs als künstlich erzeugt markiert werden. Die nachfolgenden Absätze adressieren diejenigen, die KI-Systeme nutzen und Output generieren. Abs. 3 normiert Spezialfälle. Er erfasst den Einsatz eines Emotionserkennungssystems oder eines Systems zur biometrischen Kategorisierung. Abs. 4 adressiert alle übrigen Nutzer. Darauf liegt im Folgenden der Schwerpunkt, da insbesondere im politischen Betrieb typischerweise Art. 50 Abs. 4 KI-VO greift. Einen Überblick über die Regelungen des Art. 50 KI-VO in seiner Gesamtheit gibt hierüber hinaus die in diesem Beitrag angehängte Kurzübersicht.[1]

II. KI-generierte Bilder (Deep Fakes)

Für die Veröffentlichung von KI-generieren Bildern und Videos gelten strenge Maßstäbe. Immer dann, wenn ein Bild einer wirklichen Person, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt, handelt es sich um einen sog. Deepfake und muss als KI-generiert gekennzeichnet werden.[2] Entscheidend hierbei ist, dass keine Ähnlichkeit zu einer real existierenden Person oder einem tatsächlichen Ereignis bestehen muss. Es genügt, dass das Bild jemandem oder etwas ähnelt, das in der Realität existieren kann oder hätte existieren können.[3] Das bedeutet ein Bild, das auch ein Foto sein könnte und das KI-generiert ist, muss als solches gekennzeichnet sein, wenn es nicht völlig offenkundig künstlich ist, wie ein Dinosaurier, der den Kölner Dom bestaunt. Diese Pflicht gilt zwar immer, gerade im Wahlkampf muss hierauf aber besonders geachtet werden. Denn der Wahlkampf bewegt sich in einem für die Demokratie besonders sensiblen Bereich, in dem besondere Vorsicht geboten ist.[4]

1 Die Übersicht ist der Schulungsunterlage des Kurses GDD-AI-Privacy-Expert entnommen.

2 Art. 3 Nr. 60 KI-VO.

3 Europäische Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), 2026, Rn. 107.

4 Die Schwelle des Anhang III Nr. 8 b) dürfte dann überschritten sein, wenn kein Mensch mehr zwischen die demokratierelevante Äußerung des Bots und den Wähler tritt.

Wo die Grenze der Transparenzpflicht verläuft, lässt sich mit obiger Bilderfolge erläutern. Die Bilder zeigen die Sichtung des „KI-Nutzer-Nachwuchses" beim Erwerb des KI-Seepferdchens durch die Mitglieder der unabhängigen Expertenkommission zum Schutz von Kindern und Jugendlichen in der Digitalen Welt. Sie wurde im September 2025 eingesetzt. In Handlungsempfehlung 12 schlägt die Kommission das „KI-Seepferdchen" vor. Als Trainer fungieren der Direktor der Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ) Sebastian Gutknecht und der Mitautor dieses Beitrages Rolf Schwartmann, der das „KI-Seepferdchen" in die Kommission eingebracht hat. Dargestellt ist die Sichtung der „KI-Seepferdchen-Aspiranten" beim Absolvieren der Prüfung. Die Grundlage (Bild 1) stammt von Heiko Sakurai. Bilder 2 und 3 sind KI-generiert durch ChatGPT sprich DALL-E. Welches der Bilder bedarf der Kennzeichnung?

Kennzeichnungspflichtig ist nur Bild 3. Damit der Betrachter es nicht für real hält, muss er darauf hingewiesen werden, dass das Bild künstlich erzeugt wurde. Denn es könnte ein Foto sein, da Kinder, Ponys und Schiedsrichter reale Personen sind oder sein könnten. Da für jeden erkennbar ist, dass Kinder nicht auf Seepferden über einen Parcours und dann auch noch nicht im Wasser reiten, kann Bild 2 nicht real sein und die Kennzeichnungspflicht entfällt ebenso wie in Bild 1, das als Cartoon erkennbar keine echte Lebenssituation darstellt.

Losgelöst von der Rechtsfrage wird die Frage erörtert, ob Bilder in der Politik überhaupt mithilfe von KI generiert werden sollten. Dieser Streit entbrannte kürzlich aufgrund eines erkennbar KI-generierten Bildes auf dem Instagram-Profil der Bundespräsidentin Julia Klöckner, das die Politikerin gemeinsam mit Kindern und dem Slogan „Alles Gute zum Schulstart" zeigt. Kritiker wenden ein, die Nutzung KI-generierter Bilder schädige das Handwerk des Grafik-Designs und sorge für einen grafischen Qualitätsabfall. Die Bundespräsidentin will mit synthetischen Kinderbildern die Rechte von existierenden Kindern schützen, die anderenfalls im Internet zu sehen gewesen wären. Konkretes Ergebnis ist ein Diskurs über das Thema.

III. KI-Einsatz bei Texterstellung

Auch bezüglich KI-generierter oder mithilfe von KI überarbeiteter Texte schreibt die KI-VO grundsätzlich eine Kennzeichnungspflicht vor. Eine Ausnahme besteht nach der KI-VO dann, wenn der Text vor der Veröffentlichung in einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurde.[5] Zudem muss ein Mensch oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung übernehmen, d.h. für die Inhalte haften.[6] Auf eine Kennzeichnung kann daher nur verzichtet werden, wenn eine gründliche Kontrolle erfolgt, die über eine oberflächliche oder rein formale Korrektur hinausgeht und sich substanziell mit dem Text auseinandersetzt. Durchführen muss diese Kontrolle eine fachlich kompetente natürliche Person, die den Text inhaltlich beurteilen und über seine Veröffentlichung entscheiden kann.[7] Eine zusätzliche Ausnahme besteht, wenn der Text nicht dazu dient, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren. Diese Ausnahme dürfte bei der Kommunikation eines politischen Akteurs nach außen selten erfüllt sein. Sie gilt aber für etwa für die interne Einladung zu einer Weihnachtsfeier.

In vielen Fällen wird der Einsatz von KI die menschliche Arbeit verbessern, aber nicht zwangsläufig beschleunigen können. Der Mensch muss sich schließlich kritisch mit weiteren Impulsen auseinandersetzen und diese in sein Ergebnis einbeziehen. Erfolgt der Einsatz von KI, muss man sich aber der besonderen Verantwortung beim Einsatz des autonomen Werkzeugs gerade im politischen Kontext bewusst sein. Der Weg von einer Idee hin zu einer oft nicht durchdachten, aber so klingenden Ausformulierung ist wegen der großen Sprach-

5 Art. 50 Abs. 4 UAbs. 2, S. 2.

6 Europäische Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), 2026, Rn. 128.

7 Europäische Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), 2026, Rn. 126-127.

modelle kurz. Auch Überarbeitungen erfolgen häufig nicht mehr rein menschlich. Das kann Erleichterung schaffen und dazu dienen, die Qualität menschlicher Beiträge zu erhöhen.

Allerdings birgt der Einsatz von KI bei der Texterstellung auch erhebliche Risiken. Immerhin transportieren Texte unsere Ideen, Ziele und Werte. Nutzt man KI also leichtfertig, nimmt diese dem Menschen nicht nur das Formulieren ab, sondern ersetzt auch das Denken. Sie bewertet an unserer Stelle. Promptet man etwa schlicht „Formuliere eine Rede für die Ausschusssitzung zum Thema Kinderarmut passend zum Wahlprogramm", ersetzt die KI einen großen Teil des Denkens, der beim Menschen liegen muss. Welche Aspekte sollen besonders betont werden? Anhand welcher Werte werden die allgemeinen Ziele ausdifferenziert? Aus welchem gesellschaftlichen Bereich werden Beispiele gewählt? Für wen setzt man sich konkret ein? All diese Entscheidungen darf die KI nicht für uns treffen. Und selbst wenn das fertige Ergebnis von einem Menschen überarbeitet wird, ähnelt es dem Output der KI oft noch. Denn wenn man sich nicht dagegen schützt, wirkt der erste Impuls der KI als Anker, an dem sich jede weitere Entscheidung unbewusst ausrichtet (sog. Ankereffekt).[8]

IV. KI in der politischen und parlamentarischen Arbeit

Besonders anspruchsvoll und potenziell gefährlich ist der KI-Einsatz im Kern der Demokratie, der parlamentarischen Arbeit. KI darf als mathematischer Impuls keine Überzeugungen auslösen. Die Gefahr dafür ist aber bei der Sprachgewalt von KI sehr hoch.[9] Dem muss man aktiv entgegenwirken.[10] KI ist schließlich weder einem menschlichen Wesen mit Verantwortung zurechenbar[11], noch ist der mathematische Impuls (politisch) neutral[12]. Jede Ausgabe der KI ist mit einer Tendenz versehen, die schon in der Datenbasis angelegt ist und die sich dem Einfluss des Menschen entzieht.[13]

1. KI darf Menschen unterstützen, nicht ersetzen

Auf KI muss deswegen nicht verzichtet werden. Das tragende Prinzip lautet aber: KI darf den Menschen unterstützen, ersetzen darf sie ihn nicht.[14] Das gilt neben der Bildgenerierung durch KI auch für den Bereich der Textgenerierung, insbesondere dann, wenn Texte für die öffentliche Meinungsbildung formuliert werden. Allein vertretbar ist daher ein Vorgehen nach dem Prinzip „Mensch-Maschine-Mensch". In vielen Fällen bedeutet das, zunächst denkt der Mensch und verfasst einen ersten Entwurf zumindest in substanziellen Stichpunkten und sortiert seine tragenden Ideen. Dann nutzt er die KI zur Optimierung seiner Ergebnisse per Austausch über die Textgestaltung. Über das Ergebnis entscheidet am Ende der Mensch nach eigener Kontrolle, Recherche und Abwägung. Nur so lässt sich verhindern, dass die KI prägt und der Mensch geprägt wird. Hinzu kommt, dass KI-generierte Texte bisweilen erkennbaren sprachlichen Mustern folgen. Solchen Texten fehlt es oft an menschlicher Originalität. Vermeiden lässt sich „KI-Sound", indem man Substanz und Formulierungen selbst liefert und KI nur bei einer nachträglichen Durchsicht nutzt.

2. Kontext und Zweck des KI-Einsatzes bestimmen

Beim Einsatz von KI gilt es immer, den Kontext und den Einsatzzweck des Werkzeugs zu bestimmen.[15] In risikolosen Kontexten gelten andere Anforderungen als in riskanten. Es macht einen Unterschied, ob man einen Social-Media-Post über das Sommerfest der eigenen Partei schreibt, einen Post über eine Rede im Wahlkreis oder gar eine Wahlkampfrede entwirft. Während der Bericht über das Sommerfest kaum demokratische Bedeutung hat, ist das bei einer Wahlkampfrede unbestreitbar. Die KI-Verordnung ordnet KI-Systeme, die bestimmungsgemäß verwendet werden sollen, um das Ergebnis einer Wahl oder das Verhalten natürlicher Personen bei der Ausübung ihres Wahlrechts bei der Wahl zu beeinflussen, als hochriskant ein.[16] Anders als im täglichen politischen Betrieb ist der Einsatz von KI im Wahlkampf daher besonders kritisch zu betrachten. Hochriskant ist beispielsweise eine unmittelbare Beeinflussung der Wähler durch personalisierte Wahlwerbung auf Social-Media oder Tools wie den Wahl-O-Maten, insofern diese KI-gestützt arbeiten. Ebenfalls hochriskant ist etwa der Fall, dass ein Chatbot auf der Website einer Partei eigenständig für die Partei wirbt oder Auskünfte gibt.

3. KI-Einsatz im Wahlkampf

Die Risikobewertung des Einsatzes KI-generierter Inhalte im Kontext des Wahlkampfes ist bisher noch nicht eindeutig geklärt. Es spricht jedoch einiges dafür, einen hochriskanten Zweck nur dann anzunehmen, wenn KI-Systeme genutzt werden, die Inhalte nicht nur generieren, sondern auch selbst verbreiten. Dies umfasst beispielsweise einen Chatbot, der in einem Forum selbstständig Werbung für einen Kandidaten macht. Ebenfalls umfasst ist die Erstellung von Bildern und Videos zu Wahlkampfzwecken, wenn diese unmittelbar von dem generierenden KI-System auf YouTube oder Instagram veröffentlicht werden. Rechtlich auf der sicheren Seite ist man dann, wenn KI nur eingesetzt wird, um menschlich erzeugte Inhalte zu überarbeiten. In jedem Fall müssen Texte und Bilder eines politischen Akteurs um deren Bedeutung für den demokratischen Willensbildungsprozess gerecht zu werden vor der Veröffentlichung substanziell von einem Menschen geprüft werden. Nach Ansicht der EU-Kommission ist die KI-gestützte Generierung politischer Werbeinhalte im Wahlkampf wohl nicht hochriskant im Sinne von Anhang III Nr. 8 b), wenn die Inhalte nicht unmittelbar von einem Chatbot, sondern von einem Menschen verbreitet werden.[17] Um nicht in den Anwendungsbereich der hochriskanten Fälle zu geraten, genügt bei derartiger Lesart der KI-VO die formale Kontrolle des „Ob" der Veröffentlichung. Ob eine inhaltliche Prüfung der Beiträge stattfindet, ist für die Einordnung

8 Köhler, Richterliche Verantwortung und Künstliche Intelligenz, 2026, S. 53.; Schwartmann, Über Leben mit KI, S. 106 ff.

9 Schwartmann, Über Leben mit KI, S. 54.

10 Dazu eingehend unter Entwicklung eines Verfahrens zur Kontrolle, Schwartmann, Über Leben mit KI, S. 146 ff.

11 Schwartmann, Über Leben mit KI, S. 225 ff.

12 Schwartmann, Über Leben mit KI, S. 74.

13 Schwartmann, Über Leben mit KI, S. 69 ff.

14 Schwartmann, Über Leben mit KI, S. 247 ff. m.w.N.

15 Dazu am Beispiel der Bilderstellung eingehend, Schwartmann, Über Leben mit KI, S. 146 ff.

16 Anhang III Nr. 8 b) KI-VO.

17 Europäische Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), 2026, Rn. 447.

als hochriskant dann nicht entscheidend. Eindeutig sind die Kommissionsleitlinien diesbezüglich allerdings nicht. Zwar stellen sie auf die formale Verbreitungsform der Inhalte als Abgrenzungsmerkmal ab, als Beispiel für nicht hochriskantes Verhalten nennen sie jedoch die Verbreitung und Prüfung von Inhalten durch eine Partei. Selbst aber wenn es der Kommission auf eine Prüfung tatsächlich nicht ankommt, ist unklar, ob auch der EuGH dieser Einschätzung folgen würde. Plausibel wäre es auch, die Einordnung von KI-generierter Wahlwerbung anhand einer Abgrenzung zwischen inhaltlicher Unterstützung und Ersetzung der menschlichen Aussagen zu bemessen.[18] Die Grenzen sind dabei aktuell noch offen. Eindeutig nicht erfasst wäre die rein stilistische Überarbeitung bereits verfasster Kampagnentexte, so beispielsweise die Kennzeichnung unklarer Formulierungen oder Widersprüche zu vorhandenem Parteimaterial.[19] Bei einer Rede könnte für die Annahme einer bloßen Unterstützung sprechen, dass sich bereits im Vortrag ein durchaus erhebliches menschliches Element zeigt. („Es gilt das gesprochene Wort").

4. „KI-Bekenntnis"

Unabhängig von rechtlichen Pflichten steht es einer staatlichen Stelle und politischen Akteuren gut zu Gesicht, offen zum Einsatz von KI zu bekennen, wenn sie sich zum Einsatz entscheidet. So könnte ein allgemeiner Hinweis auf der Website einer staatlichen Stelle und insbesondere auch politischen Akteurs platziert werden. Der konkrete Wortlaut hängt dabei vom tatsächlichen Einsatz der KI ab. Zentral ist es nicht nur, die rechtlichen Grenzen einzuhalten, sondern ehrlich und transparent zu kommunizieren und den Einsatz so zu beschreiben, wie er in der Praxis tatsächlich erfolgt. Ein Hinweis könnte zum Beispiel wie folgt lauten:

Bei der Erstellung von Texten und Bildern und sonstigen Inhalten wie Übersichten oder Grafiken setzen wir Künstliche Intelligenz unterstützend ein. Wir sind uns der Möglichkeiten und Risiken der autonomen Technik bewusst. Wir differenzieren nach den Zwecken des Einsatzes der KI und beachten die rechtlichen Vorgaben für die Unterstützung des Menschen durch KI. Wir haben darüber hinausgehende Standards, die unserer politischen und demokratischen Verantwortung gerecht werden. Dazu stellen wir sicher und versichern, dass der Einsatz von KI als Werkzeug gewissenhaft und gründlich menschlich kontrolliert wird. Wir setzen KI zu rechtlich zulässigen und politisch verantwortbaren Zwecken ein. Wir nutzen KI bei der Texterstellung etwa bei der konkreten und kontextbezogenen Recherche zu klar vorgegebenen Inhalten, bei formalen Korrekturen sowie bei der sprachlichen Optimierung von Texten. Das bedeutet, dass wir Ideen selbst entwickeln und textlich konkrete Vorgaben machen. Der entscheidende und insbesondere erste Impuls geht dabei von uns aus. Die Reihenfolge lautet stets Mensch-Maschine-Mensch. Sämtliche Impulse der KI prüfen wir gewissenhaft. Jede Formulierung und jeder Gedanke werden bewusst von uns verantwortet und getragen. Die inhaltliche und redaktionelle Verantwortung liegt vollständig bei uns. Bei Bildern, Übersichten und Grafiken etc., wägen wir den Einsatz gewissenhaft ab und achten auf die Wahrung von Transparenz- und Kennzeichnungspflichten.

5. Selbstverpflichtung

Neben dem so formulierten Selbstbekenntnis mit Blick auf den Umfang der Unterstützung durch Künstliche Intelligenz sollte im politischen Betrieb ein Bekenntnis insbesondere zum politisch faire Einsatz der Technologie erfolgen. Deepfakes stellen nämlich eine ernst zu nehmende Gefahr für die demokratische Willensbildung dar. Im Wahlkampfsommer 2026 kursieren in sozialen Netzwerken gefälschte Videos und Art. über deutsche Politikerinnen und Politiker. Ihnen werden Suchtprobleme, Korruption und sexuelle Übergriffe unterstellt. Als Initiator der Kampagne wird Russland vermutet. Durch die neuen Möglichkeiten, die mit KI entstehen, lassen sich solche Deepfakes leicht erstellen. Einfluss gewinnen solche Kampagnen nicht nur darüber, dass sie täuschend echte Ergebnisse produzieren, sondern auch über die Masse an Uploads. Wenn sich der Wähler aber nicht mehr darauf verlassen kann, dass das, was er sieht, Realität ist, ist kaum noch echter Wahlkampf möglich. Da in einem solchen Fall der gesellschaftliche Schaden besonders groß ist, bietet sich eine gemeinsame Selbstverpflichtung aller parlamentarischen Parteien an. Verboten ist die Verbreitung eines KI-generierten Bildes als Fotografie zwar schon jetzt, genauso wie das Publizieren von zahllosen Texten ohne, dass ein Mensch dafür einsteht und ohne, dass auf die nicht menschliche Herkunft hingewiesen wird. Ein Verbot hat aber leider allzu oft keine durchschlagende Kraft. Daher würde eine zusätzliche Selbstverpflichtung einen Teil zur Sicherung der Fairness im Wahlkampf beitragen, indem sie noch einmal an demokratische Werte erinnert. Sie hält dazu an, das eigene Verhalten an den öffentlich vertretenen Werten auszurichten.

V. Fazit

Künstliche Intelligenz eröffnet Chancen und birgt Risiken. Ein verantwortungsbewusster Umgang mit der Technik ist daher gerade für politische Akteure unerlässlich. Dazu gehört, ihren Einsatz zu kennzeichnen. Den Mindeststandard setzt Art. 50 KI-VO. Konsequent als KI generiert auszuweisen sind daher Texte, die keiner sorgfältigen Kontrolle unterlagen, ebenso Bilder, die für eine Fotografie gehalten werden können, da ihr Gegenstand real ist oder sein könnte. Es sprechen aber gute Gründe dafür, den Einsatz auch unterhalb dieser Schwelle offen zu legen. Ein „KI-Bekenntnis" öffnet den Diskurs über den gesellschaftlich verantwortbaren Nutzen von KI. Politische Akteure sollten außerdem Bewusstsein für den Ankereffekt schaffen und ihm durch den Dreischritt „Mensch-Maschine-Mensch" beim Einsatz der Technik bestmöglich begegnen. So kann vermieden werden, dass mit Hilfe von Maschinen erzeugte Inhalte unbemerkt Einfluss auf Werte und Positionen im Wahlkampf nehmen.

18 Als Tatbestandsmerkmale zur Anknüpfung kommen zwei Aspekte in Anhang III Nr. 8 b KI-VO in Betracht. Zum einen „Beeinflussung" (S. 1): Das KI-System wird nicht verwendet, „um zu beeinflussen", wenn es einen in der Gesamtbetrachtung gegenüber den menschlichen Aussagen unbedeutenden Beitrag zur Rede leistet. Zum anderen "nicht direkt ausgesetzt" (S. 2): Die Hörer sind den Ausgaben des KI-Systems nicht direkt ausgesetzt, wenn die Ausgaben aufgrund der bloßen Unterstützungsfunktion des KI-Systems in den menschlichen Aussagen aufgehen.

19 Europäische Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), 2026, Rn. 447.

Betroffene Systeme	Adressaten	Pflicht	Ausnahmen
Emotionserkennungssystem	Betreiber	Information der betroffenen natürlichen Person über den Betrieb	Gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme
System zur biometrischen Kategorisierung			
Erzeugung oder Manipulation von Bild-, Ton- oder Videoinhalten, die ein Deepfake sind	Betreiber	Offenlegung der künstlichen Erzeugung oder Manipulation	Gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme
			Inhalt ist Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms: Offenlegung ohne Beeinträchtigung der Darstellung oder des Genusses des Werks
Erzeugung oder Manipulation von Text, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren	Betreiber	Offenlegung der künstlichen Erzeugung oder Manipulation	Gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme
			Menschliche Überprüfung oder redaktionelle Kontrolle der erzeugten Inhalte und redaktionelle Verantwortung einer Person

Betroffene Systeme	Adressaten	Pflicht	Ausnahmen
Direkte Interaktion mit natürlichen Personen	Anbieter	Konzeption und Entwicklung, sodass die natürlichen Personen informiert werden, dass sie mit einem KI-System interagieren	informierten, aufmerksamen und verständigen natürlichen Person aufgrund der Umstände und des Kontexts der Nutzung offensichtlich
			gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme
Erzeugung synthetischer Audio-, Bild-, Video- oder Textinhalte	Anbieter	Sicherstellen einer Kennzeichnung in maschinenlesbarem Format Sicherstellen der Erkennbarkeit einer künstlichen Erzeugung	Ausführung einer unterstützenden Funktion für die Standardbearbeitung
			keine wesentliche Veränderung der Eingabedaten oder ihrer Semantik
			gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Lucia Burkhardt
ist wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln.
Foto: TH Köln/Schmülgen

KURZBEITRÄGE

Denis Lehmkemper/Dr. Henning Dehnert*

Innovationsförderung durch Einrichtung von KI-Reallaboren bei den Landesdatenschutzbehörden

KI-Reallabore[1] im Sinne von Art. 57 KI-VO dienen der Innovationsförderung. Anbieter innovativer KI-Systeme können diese in KI-Reallaboren unter regulatorischer Aufsicht und Realbedingungen entwickeln und erproben, um Rechtskonformität herzustellen.[2] Unter bestimmten Bedingungen können die Unternehmen dabei von einer Beschränkung der aufsichtsbehördlichen Sanktionsmöglichkeiten profitieren. Für die Weiterverarbeitung personenbezogener Daten zur Entwicklung, zum Training und zum Testen bestimmter KI-Systeme im KI-Reallabor können sich Anbieter auf Art. 59 KI-VO als Rechtsgrundlage stützen. Dadurch soll der Marktzugang beschleunigt und es sollen regulatorische Hindernisse abgebaut werden.[3] Dieses Angebot richtet sich insbesondere an KMU einschließlich Start-up-Unternehmen, denn Art. 62 Abs. 1 lit. a) KI-VO verpflichtet die Mitgliedstaaten, solchen Unternehmen vorrangigen Zugang zu den KI-Reallaboren zu gewähren. Bislang ist noch offen, welchen Behörden in Deutschland neben der Bundesnetzagentur die Aufgabe der Errichtung und des Betriebes von KI-Reallaboren im Sinne von Art. 57 KI-VO übertragen werden soll.

I. KI-Reallabore als Teil der KI-Marktüberwachung

Die Mitgliedstaaten der Europäischen Union sorgen dafür, dass ihre zuständigen Behörden[4] mindestens ein KI-Reallabor einrichten.[5] Art. 57 Abs. 2 KI-VO gestattet die Einrichtung zusätzlicher KI-Reallabore auf regionaler oder lokaler Ebene. Damit ist aus europarechtlicher Sicht die Einrichtung mehrerer regionaler KI-Reallabore in der Bundesrepublik bei den notifizierenden Behörden[6] oder Marktüberwachungsbehörden[7] zulässig.[8]

Beim Betrieb eines Reallabors haben die zuständigen Behörden insbesondere Anleitung, Aufsicht und Unterstützung bereitzustellen, um Risiken und Risikominderungsmaßnahmen sowie deren Wirksamkeit hinsichtlich der Pflichten und Anforderungen der KI-VO zu ermitteln.[9] Diese Aufgaben können in erster Linie durch die KI-Marktüberwachungsbehörden sachgerecht wahrgenommen werden, denn diese müssen sicherstellen, dass KI-Systeme die Anforderungen der KI-VO einhalten.[10] Daher verfügen die KI-Marktüberwachungsbehörden über praktische Erfahrungen bei der Herstellung von Konformität mit den Vorgaben der KI-VO. Diese können sie einerseits beim Betrieb der KI-Reallabore an die Unternehmen weitergeben. Andererseits können die Behörden beim Betrieb des KI-Reallabors wertvolle Erfahrungen sammeln, die ihnen in ihrer regulatorischen Praxis als KI-Marktüberwachungsbehörde zu Gute kommen.

Die von den Mitgliedstaaten der Europäischen Union benannten Marktüberwachungsbehörden üben gem. Art. 70 Abs. 1 S. 2 KI-VO ihre Befugnisse unabhängig aus. Für bestimmte Hochrisiko-KI-Systeme ist sogar die völlige Unabhängigkeit der Marktüberwachungsbehörden, d.h. die organisatorische und institutionelle Unabhängigkeit, erforderlich.[11]

II. Regelung der Zuständigkeit für die Marktüberwachung im KI-MIG

Der Bund hat diese europarechtlichen Vorgaben im Gesetz zur Marktüberwachung und Innovationsförderung von Künstlicher Intelligenz (KI-MIG) vom 22.7.2026[12] umgesetzt. In § 2 Abs. 1 KI-MIG wird grundsätzlich die Bundesnetzagentur zur KI-Marktüberwachungsbehörde bestimmt. Folgerichtig überträgt § 13 Abs. 1 S. 1 KI-MIG der Bundesnetzagentur die Aufgabe, mindestens ein KI-Reallabor einzurichten. § 13 Abs. 1 S. 2 KI-MIG stellt klar, dass von dieser Aufgabenzuweisung die Möglichkeit der Einrichtung und des Betriebs von KI-Reallaboren durch andere zuständige nationale Behörden unbe-

* Denis Lehmkemper ist der Landesbeauftragte für den Datenschutz Niedersachsen. Dr. Henning Dehnert ist Referent in der beim Landesbeauftragten für den Datenschutz Niedersachsen eingerichteten Stabsstelle für Künstliche Intelligenz.

1 Häufig wird auch die englische Bezeichnung AI regulatory sandboxes verwendet.

2 Die Autoren danken Frau Dr. Silke Jandt und Herrn Maximilian Frisch für den wertvollen Gedankenaustausch bei der Erstellung des Manuskripts.

3 Siehe Göbel/von Kruedener, GRUR-Prax 2024, 755 (756 f.) für eine ausführliche Darstellung der Anreize für die Teilnahme an KI-Reallaboren.

4 Art. 3 Nr. 48 KI-VO definiert die zuständige nationale Behörde als eine notifizierende Behörde oder eine Marktüberwachungsbehörde in Bezug auf KI-Systeme, die von Organen, Einrichtungen und sonstigen Stellen der Union in Betrieb genommen oder verwendet werden, sind.

5 Dies folgt aus Art. 57 Abs. 1 S. 1 KI-VO.

6 Art. 3 Nr. 19 KI-VO.

7 Art. 3 Nr. 26 KI-VO.

8 Botta in Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 57 Rn. 20.

9 Vgl. Art. 57 Abs. 6 KI-VO.

10 Vgl. zu den Aufgaben der Marktüberwachung Art. 3 Nr.3 Verordnung (EU) 2019/1020 des europäischen Parlaments und des Rates vom 20.6.2019.

11 Diese Anforderung ergibt sich aus Art. 74 Abs. 8 KI-VO. Eine ausführliche Darstellung hierzu findet sich bei Wünschelbaum, MMR 2025, 259 (260 f.).

12 Bundesgesetzblatt Teil 1 2026, Nr. 223 ausgegeben zu Bonn am 27.7.2026.

rührt bleibt. § 2 Abs. 6 KI-MIG überträgt für die Fälle, in denen öffentliche Stellen der Länder KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden, den Ländern die Zuständigkeit für die KI-Marktüberwachung. Die Länder sind daher verpflichtet, für diese Fälle Marktüberwachungsbehörden zu benennen. Dies ist allerdings bislang noch nicht geschehen. Bei diesen zukünftigen Marktüberwachungsbehörden können KI-Reallabore eingerichtet werden. Der Nutzerkreis dieser KI-Reallabore muss nicht auf öffentliche Stellen der Länder beschränkt sein, denn weder Art. 57 KI-VO noch § 13 KI-MIG enthält eine derartige Beschränkung.

III. Wechselwirkungen zwischen dem Betrieb von KI-Reallaboren und Datenschutzaufsicht

Sofern in KI-Reallaboren mit dort erprobten KI-Systemen personenbezogene Daten verarbeitet werden, ist neben der Herstellung der Rechtskonformität mit der KI-VO die Einhaltung der datenschutzrechtlichen Vorgaben der DS-GVO erforderlich. Um das zu gewährleisten, verpflichtet Art. 57 Abs. 10 KI-VO die zuständige nationale Behörde, welche das KI-Reallabor betreibt, die zuständigen Datenschutzbehörden einzubeziehen. In Deutschland sind das neben der Bundesbeauftragten für den Datenschutz die 17 Landesdatenschutzbehörden, die für die Aufsicht über die öffentlichen Stellen der Länder und den Großteil der Wirtschaft zuständig sind. Zielsetzung dieser Einbeziehung ist, dass die Datenschutzbehörden die Nutzer der KI-Reallabore hinsichtlich der Einhaltung der datenschutzrechtlichen Vorgaben beraten. Umgesetzt werden kann diese Beratung beispielsweise durch die Mitwirkung am Plan für das KI-Reallabor. Dieser ist ein zwischen dem teilnehmenden Anbieter und der zuständigen Behörde vereinbartes Dokument, in dem die Ziele, die Bedingungen, der Zeitrahmen, die Methodik und die Anforderungen für die im KI-Reallabor durchgeführten Tätigkeiten beschrieben werden.[13] Sofern die Datenschutzaufsichtsbehörde am Plan für das KI-Reallabor mitgewirkt und der Anbieter sich daran gehalten hat, kommt dieser nicht nur in den Genuss des Sanktionsausschlusses des Art. 57 Abs. 12 S. 2 KI-VO, sondern auch des Art. 57 Abs. 12 S. 3 KI-VO.[14] In dessen Folge können gegen die Anbieter der KI-Systeme bei der Nutzung des KI-Reallabors weder Geldbußen nach der KI-VO noch nach der DS-GVO[15] verhängt werden. Somit hat die Einbeziehung der zuständigen Datenschutzaufsichtsbehörden aus Sicht der Anbieter der KI-Systeme große Vorteile. Gerade für kleinere, neu gegründete Unternehmen, die nicht über die notwendigen Ressourcen für die Einbeziehung externer Compliance-Berater verfügen, sind diese Vorteile besonders attraktiv.

Den Ländern ist zunächst zu raten, die Einrichtung eigener KI-Reallabore als aktive Innovationsförderung und Chance zur Stärkung junger, innovativer (Start-up-)Unternehmen zu begreifen und diese Chance zu nutzen. Die Gesetzgeber in den Ländern stehen sodann vor der Fragestellung, durch welche Behördenstruktur die mit der Einrichtung von regionalen KI-Reallaboren bestehenden Möglichkeiten zur Förderung innovativer Anbieter bestmöglich genutzt werden können und welche Rolle die Datenschutzbehörden dabei spielen sollen. Denkbar wäre zunächst, die Aufgabe der KI-Marktüberwachung und damit auch der Einrichtung von KI-Reallaboren anderen Behörden als den Landesdatenschutzbeauftragten zu übertragen. Dieser Weg soll in Nordrhein-Westfalen beschritten werden. Der Entwurf eines Gesetzes für KI-Reallabore in NRW[16] sieht vor, dass das für Wirtschaft zuständige Ressort in Nordrhein-Westfalen die Aufgaben der zuständigen KI-Reallabor-Marktüberwachungsbehörde wahrnimmt und die Einrichtung und den Betrieb eines KI-Reallabors sicherstellt. Die sonstigen Aufgaben der KI-Marktüberwachung über öffentliche Stellen in Nordrhein-Westfalen sollen offenbar an eine andere Behörde übertragen werden. Zudem soll nicht die Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen, sondern eine neu zu gründende unabhängige Behörde die Aufgaben der Datenschutzaufsicht über KI-Reallabore in Nordrhein-Westfalen wahrnehmen. Sobald das KI-System in den Regelbetrieb wechselt, würde die datenschutzrechtliche Aufsicht allerdings in die Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen wechseln. Ob dadurch eine bürokratiearme Lösung für kleine Unternehmen, welche das KI-Reallabor nutzen möchten, erreicht werden kann, bleibt abzuwarten. In jedem Fall würden die Anbieter von KI-Systemen in der Regel mit bis zu vier verschiedenen Aufsichtsbehörden zu tun haben. Das wären bei der Erprobung des KI-Systems im KI-Reallabor die KI-Reallabor-Marktüberwachungsbehörde und die neu zu gründende unabhängige Datenschutzaufsichtsbehörde für KI-Reallabore. Bei Beginn des Regelbetriebes würde dann die Zuständigkeit zur Bundesnetzagentur als Marktüberwachungsbehörde und der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen als Datenschutzaufsichtsbehörde wechseln.

Vor diesem Hintergrund liegt es nahe, den gegenteiligen Weg zu erwägen und über die Konzentration der Zuständigkeiten bei einer völlig unabhängigen Behörde nachzudenken. Bei einer solchen Lösung würden die Anbieter von KI-Systemen in den Genuss eines One-Stop-Shops, d.h. einer umfassend zuständigen Behörde als einzigen Ansprechpartner, kommen. Die Anbieter würden einen intern in einer Behörde abgestimmten Plan für das KI-Reallabor von einem Ansprechpartner erhalten und könnten sich darauf verlassen, dass sie bei dessen Befolgung in allen Fällen in den Genuss des umfassenden Sanktionsausschlusses gem. Art. 57 Abs. 12 S. 2 KI-VO und Art. 57 Abs. 12 S. 3 KI-VO kommen. Bei einer Zuständigkeitskonzentration bei den Landesdatenschutzbeauftragten würde das Erfordernis der völligen Unabhängigkeit keine Herausforderung darstellen, weil diese bereits wegen Art. 52 DS-GVO besteht. Dadurch würden auch die Anforderungen des Art. 74 Abs. 8 DS-GVO erfüllt werden und ein solches KI-Reallabor wäre auch für die Erprobung von Hochrisiko-KI-Systemen sehr breit nutzbar. Dieser Vorteil entfiele hingegen bei der Übertragung der Aufgabe des Betriebes eines KI-Reallabors an eine bereits bestehende Behörde in der Landesverwaltung, die über keine völlige, d.h. organisatorische und institutionelle Unabhängigkeit, verfügt. Sofern die Zuständig-

13 Art. 3 Nr. 54 KI-VO.

14 Siehe hierzu auch Sanders-Winter/Keber/Sahm, EuDIR 2026, 44 (47).

15 So auch Botta in Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 57 Rn. 50.

16 LT-Vorlage 18/5264. Abrufbar unter https://opal.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-5223.pdf.

keitskonzentration bei den Landesdatenschutzbeauftragten erfolgen würde, würde zudem bezüglich der datenschutzrechtlichen Aufsicht bei der Überführung des im KI-Reallabors getesteten KI-Systems grundsätzlich kein Zuständigkeitswechsel erfolgen. Die Unternehmen hätten es im Ergebnis nicht mit vier verschiedenen Aufsichtsbehörden zu tun, sondern nur mit einer für den Betrieb des KI-Reallabors sowie die Datenschutzaufsicht umfassend zuständigen Behörde und ggf. der Bundesnetzagentur als zuständiger Marktüberwachungsbehörde für den Regelbetrieb des KI-Systems.

IV. Fazit und Regelungsvorschlag

Die Einrichtung regionaler KI-Reallabore stellt für die Länder eine große Chance zur Innovationsförderung dar. Davon profitieren würden insbesondere KMU einschließlich Start-up-Unternehmen. Bei der Festlegung der Zuständigkeit für die Errichtung und den Betrieb von KI-Reallaboren sollte von der Möglichkeit einer One-Stop-Shop Lösung zugunsten der Anbieter der KI-Systeme Gebrauch werden. Die damit verbundenen Vorteile des einheitlichen Ansprechpartners und des umfassenden Sanktionsausschlusses aus Art. 57 Abs. 12 S. 2 KI-VO und Art. 57 Abs. 12 S. 3 KI-VO sowie die Möglichkeit, das KI-Reallabor auch für die Erprobung von Hochrisiko-KI-Systemen sehr breit zu nutzen, würden die Attraktivität des regionalen KI-Reallabors erheblich steigern. Bei den Landesdatenschutzbeauftragten würde sich eine solche One-Stop-Shop Lösung ohne Weiteres realisieren lassen.

KI-Kompetenz aufbauen und nachweisen

70 Minuten Videoschulung 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-Expert/innen Prof. Dr. Rolf Schwartmann, Kristin Benedikt, RA Andreas Jaspers

Jetzt bestellen: www.datakontext.com/Video-KI-Kompetenz

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

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

Praxisfälle zum Datenschutzrecht XLII: Informationspflichten bei der Videoüberwachung

I. Sachverhalt

Der Lebensmittelhersteller L beabsichtigt, infolge mehrerer Vandalismusvorfälle, die sich in den vergangenen Monaten zu unterschiedlichen Tages- und Nachtzeiten ereignet haben, auf dem Gelände seines Produktionsstandorts Videokameras zu installieren.

L hat zuvor bereits andere Maßnahmen, wie verstärkte Beleuchtung zu Nachtzeiten und regelmäßige Kontrollgänge, umgesetzt, mit denen sich aber die Vorfälle nicht verhindern ließen. Es wurde auch eine vollständige Umzäunung des Geländes erwogen, was aber mit einem erheblichen technischen und wirtschaftlichen Aufwand verbunden wäre. Zudem ist nicht klar, ob die Täter/-innen ggf. eigene Beschäftigte sind, für die der Zaun kein Hindernis wäre.

Die Kameras sollen gut sichtbar an den Produktionshallen sowie an den auf dem Grundstück befindlichen Laternenmasten angebracht werden. Erfasst werden soll ausschließlich das Betriebsgelände, keine öffentlichen Verkehrsflächen. Von der Videoüberwachung betroffen sind Beschäftigte von L, Lieferanten, Besucher und Besucherinnen sowie Personen, die das Firmengelände unbefugt betreten.

Zur Gewährleistung des technisch-organisatorischen Datenschutzes existiert ein umfassendes Konzept, das insbesondere eine automatische Löschung nach kurzer Frist, eingeschränkte Zugriffsrechte, die Protokollierung stattfindender Auswertungen und eine räumliche Beschränkung der Maßnahme vorsieht.

Zur Information der sich auf dem Gelände aufhaltenden Personen hat L Hinweisschilder vorgesehen. Neben einem großen Kamerasymbol enthalten die geplanten Schilder einen QR-Code, der hinsichtlich der Informationen zu der Videoüberwachung auf die Datenschutzinformationen auf der Webseite des L verweist, wo sich ein eigener Unterabschnitt mit der Überschrift „Videoüberwachung am Produktionsstandort P“ findet. Dort weist L darauf hin, dass die Videoüberwachung auf berechtigte Interessen im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO gestützt wird sowie auf das diesbezügliche Widerspruchsrecht der betroffenen Person aus Art. 21 Abs. 1 DS-GVO. Eine nähere Konkretisierung der verfolgten berechtigten Interessen seitens L erfolgt nicht.

Einen Betriebsrat gibt es bei L nicht.

Ist die von L beabsichtigte Maßnahme grundsätzlich rechtmäßig durchführbar? Genügen die Angaben mit Blick auf die berechtigten Interessen? Genügt die Art und Weise der Informationsbereitstellung insgesamt den Vorgaben der DS-GVO? Sofern Informationspflichten verletzt werden: Welche Auswirkungen ergeben sich hierdurch für die Rechtmäßigkeit der Datenverarbeitung?

II. Musterlösung

1. Allgemeines

Die geplante Videoüberwachung unterfällt als automatisierte Verarbeitung personenbezogener Daten dem sachlichen Anwendungsbereich der DS-GVO (Art. 2 Abs. 1). Die entstehenden Bildaufnahmen stellen personenbezogene Daten im Sinne des Art. 4 Nr. 1 DS-GVO dar, da die abgebildeten Personen jedenfalls identifizierbar sind.

Damit eine Verarbeitung personenbezogener Daten rechtmäßig ist, müssen die Informationen mit Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden, vgl. ErwG 40 DS-GVO. Es stellt sich damit die Frage nach der Rechtsgrundlage für die Videoüberwachungsmaßnahme. Findet sich eine solche, kann die geplante Maßnahme grundsätzlich rechtmäßig durchgeführt werden.

Daneben treffen den Verantwortlichen mit Blick auf die Datenverarbeitung Transparenz- und Informationspflichten (Art. 12 bis 14 DS-GVO). Die Pflichten konkretisieren den Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a) DS-GVO und sollen sicherstellen, dass die Datenverarbeitung für die betroffene Person nachvollziehbar und fair ausgestaltet ist.[1] Die betroffene Person soll wissen, wer ihre Daten verarbeitet, warum, auf welcher Rechtsgrundlage, wie lange, an wen die Daten gehen und welche Rechte sie hat.

Art. 13 DS-GVO regelt die Informationspflichten, sofern personenbezogene Daten bei der betroffenen Person selbst erhoben werden (sog. Direkterhebung), z.B. mittels eines Onlineformulars. Die in Abs. 1 und Abs. 2 der Vorschrift genannten Informationen sind dieser „zum Zeitpunkt der Erhebung“ mitzuteilen.[2] Nach dem Sinn und Zweck der Bestimmung ist dies so zu verstehen, dass die Informationen (ggf. unmittelbar) vor Beginn der Datenerhebung zu geben sind.[3]

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben (sog. indirekte Erhebung), gilt Art. 14 DS-GVO. Dies ist etwa der Fall, wenn der Verantwortliche personenbezogene Daten von einer anderen Stelle erhält, z.B. von einem konzernverbundenen Unternehmen, oder aus einer anderen Quelle entnimmt, z.B. einem öffentlichen Verzeichnis.

Die im Rahmen von Art. 13 bzw. Art. 14 DS-GVO mitzuteilenden Informationen sind inhaltlich in weiten Teilen identisch.[4] Im Rahmen von Art. 14 DS-GVO trifft den Verant-

* RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl. 2016. RA Dr. Johannes Zhou ist bei der Kanzlei FPS in Frankfurt a.M. im IT- und Datenschutzrecht tätig.

1 Brink, RDV 2026, 117 (118).

2 Zu den Informationsinhalten iE vgl. unter III. 1.

3 Kühling/Buchner/Bäcker, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 13 Rn. 56.

4 Laue/Nink/Kremer, Datenschutzrecht in der betrieblichen Praxis, 3. Aufl. 2024, § 3 Rn. 3.

wortlichen zusätzlich die Pflicht, über die von der Erhebung betroffenen Datenkategorien sowie die Herkunft der Daten zu informieren (Art. 14 Abs. 1 lit. d) und Abs. 2 lit. f) DS-GVO). Da bei einer indirekten Erhebung personenbezogener Daten eine Information der betroffenen Person zum Zeitpunkt der Datenerhebung regelmäßig nicht möglich ist, bestimmt Art. 14 Abs. 3 lit. a) bis c) DS-GVO den Zeitpunkt der Information in Abhängigkeit von der jeweiligen Situation. Grundsätzlich hat die Information innerhalb einer angemessenen Frist nach Erlangung der Daten zu erfolgen, spätestens jedoch innerhalb eines Monats (Art. 14 Abs. 3 lit. a) DS-GVO).

Die Pflichten nach Art. 13 f. DS-GVO werden ergänzt durch die allgemeinen Vorgaben des Art. 12 DS-GVO zur Form und Übermittlung der Informationen. Dieser verlangt insbesondere, dass die Informationen präzise, transparent, verständlich und leicht zugänglich in einer klaren und einfachen Sprache bereitgestellt werden.

Wichtig ist, dass es sich beim Erfordernis der Rechtmäßigkeit der Datenverarbeitung und den Transparenzpflichten im Ausgangspunkt um zwei unterschiedliche Anforderungen handelt. Ein Verstoß gegen die Informationspflichten der DS-GVO führt nicht ohne Weiteres zur Rechtswidrigkeit der Datenverarbeitung. Insbesondere wenn zentrale Informationen, etwa zu den Zwecken der Datenverarbeitung oder – im Falle des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO – zu den verfolgten berechtigten Interessen, nicht oder nicht hinreichend bereitgestellt werden, stellt sich jedoch die Frage, ob und unter welchen Voraussetzungen sich ein solcher Verstoß auf die Rechtmäßigkeit der Verarbeitung als solcher auswirken kann.

2. Vorliegen eines Erlaubnistatbestands für die geplante Videoüberwachungsmaßnahme

a) Allgemeines

Bzgl. der Videoüberwachung hat der nationale Gesetzgeber in § 4 BDSG einen speziellen Erlaubnistatbestand vorgesehen. Nach dem BVerwG bietet § 4 BDSG für die Videoüberwachung durch nichtöffentliche Stellen aber keine eigenständige Rechtsgrundlage; maßgeblich ist vielmehr Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO.[5] Ohnedies wäre vorliegend auch der sachliche Anwendungsbereich von § 4 BDSG nicht eröffnet, da die Vorschrift sich nur auf die Beobachtung öffentlich zugänglicher Räume bezieht.

Öffentlich zugängliche Räume sind Bereiche, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach hierzu bestimmt sind, z.B. Verkaufsbereiche von Geschäften, Kaufhäusern und Tankstellen, Einkaufspassagen, Restaurants und Cafés sowie Schalterhallen von Banken.[6] Firmen- und Werksgelände, Betriebsstätten, Produktionsbereiche, Lager- und Personalräume sowie Büros und Arbeitsplätze ohne Publikumsverkehr stellen regelmäßig keinen öffentlich zugänglichen Bereich dar.[7] Für die Einordnung eines Raumes als öffentlich zugänglich kommt es dabei nicht entscheidend auf die bauliche Gestaltung oder eine entsprechende Beschilderung an. Maßgeblich ist vielmehr, ob der Berechtigte den Zutritt nach außen erkennbar auf einen bestimmten Personenkreis beschränkt.[8]

b) Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO

Eine Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO rechtmäßig, wenn die folgenden drei Voraussetzungen kumulativ erfüllt sind:[9]

1. Der Verantwortliche oder ein Dritter verfolgen berechtigte Interessen mit der Verarbeitung.
2. Die Verarbeitung ist zur Wahrung der berechtigten Interessen erforderlich.
3. Die Interessen bzw. Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen nicht die berechtigten Interessen.

Diese Voraussetzungen sind in Bezug auf die von L beabsichtigte Videoüberwachung, konkret die Erhebung und -speicherung der Videodaten, grundsätzlich gegeben:

Berechtigte Interessen sind nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen.[10] Darunter fallen auch die von L mit der Videoüberwachung verfolgten Interessen, die namentlich im Schutz des Eigentums vor Vandalismus sowie der Beweissicherung zur Durchsetzung von Rechtsansprüchen bestehen.[11]

Die Erhebung und -speicherung der Videodaten ist zur Wahrung der berechtigten Interessen erforderlich, da sie geeignet ist, weitere Vandalismusschäden durch ihre abschreckende Wirkung möglichst zu verhindern bzw. zukünftige Taten aufzuklären und Beweise zu sichern. Angesichts der bereits mehrfach eingetretenen Vandalismusvorfälle ist kein gleich wirksames, die betroffenen Personen weniger beeinträchtigendes Mittel ersichtlich. Insbesondere konnten die verstärkte Beleuchtung sowie Kontrollgänge weitere Vorfälle nicht verhindern. Auch dass das Betriebsgelände nicht vollständig eingefriedet ist, steht der Erforderlichkeit der Maßnahme nicht entgegen. Denn eine solche Maßnahme wäre nach den Angaben im Sachverhalt sehr aufwendig, ohne dass klar ist, dass die Vorfälle hierdurch verhindert werden könnten. Auf eine solche Maßnahme muss sich L daher nicht verweisen lassen. Zudem wäre auch eine "bemannte Beobachtung" als Alternative zur Speicherung der Videodaten nicht weniger eingriffsintensiv. Bei einer solchen Vorgehensweise werden zwar keine Daten gespeichert. Allerdings werden die den relevanten Bereich passierenden Personen aber zwangsläufig beobachtet, während bei einer Speicherung die Daten für die allermeisten betroffenen Personen im Ergebnis ohne Sichtung automatisch gelöscht werden.

Schließlich ist davon auszugehen, dass auch im Rahmen einer Interessenabwägung im Einzelfall jedenfalls grundsätzlich die beschriebenen berechtigten Interessen des Verantwortlichen L überwiegen. In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass die Kameras sichtbar im Außenbereich und nicht im Innenbereich des Produktionsstandortes angebracht werden sollen. Vorausgesetzt, die überwachten Bereiche dienen nicht dem längerfristigen Aufenthalt, sondern werden von Beschäftigten, Besuchern

5 BVerwG, Urt. v. 27.3.2019 – 6 C 2.18.

6 Simitis/Hornung/Spiecker gen. Döhmann/Schindler/Scholz, Datenschutzrecht, 2. Aufl. 2025, BDSG § 4 Rn. 53.

7 Simitis/Hornung/Spiecker gen. Döhmann/Schindler/Scholz, Datenschutzrecht, 2. Aufl. 2025, BDSG § 4 Rn. 57.

8 Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 56. Ed. 1.8.2024, BDSG § 4 Rn. 10.

9 EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, 8.10.2024, S. 2.

10 Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 146a.

11 DSK, Orientierungshilfe Videoüberwachung durch nicht öffentliche Stellen, 17.7.2020, S. 8, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_vü_dsk.pdf; Kühling/Buchner/Buchner/Petri, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 6 Rn. 172a.

und Besucherinnen sowie sonstigen Personen im Alltag typischerweise nur kurz passiert, ist die damit verbundene Eingriffsintensität tendenziell als gering einzustufen. Zudem werden keine öffentlichen Flächen und sich dort aufhaltende Personen erfasst durch die Maßnahme.

Zwischenergebnis: Die beabsichtigte Maßnahme ist über Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO grundsätzlich legitimierbar.

Zu klären ist allerdings noch, ob vorliegend die Informationspflichten nach Art. 13 f. DS-GVO eingehalten wurden und, falls dies nicht der Fall ist, ob sich ein Verstoß gegen die Transparenzpflichten auf die Rechtmäßigkeit der Videoüberwachung auswirkt.

3. Transparenzpflichten und Auswirkungen auf die Rechtmäßigkeit der Datenverarbeitung

a) Abgrenzung von Art. 13 und 14 DS-GVO

Bei einer Erhebung durch Videoüberwachung handelt es sich grundsätzlich um eine Direkterhebung im Sinne von Art. 13 DS-GVO.[12] Dass die betroffene Person die Datenerhebung nicht selbst veranlasst oder aktiv an ihr mitwirkt, steht dem nicht entgegen.

Ließe man die Anwendung des Art. 14 DS-GVO auf Fälle zu, in denen personenbezogene Daten mittels Videoaufzeichnung erhoben werden, hätte dies zur Folge, dass die betroffenen Personen nicht bereits zum Zeitpunkt der Datenerhebung informiert werden müssten, obwohl sie selbst die Quelle der erhobenen Daten sind. Nach Auffassung des EuGH bestünde dadurch die Gefahr einer von der betroffenen Person unbemerkten Datenerfassung und damit verdeckter Überwachungspraktiken.[13] Eine solche Folge wäre mit dem Ziel der DS-GVO, ein hohes Schutzniveau für die Grundfreiheiten und Grundrechte natürlicher Personen zu gewährleisten, unvereinbar, so der EuGH.[14]

Maßstab für die korrekte Information ist hier also Art. 13 DS-GVO.

Die Einordnung als Direkterhebung hat zur Konsequenz, dass grundsätzlich bereits zum Zeitpunkt der Erhebung informiert werden muss – also praktisch vor bzw. beim Betreten des überwachten Bereichs. Die Leitlinien des Europäischen Datenschutzausschusses (EDSA)[15] sehen hierfür einen mehrstufigen („layered") Informationsansatz vor, den auch der EuGH[16] bestätigt hat.[17]

b) Vorliegen von Verstößen gegen Art. 13 DS-GVO

aa) Fehlende Mitteilung der konkret verfolgten berechtigten Interessen

Nach Art. 13 Abs. 1 lit. d) DS-GVO[18] hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Datenerhebung die berechtigten Interessen mitzuteilen, die von dem Verantwortlichen oder einem Dritten verfolgt werden, wenn die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO beruht.

Nach der Rechtsprechung des EuGH müssen im Rahmen der Information nach Art. 13 Abs. 1 lit. d) DS-GVO „die verfolgten berechtigten Interessen" mitgeteilt werden.[19] Das bedeutet, es ist das jeweilige konkrete berechtigte Interesse zu identifizieren, das mit der Verarbeitung verfolgt wird. Eine bloße Wiedergabe der gesetzlichen Formel oder eine rein abstrakte Bezugnahme auf „berechtigte Interessen" genügt nach der Vorschrift grundsätzlich nicht.[20] Eine ausdrückliche Verpflichtung, im Rahmen der Information nach Art. 13 Abs. 1 lit. d) DS-GVO über die vorgenommene Interessenabwägung zu informieren,[21] wie sie teilweise in der Literatur vertreten wird, lässt sich der bisherigen Rechtsprechung des EuGH hingegen nicht entnehmen.

Über die vom EuGH ausdrücklich hervorgehobene Pflicht zur Information über die verfolgten berechtigten Interessen hinaus konkretisiert der EDSA in Rn. 67 der Leitlinien 1/2024, dass diese Interessen „präzise" zu identifizieren sind.[22] Zudem sieht Rn. 68 vor, dass die Information gegenüber der betroffenen Person erkennen lassen soll, dass diese auf Anfrage weitere Informationen über die vorgenommene Interessenabwägung erhalten kann. Mit Blick auf die letztgenannte Anforderung stellt sich allerdings die Frage, ob sich eine entsprechende Informationspflicht noch unmittelbar aus der DS-GVO ableiten lässt oder ob der EDSA mit Rn. 68 eine über die ausdrücklich normierten Informationspflichten hinausgehende Transparenzanforderung formuliert.

Die pauschale Angabe durch L, dass die Videoüberwachung auf berechtigte Interessen im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO gestützt wird, ohne diese Interessen näher zu konkretisieren, genügt den dargestellten Anforderungen aus Art. 13 Abs. 1 lit. d) DS-GVO nicht. L hätte zumindest angeben müssen, dass die Maßnahme dem Schutz seines Eigentums vor Vandalismus sowie der Beweissicherung zur Durchsetzung von Rechtsansprüchen dient.

Zwischenfazit: Wird die Maßnahme durchgeführt wie geplant, so wird Art. 13 Abs. 1 lit. d) DS-GVO verletzt.

bb) Unzulässiger Medienbruch

Der Verantwortliche ist nach Art. 12 Abs. 1 S. 1 DS-GVO verpflichtet, die Informationen nach Art. 13 DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache bereitzustellen. Die betroffene Person muss also in der Lage sein, die Informationen ohne unverhältnismäßige tatsächliche oder technische Hürden zur Kenntnis zu nehmen.

In der Praxis ist es nicht unüblich, dass betroffene Personen „Erstinformationen" zum Datenschutz über einen physischen Informationsträger, etwa ein Hinweisschild oder ein Papierformular, erhalten, für weiterführende Datenschutzinformationen aber auf ein digitales Medium verwiesen werden, z.B. auf eine über einen Link bzw. QR-Code abrufbare Website. Dieser sog. „Medienbruch" im Zusammenhang mit der Informationserteilung ist in der DS-GVO nicht ausdrücklich geregelt.

12 EuGH, Urt. v. 18.12.2025 – C-422/24 („Bodycam").

13 EuGH, Urt. v. 18.12.2025 – C-422/24 („Bodycam") Rn. 41.

14 EuGH, Urt. v. 18.12.2025 – C-422/24 („Bodycam") Rn. 40.

15 Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Vers. 2.0 v. 29.1.2020, Rn. 110 ff.

16 EuGH, Urt. v. 18.12.2025 – C-422/24 Rn. 42.

17 Vgl. dazu nachfolgend b) bb).

18 S. auch Art. 14 Abs. 2 lit. b) DS-GVO.

19 EuGH, Urt. v. 9.1.2025 – C-394/23 Rn. 46 und 52; EuGH, Urt. v. 4.10.2024 – C-621/22 Rn. 41; EuGH, Urt. v. 4.7.2023 – C-252/21 Rn. 107.

20 Simitis/Hornung/Spiecker gen. Döhmann/Dix, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 13 Rn. 10; Gola/Heckmann/Rost/Franck, DS-GVO BDSG, 4. Aufl. 2026, DS-GVO Art. 13 Rn. 15; ähnlich Wolff/Brink/v. Ungern-Sternberg/Schmidt-Wudy, BeckOK Datenschutzrecht, 56. Ed. 1.5.2026, DS-GVO Art. 13 Rn. 49; Sydow/Marsch/Ingold, DS-GVO BDSG, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 18.

21 Vgl. etwa Ehmann/Selmayr/Knyrim, Datenschutz-Grundverordnung, 3. Aufl. 2024, DS-GVO Art. 13 Rn. 49; Kühling/Buchner/Bäcker, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 13 Rn. 27; Taeger/Gabel/Mester, DSGVO-BDSG-TDDDG, 5. Aufl. 2026, DS-GVO Art. 13 Rn. 13.

22 EDSA, Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Vers. 1.0, adopted on 8 October 2024.

Die Vorgaben des Art. 12 Abs. 1 S. 1 DS-GVO stehen einer solchen Vorgehensweise nicht entgegen, sofern die erforderlichen Informationen für die betroffenen Personen leicht zugänglich bleiben. Die gestufte Erteilung der Datenschutzinformationen kann nach dem EDSA aus Sicht der betroffenen Personen sogar Vorteile bieten, da auf der ersten Ebene eine Konzentration auf die wesentlichen Informationen erfolgt und auf diese Weise einer Überforderung durch die Vielzahl der rechtlich erforderlichen Informationen entgegengewirkt werden kann.[23] Für nicht digitale Umgebungen erkennt der EDSA in diesem Zusammenhang auch eine gestufte Informationserteilung über unterschiedliche Kommunikationsmodalitäten an, bei der ein Teil der Informationen über ein anderes Medium bereitgestellt wird.[24] In seiner Entscheidung zu den „Bodycams" hat der EuGH diese Interpretation der Transparenzregelungen durch den EDSA bestätigt.[25]

Sofern ein Medienbruch erfolgt,[26] ist von praktischer Bedeutung allerdings, dass Teile der Datenschutzinformationen aufgrund ihrer besonderen Bedeutung bereits unmittelbar bei Datenerhebung zu erteilen sind und nur mit Blick auf die weiteren notwendigen Informationen zum Datenschutz auf nachfolgende Ebenen verwiesen werden darf. In diesem Zusammenhang wird insofern auch von „First-Level-" und „Second-Level-Informationen" gesprochen. Zur Vermittlung der Informationen auf der zweiten Ebene kann nach den Leitlinien des EDSA ausdrücklich auch ein QR-Code zum Einsatz kommen.[27] Voraussetzung sei jedoch, dass die Informationen daneben auch auf nicht digitalem Wege leicht verfügbar sind.[28]

Der allgemeine Ansatz der gestuften Informationserteilung wird in den Leitlinien 3/2019 des EDSA[29] zur Verarbeitung personenbezogener Daten durch Videogeräte für diese spezifische Konstellation konkretisiert. Nach der DSK-Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen" aus dem Jahr 2020, bei deren Erstellung die EDSA-Leitlinien 3/2019 berücksichtigt wurden, sind im Rahmen der Videoüberwachung die wesentlichen Informationen auf der ersten Informationsebene durch ein vorgelagertes Hinweisschild bereitzustellen.[30]

Nach der DSK-Orientierungshilfe muss das vorgelagerte Hinweisschild, für das die Orientierungshilfe auch ein Muster enthält, mindestens über folgende Punkte informieren:[31]

- den Umstand der Beobachtung, insbesondere durch ein Piktogramm bzw. Kamerasymbol,
- die Identität des Verantwortlichen sowie ggf. des Vertreters nach Art. 27 DS-GVO einschließlich der Kontaktdaten,
- die Kontaktdaten des betrieblichen Datenschutzbeauftragten, soweit ein solcher benannt wurde,
- die Verarbeitungszwecke und die Rechtsgrundlage in Schlagworten,
- das berechtigte Interesse, soweit die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO beruht,
- ggf. die Dauer der Speicherung sowie
- einen Hinweis auf die weiteren Pflichtinformationen, insbesondere das Auskunfts- und Beschwerderecht sowie gegebenenfalls die Empfänger der Daten, und deren Zugang.

Darüber hinaus sind nach der DSK jedenfalls der Umstand der Beobachtung sowie der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Die betroffenen Personen müssen somit erkennen können, dass sie einen überwachten Bereich betreten.[32]

Dem hier zu beurteilenden Sachverhalt ist nicht eindeutig zu entnehmen, ob betroffene Personen bereits vor Betreten des überwachten Bereichs erkennen können, dass eine Videoüberwachung stattfindet. Dies kann aber auch dahinstehen, da die Transparenzanforderungen im vorliegenden Fall in jedem Fall nicht gewahrt sind. Ein vorgelagertes Hinweisschild, das lediglich die Abbildung einer Kamera und einen QR-Code enthält, die wesentlichen „First-Level"-Informationen jedoch nicht selbst bereitstellt, genügt den Anforderungen der Aufsichtsbehörden nicht.

Zwischenfazit: Die Art und Weise der Bereitstellung der Datenschutzinformationen entspricht insgesamt nicht den Vorgaben der DS-GVO.

c) Auswirkungen der Transparenzverstöße auf die Rechtmäßigkeit der Verarbeitung

Fraglich ist zunächst, ob sich die fehlende Mitteilung der konkret verfolgten berechtigten Interessen auf die Rechtmäßigkeit der Videoüberwachung auswirkt. Wie unter 1. dargestellt, stellen das Erfordernis einer wirksamen Rechtsgrundlage und die Einhaltung der Transparenzpflichten im Ausgangspunkt getrennte Anforderungen dar. Nicht jede geringe Verletzung der Pflichten aus Art. 13 f. DS-GVO kann insofern die Rechtswidrigkeit der Verarbeitung begründen. Auch der Wortlaut des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO nimmt keinen Bezug auf die Mitteilung der berechtigten Interessen.

Eine Verletzung der Art. 13 f. DS-GVO wird nach hier vertretener Ansicht aber dann zur materiellen Unrechtmäßigkeit der Verarbeitung führen können, wenn das Transparenzdefizit über ein bloßes Informationsdefizit hinausgeht und die materiellen Voraussetzungen der einschlägigen Rechtsgrundlage berührt. Denn die Intransparenz der Datenverarbeitung, insbesondere im Hinblick auf die verfolgten Zwecke und berechtigten Interessen, kann sich im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO zulasten der verarbeitenden Stelle auswirken. Dies gilt insbesondere, wenn Mängel bei der Transparenz dazu führen,

23 Art.-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01) v. 11.4.2018, Rn. 35, bestätigt durch den EDSA am 25.5.2018.

24 Art.-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01) v. 11.4.2018, Rn. 38, bestätigt durch den EDSA am 25.5.2018; EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Vers. 2.0 v. 29.1.2020, Rn. 110 ff.

25 EuGH, Urt. v. 18.12.2025 – C-422/24 („Bodycam") Rn. 42.

26 Eine gestufte Informationserteilung ist auch möglich, ohne dass ein Medienbruch erfolgt, z.B. in digitalen Umgebungen durch den Einsatz von Links.

27 EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Vers. 2.0 v. 29.1.2020 Rn. 117.

28 EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Vers. 2.0 v. 29.1.2020 Rn. 117.

29 EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Vers. 2.0 v. 29.1.2020.

30 DSK, Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen" v. 17.7.2020, S. 17 f.

31 DSK, Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen" v. 17.7.2020, S. 17 f. und S. 40 f.

32 DSK, Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen" v. 17.7.2020, S. 17.

dass die betroffene Person vernünftigerweise nicht mit der betreffenden Verarbeitung rechnen muss. Dass die vernünftigen Erwartungen der betroffenen Person im Rahmen der Interessenabwägung zu berücksichtigen sind, ergibt sich ausdrücklich aus ErwG 47 S. 4 DS-GVO.

Mit den Auswirkungen einer unterbliebenen Information über die verfolgten berechtigten Interessen nach Art. 13 Abs. 1 lit. d) DS-GVO hatte sich auch der EuGH in der Rechtssache Mousse[33] zu befassen. Er stellte fest, dass die Verarbeitung personenbezogener Daten hinsichtlich der Anrede der Kunden eines Transportunternehmens, die darauf abzielt, die geschäftliche Kommunikation aufgrund ihrer Geschlechtsidentität zu personalisieren, nicht als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich angesehen werden kann, wenn den Kunden bei der Erhebung dieser Daten das verfolgte berechtigte Interesse nicht mitgeteilt wurde.[34] Der EuGH beschränkt die Wirkung der unterbliebenen Information also nicht auf einen Verstoß gegen die Transparenzpflicht nach Art. 13 Abs. 1 lit. d) DS-GVO, sondern misst ihr Bedeutung auch für die materielle Rechtmäßigkeit der Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO zu.[35]

Die Rechtsprechung des EuGH ist in ihrer Pauschalität allerdings kritisch zu sehen. Zwar folgt aus Art. 13 Abs. 1 lit. d) DS-GVO grundsätzlich die Pflicht, der betroffenen Person zum Zeitpunkt der Datenerhebung die konkret verfolgten berechtigten Interessen mitzuteilen. Die fehlende Mitteilung dieser Interessen als generelle Tatbestandsvoraussetzung[36] bzw. als Ausschlussgrund für die Heranziehung von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO einzuordnen, kann jedoch zu unverhältnismäßigen Ergebnissen führen. Dies gilt insbesondere in Fällen, in denen für die betroffene Person auch ohne ausdrückliche Mitteilung des berechtigten Interesses ohne Weiteres erkennbar ist, welchem berechtigten Interesse die Verarbeitung dient.

Für eine zurückhaltendere Betrachtung spricht auch die systematische Unterscheidung der DS-GVO zwischen den materiellen Voraussetzungen einer rechtmäßigen Verarbeitung und den eigenständigen Transparenzpflichten. Nach hier vertretener Ansicht bedarf es insofern jeweils der konkreten Prüfung im Einzelfall, ob das Transparenzdefizit über die Verletzung einer eigenständigen Informationspflicht hinausgeht und tatsächlich eine materielle Voraussetzung der einschlägigen Rechtsgrundlage berührt.[37]

Wenn, wie vorliegend, eine Videoüberwachung auf Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO gestützt wird und der Verantwortliche den betroffenen Personen bei Datenerhebung das von ihm verfolgte berechtigte Interesse überhaupt nicht mitteilt, bestehen nach der EuGH-Entscheidung in der Rechtssache Mousse[38] erhebliche Gründe dafür, nicht nur einen Verstoß gegen die Transparenzpflichten anzunehmen, sondern die Rechtswidrigkeit der Datenverarbeitung für die Videoüberwachung als solcher.

Zwischenergebnis: Die fehlende Mitteilung der konkret verfolgten berechtigten Interessen mit Blick auf die Videoüberwachungsmaßnahme durch L führt zur Rechtswidrigkeit der mit der Maßnahme zusammenhängenden Verarbeitung personenbezogener Daten.

Zu der Frage, welche Folgen ein gegen Art. 13 DS-GVO verstoßender Medienbruch hat, hat sich der EuGH, soweit ersichtlich, bislang nicht geäußert. Es spricht jedoch einiges dafür, dass der EuGH auch in diesem Fall eine strenge Linie verfolgen und damit eine Rechtswidrigkeit der Datenverarbeitung annehmen würde. Den betroffenen Personen werden im unmittelbaren Zeitpunkt der Datenerhebung sämtliche zentralen Informationen über die konkrete Verarbeitung vorenthalten. Sie erfahren zu diesem Zeitpunkt lediglich, dass eine Videoüberwachung stattfindet, nicht jedoch, wer für die Verarbeitung verantwortlich ist, zu welchen Zwecken die Aufnahmen erfolgen und auf welcher Rechtsgrundlage dies geschieht. Damit können sie die Verarbeitung im Zeitpunkt der Erhebung nicht in der von Art. 13 DS-GVO vorausgesetzten Weise nachvollziehen und ihre Rechte nicht sachgerecht wahrnehmen.[39]

Da sich die Rechtswidrigkeit der Datenverarbeitung zumindest mit Blick auf die fehlende Mitteilung der verfolgten berechtigten Interessen durch L ergibt, kann die Beantwortung der Frage hier letztlich offenbleiben.

4. Ergebnis

Die von L vorgesehene Maßnahme ist grundsätzlich über Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO legitimierbar. Wird die Maßnahme durchgeführt wie geplant, würden die datenschutzrechtlichen Informationspflichten nach der Rechtsprechung des EuGH allerdings in einem solchen Maße verletzt, dass dies wohl auch die Rechtswidrigkeit der Erhebung und Speicherung der Videodaten zur Folge hat. L sollte die vorgelagerten Hinweisschilder zur Videoüberwachung an die Mustervorgaben der DSK anpassen sowie insbesondere die von ihm verfolgten berechtigten Interessen konkretisieren.[40]

III. Ergänzende Informationen

1. Inhalte der Informationspflicht

Verantwortliche sind nach Art. 13 Abs. 1 DS-GVO verpflichtet, der betroffenen Person folgende Informationen mitzuteilen:

- Name und Kontaktdaten des Verantwortlichen, ggf. seines Vertreters (lit. a)),
- ggf. die Kontaktdaten des Datenschutzbeauftragten (lit. b)),
- Zwecke und Rechtsgrundlage für die Verarbeitung (lit. c)),
- bei Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO die verfolgten berechtigten Interessen (lit. d)),
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (lit. e)) und
- ggf. die Absicht einer Übermittlung an ein Drittland oder eine internationale Organisation sowie das Bestehen oder Fehlen eines Angemessenheitsbeschlusses bzw. – bei Übermittlungen auf Grundlage geeigneter

33 EuGH, Urt. v. 9.1.2025 – C-394/23.

34 EuGH, Urt. v. 9.1.2025 – C-394/23 Ls. 1.

35 Zur engen Verknüpfung der Mitteilung des berechtigten Interesses mit den materiellen Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO durch den EuGH vgl. auch Urt. v. 4.7.2023 – C-252/21 (Meta Platforms), Rn. 107, 126.

36 Leicht/Baumann, NJW 2025, 2126 Rn. 22.

37 Pauschale Beurteilungen ablehnend auch Gola/Heckmann/Rost/Franck, DS-GVO BDSG, 4. Aufl. 2026, DS-GVO Art. 13 Rn. 59.

38 EuGH, Urt. v. 9.1.2025 – C-394/23.

39 Zum Sinn und Zweck der Transparenzvorgaben Art.-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev.01) v. 11.4.2018, Rn. 4, bestätigt durch den EDSA am 25.5.2018.

40 DSK, Orientierungshilfe „Videoüberwachung durch nicht öffentliche Stellen" v. 17.7.2020, S. 40 f.

oder angemessener Garantien – einen Hinweis auf die einschlägigen Garantien und darauf, wie eine Kopie von ihnen erhältlich ist oder wo sie verfügbar sind (lit. f)).

Zusätzlich hat der Verantwortliche der betroffenen Person nach Art. 13 Abs. 2 DS-GVO folgende Informationen zur Verfügung zu stellen:

- Speicherdauer der Daten oder, falls nicht möglich, zumindest Kriterien für ihre Festlegung (lit. a)),
- das Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit (lit. b)),
- bei einwilligungsbasierter Verarbeitung: das Bestehen eines Rechts auf jederzeitigen Widerruf mit Wirkung für die Zukunft (lit. c)),
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (lit. d)),
- ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob eine Bereitstellungspflicht besteht und welche Folgen die Nichtbereitstellung hätte (lit. e)) und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DS-GVO sowie aussagekräftige Informationen über die Logik, Tragweite und Auswirkungen (lit. f)).

Die Trennung der Inhalte auf zwei Absätze hat keinen Einfluss auf die Informationspflicht, da sämtliche Informationen der betroffenen Person gleichermaßen zur Verfügung zu stellen sind.[41]

Bei der Informationspflicht nach Art. 14 DS-GVO hat der Verantwortliche neben den genannten Inhalten zudem über die Kategorien der verarbeiteten personenbezogenen Daten (Art. 14 Abs. 1 lit. d) DS-GVO) und die Quelle der erhobenen Daten (Art. 14 Abs. 2 lit. f) DS-GVO) zu informieren.

2. Ausnahmen von der Informationspflicht

Nach Art. 13 Abs. 4 DS-GVO finden die Absätze 1 bis 3 keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt. Aufgrund des Wortlautes („soweit") ist es möglich, dass die Informationspflicht insgesamt oder auch teilweise entfallen kann.[42]

Art. 14 Abs. 5 DS-GVO sieht demgegenüber zusätzliche Ausnahmen von der Informationspflicht bei indirekter Erhebung vor, und zwar, wenn sich die Erteilung der Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde bzw. die Erteilung die Verwirklichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde (lit. b)), die Erlangung oder Offenlegung der personenbezogenen Daten durch Rechtsvorschriften der Union oder der Mitgliedstaaten ausdrücklich geregelt ist (lit. c)) oder die personenbezogenen Daten aufgrund einer gesetzlichen Geheimhaltungspflicht oder eines Berufsgeheimnisses vertraulich behandelt werden müssen (lit. d)).

Weitere Ausnahmen von den Informationspflichten sind im nationalen Recht in den §§ 29, 32, 33 BDSG geregelt.

41 Taeger/Gabel/Mester, DSGVO-BDSG-TDDDG, 5. Aufl. 2026, DS-GVO Art. 13 Rn. 17.

42 Ehmann/Selmayr/Knyrim, Datenschutz-Grundverordnung, 3. Aufl. 2024, DS-GVO Art. 13 Rn. 78.

Best Practice.
Best Command.

Alles für die Vertragsgestaltung im IT- und telekommunikationsrechtlichen Bereich

Das praxisnahe Werk zur Vertragsgestaltung in den IT- und telekommunikationsrechtlichen Bereichen enthält zahlreiche ausführlich kommentierte Vertragsmuster. Klausel für Klausel nehmen erfahrene Praktiker zu allen praxisrelevanten Fragen Stellung und liefern Lösungen.

Updates im September 2026:
› Standardsoftware-Kauf (B2B)
› Anpassung von Standardsoftware
› Auftragsverarbeitung

Für Abonnenten inklusive Datenbank Redeker online u. a. mit folgenden Inhalten: *Redeker* Handbuch der IT-Verträge, *Härting* Internetrecht, *Schneider* Handbuch EDV-Recht, *Schuster/Grützmacher* IT-Recht Kommentar.

Leseprobe und Bestellung: **otto-schmidt.de**

Redeker (Hrsg.) **Handbuch der IT-Verträge**
Herausgegeben von RA, FA IT-Recht, Dipl.-Informatiker Dr. Helmut Redeker. Loseblatt, 3 Bände. Grundwerk mit Fortsetzungsbezug für mindestens 2 Jahre, 199 €, ca. 2–3 Ergänzungslieferungen pro Jahr, für Abonnenten inklusive der Datenbank Redeker online, je zzgl. 23 € inkl. MwSt. für Redeker online.
ISBN 978-3-504-56008-9.

Das Werk online
otto-schmidt.de/bmitr
juris.de/itr

Answers
otto-schmidt.de/answers

ottoschmidt

Prof. Dr. Tobias Keber/Tobias List*

Die „Stuttgarter Impulse zur Modernisierung des Datenschutzes" Eckpunkte aus Sicht der Aufsichtspraxis

Zukunftsfähiger Datenschutz schützt die Grundrechte der Menschen und gewährleistet gleichermaßen eine effektive Datennutzung. Mit den „Stuttgarter Impulsen" zur Modernisierung des Datenschutzes haben die Datenschutzaufsichtsbehörden der Länder auf der 111. Datenschutzkonferenz im Juni einstimmig Vorschläge für Reformen unterbreitet, sowohl im materiellen Datenschutzrecht als auch in der Datenschutzaufsichtsstruktur im kooperativen Föderalismus.[1] Damit werden die Ziele der föderalen Modernisierungsagenda[2] ebenso erreicht, wie sich die Stärken der föderalen Aufsichtsstruktur nutzen lassen. Die Initiative nebst Konsultation soll zu einer evidenzbasierten Reformdebatte beitragen.

I. Wegmarken der Reformdebatte

Die Debatte um eine Neuordnung der Datenschutzaufsicht in Deutschland ist nicht neu, sie hat aber im vergangenen Jahr im Zuge einer von der Politik (einmal mehr)[3] identifizierten Notwendigkeit zum Bürokratieabbau Fahrt aufgenommen. Die Initiative für einen handlungsfähigen Staat beklagt zunächst in einem Zwischenbericht und dann in ihrem im Juli 2025 vorgestellten Abschlussbericht, „ein überzogener Datenschutz [sei] für viele inzwischen zum Ärgernis geworden". Es folgen zahlreiche Behauptungen zu einem angeblich „in Deutschland strenger angewendetem Datenschutz als in anderen EU-Staaten".[4] Nachweise oder Belege für die aufgestellten Thesen gibt es nicht. Die Initiative schlägt zahlreiche materiell-rechtliche Änderungen vor, wie beispielsweise eine Reduktion von Informationspflichten, eine „Grundsatzumkehr" weg von der vorherigen Einwilligung hin zu einer grundsätzlichen Verwertung mit Widerspruchslösung, der gänzlichen Ausnahme von nicht-kommerziellen Tätigkeiten aus der DS-GVO sowie der Abschaffung von Datenschutzbeauftragten für kleine und mittlere Unternehmen. Auch mit Blick auf die Aufsichtsstruktur enthält der Abschlussbericht konkrete Forderungen:

„Die Aufsicht über den nicht öffentlichen Bereich (Unternehmen), die heute durch die Datenschutzaufsichtsbehörden der Länder ausgeübt wird, sollte bei der Bundesbeauftragten erfolgen, um eine uneinheitliche Rechtsauslegung zu vermeiden, die Effizienz zu steigern und eine Spezialisierung zu ermöglichen (etwa auf KI, Wissenschaft, Werbung, Kreditwirtschaft). Dies muss insbesondere für länderübergreifend arbeitende und international agierende Unternehmen gelten."[5]

Zwischen der Veröffentlichung des Zwischenberichts und des Abschlussberichts der Initiative für einen handlungsfähigen Staat fällt der Koalitionsvertrag „Verantwortung für Deutschland" zwischen CDU/CSU und SPD für die 21. Legislaturperiode, der ebenfalls eine Datenschutzaufsichtsreform beinhaltet, die (wenngleich möglicherweise nur aufgrund redaktioneller Ungenauigkeiten) an zwei verschiedenen Stellen des Papiers zu finden sind. So heißt es auf Seite 65 (Zeile 2094 ff.) unter der Überschrift „Datenschutz entbürokratisieren", dass die regierenden Parteien „die Datenschutzaufsicht [reformieren] und [diese] beim Bundesdatenschutzbeauftragten [bündeln]", was wenig später nochmals konkretisiert wird: „Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an."[6] Inwieweit überhaupt ein einheitliches Interesse der Wirtschaft definierbar ist, bleibt dabei ebenso offen wie eine genaue Definition, was eine „Bündelung der Zuständigkeiten und Kompetenzen" umfassen könnte. Gleichzeitig solle die Datenschutzkonferenz gesetzlich im BDSG verankert werden, so der Koalitionsvertrag weiter.[7]

Die 5. Digitalministerkonferenz (DMK) am 12. und 13.5.2026 in Hamburg sprach sich für einen „Paradigmenwechsel im Datenschutz" sowie für mehr risikoabhängige Pflichten und eine Entlastung von KMUs und Start-ups aus.[8] Ein erster konkreter Vorschlag zur gesetzlichen Ausgestaltung der Datenschutzaufsichtsreform liegt seit Juni 2026 vor, eingebracht allerdings nicht von der Bundesregierung, sondern als Bundesratsinitiative der Freien und Hansestadt Hamburg, die vom Bundesrat am 10.7.2026[9] beschlossen wurde. Darin wird

* Prof. Dr. Tobias Keber ist Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Tobias List ist persönlicher Referent ebenda. Transparenzhinweis: Die Autoren des Beitrags haben maßgeblich an der Formulierung der Stuttgarter Impulse mitgearbeitet.

1 Die Stuttgarter Impulse zur Modernisierung des Datenschutzes (SIMD) sind abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2026/06/Stuttgarter-Impulse.pdf.

2 Ziel 158 der Föderalen Modernisierungsagenda, online abrufbar unter: https://www.bundesregierung.de/resource/blob/975228/2397654/c57248be7fa2d61ab6d8b12c0f29f05b/2025-12-04-mpk-staatsmodernisierung-data.pdf?download=1.

3 Für eine kurze Geschichte politischer Bürokratieabbauprojekte seit 1846 Roßnagel/Wallmann/Keber, Bürokratieabbau im Datenschutz, Nomos 2025, S. 113 ff.

4 Initiative für einen handlungsfähigen Staat (2025): Abschlussbericht. Online verfügbar unter: https://www.ghst.de/fileadmin/images/01_Bilddatenbank_Website/Demokratie_staerken/Initiative_f%C3%BCr_einen_handlungsf%C3%A4higen_Staat/Abschlussbericht/Abschlussbericht_neu.pdf.

5 Ebd.

6 Koalitionsvertrag "Verantwortung für Deutschland", Zeile 2106 f.

7 Ebd., Zeile 2100 f.

8 DMK: Paradigmenwechsel im Datenschutz abrufbar unter: https://digital.hamburg.de/resource/blob/1174752/04e513c6e2b24ec1e19237d8236025d1/dmk-top-5-8-datenschutz-data.pdf.

9 BR-Drs. 356/26 (Beschluss), abrufbar unter: https://dserver.bundestag.de/brd/2026/0356-26.pdf.

eine BDSG-Änderung vorgeschlagen, die die föderale Aufsichtsstruktur erhält, jedoch die Kooperationsmechanismen verbindlicher ausgestaltet, unter anderem durch die Einführung eines „Einer-für-Alle-Prinzips".

II. Ausgangssituation und Struktur der Stuttgarter Impulse

Mit den Stuttgarter Impulsen greifen die Datenschutzaufsichtsbehörden der Länder die Vorschläge aus Hamburg auf und stellen weitergehende Eckpunkte einer modernisierten Datenschutzaufsicht im kooperativen Föderalismus vor, die eine einheitliche und effiziente Anwendung des Datenschutzrechts in Deutschland sicherstellt, ohne dabei regionale Spezifika zu vernachlässigen und den Grundrechtsschutz durch Personalabbau aufgrund reiner Zuständigkeitsverlagerungen zurückzufahren.[10] Mit den Impulsen beteiligen sich die Datenschutzaufsichtsbehörden der Länder an der Reformdebatte und wollen dazu beitragen, die bisher durch Wissenschaft, Politik, Wirtschaft und Zivilgesellschaft aufgezeigten Reformerfordernisse auf Grundlage ihrer Vollzugserfahrungen durch Handlungsempfehlungen aufzugreifen, die – unbeschadet des Zeitbedarfs der teils erforderlichen Gesetzesänderungen –, zeitnah umsetzbar sind und kurzfristig praktische Wirkung entfalten können.

Rechtlicher Ausgangspunkt und damit Horizont politischer Machbarkeit ist dabei zunächst, dass Kernbereiche des Datenschutzes, des Schutzes der Privatsphäre und des freien Verkehrs personenbezogener Daten sowie die Existenz unabhängiger Aufsichtsbehörden mit Art. 7 und 8 der Grundrechtecharta (GRCh) sowie Art. 16 AEUV auf europäischer Ebene grundrechtlich geschützt sind. Der Zugriff hierauf ist dem Unionsgesetzgeber vorbehalten und damit in weiten Bereichen nationaler Ausgestaltung entzogen. Die Zweckbindung, die Abwägung aller Interessen im Rahmen einer Rechtsgrundlage, die Einwilligung und die Interventionsrechte der betroffenen Personen machen den Wesenskern des Rechts auf Schutz der personenbezogenen Daten (Art. 8 GRCh) aus. Das bedeutet, ein Konzept der „Erlaubnis für kompatible Zwecke" kann nicht einseitig an den Interessen der verarbeitenden Stellen ausgerichtet sein, sondern muss die Interessen der betroffenen Personen gleichermaßen berücksichtigen. Alles andere hieße, den durch Art. 8 GRCh gesetzten Rahmen zu verlassen und den Schutzstandard der Grundrechte zu senken.

Die Stuttgarter Impulse stellen einige Eckpunkte aus Sicht der Aufsichtspraxis vor, die sich in vier Kapitel aufteilen. Dabei ist es den Datenschutzaufsichtsbehörden der Länder nach Darstellung der Ausgangssituation (Teil A) zunächst ein Anliegen, in der Reformdebatte Fehlvorstellungen, die sich evidenzbasiert nicht belegen lassen, zu entkräften (Teil B). Anschließend erfolgen zehn Vorschläge zur Modernisierung der Datenschutzaufsicht (Teil C) sowie Überlegungen zu Änderungen im materiellen Datenschutzrecht (Teil D).

III. Fakten zur Praxis der Datenschutzaufsicht

Der Abschnitt zu Mythen und Fakten zur Datenschutzaufsicht arbeitet in der Debatte häufig zu Tage tretende Fehlvorstellungen auf.

Die Datenschutzaufsicht in der Bundesrepublik Deutschland lässt sich nicht beliebig strukturieren, der Föderalismus determiniert die Aufsichtsstruktur verfassungsrechtlich.[11] Die Aufsicht über die öffentlichen Stellen der Länder und Kommunen, aber auch Aufsichtstätigkeiten in den Bereichen medizinischer Versorgung, Lehre und Forschung, Schulen, Kultur und Medien sowie Gerichte, liegt originär bei den Bundesländern. Dass dieser Bereich verfassungsrechtlich determiniert pluralistisch und damit koordinierungsbedürftig ist, wird in der Debatte auch nicht ernsthaft bestritten. Die Forderung nach einem grundlegenden Perspektivwechsel zugunsten von Innovationsförderung und Datennutzung sollte weiter den realen Bedarf an staatlicher Rechtsdurchsetzung, der sich in massiv gestiegenen Beschwerdezahlen im nicht öffentlichen Bereich der Aufsichtstätigkeit zeigt, nicht ausblenden. Beschwerdebearbeitung ist kein skalierbares Massengeschäft, das sich durch Zuständigkeitskonzentration effizient rationalisieren lässt.

Der überwiegende Teil der Beschwerden betrifft den Bereich der Wirtschaft und damit eine äußerst heterogene Landschaft mit sehr unterschiedlichen Interessen.[12] Örtliche Ansprechbarkeit bedarf dezentraler Strukturen. Wer über eine Bündelung oder Zentralisierung der Datenschutzaufsicht nachdenkt, wird berücksichtigen müssen, dass diese Beschwerden weder personalneutral noch kostenneutral zentralisiert bearbeitet werden können. Ein Personalabbau führt zu weniger Grundrechtsschutz.

Eine zu strenge Interpretation der DS-GVO durch die deutschen Datenschutzaufsichtsbehörden, die vom EuGH hätte korrigiert werden müssen, existiert nicht. Bei den wenigen Entscheidungen des EuGH, die sich bisher mit aufsichtsbehördlichen Maßnahmen aus Deutschland befasst haben, hat der Gerichtshof das Datenschutzrecht überwiegend strenger ausgelegt, als dies zuvor von den deutschen Aufsichtsbehörden bewertet wurde. Auch das Narrativ einer uneinheitlichen Datenschutzaufsicht in Deutschland wird ungeprüft zum Anlass einer Modernisierung der Datenschutzaufsicht herangezogen, das jedoch der aktuellen Vollzugspraxis strukturell koordinierter Zusammenarbeit in der Datenschutzkonferenz nicht Stand hält.[13]

Die DSK hat sich auf eine Vielzahl von Orientierungshilfen und Beschlüssen geeinigt, die einen einheitlichen Vollzug des Datenschutzrechts garantieren sollen. Die geringe Anzahl von Entscheidungen des Bundesverwaltungsgerichtes unterstreicht die weitgehende Einheitlichkeit der Entscheidungspraxis der deutschen Datenschutzaufsichtsbehörden.

10 Zu möglichen Folgen einer vollständigen Zentralisierung sei verwiesen auf Wünschelbaum (2025): „Reform der Datenschutzaufsicht: Alle Macht nach Bonn?" In LTO online, abrufbar unter: https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn.

11 Roßnagel: „Weg mit den Landesdatenschutzbeauftragten?", ZD 4/2025, 181.

12 Ketteler: „Bündelung der Datenschutzaufsicht – Die Wünsche der Wirtschaft gehen auseinander", Tagesspiegel; Fuchs/Kamp/Roßnagel: „Reform der Datenschutzaufsicht – was ist denn im Interesse der Wirtschaft?", FAZ-Einspruch vom 9.7.2025, abrufbar unter: https://www.faz.net/premium/einspruch/die-datenschutzaufsicht-reformieren-110581416.html.

13 Budras: „Der vielstimmige Chor der Datenschützer", Anwaltsblatt vom 12.9.2025, online unter: https://anwaltsblatt.anwaltverein.de/de/themen/recht-gesetz/datenschutz-reform.

IV. Modernisierung der Datenschutzaufsicht

Abseits des wie dargestellt bisweilen unzutreffenden Ausgangsbildes verkennen auch die Aufsichtsbehörden der Länder die Modernisierungsnotwendigkeit der Datenschutzaufsicht in Deutschland nicht. Aus diesem Grunde formulieren die Stuttgarter Impulse zehn konkrete Vorschläge für zielführende Verbesserungen. Inhaltlich lassen sich diese grob den übergeordneten Zielen der Verbesserung bestehender Abstimmungsprozesse, der weitergehenden Konzentration bestehender Expertise[14] und der Kommunikation (nach innen wie nach außen) zuordnen.

Zur Verbesserung der Abstimmungsprozesse wären eine gesetzliche Verankerung der DSK ebenso erforderlich, wie verbindliche Mehrheitsentscheidungen etabliert werden müssten und durch Schaffung einer Geschäftsstelle mehr Kontinuität der Prozesse sichergestellt werden könnte.[15] Ein wesentliches Effizienzproblem der aktuellen Aufsichtsstruktur im nicht öffentlichen Bereich besteht in parallelen Prüfungen ähnlicher oder identischer Sachverhalte durch mehrere Behörden. Mit konsequenter Etablierung des „Einer-für-Alle"-Prinzips könnte die Prüfung eines Sachverhalts durch eine zuständige Aufsichtsbehörde bundesweit Verbindlichkeit entfalten, sofern dieser Sachverhalt bundesweit gesetzlich einheitlich geregelt ist. Damit wäre sichergestellt, dass identische Fragestellungen nicht mehrfach geprüft werden müssen, wodurch insbesondere bei komplexen, länderübergreifenden Sachverhalten erhebliche Effizienzgewinne erzielt werden könnten. Insgesamt könnten Verfahren stärker standardisiert und Bewertungskriterien vereinheitlicht werden,[16] auch einheitliche Ansprechpartner, etwa im Sinne eines (nationalen) One-Stop-Shop-Modells, wären zielführend.

Bereits bestehende Expertise noch mehr zu konzentrieren[17] ermöglicht es, passgenaue Beratung und praktikable Lösungen unter Einbeziehung lokaler Besonderheiten und heterogener Bedürfnisse abzubilden. Durch die gezielte Bündelung von Spezialkompetenzen, wie sie bereits jetzt in den Arbeitskreisen vorhanden sind, können Ressourcen effizient genutzt und (weitere) Kompetenzschwerpunkte aufgebaut werden. Dabei kann bereichsspezifisch auch eine Bündelung von Kompetenzen bei der BfDI, etwa für „Marktortfälle" nach Art. 3 Abs. 2 DS-GVO oder bei der zentralen Beratung von Anbietern von Datenverarbeitungsdiensten mit Infrastrukturcharakter für viele Nutzerinnen und Nutzer im Bundesgebiet in Betracht kommen.

Weiter verbessern lassen sich schließlich auch die interne und externe Kommunikation sowie die Zugänglichkeit zur Datenschutzaufsicht.[18] Die Aufsichtsbehörden haben bereits in der Vergangenheit regelmäßig einstimmig eine Fülle von Leitfäden, Praxis- und Orientierungshilfen veröffentlicht. Entlang der Helsinki-Vorgaben sollen Dialog und Orientierungshilfen für die Praxis künftig weiter ausgebaut werden.

Die Einrichtung eines einheitlichen digitalen Zugangs zur Datenschutzaufsicht im nicht öffentlichen Bereich ("single entry point" & „no wrong door") ist ein zentraler Baustein für eine moderne und nutzerfreundliche Verwaltung, um künftig alle Anfragen unabhängig von der (sachlichen und räumlichen) Zuständigkeit der Datenschutzbehörde über ein zentrales digitales Portal entgegen nehmen zu können.

Entscheidungen der deutschen Datenschutzaufsichtsbehörden werden bislang nicht systematisch gebündelt und veröffentlicht. Eine gemeinsame Datenbank der Datenschutzaufsicht für Entscheidungen und Veröffentlichungen wie Orientierungshilfen und Handreichungen könnte hier Abhilfe schaffen, wenn eine Geschäftsstelle der DSK eine solche Arbeit unterstützt und im Bußgeldbereich eine gesetzliche Veröffentlichungserlaubnis geschaffen würde.

V. Modernisierung des Datenschutzrechts

Neben Modernisierungsvorschlägen zur Datenschutzaufsicht stellen die Stuttgarter Impulse fünf Kernthesen zum materiellen Datenschutzrecht vor. Diese Vorschläge knüpfen zum Teil an bereits von der DSK vorgestellte Ansätze an, gehen aber auch darüber hinaus.[19]

Ein wichtiger Punkt, der im Digitalen Omnibus bisher nur ausschnittsweise und daher nicht zufriedenstellend adressiert wird, betrifft gesetzliche Regeln zum Einsatz von KI. An die Seite der bereits diskutierten Vorgaben für ein angemessenes Training der KI mit personenbezogenen Daten muss die Sicherstellung einer effektiven Durchsetzung der Betroffenenrechte treten. Beim Einsatz von KI-Systemen ist durch technisch-organisatorische und rechtliche Vorkehrungen die effektive Wirksamkeit der grundlegenden Prinzipien des Datenschutzes sicherzustellen.

Eine Reihe von Regelungen der DS-GVO sollten einer verbesserten Operationalisierung zugeführt werden. Bisher dysfunktionale Instrumente zur Selbstregulierung vor allem der Wirtschaft bedürfen der Vereinfachung. Dies betrifft insbesondere die Zertifizierung oder die Verhaltenskodizes (Art. 40 ff. DS-GVO).

In die DS-GVO könnten tatsächlich, wie vielfach politisch gefordert, risikobasierte(re) Ansätze aufgenommen werden, allerdings mit Bedacht. Gegenstände insoweit könnten beispielsweise die Verarbeitung von Daten besonderer Kategorien (Art. 9 DS-GVO) oder die Übermittlung von Daten in Drittstaaten (Art. 44 ff. DS-GVO) sein. Dies kann zu Erleichterungen bei manchen Datenverarbeitungen, aber auch zu höheren Anforderungen bei anderen führen.

Die Rechtsrahmen für Auftragsverarbeitungsverhältnisse bieten erhebliche Vereinfachungspotenziale, ohne dass dadurch Abstriche beim Datenschutz hingenommen werden müssen: durch Umgestaltung der Auftragsverarbeitung zu

14 Vgl. dazu auch Keber: „Reform der Datenschutzaufsicht, Föderale Konzentration statt ineffiziente Zentralisierung", in RDV 4/2025; Wünschelbaum: „Zentrale Koordinierung oder Zentralisierung? Reformoptionen für die deutsche Datenschutzaufsicht", ZD-Aktuell 2025, 1250.

15 Dazu insbesondere SIMD, Teil C, Ziff. n 2, 3, 4, 9, 10.

16 Hansen: „Datenschutzkonferenz: Brauchen einheitliche Schutzmaßstäbe", Die Zeit vom 23.11.2023.

17 Vgl. insbesondere SIMD, Teil C, Ziff. n 1, 5.

18 Vgl. insbesondere SIMD, Teil C, 6, 7, 8.

19 Vgl. Entschließung der DSK zum Digital Fitness Check: Vorschläge zu Modifikationen der DS-GVO vom 10.3.2026, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2026-03-10_DSK_Entschliessung-Digital_Fitness_Check.pdf"; Vgl. ferner Hansen/Kamp/Keber (2026): Gedanken zur Reform der DS-GVO aus Sicht der Aufsichtspraxis, in DuD (Volume 50, S. 22-27): https://doi.org/10.1007/s11623-026-2198-4.

einem gesetzlichen Schuldverhältnis könnten unnötige Prüferfordernisse und Fehlerquellen verringert werden. Gleichzeitig wird arbeitsteilige Datenverarbeitung vereinfacht und entbürokratisiert. Damit kann zur Entlastung von KMU beigetragen werden und die Pflichten der Akteure von Datenverarbeitungen würden gerechter verteilt. Die Hersteller von Anwendungen müssen für ihre Produkte und Lösungen nach dem Vorbild der KI-Verordnung auch im Rahmen der DS-GVO verantwortlich sein.

Das Datenschutzrecht könnte insgesamt stärker auf die Mehrung gesellschaftlichen Nutzens ausgerichtet werden, ohne den Grundrechtsschutz zu schwächen. Im Fokus sollten risikoreiche Datenverarbeitungen stehen. Dazu sollte die Bearbeitung von Beschwerden priorisiert werden können, auch um Raum für die gezielte Unterstützung innovativer und datenschutzgerechter Anwendungen zu schaffen. Wie eingangs erwähnt und um den Kreis zu schließen: Bei allen Änderungen der DS-GVO sind der Schutz personenbezogener Daten durch Art. 8 GRCh, Art. 16 AEUV und die allgemeinen Prinzipien des Art. 5 DS-GVO zu wahren.

VII. Stuttgarter Impulse – Wie es weitergeht

Mit den Stuttgarter Impulsen gelingt es den Aufsichtsbehörden der Länder, ihre Erfahrungen aus der Aufsichtspraxis in bestehende Optimierungspotenziale zu übersetzen, die sowohl bei einer Modernisierung der Datenschutzaufsicht in Deutschland als auch bei der Fortentwicklung des materiellen Datenschutzrechts Berücksichtigung finden sollten. Dabei zeigen die Datenschutzaufsichtsbehörden der Länder auf, dass einigen Argumenten in der politischen Debatte kein evidenzbasiertes Fundament zugrunde liegt. Mit den Impulsen gehen konkrete Vorschläge einher, die mit geringem Aufwand zu einer echten Modernisierung der Datenschutzaufsicht führen, die die föderale Aufsichtsstruktur verbindlicher macht.

Die Stuttgarter Impulse sind bewusst als Debattenbeitrag angelegt, zu welchem nach Veröffentlichung ein Konsultationsprozess gestartet wurde. Bis zum 10.9.2026 können Bürgerinnen und Bürger, Behörden, Unternehmen, NGOs und Initiativen die Vorschläge kommentieren und eigene Vorschläge einbringen.[20] Die Rückmeldungen werden anschließend systematisiert und ausgewertet und wesentliche Punkte in einem Stakeholder-Event am 30.9.2026 in Berlin diskutiert.[21] Damit öffnen die Datenschutzaufsichtsbehörden der Länder den Debattenraum auf sämtliche Stakeholder, die konkrete Erfahrungen aus ihrer eigenen Praxis einbringen und so dazu beitragen können, die moderne Datenschutzaufsicht in Deutschland mitzugestalten.

20 Abgabe von Stellungnahmen möglich unter: https://www.baden-wuerttemberg.datenschutz.de/stuttgarter-impulse-konsultation/.

21 Informationen dazu unter: https://www.stuttgarter-impulse.de.

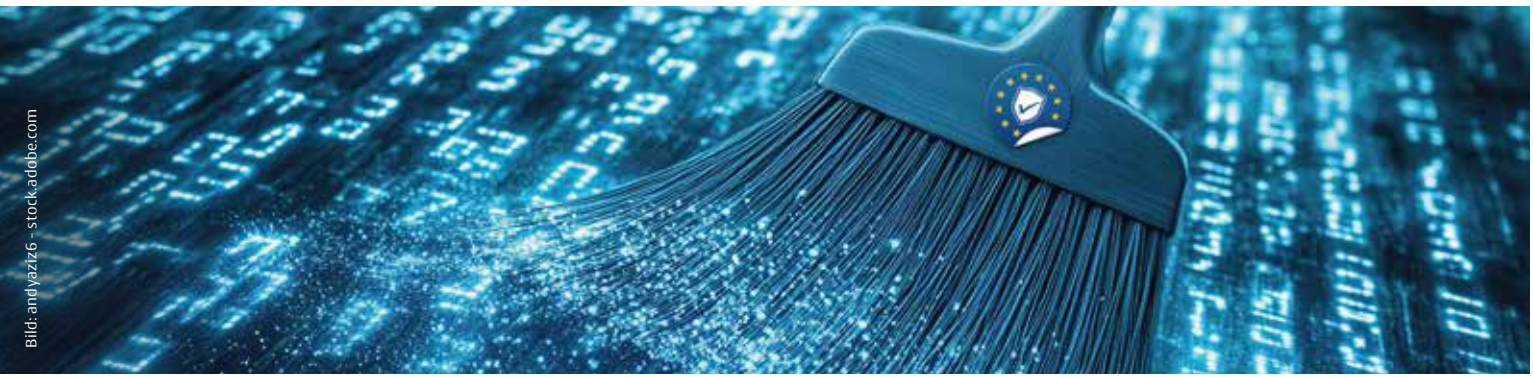


Bild: andyazi26 - stock.adobe.com

Löschen nach DS-GVO

Löschpflichten nach Art. 17 DS-GVO rechtssicher umsetzen

3. November 2026 | online | 10:00 Uhr – 17:00 Uhr
Referenten: Sascha Kremer, Dr. Oliver Stiemerling

Schwerpunktthemen:

✓ Löschen nach Art. 17 DS-GVO im Zusammenspiel mit Betroffenenrechten
✓ Einschränkungen der Löschpflicht durch nationale Öffnungsklauseln
✓ Löschmethoden und Arten des Löschens von personenbezogenen Daten
✓ Löschen in KI-Systemen und KI-Modellen u.v.m.

Jetzt anmelden:
www.datakontext.com

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Lucia Burkhardt/Prof. Dr. Rolf Schwartmann/Dr. Gero Ziegenhorn*

Die Änderung der KI-Verordnung durch den Digital-Omnibus

I. Überblick

Zeitplan (Art. 113, 111) Der Geltungsbeginn der Hochrisiko-Pflichten wird auf den 2.12.2027 für Anhang-III-Systeme und den 2.8.2028 für Anhang-I-Systeme verschoben (zuvor einheitlich 2.8.2027). Der Bestandsschutz für Altsysteme wandert mit diesem Stichtag mit. Anbieter schon vermarkteter generativer Systeme müssen die Kennzeichnungspflicht des Art. 50 Abs. 2 bis 2.12.2026 erfüllen.

KI-Kompetenz (Art. 4) Die Pflicht zur KI-Kompetenz wird umformuliert. Anbieter und Betreiber müssen die Entwicklung der KI-Kompetenz ihres Personals nur noch durch Maßnahmen unterstützen statt sie nach besten Kräften sicherzustellen, ausdrücklich ohne ein bestimmtes Kompetenzniveau zu garantieren. Kommission und Mitgliedstaaten unterstützen die Anbieter und Betreiber bei der Pflichterfüllung. Konkret veröffentlicht die Kommission praktische Beispiele auf der zentralen Informationsplattform, und das KI-Gremium nimmt Empfehlungen zur Förderung der KI-Kompetenz an.

Verbotene Praktiken (Art. 5) Zwei neue Verbote ab dem 2.12.2026. KI-Systeme, die nicht einvernehmliche sexualisierte Darstellungen bestimmbarer Personen erzeugen oder manipulieren, und solche, die Darstellungen sexuellen Kindesmissbrauchs erzeugen, sind verboten. Anbieter sind erfasst bei entsprechender Zweckbestimmung oder wenn solche Ausgaben absehbar reproduzierbar sind und Schutzvorkehrungen fehlen. Betreiber bei gezielter Nutzung.

Datenschutz (Art. 4a, 10) Die Erlaubnis, besondere Kategorien personenbezogener Daten zur Bias-Erkennung und -Korrektur zu verarbeiten (bisher Art. 10 Abs. 5, nur Anbieter von Hochrisiko-Systemen), wird als neuer Art. 4a auf Anbieter und Betreiber praktisch aller KI-Systeme und KI-Modelle erweitert. Die Bedingungen bleiben, eine Korrekturpflicht entsteht nicht.

Verzahnung mit dem Produktsektorrecht (Art. 2, 6, 28–30, 40, 42, 43, 96, Anhänge I und XIV) Die Maschinenverordnung wechselt von Anhang I Abschnitt A nach Abschnitt B. KI in Maschinen unterliegt damit nur noch dem Minimalregime des Art. 2 Abs. 2, die Anforderungen werden ins Maschinenrecht selbst verlagert. Für Anhang-I-A-Systeme kann die Kommission die Hochrisiko-Pflichten per delegiertem Rechtsakt beschränken, wenn das Sektorrecht gleichwertigen Schutz bietet (Art. 2 Abs. 13). Der Begriff des Sicherheitsbauteils wird eingegrenzt (Art. 6 Abs. 1a–1c). Neu sind ein einheitliches Benennungsverfahren für notifizierte Stellen beider Regime (Art. 28 Abs. 8/9, Anhang XIV mit Code-Verzeichnis), der Ausbau des integrierten Konformitätsbewertungsverfahrens samt Wahlfreiheit des Herstellers (Art. 43 Abs. 3), eine Konformitätsvermutung bei Einhaltung der Cyberresilienz-VO (Art. 42 Abs. 3) und ein Normungsauftrag für gemeinsame Normen (Art. 40).

Aufsichtsarchitektur (Art. 64, 75, 75a–75d, 77) Das Büro für Künstliche Intelligenz erhält die ausschließliche Zuständigkeit für KI-Systeme auf eigenen KI-Modellen mit allgemeinem Verwendungszweck und für Systeme sehr großer Online-Plattformen und -Suchmaschinen. Dazu bekommt es ein vollständiges Durchsetzungsinstrumentarium: Inspektionen, Auskunftsanordnungen, bindende Verpflichtungszusagen, eigene Geldbußen und Zwangsgelder mit EuGH-Kontrolle sowie Verfahrensgarantien und eine Ressourcen-Garantie. Der Dokumentationszugang der Grundrechtsbehörden läuft künftig über die Marktüberwachungsbehörden und ist nicht mehr auf Anhang-III-Systeme beschränkt.

Innovation und Reallabore (Art. 57–60a) Die Frist für die nationalen Reallabore verschiebt sich auf den 2.8.2027. Das KI-Büro kann ein Unions-Reallabor einrichten. Tests unter Realbedingungen stehen jetzt auch Anhang-I-A-Anbietern offen (Art. 60), für Anhang-I-B-Systeme gibt es ein eigenes Opt-in-Testregime der Mitgliedstaaten (Art. 60a).

Wertschöpfungskette (Art. 25, 99) Die Kooperationspflichten des Erstanbieters beim Anbieterwechsel werden konkretisiert (Unterlagen, Fehlerarten, technischer Zugang). Die schriftliche Zuliefer-Vereinbarung erfasst jetzt auch KI-Modelle. Beides ist neu bußgeldbewehrt (Art. 99 Abs. 4 lit. da).

Erleichterungen für KMU und kleine Midcap-Unternehmen (Art. 3, 11, 17, 63, 99 u.a.) Kleine Midcap-Unternehmen werden als neue Kategorie definiert und in die bestehenden KMU-Erleichterungen einbezogen (vereinfachte technische Dokumentation, Verhältnismäßigkeit des Qualitätsmanagementsystems, Bußgeld-Deckelung auf den jeweils niedrigeren Betrag). Das vereinfachte Qualitätsmanagement nach Art. 63 steht statt nur Kleinstunternehmen jetzt allen KMU offen.

Weichere Instrumente statt verbindlicher Rechtsakte (Art. 49/Anhang VIII, 50/56, 72) Die Registrierung selbsteingestufter Nicht-Hochrisiko-Systeme wird inhaltlich verschlankt. Die Befugnis der Kommission, Praxisleitfäden per Durchführungsrechtsakt allgemeine Gültigkeit zu verleihen, entfällt zugunsten einer bloßen Angemessenheitsprüfung. Das Muster für den Beobachtungsplan kommt statt per Durchführungsrechtsakt nur noch als Leitlinie, mit Frist zum 2.9.2027.

* Lucia Burkhardt ist wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln. Prof. Dr. Rolf Schwartmann ist an der Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln und Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. Dr. Gero Ziegenhorn ist Rechtsanwalt für Digitalisierungsrecht und Partner der Sozietät Redeker Sellner Dahs in Berlin sowie Lehrbeauftragter für Datenschutzrecht an der FernUniversität in Hagen.

Synopse

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Kapitel I. Allgemeine Bestimmungen		
Art. 1	Gegenstand	Abs. 2 lit. g) ergänzt: Kleine Midcap-Unternehmen bei der Innovationsförderung ergänzt, sonst nur redaktionell.
Art. 2	Anwendungsbereich	Abs. 2 ergänzt: Der Anwendungsbefehl des S. 1 für Systeme, die unter Anhang I Abschnitt B fallen, wurde erweitert. Nunmehr wird auch der neu geschaffene Art. 60a, Art. 110 und Art. 111 erfasst. Mit dem neuen Art. 60a steht jetzt auch für Anhang I Abschnitt B Systeme ein Test unter Realbedingungen zur Verfügung. Mit Art. 111 gelten für diese jetzt auch die Bestimmungen für Systeme, die schon vor dem Geltungsbeginn am Markt waren. Die Inkorporation des Art. 110 ist lediglich redaktionell. S. 2 erweitert den Kreis der erfassten Artikel. Nunmehr gelten auch Art. 58 und 59 für Reallabore, an denen Anhang I Abschnitt B Systeme teilnehmen. Abs. 7 redaktionell angepasst: nur Verweisanpassung, da Art. 10 Abs. 5 jetzt Art. 4a ist. Abs. 13 neu angefügt: Möglichkeit für bestimmte Hochrisiko-Systeme Anwendung einzelner Pflichten zu beschränken, sofern sektorspezifische Vorschriften bereits gleichwertiges Schutzniveau bieten. Die Beschränkung betrifft nur Systeme nach Anhang I Abschnitt A. Sie erfolgt durch delegierten Rechtsakt der Kommission.
Art. 3	Begriffsbestimmungen	Nr. 14 neu gefasst: Begriff „Sicherheitsbauteil". Nr. 14a und 14b neu eingefügt: Begriffsbestimmungen „KMU" und „kleines Midcap-Unternehmen".
Art. 4	KI-Kompetenz	Art. insgesamt neu gefasst: Pflicht in Abs. 1 umformuliert (Unterstützung statt Sicherstellung, kein garantiertes Kompetenzniveau). Abs. 2 und 3 sind dabei neu hinzugekommen: Flankierung durch Kommission/Mitgliedstaaten, Empfehlungen des KI-Gremiums.
Art. 4a	Verarbeitung besonderer Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen	Neu eingefügt: ersetzt Art. 10 Abs. 5. Abs. 1 unverändert übernommen: Inhalt des bisherigen Art. 10 Abs. 5. Abs. 2 neu eingefügt: Erweitert die Verarbeitungserlaubnis zur Bias-Korrektur auf Anbieter und Betreiber aller KI-Systeme und -Modelle, soweit zur Erkennung und Korrektur von Verzerrungen mit Risiken für Gesundheit, Sicherheit, Grundrechte oder Diskriminierungsverbote unbedingt erforderlich. Eine Pflicht zur Korrektur besteht nicht.
Kapitel II. Verbotene Praktiken im KI-Bereich		
Art. 5	Verbotene Praktiken im KI-Bereich	Abs. 1 UAbs. 1 lit. ba) neu eingefügt: Verbot, ein KI-System in Verkehr zu bringen, in Betrieb zu nehmen oder zu verwenden, das ohne ausdrückliche Zustimmung der betroffenen Person realistische Darstellungen ihrer intimen Körperteile oder ihrer Beteiligung an eindeutig sexuellen Handlungen erzeugt oder manipuliert (sexualisierte Deepfakes). Abs. 1 UAbs. 1 lit. bb) neu eingefügt: Verbot, ein KI-System in Verkehr zu bringen, in Betrieb zu nehmen oder zu verwenden, das Darstellungen sexuellen Kindesmissbrauchs (Material i.S.d. Art. 2 lit. c) und e) RL 2011/93/EU) erzeugt oder manipuliert. Abs. 1a neu eingefügt: Einschränkung von lit. ba und bb. Das Inverkehrbringen ist nur bei entsprechender Zweckbestimmung oder bei absehbarem, reproduzierbarem Ergebnis ohne zumutbare Schutzvorkehrungen verboten, die Verwendung nur bei entsprechender Zwecksetzung des Betreibers. Abs. 1b neu eingefügt: Negativabgrenzung des Merkmals „manipulativ" des Abs. 1 UAbs. 1 lit. ba).

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Kapitel III. Hochrisiko-KI-Systeme		
Art. 6	Einstufungsvorschriften für Hochrisiko-KI-Systeme	Abs. 1a neu eingefügt: Ausnahme von „Sicherheitsbauteil". Abs. 1b neu eingefügt: Konkretisierung von „Sicherheitsbauteil". Abs. 1c neu eingefügt: Konkretisierung von Abs. 1b.
Art. 10	Daten und Daten-Governance	Abs. 1 redaktionell angepasst: reine Verweisanpassung (Art. 4a). Abs. 5 gestrichen: in den neuen Art. 4a verschoben. Abs. 6 redaktionell angepasst: reine Verweisanpassung (Art. 4a).
Art. 11	Technische Dokumentation	Abs. 1 UAbs. 2 ergänzt: vereinfachte technische Dokumentation (Anhang IV) jetzt auch für kleine Midcap-Unternehmen.
Art. 17	Qualitätsmanagement-system	Abs. 2 ergänzt: Verhältnismäßigkeit des Qualitätsmanagementsystems nennt jetzt ausdrücklich KMU, einschließlich Start-up-Unternehmen, und kleine Midcap-Unternehmen.
Art. 25	Verantwortlichkeiten entlang der KI-Wertschöpfungskette	Abs. 2 neu gefasst: Kooperationspflicht des Erstanbieters beim Anbieterwechsel konkretisiert (technische Unterlagen, Unterrichtung über Einschränkungen und Fehlerarten, gezielter technischer Zugang). Opt-out bei untersagter Hochrisiko-Umwandlung entsprechend erweitert. Abs. 4 UAbs. 1 ergänzt: Schriftliche Zuliefer-Vereinbarung (Informationen, technischer Zugang, Unterstützung für die Pflichterfüllung des Hochrisiko-Anbieters) erfasst jetzt auch KI-Modelle. Maßstab: allgemein anerkannter Stand der Technik.
Art. 27	Grundrechte-Folgenabschätzung für Hochrisiko-KI-Systeme	Abs. 4 neu gefasst: Verzahnung mit der Datenschutz-Folgenabschätzung konkretisiert: Der Betreiber kann Verweise auf einschlägige Abschnitte der nach Art. 35 DS-GVO bzw. Art. 27 der Richtlinie (EU) 2016/680 durchgeführten Datenschutz-Folgenabschätzung oder deren Teile unmittelbar in die Grundrechte-Folgenabschätzung aufnehmen (zuvor nur: Grundrechte-Folgenabschätzung „ergänzt" die Datenschutz-Folgenabschätzung). Abs. 5 ergänzt: Das Fragebogen-Muster des Büros für Künstliche Intelligenz muss diese Verweismöglichkeit vorsehen.
Art. 28	Notifizierende Behörden	Abs. 8 und 9 neu angefügt: Einheitliches Benennungsverfahren für Konformitätsbewertungsstellen: Ein einziger Antrag und ein einheitliches Bewertungsverfahren für die Benennung nach KI-VO und Anhang-I-A-Sektorrecht (sofern dieses das vorsieht). Eine Benennung wirkt für alle erfassten Rechtsakte. Zuständig ist die nach Sektorrecht benannte notifizierende Behörde, sofern der Mitgliedstaat keine andere bestimmt.
Art. 29	Antrag einer Konformitätsbewertungsstelle auf Notifizierung	Abs. 4 ergänzt (Folgeänderung zu Art. 28 Abs. 8): Der einzige Antrag im einheitlichen Bewertungsverfahren ist bei der nach Anhang-I-A-Sektorrecht benannten notifizierenden Behörde zu stellen. Unterlagen aus anderen Benennungen dienen auch der Beschleunigung des Verfahrens.
Art. 30	Notifizierungsverfahren	Abs. 2 ergänzt: Notifizierung erfolgt anhand des Code-Verzeichnisses des neuen Anhangs XIV. Neue Befugnis der Kommission, Anhang XIV per delegiertem Rechtsakt (Art. 97) zu ändern.

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Art. 40	Harmonisierte Normen und Normungsdokumente	Abs. 2 UAbs. 4 neu angefügt: Auftrag an die europäischen Normungsorganisationen, Normungsprodukte für die gemeinsame Einhaltung und Konformitätsvermutung von KI-VO-Anforderungen (Kapitel III Abschnitte 2 und 3) und Anhang-I-Sektorrecht auszuarbeiten.
Art. 42	Vermutung der Konformität mit bestimmten Anforderungen	Abs. 3 neu angefügt: Konformitätsvermutung: Hochrisiko-KI-Systeme, die die Bedingungen des Art. 12 Abs. 1 Cyberresilienz-VO (EU) 2024/2847 erfüllen, gelten als konform mit den Cybersicherheitsanforderungen des Art. 15.
Art. 43	Konformitätsbewertung	Abs. 3 neu gefasst: integriertes Verfahren für Anhang-I-A-Systeme ausgebaut: Qualitätsmanagement-Bewertung (Art. 17) einbezogen. Sektorale notifizierte Stellen bewerten die KI-Anforderungen mit (Benennungsantrag bis 28.1.2028). Keine Pflicht zur Drittprüfung allein wegen eines Hochrisiko-Sicherheitsbauteils. Bei Doppel-Einstufung (Anhang I A und Anhang III) Vorrang des sektoralen Verfahrens.
Kapitel IV. Transparenzpflichten		
Art. 50	Transparenzpflichten für Anbieter und Betreiber bestimmter KI-Systeme	Abs. 7 neu gefasst: Praxisleitfäden-Förderung jetzt bei der Kommission (statt KI-Büro). Keine Genehmigung per Durchführungsrechtsakt mehr, stattdessen Angemessenheitsprüfung nach Art. 56 Abs. 6 UAbs. 1 (mit KI-Gremium). Gegenstand um „Markierung" erweitert. Der Auffang-Durchführungsrechtsakt bleibt.
Kapitel V. KI-Modelle mit allgemeinem Verwendungszweck		
Art. 56	Praxisleitfäden	Abs. 6 neu gefasst (entspr. Art. 50 Abs. 7): Überwachung und Angemessenheitsbewertung der Praxisleitfäden jetzt bei Kommission und KI-Gremium. Befugnis zur Genehmigung per Durchführungsrechtsakt mit allgemeiner Gültigkeit gestrichen.
Kapitel VI. Maßnahmen zur Innovationsförderung		
Art. 57	KI-Reallabore	Abs. 1 UAbs. 1 ergänzt: Einrichtungsfrist auf 2.8.2027 verschoben. Abs. 3 neu gefasst: Reallabor des Europäischen Datenschutzbeauftragten jetzt als Kann-Vorschrift. Abs. 3a neu eingefügt: Unions-Reallabor des Büros für Künstliche Intelligenz für Systeme nach Art. 75 Abs. 1 mit vorrangigem Zugang für KMU und kleine Midcap-Unternehmen. Abs. 5 ergänzt: Reallabor-Plan kann Tests unter Realbedingungen nach Art. 60/60a einschließen. Abs. 9 lit. e) ergänzt: kleine Midcap-Unternehmen ergänzt. Abs. 10 redaktionell angepasst: „zuständige" statt „nationale" Datenschutzbehörden (Folgeänderung zum Unions-Reallabor nach Abs. 3a, dort ist der EDSB zuständig) Abs. 14 ergänzt: Koordination einschließlich KI-Büro.
Art. 58	Detaillierte Regelungen für KI-Reallabore und deren Funktionsweise	Abs. 1 UAbs. 1 ergänzt: Durchführungsrechtsakte erfassen jetzt auch die Führung der Reallabore. Abs. 1 UAbs. 1 lit. d) neu angefügt: detaillierte Führungs-Vorschriften einschließlich Einbeziehung und Aufsicht der Datenschutzbehörden.
Art. 60	Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren	Abs. 1 UAbs. 1 und Abs. 2 ergänzt: Tests unter Realbedingungen außerhalb von Reallaboren jetzt auch für Anhang-I-A-Hochrisiko-Systeme (zuvor nur Anhang III). Verfahren unverändert.

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Art. 60a	Test von Hochrisiko-KI-Systemen, die unter die in Anhang I Abschnitt B aufgeführten Harmonisierungsrechtsvorschriften der Union fallen, unter Realbedingungen außerhalb von KI-Reallaboren	Neu eingefügt: Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von Reallaboren für Anhang-I-B-Systeme: als Opt-in der Mitgliedstaaten (Zulassung + Rahmen, Mitteilung an die Kommission). Materielle Schutzstandards über Verweis auf Art. 60 (Abs. 2, 3, 4 lit. d)-j), 5-9), an die Stelle der Marktüberwachungsbehörde tritt die zuständige Sektorbehörde.
Art. 63	Ausnahmen für bestimmte Akteure	Abs. 1 ergänzt: Vereinfachte Einhaltung des Qualitätsmanagementsystems (Art. 17) jetzt für alle KMU einschließlich Start-up-Unternehmen (zuvor nur Kleinstunternehmen). Die Bedingung, dass keine Partner- oder Verbundunternehmen bestehen, bleiben.
Kapitel VII. Governance		
Art. 64	Büro für Künstliche Intelligenz	Abs. 3 neu angefügt: Ressourcen-Garantie für das Büro für Künstliche Intelligenz zur wirksamen Wahrnehmung seiner Durchsetzungsaufgaben (Begleitregelung zu den neuen Art. 75a–75d).
Art. 69	Zugang zum Pool von Sachverständigen durch die Mitgliedstaaten	Abs. 2 neu gefasst: Gebühren der Mitgliedstaaten für Sachverständigen-Beratung jetzt in Höhe der für die Kommission geltenden Vergütungssätze (Durchführungsrechtsakt nach Art. 68 Abs. 1).
Art. 70	Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle	Abs. 8 ergänzt: Anleitung und Beratung der nationalen Behörden jetzt ausdrücklich auch für kleine Midcap-Unternehmen.
Kapitel IX. Beobachtung nach dem Inverkehrbringen, Informationsaustausch und Marktüberwachung		
Art. 72	Beobachtung nach dem Inverkehrbringen durch die Anbieter und Plan für die Beobachtung nach dem Inverkehrbringen für Hochrisiko-KI-Systeme	Abs. 3 neu gefasst: Muster für den Beobachtungsplan jetzt per Kommissions-Leitlinien (mit KI-Gremium) bis 2.9.2027 statt per Durchführungsrechtsakt bis 2.2.2026.
Art. 75	Marktüberwachung und Kontrolle von KI-Systemen sowie Amtshilfe	Überschrift und Abs. 1 neu gefasst: Aus der bloßen Mitüberwachungsbefugnis des KI-Büros bei Anbieteridentität von Modell und System wird eine ausschließliche Zuständigkeit für Aufsicht und Durchsetzung. Der Anwendungsbereich wird auf den Konzernfall (Anbieter desselben Unternehmens) und auf Systeme sehr großer Online-Plattformen und -Suchmaschinen erweitert. Vier Fallgruppen bleiben bei den nationalen Behörden (Anhang-I-Produkte, kritische Infrastruktur, Strafverfolgung/Grenze/Finanzinstitute nach Art. 74 Abs. 6, Rechtspflege). Fremde Betreiber sind nicht erfasst. Abs. 1a–1e und 2a neu eingefügt: Flankierung durch direkte Vorfallsmeldung, Kooperationspflichten der nationalen Behörden und Zuständigkeit für Konformitätsbewertungen.
Art. 75a	Aufsichts- und Durchsetzungsbefugnisse des Büros für Künstliche Intelligenz	Neu eingefügt: Aufsichts- und Durchsetzungsbefugnisse des KI-Büros für die Systeme des Art. 75 Abs. 1: volle Marktüberwachungsbefugnisse, Auskunfts- und Dokumentenanforderung, Inspektionen (auch vor Ort, mit Unterstützung nationaler Behörden), Zugangs-Anweisungen, externe Sachverständige. Zweckbindung der erhobenen Informationen.
Art. 75b	Verpflichtungszusagen	Neu eingefügt: Das KI-Büro kann im Verfahren angebotene Verpflichtungszusagen per Beschluss für bindend erklären und das Verfahren beenden. Wiederaufnahme bei Sachverhaltsänderung, Zuwiderhandlung oder irreführenden Angaben. Unzureichende Zusagen werden durch begründeten Beschluss abgelehnt.

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Art. 75c	Verstöße, Geldbußen und Zwangsgelder	Neu eingefügt: Beschluss- und Sanktionsregime des KI-Büros: Feststellung von Verstößen mit Abhilfeanordnung, Geldbußen (Art. 99 Abs. 3–7 sinngemäß), Zwangsgelder zur Durchsetzung von Untersuchungen und Informationsersuchen. Unbeschränkte Nachprüfung durch den EuGH. Verjährung fünf Jahre.
Art. 75d	Schutzvorkehrungen und weitere Spezifizierung	Neu eingefügt: Verfahrensgarantien im Durchsetzungsregime des KI-Büros: Verfahrensrechte nach Art. 18 VO (EU) 2019/1020 sinngemäß, Verteidigungsrechte und Akteneinsicht (mit Geschäftsgeheimnisschutz), Durchführungsrechtsakte zu den Modalitäten, Veröffentlichung der Beschlüsse nach Art. 75b/75c unter Wahrung vertraulicher Informationen.
Art. 76	Beaufsichtigung von Tests unter Realbedingungen durch Marktüberwachungsbehörden	Abs. 1 UAbs. 2 neu angefügt: bei Tests nach Art. 60a tritt die zuständige Sektorbehörde an die Stelle der Marktüberwachungsbehörde (Folgeänderung zu Art. 60a).
Art. 77	Befugnisse der für den Schutz der Grundrechte zuständigen Behörden und Zusammenarbeit mit den Marktüberwachungsbehörden	Überschrift und Abs. 1 neu gefasst: Der Dokumentationszugang der Grundrechtsbehörden läuft jetzt über die Marktüberwachungsbehörde (maschinenlesbar, elektronisch), die die Unterlagen nötigenfalls beim Anbieter oder Betreiber beschafft. Die Beschränkung auf Anhang-III-Systeme ist entfallen. Abs. 1a und 1b neu eingefügt: Abs. 1b regelt die wechselseitige Amtshilfe und den Informationsaustausch zwischen Marktüberwachungs- und Grundrechtsbehörden.
Kapitel X. Verhaltenskodizes		
Art. 95	Verhaltenskodizes für die freiwillige Anwendung bestimmter Anforderungen	Abs. 4 ergänzt: Interessen kleiner Midcap-Unternehmen bei der Förderung von Verhaltenskodizes ergänzt.
Art. 96	Leitlinien der Kommission zur Durchführung dieser Verordnung	Abs. 1 lit. a) ergänzt: Erfasst jetzt auch Art. 26. Abs. 1 lit. g) neu angefügt: verlangt bis 1.8.2027 Leitlinien zum Zusammenspiel von Art. 8 Abs. 2, Art. 9 Abs. 10 und Art. 17 Abs. 3 mit dem Anhang-I-A-Sektorrecht. Abs. 1 UAbs. 2 ergänzt: bezieht das KI-Gremium ein und ergänzt kleine Midcap-Unternehmen.
Kapitel XI. Befugnisübertragung und Ausschlussverfahren		
Art. 97	Ausübung der Befugnisübertragung	Abs. 2, 3 und 6 ergänzt (Folgeänderung): Die neuen Delegationsbefugnisse aus Art. 2 Abs. 13 und Art. 30 Abs. 2 werden eingefügt, Übertragung für fünf Jahre ab 27.7.2026, mit Widerrufs- und Einspruchsrecht von Parlament und Rat.
Kapitel XII. Sanktionen		
Art. 99	Sanktionen	Abs. 1 ergänzt: Geldbußen ausdrücklich genannt, Rücksichtnahme auch auf kleine Midcap-Unternehmen. Abs. 4 lit. da) neu eingefügt: neuer Bußgeldtatbestand für Verstöße gegen Art. 25 Abs. 2 und 4. Abs. 6a neu eingefügt: für kleine Midcap-Unternehmen gilt der jeweils niedrigere Bußgeldbetrag.
Kapitel XIII. Schlussbestimmungen		
Art. 111	Bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme und bereits in Verkehr gebrachte KI-Modelle mit allgemeinem Verwendungszweck	Abs. 2 neu gefasst: Bestandsschutz-Stichtag dynamisiert, statt des festen Datums 2.8.2026 gilt jetzt der Beginn der Anwendung des Kapitels III nach Art. 113 (mitwandernd mit der verschobenen Geltungsstaffel). Abs. 4 neu angefügt: Anbieter vor dem 2.8.2026 in Verkehr gebrachter generativer KI-Systeme müssen die Kennzeichnungspflicht des Art. 50 Abs. 2 bis 2.12.2026 erfüllen.

Erl.	Amtliche Überschrift	Änderungen gem. Digital-Omnibus-Verordnung (EU) 2026/1744 vom 8.7.2026
Art. 113	Inkrafttreten und Geltungsbeginn	Abs. 3 lit. a) ergänzt: Die neuen Art.-5-Verbote (lit. ba)/bb), Abs. 1a/1b) gelten ab 2.12.2026. Abs. 3 lit. c) neu gefasst: Geltungsbeginn der Hochrisiko-Ebene (Kapitel III Abschnitte 1–3) verschoben auf 2.12.2027 für Anhang-III-Systeme und 2.8.2028 für Anhang-I-Systeme (zuvor einheitlich 2.8.2027). Abs. 3 lit. d) neu angefügt: Art. 102–110 gelten ab 27.7.2026.
Anhänge		
Anhang I	Liste der Harmonisierungsrechtsvorschriften der Union	Abschnitt A Nr. 1 gestrichen: Die Maschinenverordnung (EU) 2023/1230 entfällt in Abschnitt A. Abschnitt B Nr. 21 neu angefügt: Die Maschinenverordnung (EU) 2023/1230 wechselt damit nach Abschnitt B: KI-Systeme in Maschinen unterliegen nur noch dem Sonderregime des Art. 2 Abs. 2 statt des vollen Kapitels III (Anforderungen künftig im Maschinenrecht selbst, vgl. Art. 3 der Omnibus-VO).
Anhang VIII	Bei der Registrierung von Hochrisiko-KI-Systemen gem. Art. 49 bereitzustellenden Informationen	Abschnitt B: Nr. 7 und 9 gestrichen: bei der Registrierung nach Art. 49 Abs. 2 entfallen die Begründungszusammenfassung zur Nicht-Hochrisiko-Einstufung (Art. 6 Abs. 3) und die Angabe der Mitgliedstaaten des Inverkehrbringens.
Anhang XIV	Verzeichnis der Codes, Kategorien und entsprechenden Arten von KI-Systemen für die Zwecke des Notifizierungsverfahren gem. Art. 30 mit Angabe des Geltungsbereichs der Benennung als notifizierende Stellen	Neu angefügt: Code-Verzeichnis (Codes, Kategorien, Arten von KI-Systemen) zur standardisierten Angabe des Geltungsbereichs der Benennung notifizierter Stellen im Notifizierungsverfahren nach Art. 30, durch die Kommission per delegiertem Rechtsakt (Art. 97) fortschreibbar.

Transparenzhinweis

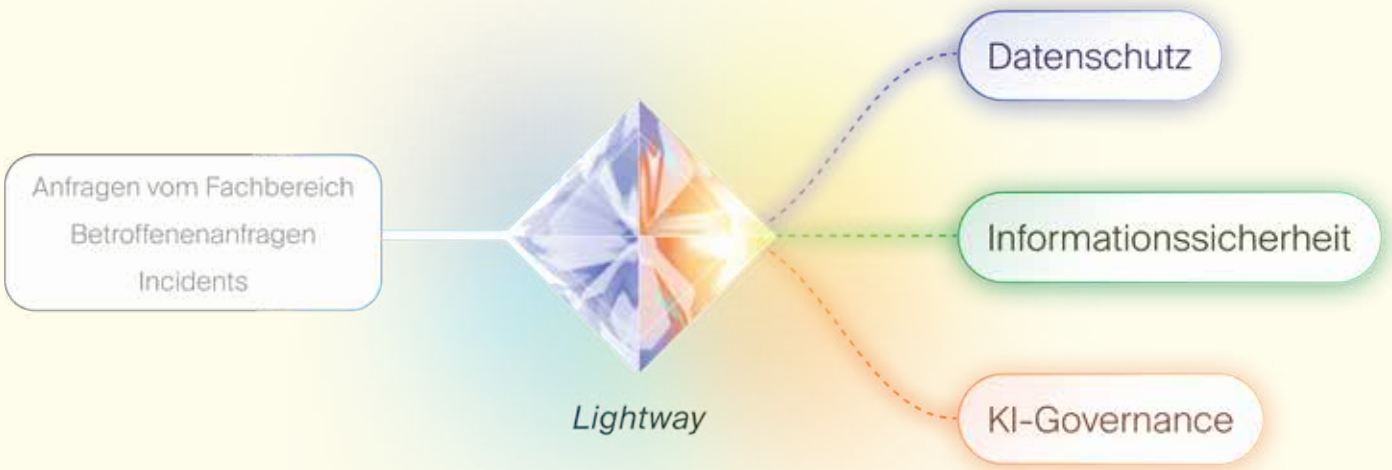
Bei der Erstellung dieses Beitrags haben wir Künstliche Intelligenz unterstützend eingesetzt. Die KI kam hier als Werkzeug für den systematischen Abgleich der Fassungen der KI-Verordnung vor und nach der Digital-Omnibus-Verordnung (EU) 2026/1744 zum Einsatz, außerdem unterstützte KI bei der Strukturierung der Synopse sowie bei formalen Korrekturen und der sprachlichen Zusammenfassung der Änderungen. Die von der KI gelieferten Befunde haben wir am amtlichen Normtext geprüft. Jede Aussage zu Inhalt und Reichweite der Änderungen wird bewusst von uns verantwortet und getragen. Die inhaltliche und redaktionelle Verantwortung liegt vollständig bei uns.

caralegal

Lightway

Der leichtere Weg durch jede datenrechtliche Anfrage.

Lightway bündelt Anliegen aus Fachbereichen an Datenschutz, Informationssicherheit und KI-Governance konzernweit in einem Vorgang. Zuständigkeit, Status, alle Nachweise und Fristen liegen an einem Ort. Die Ergebnisse fließen direkt in Ihre Dokumentation.



So funktioniert es:

1 **Anliegen vollständig abholen**

Meldungen kommen aus verschiedenen Quellen, wie bspw. Microsoft Teams. Die KI-Assistenz prüft vor der Einreichung auf fehlende Angaben.

2 **Ein Vorgang über alle Bereiche**

Datenschutz, KI-Governance und Informationssicherheit laufen in einem Vorgang zusammen, statt in drei Postfächern. Die Zuständigkeiten sind sinnvoll verteilt.

3 **Kommunikation direkt im Vorgang**

Antworten, Dateien und Statuswechsel liegen in einem Verlauf. Der Fachbereich sieht den aktuellen Stand.

4 **Die Dokumentation baut sich nebenbei auf**

Jede Nachricht, Datei und Entscheidung liegt im Vorgang. VT, DSFA, Anfragen und Vorfälle lassen sich direkt verknüpfen.

Über 1.000 Unternehmen setzen auf caralegal

ProSiebenSat.1 Media SE RWE GLS.

Jetzt Produktvorstellung vereinbaren:

caralegal.eu/lightway

RECHTSPRECHUNG

HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

Kein Anspruch auf Kopie eines Compliance-Abschlussberichts

(BAG, Urteil vom 16. April 2026 – 8 AZR 169/25 –)

Relevanz für die Praxis

Das BAG stellt erneut klar, das datenschutzrechtliche Auskunftsrecht ist kein Recht auf Aktenkopie. Wer eine interne Untersuchung durchführen lässt, schuldet der betroffenen Beschäftigten nach Art. 15 Abs. 3 DS-GVO nur eine Kopie der in dem Bericht über sie erhobenen Daten, nicht den Bericht selbst. Die Übersendung einer geschwärzten Fassung des Gesamtberichts bleibt dem Arbeitgeber als Weg der Erfüllung zwar offen, geschuldet ist sie aber nicht.

Das BAG wendet im Wesentlichen die Rechtsprechung des EuGH zur Datenkopie an. Der Anspruch auf Kopie nach Abs. 3 reicht, ebenso wie der Auskunftsanspruch nach Abs. 1, nur so weit wie der Datenbegriff. Nicht erfasst sind daher rechtliche Analysen. Sie enthalten keine Information über die Beschäftigte, allenfalls eine Einschätzung des Arbeitgebers zur Rechtslage. Zu einem Anspruch auf das Dokument verdichtet sich der Anspruch nur ausnahmsweise, wenn die Kopie des Dokuments unerlässlich ist, um die Daten verständlich zu machen. Daran fehlt es, wenn auch rechtliche Analysen enthalten sind, da Sachverhaltsteil und rechtliche Bewertung der Sache nach trennbar sind. Auch die Personalakte führt nicht weiter: § 83 Abs. 1 BetrVG und § 26 Abs. 2 SprAuG erlauben Kopien nur in angemessenem Umfang und geben kein Recht, die Unterlagen als Ganzes zu kopieren.

Arbeitgeber sollten Abschlussberichte deshalb schon bei der Erstellung in einen Sachverhaltsteil und eine gesonderte rechtliche Bewertung gliedern und die Aussagen von Hinweisgebern und Zeugen so festhalten, dass sie sich im Einzelfall entfernen lassen. So lässt sich ein späteres Auskunfts- oder Einsichtsverlangen ohne Mehraufwand erfüllen.

1. **Art. 15 Abs. 3 S. 1 DS-GVO gewährt keinen eigenständigen Anspruch auf ein Dokument als solches, sondern auf die darin enthaltenen personenbezogenen Daten. Die Kopie ganzer Dokumente ist nur geschuldet, wenn sie unerlässlich ist, um die Rechte aus der Verordnung wirksam auszuüben.**
2. **Eine in einem Compliance-Abschlussbericht enthaltene rechtliche Analyse ist kein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DS-GVO, sondern eine Information darüber, wie der Verantwortliche die Rechtslage einschätzt.**
3. **Aus § 26 Abs. 2 SprAuG und § 83 Abs. 1 BetrVG folgt kein Anspruch auf eine Kopie des vollständigen Berichts. Das Recht, auf eigene Kosten Kopien aus der Personalakte zu fertigen, ist auf einen angemessenen Umfang begrenzt.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Rn. 11 I. Die Revision der Klägerin hat keinen Erfolg. Das Landesarbeitsgericht hat im Ergebnis zutreffend entschieden, dass die Klägerin keinen Anspruch auf Herausgabe einer Kopie der Compliance-Abschlussberichte hat.

[…]

Rn. 19 2. Die zulässige Revision ist unbegründet, soweit die Klägerin mit ihrem zuletzt zu Ziff. 3. gestellten Antrag hilfsweise begehrt, die Beklagte zu verurteilen, eine Kopie des Compliance-Abschlussberichts in der Fassung vom 31.1.2024 zur Verfügung zu stellen.

Rn. 20 a) Das Landesarbeitsgericht ist zutreffend davon ausgegangen, dass der Klägerin kein Anspruch auf Zurverfügungstellung einer Kopie nach Art. 15 Abs. 1 i.V.m. Abs. 3 DS-GVO hinsichtlich des gesamten Compliance-Abschlussberichts in der Fassung vom 31.1.2024, d.h. einschließlich der rechtlichen Ausführungen und Mandantenhinweise, zusteht.

Rn. 21 aa) Nach Art. 15 Abs. 1 Hs. 1 DS-GVO hat die betroffene Person grundsätzlich das Recht von ihrem Arbeitgeber als Verantwortlichem (Art. 4 Nr. 7 DS-GVO) eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sofern dies der Fall ist, steht der betroffenen Person nach Art. 15 Abs. 1 Hs. 2 DS-GVO ein Recht auf Auskunft über diese personenbezogenen Daten und die in Art. 15 Abs. 1 lit. a) bis h) DS-GVO näher bezeichneten Informationen zu. Art. 15 Abs. 3 S. 1 DS-GVO gewährt der betroffenen Person zudem einen Anspruch auf Zurverfügungstellung einer Kopie der personenbezogenen Daten. Art. 15 Abs. 1 und 3 DS-GVO gehören zu den Bestimmungen, die das Auskunftsrecht sowie die Transparenz über die Art und Weise der Verarbeitung der personenbezogenen Daten gegenüber der betroffenen Person gewährleisten sollen (EuGH 26.10.2023 – C-307/22 – [FT] Rn. 49) . Das in Art. 15 DS-GVO vorgesehene Auskunftsrecht muss der betroffenen Person nach der Rechtsprechung des Gerichtshofs der Europäischen Union ermöglichen, zu überprüfen, ob sie betreffende Daten richtig sind und ob sie in zulässiger Weise verarbeitet werden. Dieses Auskunftsrecht ist erforderlich, um die betroffene Person in die Lage zu versetzen, gegebenenfalls ihr Recht auf Berichtigung, ihr Recht auf Löschung („Recht auf Vergessenwerden“) und ihr Recht auf Einschränkung der Verarbeitung, die ihr nach den Art. 16, 17 bzw. 18 DS-GVO zukommen, sowie ihr in Art. 21 DS-GVO vorgesehenes Recht auf Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten oder ihre in den Art. 79 und 82 DS-GVO vorgesehenen Rechte auf Einlegung eines gerichtlichen Rechtsbehelfs bzw.

auf Schadenersatz auszuüben (EuGH 27. 2.2025 – C-203/22 – [Dun & Bradstreet Austria] Rn. 53 f.) .

Rn. 22 bb) Art. 15 Abs. 3 S. 1 DS-GVO stellt kein anderes Recht dar, als das in Art. 15 Abs. 1 DS-GVO vorgesehene und gewährt keinen eigenständigen Anspruch gegen den Verantwortlichen auf Zurverfügungstellung des Dokuments als solches, sondern auf die personenbezogenen Daten, die es enthält und die vollständig sein müssen (EuGH 26.10.2023 – C-307/22 – [FT] Rn. 72; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] Rn. 32, 39) . Damit regelt Art. 15 Abs. 3 DS-GVO eine Modalität der Anspruchsausübung und ist untrennbar mit Art. 15 Abs. 1 DS-GVO verbunden. Die Kopie muss alle personenbezogenen Daten enthalten, die Gegenstand der Verarbeitung sind (EuGH 26.10.2023 – C-307/22 – [FT] a.a.O.; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] a.a.O.) . Dies bedeutet, dass der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten überlassen wird. Dieses Recht setzt das Recht voraus, eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder auch von Auszügen aus Datenbanken, die ua. diese Daten enthalten, zu erlangen, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen Rechte zu ermöglichen, wobei insoweit die Rechte und Freiheiten anderer zu berücksichtigen sind (EuGH 26.10.2023 – C-307/22 – [FT] Rn. 75; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] Rn. 45) . Dabei hat der Gerichtshof der Europäischen Union im Hinblick auf Art. 12 Abs. 1 DS-GVO i.V.m. dem 58. ErwG der DS-GVO ausgeführt, dass sich die Reproduktion von Auszügen aus Dokumenten oder gar von ganzen Dokumenten insbesondere zur Gewährleistung der leichten Verständlichkeit der bereitgestellten Informationen als unerlässlich erweisen kann, wenn die Kontextualisierung der verarbeiteten Daten erforderlich ist, um ihre Verständlichkeit zu gewährleisten (EuGH 26.10.2023 – C-307/22 – [FT] Rn. 74; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] Rn. 41; vgl. auch BGH 5.3.2024 – VI ZR 330/21 – Rn. 18) .

Rn. 23 cc) Ausgehend hiervon ist das Landesarbeitsgericht im Ergebnis zutreffend davon ausgegangen, dass der Compliance-Abschlussbericht in der Fassung vom 31.1.2024 nicht ausschließlich personenbezogene Daten enthält. Das Landesarbeitsgericht hat auch zutreffend angenommen, die Klägerin könne eine Kopie des gesamten Berichts nicht unter dem Gesichtspunkt verlangen, dass eine Kontextualisierung der personenbezogenen Daten erforderlich wäre, um ihre Verständlichkeit zu gewährleisten.

Rn. 24 (1) Der Compliance-Abschlussbericht in der Fassung vom 31.1.2024 enthält zwar personenbezogene Daten. Nach der in Art. 4 Nr. 1 DS-GVO enthaltenen Legaldefinition sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person – die betroffene Person – beziehen. Der Begriff der personenbezogenen Daten ist vor dem Hintergrund der Formulierung „alle Informationen" weit zu verstehen (vgl. EuGH 22.6.2023 – C-579/21 – [Pankki S] Rn. 42; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] Rn. 23) . Er ist nicht auf sensible oder private Informationen beschränkt, sondern umfasst potenziell alle Arten von Informationen sowohl objektiver als auch subjektiver Natur in Form von Stellungnahmen oder Beurteilungen, unter der Voraussetzung, dass es sich um Informationen „über" die in Rede stehende Person handelt (EuGH 22.6.2023 – C-579/21 – [Pankki S] a.a.O.; 4.5.2023 – C-487/21 – [Österreichische Datenschutzbehörde] a.a.O.; 20.12.2017 – C-434/16 – [Nowak] Rn. 34) . Der Compliance-Abschlussbericht in der Fassung vom 31.1.2024 befasst sich mit dem Führungsverhalten der Klägerin und enthält aus diesem Grund zwangsläufig Informationen „über" die Person der Klägerin.

Rn. 25 (2) Der Compliance-Abschlussbericht in der Fassung vom 31.1.2024 enthält aber nicht ausschließlich personenbezogene Daten i.S.v. Art. 4 Nr. 1 DS-GVO. Die allein in der Fassung vom 31.1.2024 enthaltenen rechtlichen Ausführungen stellen jedenfalls insoweit keine personenbezogenen Daten dar, als sie eine rechtliche Analyse enthalten. Bei einer rechtlichen Analyse handelt es sich nicht um eine Information über die betroffene Person, sondern höchstens, soweit sie sich nicht ohnehin auf eine rein abstrakte Rechtsauslegung beschränkt, um eine Information darüber, wie der Verantwortliche die rechtliche Situation einschätzt (vgl. EuGH 17.7.2014 – C-141/12 u.a. – [YS ua.] Rn. 40) . Die Rechtslage ist insoweit durch den Gerichtshof der Europäischen Union unabhängig davon hinreichend geklärt, dass die Entscheidung zum Begriff der personenbezogenen Daten bezogen auf Art. 2 lit. a) der Richtlinie 95/46/EG ergangen ist (a.A. Tegel/Lembke NZA-RR 2026, 121, 125) . Diese Vorgängervorschrift ist mit Art. 4 Nr. 1 DS-GVO vergleichbar (vgl. BGH 15.6.2021 – VI ZR 576/19 – Rn. 29) .

Rn. 26 (3) Anhaltspunkte dafür, dass die Klägerin eine Kopie des Abschlussberichts in der Fassung vom 31.1.2024 unter Einschluss der rechtlichen Ausführungen und Mandantenhinweise benötigt, um die Verständlichkeit der im Abschlussbericht enthaltenen personenbezogenen Daten zu gewährleisten, sind nicht ersichtlich. Es handelt sich der Sache nach um unterschiedliche Bestandteile des Berichts, auch wenn sie in einem inhaltlichen Zusammenhang stehen (a.A. Zöll/Kielkowski jurisPR-Compl 1/2026 Anm. 3) . Die Klägerin benötigt auch keine Kenntnis der rechtlichen Ausführungen und Mandantenhinweise, um die ihr durch die Datenschutz-Grundverordnung verliehenen Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung nach den Art. 16, 17 bzw. 18 DS-GVO bezogen auf ihre personenbezogenen Daten ausüben zu können. Soweit sie sich gegen eine ihrer Ansicht nach unzutreffende Rechtsauffassung der Beklagten bzw. ihrer Berater zu Wehr setzen will, kann sie ggf. von ihren prozessualen Möglichkeiten – z.B. im Rahmen eines Kündigungsschutzprozesses – Gebrauch machen. Deshalb ergibt sich aus dem Erfordernis, eine vollständige Auskunft über personenbezogene Daten zu erteilen, kein Anspruch der Klägerin darauf, dass – wie von ihr gefordert – der Abschlussbericht im Gesamten, wenn auch ggf. teilgeschwärzt, als Kopie überlassen wird (vgl. BGH 16.4.2024 – VI ZR 223/21 – Rn. 18; vgl. zur Schwärzung unten Rn. 32) .

Rn. 27 b) Ein Anspruch auf Herausgabe einer Kopie des Compliance-Abschlussberichts in der Fassung vom 31.1.2024 ergibt sich auch weder aus § 26 Abs. 2 SprAuG noch aus § 83 Abs. 1 BetrVG. Es kann daher dahinstehen, ob die Klägerin – entsprechend der Auffassung der Parteien – eine leitende Angestellte iSv. § 5 Abs. 3 BetrVG ist bzw. war.

Rn. 28 aa) Arbeitnehmer haben nach § 26 Abs. 2 SprAuG sowie dem wort- und inhaltsgleichen § 83 Abs. 1 BetrVG (vgl. BAG 16.11.2010 – 9 AZR 573/09 – Rn. 21, BAGE 136, 156) das Recht, in die über sie geführten Personalakten Einsicht zu nehmen. Nach dem materiellen Begriffsverständnis sind Personalakten eine Sammlung von Urkunden und Vorgängen, die die persönlichen und dienstlichen Verhältnisse des Bediensteten betreffen und in einem inneren Zusammenhang mit dem Dienstverhältnis stehen. Auf eine äußere Zuordnung kommt es dabei nicht an (BAG 17.10.2024 – 8 AZR 42/24 – Rn. 28 m.w.N.) .

Rn. 29 bb) Das Einsichtsrecht umfasst das Recht, auf eigene Kosten Kopien aus der Personalakte zu fertigen (ErfK/Kania 26. Aufl. BetrVG § 83 Rn. 4 m.w.N.) . Dieser Anspruch ist jedoch begrenzt auf einen angemessenen Umfang. Dieser Umfang ist nicht mehr gewahrt, wenn der Arbeitnehmer die Personalunterlagen als Ganzes kopieren möchte (GK-BetrVG/Franzen 13. Aufl. BetrVG § 83 Rn. 24 f.; Richardi BetrVG/Thüsing 18. Aufl. BetrVG § 83 Rn. 17; HaKo-BetrVG/Boemke 7. Aufl. BetrVG § 83 Rn. 19) . Hiervon ausgehend ergibt sich aus § 26 Abs. 2 SprAuG bzw. § 83 Abs. 1 BetrVG kein Anspruch der Klägerin, den Abschlussbericht in der Fassung vom 31.1.2024 vollständig in Kopie zur Verfügung gestellt zu bekommen. Unabhängig davon erscheint es zweifelhaft, ob die in der Fassung vom 31.1.2024 enthaltenen rechtlichen Ausführungen und Mandantenhinweise als Teil der materiellen Personalakte angesehen werden können.

Zur Vertiefung

Auskunft auch über Betriebs- und Geschäftsgeheimnisse? = RDV 6/2023

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

[Urteil] BGH bestimmt Voraussetzungen für das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO = RDV 4/2024

[Urteil] Recht auf kostenlose Kopie der eigenen Patientenakte = RDV 1/2024

[Urteil] Recht auf Datenkopie – Zulässigkeit der Schwärzung drittbezogener Daten vor Herausgabe = RDV 3/2026

Keine Haushaltsausnahme für die kollegiale WhatsApp-Chatgruppe

(ArbG Siegburg, Urteil vom 22. Mai 2026 – 1 Ca 1741/25 –)

Relevanz für die Praxis

Das ArbG Siegburg stellt in seinem Urteil fest, die kollegiale WhatsApp-Gruppe ist kein privater Raum. Jedenfalls wenn dort zu einem nennenswerten Teil Dienstliches besprochen wird und auch die beanstandete Nachricht einen dienstlichen Hintergrund hat, greift die Haushaltsausnahme des Art. 2 Abs. 2 lit. c) DS-GVO nicht. Dem Arbeitsgericht genügte ein arbeitsbezogener Anteil von rund 30 Prozent.

In solchen Gruppen gilt damit das volle Datenschutzrecht, hier Art. 9 DS-GVO für die Gesundheitsdaten eines Kollegen, dessen Behandlung und Befunde eine Ärztin in der Abteilungsgruppe wiedergab. Die Haftung traf die Beschäftigte im entschiedenen Fall aber persönlich, da sie ohne dienstlichen Anlass handelte. Wer den Rahmen der eigenen Aufgaben verlässt, wird eigene Verantwortliche nach Art. 4 Nr. 7 DS-GVO.

Arbeitgeber sollten auch für kollegiale Chatgruppen klare Vorgaben machen, und beispielsweise vorgeben, dass Krankmeldungen und Vertretungsfragen dort ohne Angaben zu Diagnosen und Befunden kommuniziert werden. Dann bleibt der Austausch über den Ausfall eines Kollegen möglich, ohne dass Arbeitgeber haften oder Beschäftigte in die persönliche Haftung geraten.

1. **Art. 9 DS-GVO ist Schutzgesetz i.S.d. § 823 Abs. 2 BGB. Die unbefugte Weitergabe von Gesundheitsdaten begründet entsprechend § 1004 Abs. 1 BGB einen verschuldensunabhängigen Unterlassungsanspruch.**
2. **Eine WhatsApp-Chatgruppe von Abteilungskollegen, in der zu mindestens 30 % arbeitsbezogene Inhalte ausgetauscht werden, fällt jedenfalls dann nicht unter die Haushaltsausnahme des Art. 2 Abs. 2 lit. c) DS-GVO, wenn auch die streitgegenständliche Nachricht dienstbezogenen Hintergrund hat.**
3. **Teilt eine Ärztin ohne dienstlichen Anlass Diagnosen und Laborwerte eines Kollegen in einer solchen Chatgruppe mit, handelt sie im Exzess und wird selbst Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO.**
4. **Der Kontrollverlust über an nicht zugriffsberechtigte Gruppenmitglieder weitergegebene Gesundheitsdaten ist ein immaterieller Schaden nach Art. 82 Abs. 1 DS-GVO. Bei sieben Empfängern und einzelnen Befundangaben können 1.000,00 EUR angemessen sein.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Rn. 40 Die zulässige Klage ist teilweise begründet.

Rn. 41 1. Der Klageantrag zu 1) ist zulässig und begründet.

[…]

Rn. 46 3) Der Unterlassungsantrag ist auch begründet. Die Klägerin hat gegen die Beklagte einen Anspruch auf Unterlassung der Weitergabe personenbezogener Gesundheitsdaten des Klägers, ohne dass einer der im Antrag konkretisierten Rechtfertigungstatbestände vorliegt. Der Anspruch folgt aus § 1004 Abs. 1 BGB, § 823 Abs. 2 S. 1 BGB i.V.m. Art. 9 DS-GVO.

Rn. 47 a) Nach allgemeinen Grundsätzen kann in entsprechender Anwendung des § 1004 Abs. 1 BGB die Unterlassung objektiv rechtswidriger Eingriffe in geschützte Rechtsgüter im Sinne des § 823 Abs. 2 S. 1 BGB verlangt werden. Demnach ist derjenige, der gegen ein den Schutz eines anderen bezweckendes Gesetz im Sinne des § 823 Abs. 2 S. 1 BGB verstößt, dem anderen entsprechend § 1004 Abs. 1 BGB zur Unterlassung verpflichtet. Ist nach dem Inhalt des Geset-

zes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Unterlassungspflicht – anders als die Ersatzpflicht (§ 823 Abs. 2 S. 2 BGB) – auch ohne ein Verschulden des Verletzers ein (vgl. BGH, Urt. v. 17.7.2008 – I ZR 219/05 – Rn. 13, juris; LAG Hamm, Urt. v. 14.12.2021 – 17 Sa 1185/20 –, Rn. 98, juris).

Rn. 48 b) Die Beklagte hat zu Lasten des Klägers ein Schutzgesetz verletzt.

Rn. 49 aa) Art. 9 DS-GVO ist ein Schutzgesetz im Sinne des § 823 BGB, da die Norm dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten dient (vgl. LAG Hamm, Urt. v. 14.12.2021 – 17 Sa 1185/20 –, Rn. 99 ff., juris; OLG Köln, Urt. v. 14.11.2019 – I-15 U 126/19 –, juris, Rn. 30, zum BDSG BGH, Urt. v. 27.2.2018 – VI ZR 489/16 –, juris, Rn. 42; BGH, Urt. v. 24.7.2018 – VI ZR 330/17 –, Rn. 30, juris; a.A. LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, Rn. 150, juris).

[…]

Rn. 53 (c) Es ist entgegen der Auffassung der Beklagten auch nicht der Tatbestand einer Bereichsausnahme im Sinne des Art 2 Abs. 2 lit. c) DS-GVO erfüllt. Danach findet die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Als Ausnahmenorm ist Art. 2 Abs. 2 lit. c) DS-GVO grds. restriktiv auszulegen (vgl. EuGH, Urt. v. 11.12.2014 – C-212/13, juris, Rn. 29 f.). Eine Verarbeitung von personenbezogenen Daten dient dann der Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten, wenn sie ohne jeden Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (vgl. Paal/Pauly/Ernst, 4. Aufl. 2026, VO (EU) 2016/679 Art. 2 Rn. 16). Gemischte Verarbeitungen zu persönlichen und geschäftlichen Zwecken sind daher nicht privilegiert Die Verordnung ist dementsprechend anwendbar, wenn die Datenverarbeitung den privaten Bereich auch nur teilweise überschreitet (vgl. BeckOK DatenschutzR/Bäcker, 55. Ed. 1.8.2023, DS-GVO Art. 2 Rn. 14). Zwar dürfte der Ausnahmetatbestand des Art. 2 Abs. 2 lit. c) DS-GVO erfüllt sein, wenn Nutzende sozialer Netzwerke in geschlossenen Gruppen Daten austauschen, die keinen Bezug zu ihrer beruflichen oder wirtschaftlichen Tätigkeit haben (vgl. EuArbRK/Franzen, 5. Aufl. 2024, VO (EU) 2016/679 Art. 2 Rn. 7). Dies war vorliegend bezogen auf die Chatgruppe „Ärzte-AC" jedoch gerade nicht der Fall. Denn bereits die Bezeichnung der Chatgruppe sowie deren Zusammensetzung ausschließlich aus Kolleginnen und Kollegen einer Abteilung des Krankenhauses lässt einen beruflichen Kontext erkennen. Es kann dahinstehen, ob bereits das ausreichen würde, um den rein persönlichen Zusammenhang zu überschreiten. Jedenfalls wenn wie vorliegend in einer Chatgruppe zu mindestens 30 % arbeitsbezogene Inhalte (Organisationsfragen, Urlaubs- und Vertretungsplanung etc.) ausgetauscht werden und auch die streitgegenständliche Nachricht selbst einen eindeutig dienstbezogenen Hintergrund hat, dient die Datenverarbeitung nicht ausschließlich persönlichen Zwecken.

Rn. 54 cc) Die Beklagte ist im Hinblick auf die streitgegenständliche Datenübermittlung "Verantwortliche" i.S.d. Art. 4 Nr. 7 DS-GVO.

Rn. 55 (a) Nach Art. 4 Ziff. 7 Hs. 1 DS-GVO ist Verantwortlicher jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der DS-GVO liegt ein allgemeines Funktionsträgerprinzip zugrunde: Verarbeiten natürliche Personen im Rahmen der weisungsgemäßen Ausübung ihrer Tätigkeit Daten für ein Unternehmen, so wird die Datenverarbeitung dem Unternehmen zugerechnet. Mitarbeitende von Unternehmen sind daher grundsätzlich nicht Verantwortliche nach Art. 82 Abs. 1 DS-GVO, auch wenn sie intern für die schadensverursachende Datenverarbeitung zuständig sind (vgl. Meyer, ZD 2025, 200, 201; Ambrock, ZD 2020, 492, 493; Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 2; BeckOK DatenschutzR/Quaas, 55. Ed. 1.2.2026, DS-GVO Art. 82 Rn. 39a; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 4).

Rn. 56 (b) Etwas anderes gilt dann, wenn Beschäftigte personenbezogene Daten für eigene Zwecke verarbeiten, die sich von denen der arbeitgebenden Partei unterscheiden, das Handeln also nicht den zugewiesenen Aufgaben entspricht. Im Falle eines solchen Exzesses wird der oder die Mitarbeitende nach den Art. 4 Nr. 7 DS-GVO selbst zum Verantwortlichen (vgl. OLG Stuttgart, Beschl. v. 25.2.2025 – 16 Ss 336/24, juris, Rn. 10 unter Bezugnahme auf die Leitlinien des Europäischen Datenschutzausschuss (European Data Protection Board) vom 7.7.2021; Meyer, ZD 2025, 200, 201; Ambrock, ZD 2020, 492, 493; Sura, in NZA-RR 2025, 528 ff.; Köppen, CuA 2025, Nr 5, 30 ff.; BeckOK DatenschutzR/Quaas, 55. Ed. 1.2.2026, DS-GVO Art. 82 Rn. 39c; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 4)

Rn. 57 (c) Ein solcher Fall ist hier gegeben. Denn die Beklagte dürfte zwar im Rahmen der Ausübung ihrer Tätigkeit für ihre Arbeitgeberin gehandelt haben, indem sie in der Chatgruppe „Ärzte-AC" zu Fragen der Dienstplangestaltung und Vertretungsregelungen kommunizierte. Soweit sie darüber hinaus jedoch – nachdem der Vertretungsfall bereits abgeschlossen war – Informationen zu den medizinischen Gründen für den krankheitsbedingten Ausfall des Klägers, dessen Krankheitsgeschichte sowie den Einzelheiten der ärztlichen Behandlung offenbarte, war dies für dienstliche Zwecke weder erforderlich noch sinnvoll. Es entsprach weder den arbeitsvertraglichen Aufgaben der Klägerin noch lag es objektiv im Interesse der Arbeitgeberin. Vielmehr erfolgte die Mitteilung in den Worten der Beklagten „Nur zu jedermanns Info", letztlich um den Kläger in der Abteilung bloßzustellen.

Rn. 58 dd) Es liegt ein Verstoß gegen Art. 9 Abs. 1 DS-GVO vor. Nach dieser Vorschrift ist die Verarbeitung von Gesundheitsdaten untersagt, sofern nicht eine Ausnahme nach Art. 9 Abs. 2 DS-GVO vorliegt. Gesundheitsdaten sind gemäß Art. 4 Nr. 15 DS-GVO personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Rn. 59 (a) Gesundheitsdaten sind hier die Informationen über die Tatsache der Behandlung des Klägers im Krankenhaus, dessen Laborwerte und Diagnosen.

Rn. 60 (b) Eine Ausnahme im Sinne von Art. 9 Abs. 2 DS-GVO greift nicht ein. Insbesondere handelt es sich vorliegend nicht im Sinne des Art. 9 Abs. 2 lit. e) DS-GVO um personenbezogene Daten, die der Kläger selbst öffentlich gemacht hat. Dabei kann dahinstehen, ob der Kläger, wie von der Beklagten behauptet, einzelnen Mitgliedern der Chatgruppe bereits von seiner Erkrankung berichtet hatte. Denn

dass der Kläger sämtliche der von der Beklagten preisgegebene Einzelheiten bereits gegenüber allen Mitgliedern der Gruppe bekannt gegeben hatte, hat die Beklagte gerade nicht behauptet. Auch hatte der Kläger weder ausdrücklich noch konkludent in die Verarbeitung eingewilligt (Art. 9 Abs. 2 lit. a) DS-GVO) noch war die Verarbeitung im Rahmen der ärztlichen Tätigkeit der Beklagten erforderlich (Art. 9 Abs. 2 lit. e) DS-GVO). Die Beklagte war gerade nicht die behandelnde Ärztin des Klägers. Das Vorliegen anderer Ausnahmetatbestände ist weder von der Beklagten behauptet noch ersichtlich.

Rn. 61 c) Es besteht auch die erforderliche Wiederholungsgefahr.

Rn. 62 aa) Die Besorgnis weiterer Beeinträchtigungen (§ 1004 Abs. 1 S. 2 BGB) ist Tatbestandsmerkmal des auf §§ 1004, 823 BGB gestützten Unterlassungsanspruchs und damit materielle Anspruchsvoraussetzung (vgl. BAG, Urt. v. 20.11.2012 – 1 AZR 179/11 –, juris, Rn. 82). Für sie besteht eine tatsächliche Vermutung, wenn es bereits zu einer Verletzung des geschützten Rechts gekommen ist. Sie ist allerdings dann ausgeschlossen, wenn aus tatsächlichen oder rechtlichen Gründen keine erneute Verletzungshandlung zu erwarten ist (vgl. BAG, Beschl. v. 7.6.2017 – 1 ABR 32/15, juris, Rn. 24; LAG Niedersachsen, Urt. v. 7.4.2025 – 15 SLa 855/24 –, Rn. 72, juris; LAG Hamm, Urt. v. 14.12.2021 – 17 Sa 1185/20 –, Rn. 144, juris).

Rn. 63 bb) Unter Zugrundelegung dieser Grundsätze besteht vorliegend entgegen der Auffassung der Beklagten eine Wiederholungsgefahr. Angesichts des Verstoßes der Beklagten gegen Art. 9 Abs. 1 DS-GVO besteht hierfür eine tatsächliche Vermutung. Diese ist nicht dadurch ausgeschlossen, dass der Kläger und die Beklagte mittlerweile keine Kollegen mehr sind und der Kläger aus der Chatgruppe „Ärzte-AC" ausgetreten ist. Denn es besteht weiterhin die Gefahr, dass die Beklagte sich, wie in der Vergangenheit geschehen, in ihrer Funktion als Ärztin Zugriff auf Gesundheitsinformationen des Klägers verschafft, sollte dieser sich erneut in dem Krankenhaus behandeln lassen, in dem die Beklagte beschäftigt ist. Es erscheint auch nicht ausgeschlossen, dass die Beklagte diese Daten erneut „zur Info" an die – nun ehemaligen – Kolleginnen und Kollegen des Klägers weitergibt. Für eine Wiederholungsgefahr spricht insbesondere, dass die Beklagte weiterhin geltend macht, dass die streitgegenständliche Datenübermittlung rechtmäßig gewesen sei und sie sich keiner Schuld bewusst sei.

Rn. 64 2. Der unproblematisch zulässige Klageantrag zu 2) ist teilweise begründet. Der Kläger hat gegen die Beklagte Anspruch auf die Zahlung von 1.000,00 EUR als Entschädigung nach Art. 82 Abs. 1 DS-GVO.

Rn. 65 1) Der Kläger ist für den geltend gemachten Anspruch aktivlegitimiert. Denn anspruchsberechtigt ist nach Art. 82 Abs. 1 DS-GVO jede Person, der wegen eines Verstoßes gegen die DS-GVO ein Schaden entstanden ist.

Rn. 66 2) Die Beklagte ist als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO passivlegitimiert im Sinne von Art. 82 Abs. 1 DS-GVO. Es wird insoweit auf die Ausführungen unter I.1.2)b)cc) verwiesen.

Rn. 67 3) Es liegt auch ein Verstoß gegen die DS-GVO im Sinne von Art. 82 Abs. 1 DS-GVO vor. Die Beklagte hat gegen Art. 9 Abs. 1 DS-GVO verstoßen, indem sie am 31.5.2025 eine WhatsApp-Nachricht an den Gruppenchat „Ärzte-AC" schickte, in welcher sie mitteilte, der Kläger habe sich im Krankenhaus behandeln lassen, es sei bei ihm Adipositas und eine Fettleber bei fraglichem Durchfall diagnostiziert worden und die Laboruntersuchung sei im Übrigen unauffällig und ohne Hinweis auf eine Elektrolytstörung gewesen. Es wird insoweit auf die Ausführungen unter I.1.2)b)dd) verwiesen.

Rn. 68 4) Die Beklagte ist für den Verstoß gegen die DS-GVO verantwortlich i.S.v. Art. 82 Abs. 3 DS-GVO. Entgegenstehendes hat sie nicht dargetan.

Rn. 69 5) Der Kläger hat einen immateriellen Schaden i.S.d. Art. 82 Abs. 1 DS-GVO erlitten.

Rn. 70 a) Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten i.S.d. Bestimmung autonom unionsrechtlich zu definieren. Dabei soll nach ErwG 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht jedoch nicht aus, um einen Schadenersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens durch den Verstoß erforderlich. Es ist allerdings nicht erforderlich, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (st. Rspr., vgl. EuGH, Urteile vom 20.6.2024 – C-590/22, juris, Rn. 25; v. 11.4.2024 – C-741/21, juris, Rn. 34 – juris; v. 4.5.2023 – C-300/21, juris, Rn. 42). Schon der Verlust der Kontrolle über personenbezogene Daten kann einen immateriellen Schaden darstellen, ohne dass dieser Begriff des "immateriellen Schadens" den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (vgl. EuGH, Urt. v. 4.10.2024 – C-200/23, juris, Rn. 145, 156 m.w.N.).

Rn. 71 Durch die Weitergabe von Daten an nicht berechtigte Dritte wird ein Kontrollverlust in dem Sinne verursacht, dass unbefugte Dritte Zugriff auf personenbezogene Daten erhalten (vgl. BGH, EuGH-Vorlage vom 6.5.2025 – VI ZR 53/23 -, Rn. 46, juris). Ein Schaden kann daher ohne Hinzukommen weiterer Umstände allein darin liegen, dass personenbezogene Daten hierzu nicht berechtigten Dritten überlassen werden (vgl. BGH, Urt. v. 11.2.2025 – VI ZR 365/22 –, Rn. 16, juris; OLG Hamm, Urt. v. 20.1.2023 – I-11 U 88/22 –, Rn. 121, juris; OLG Düsseldorf, Urt. v. 28.10.2021 – I-16 U 275/20 –, juris), etwa im Falle eines Datenlecks bzgl. Gesundheitsdaten (vgl. BAG, Urt. v. 20.2.2025 – 8 AZR 61/24 -, Rn. 22, juris).

Rn. 72 b) Vorliegend hat der Kläger unter Zugrundelegung dieser Grundsätze den Eintritt eines immateriellen Schadens hinreichend dargelegt. Durch das Handeln der Klägerin sind Gesundheitsdaten des Klägers an jedenfalls sieben Mitglieder der Chatgruppe „Ärzte-AC" – exklusive des Klägers und der Beklagten selber – übermittelt worden, die insoweit nicht zugriffsberechtigt waren. Es handelte sich dabei um detaillierte und intime Informationen zu Diagnosen und Laborwerten. Es entstand ein Kontrollverlust bezüglich der Gesundheitsdaten des Klägers, die er dem Krankenhaus bzw. den ihn behandelnden Personen ausschließlich zum Zwecke der Durchführung der medizinischen Behandlung anvertraut hatte. Darüber hinaus wurde der Kläger durch die mit der Datenweitergabe verknüpfte Andeutung der Beklagten, dass eine tatsächliche Arbeitsunfähigkeit nicht vorgelegen habe („meint […] höchst

krank zu sein", „vielleicht sitzt [...] ein Pups quer "), im Kollegenkreis herabgesetzt.

Rn. 73 6) Zum Ersatz dieses immateriellen Schadens hält die Kammer einen Betrag i.H.v. 1.000,00 EUR für geboten, aber auch ausreichend.

Rn. 74 a) Bei der Bemessung der Höhe des nach Art. 82 I DS-GVO geschuldeten Schadenersatzes haben die nationalen Gerichte in Ermangelung einer Bestimmung in der Datenschutz-Grundverordnung die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden. Art. 82 I DS-GVO verlangt dabei nicht, dass die Schwere des Verschuldens des Verantwortlichen bzw. des Auftragsverarbeiters berücksichtigt wird. Die Ausgleichsfunktion des in Art. 82 I DS-GVO verankerten Schadenersatzanspruchs schließt es sogar aus, dass eine etwaige Vorsätzlichkeit des Verstoßes gegen die Datenschutz-Grundverordnung bei der Bemessung des Schadenersatzes berücksichtigt wird. Der Betrag ist jedoch so festzulegen, dass er den konkret aufgrund des Verstoßes gegen die Datenschutz-Grundverordnung erlittenen Schaden in vollem Umfang ausgleicht (vgl. EuGH 20.6.2024 – C-182/22, C-189/22, ECLI:EU:C:2024:531, juris, Rn. 27 ff. m.w.N.). Bei der nach diesen Maßgaben vorzunehmenden Bemessung der Höhe eines Schadenersatzes steht den Tatsachengerichten nach § 287 Abs. 1 ZPO ein weiter Ermessensspielraum zu, innerhalb dessen sie die Besonderheiten jedes einzelnen Falls zu berücksichtigen haben (vgl. BAG, Urt. v. 25.7.2024 – 8 AZR 225/23, juris, Rn. 37).

Rn. 75 Maßgeblich sind die Intensität der Verletzung, die betroffenen Kategorien personenbezogener Daten sowie die konkreten Folgen für die betroffene Person (vgl. BAG, Urt. v. 25.7.2024 – 8 AZR 225/23, juris, Rn. 38).

Rn. 76 b) Vorliegend war nach Auffassung der erkennenden Kammer zu Gunsten des Klägers zu berücksichtigen, dass bei dem Verstoß die besonders geschützte Kategorie der Gesundheitsdaten im Sinne von Art. 4 Nr. 15 DS-GVO betroffen war. Innerhalb dieser Kategorie handelte es sich weiter um besonders sensible Daten, nämlich konkrete Diagnosen und Laborergebnisse. Auch hat der Kläger zur Überzeugung der Kammer glaubhaft geschildert, dass der streitgegenständliche Vorfall seine Stellung im Kollegenkreis beschädigt hat und mitursächlich für seine Entscheidung war, den Arbeitsplatz zu wechseln. Auf der anderen Seite war der Personenkreis, an welchen die Weitergabe erfolgte mit sieben Personen überschaubar. Zudem hat die Beklagte keine Dokumente der Krankenakte weitergeleitet sondern lediglich einzelne Informationen preisgegeben. Vor diesem Hintergrund war davon auszugehen, dass der Schaden mit einem Betrag in Höhe von 1.000,00 EUR hinreichend ausgeglichen ist.

Rn. 77 7) Der Anspruch auf Prozesszinsen folgt aus § 291, § 288 Abs. 1 S. 2, § 247 BGB.

Rn. 78 3. Im Übrigen war die Klage abzuweisen. Der Kläger hat gegen die Beklagte keinen Anspruch auf die Zahlung von weiteren 1.000,00 EUR. Es wird insoweit auf die Ausführungen unter I.2.6) verwiesen.

Zur Vertiefung

Praxisfälle zum Datenschutzrecht XXX: Datenschutzrechtliche Folgen im Fall des Mitarbeiterexzesses = RDV 5/2024

[Urteil] Grenzen der arbeitsrechtlich zulässigen Einsichtnahme in auch privat genutzte E-Mail- und WhatsApp-Verläufe = RDV 5/2023

WICHTIGES AUS DER RECHTSPRECHUNG

Auch der erste Auskunftsantrag kann exzessiv sein

(EuGH, Urteil vom 19. März 2026 – C-526/24 – Brillen Rottler –)

1. **Art. 12 Abs. 5 der Verordnung (EU) 2016/679 [...] (Datenschutz-Grundverordnung) ist dahin auszulegen, dass ein erster von der betroffenen Person an den Verantwortlichen gerichteter Antrag nach Art. 15 dieser Verordnung auf Auskunft über personenbezogene Daten als „exzessiv" im Sinne dieses Art. 12 Abs. 5 angesehen werden kann, wenn der Verantwortliche in Ansehung aller relevanten Fallumstände nachweist, dass dieser Antrag trotz formaler Einhaltung der in diesen Bestimmungen vorgesehenen Bedingungen von der betroffenen Person nicht gestellt wurde, um sich der Verarbeitung dieser Daten bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, damit sie anschließend ihre Rechte aus der besagten Verordnung schützen kann, sondern in missbräuchlicher Absicht wie zur künstlichen Schaffung der Voraussetzungen für die Erlangung eines sich aus dieser Verordnung ergebenden Vorteils. Dass die betroffene Person nach öffentlich zugänglichen Informationen etwa mehrere Anträge auf Auskunft über ihre personenbezogenen Daten, gefolgt von Schadenersatzforderungen gegenüber verschiedenen Verantwortlichen, gestellt hat, kann für die Feststellung einer solchen missbräuchlichen Absicht berücksichtigt werden.**
2. **Art. 82 Abs. 1 der Verordnung 2016/679 ist dahin auszulegen, dass er der betroffenen Person einen Anspruch auf Ersatz des aus einer Verletzung des Auskunftsrechts nach Art. 15 Abs. 1 dieser Verordnung entstandenen Schadens verleiht.**
3. **Art. 82 Abs. 1 der Verordnung 2016/679 ist dahin auszulegen, dass der immaterielle Schaden der betroffenen Person den Verlust der Kontrolle über ihre personenbezogenen Daten oder ihre Ungewissheit darüber umfasst, ob ihre Daten verarbeitet wurden, sofern insbesondere nachgewiesen wird, dass dieser Person tatsächlich ein solcher Schaden entstanden ist und dass ihr Verhalten nicht die entscheidende Ursache für diesen Schaden war.**

Aus den Gründen:

Rn. 21 Mit seinen Fragen 1 bis 3 und 7, die zusammen und als Erstes zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 12 Abs. 5 DS-GVO dahin auszulegen ist, dass es möglich ist, einen ersten von der betroffenen Person an den Verantwortlichen gerichteten Antrag nach

Art. 15 DS-GVO auf Auskunft über personenbezogene Daten als „exzessiv" im Sinne dieses Art. 12 Abs. 5 anzusehen, und, wenn dem so ist, anhand welcher Umstände gegebenenfalls ein solcher exzessiver Charakter festgestellt werden kann.

Rn. 22 Art. 15 Abs. 1 DS-GVO garantiert insoweit das Recht der betroffenen Person, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, und, wenn dies der Fall ist, das Recht dieser Person auf Auskunft über diese Daten und die damit verbundenen Informationen (vgl. in diesem Sinne Urt. v. 26.10.2023, FT [Kopien der Patientenakte], C-307/22, EU:C:2023:811, Rn. 31).

Rn. 23 Außerdem stellt Art. 12 Abs. 5 DS-GVO den Grundsatz auf, dass der betroffenen Person durch die Ausübung des Rechts auf Auskunft keine Kosten entstehen. Gleichwohl gibt es nach dieser Bestimmung zwei Gründe, aus denen der Verantwortliche entweder ein angemessenes Entgelt in Rechnung stellen kann, bei dem die Verwaltungskosten berücksichtigt werden, oder sich weigern kann, aufgrund des Auskunftsantrags tätig zu werden. Diese Gründe beziehen sich auf Fälle von Rechtsmissbrauch, in denen die Anträge der betroffenen Person als „offenkundig unbegründet" oder – insbesondere im Fall häufiger Wiederholung – „exzessiv" anzusehen sind (Urt. v. 26.10.2023, FT [Kopien der Patientenakte], C-307/22, EU:C:2023:811, Rn. 31).

Rn. 24 Was erstens die Frage betrifft, ob ein erster Auskunftsantrag der betroffenen Person an den Verantwortlichen nach Art. 15 DS-GVO als „exzessiv" angesehen werden kann, ist darauf hinzuweisen, dass, da der Begriff „exzessive Anträge" in der DS-GVO nicht definiert wird, bei seiner Auslegung nach ständiger Rechtsprechung sowohl der Wortlaut von Art. 12 Abs. 5 DS-GVO entsprechend seinem üblichen Sinn im gewöhnlichen Sprachgebrauch als auch der Zusammenhang dieser Bestimmung und die Ziele zu berücksichtigen sind, die mit der Regelung, zu der sie gehört, verfolgt werden (vgl. Urt. v. 17.11.1983, Merck,292/82, EU:C:1983:335, Rn. 12, und v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 24 und die dort angeführte Rechtsprechung).

Rn. 25 Insoweit bezeichnet, was den Wortlaut von Art. 12 Abs. 5 DS-GVO und insbesondere den üblichen Sinn des Begriffs „exzessive Anträge" im gewöhnlichen Sprachgebrauch anbelangt, das Adjektiv „exzessiv" etwas, das über das gewöhnliche oder vernünftige Maß hinausgeht oder das erwünschte oder zulässige Maß überschreitet (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 43). Allein anhand der Verwendung dieses Adjektivs, das sich sowohl auf qualitative als auch auf quantitative Merkmale bezieht, kann daher nicht ausgeschlossen werden, dass ein erster Auskunftsantrag exzessiv sein mag.

Rn. 26 Zudem ergibt sich zwar aus Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO, dass Anträge „insbesondere im Fall von häufiger Wiederholung" exzessiv sein können. Die Häufung von Anträgen einer Person kann daher ein Indiz dafür sein, dass sie exzessiv sind (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 57). Wie der Generalanwalt in Nr. 28 seiner Schlussanträge im Wesentlichen betont hat, verlangt jedoch, da die häufige Wiederholung in dieser Bestimmung nur beispielhaft angeführt wird, die Einstufung eines Auskunftsantrags als „exzessiv" nicht, dass der betreffende Antrag notwendigerweise im Zusammenhang mit der Einreichung mehrerer Anträge durch dieselbe betroffene Person stehen muss.

Rn. 27 In Ansehung einer am Wortlaut orientierten Auslegung von Art. 12 Abs. 5 DS-GVO kann daher nicht ausgeschlossen werden, dass ein erster Auskunftsantrag als „exzessiv" i.S.d. Bestimmung angesehen werden kann.

Rn. 28 Bestätigung findet diese Feststellung im Regelungszusammenhang von Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO. Insoweit ist darauf hinzuweisen, dass dieser Art. 12, der sich in Kapitel III der DS-GVO über die Rechte der betroffenen Person findet, allgemeine Pflichten des Verantwortlichen in Bezug auf die Transparenz von Information und Kommunikation aufstellt und die Modalitäten für die Ausübung der Rechte der betroffenen Person festlegt. Nach Art. 12 Abs. 2 S. 1 DS-GVO muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß u.a. Art. 15 DS-GVO erleichtern, der den durch die DS-GVO geschaffenen Transparenzrahmen vervollständigt, indem er dieser Person ein Recht auf Auskunft über ihre personenbezogenen Daten gewährt (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 45 und 46).

Rn. 29 Indem Art. 12 Abs. 5 DS-GVO gleichzeitig den Verantwortlichen die Möglichkeit einräumt, bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten zu verlangen oder sich zu weigern, aufgrund eines Antrags tätig zu werden, sieht er mithin eine Ausnahme von der Pflicht zur Erleichterung u. a. des Auskunftsrechts vor, die eng auszulegen ist (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 33).

Rn. 30 Aus der Rechtsprechung des Gerichtshofs zur Auslegung des Begriffs „exzessive Anfragen" in Art. 57 Abs. 4 DS-GVO, die auf die vorliegende Rechtssache übertragbar ist, da Art. 57 Abs. 4 DS-GVO einen im Wesentlichen Art. 12 Abs. 5 DS-GVO entsprechenden Wortlaut hat und das gleiche Ziel wie dieser verfolgt, ergibt sich allerdings, dass in Art. 12 Abs. 5 DS-GVO ein allgemeiner Grundsatz des Unionsrechts zum Ausdruck kommt, wonach sich Einzelne nicht in betrügerischer oder missbräuchlicher Weise auf unionsrechtliche Normen berufen dürfen (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 49). Die Anwendung der Unionsregelung kann nämlich nicht so weit gehen, dass Vorgänge geschützt werden, die einem missbräuchlichen Zweck dienen (vgl. i.d.S. Urt. v. 19.9.2024, Matmut,C-236/23, EU:C:2024:761, Rn. 52 und die dort angeführte Rechtsprechung).

Rn. 31 Somit ist die Zahl der Auskunftsanträge der betroffenen Person an den Verantwortlichen für sich allein nicht ausschlaggebend für dessen Recht, von der ihm durch Art. 12 Abs. 5 DS-GVO eingeräumten Möglichkeit Gebrauch zu machen, auf den Antrag nicht tätig zu werden, so dass der Verantwortliche davon auch im Fall eines ersten Auskunftsantrags Gebrauch machen kann, wenn er in Ansehung aller relevanten Umstände des Einzelfalls dartut, dass eine Missbrauchsabsicht der betroffenen Person vorliegt (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 50).

Rn. 32 Diese systematische Auslegung steht im Einklang mit den Zielen, die mit der DS-GVO verfolgt werden. Insoweit ist festzustellen, dass diese Verordnung, wie sich aus ihren ErwG 10 und 11 ergibt, ein gleichmäßiges und hohes Schutzniveau für natürliche Personen in der Union gewährleisten und die Rechte der betroffenen Personen stärken und präzise festlegen soll. So sind die Pflichten des Verantwortlichen nach Art. 12 DS-GVO, die u. a. die Mitteilung gemäß Art. 15 DS-GVO betreffen, als ein Mechanismus konzipiert, der geeignet ist, die Rechte und Interessen der betroffenen Personen wirksam zu wahren (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 38 und 39 sowie die dort angeführte Rechtsprechung).

Rn. 33 Im vierten ErwG der DS-GVO wird jedoch ausgeführt, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist, da es im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss. Zudem hat der Gerichtshof bereits hervorgehoben, dass die Mechanismen, die es ermöglichen, einen angemessenen Ausgleich zwischen den verschiedenen berührten Rechten und Interessen zu finden, in der DS-GVO selbst festgelegt sind (Urt. v. 21.12.2023, Krankenversicherung Nordrhein, C-667/21, EU:C:2023:1022, Rn. 54 und die dort angeführte Rechtsprechung).

Rn. 34 Um die Umsetzung dieses angemessenen Ausgleichs durch die in Rede stehende Ausnahme sowie deren praktische Wirksamkeit zu gewährleisten, ist das relevante Kriterium für die Feststellung eines missbräuchlichen Verhaltens daher der exzessive Charakter des Auskunftsantrags in einer Beurteilung aus qualitativer Sicht gemäß Rn. 26 des vorliegenden Urteils, der nicht allein von der Zahl der Auskunftsanträge der betroffenen Person und damit davon abhängen kann, ob es sich um einen ersten Antrag dieser Person handelt.

Rn. 35 Daraus folgt, dass es möglich ist, einen ersten Auskunftsantrag an den Verantwortlichen nach Art. 15 DS-GVO als „exzessiv" im Sinne von Art. 12 Abs. 5 DS-GVO anzusehen. Da der Begriff „exzessive Anträge", wie sich aus Rn. 29 des vorliegenden Urteils ergibt, eng auszulegen ist, kann sich jedoch ein Verantwortlicher nur ausnahmsweise auf einen solchen exzessiven Charakter berufen, und die Maßstäbe für die Einstufung eines ersten Auskunftsantrags als „exzessiv" müssen, wie vom Generalanwalt in Nr. 34 seiner Schlussanträge ausgeführt, hoch sein. Ferner ist darauf hinzuweisen, dass nach Art. 12 Abs. 5 UAbs. 2 DS-GVO ausdrücklich der Verantwortliche den Nachweis für den exzessiven Charakter zu erbringen hat.

Rn. 36 Was zweitens die Umstände betrifft, unter denen der erste Auskunftsantrag der betroffenen Person als „exzessiv" im Sinne von Art. 12 Abs. 5 DS-GVO eingestuft werden und somit einen Rechtsmissbrauch im Sinne der oben in den Rn. 23 und 30 angeführten Rechtsprechung begründen kann, so ist für den Nachweis einer missbräuchlichen Verhaltensweise zweierlei erforderlich, nämlich zum einen eine Gesamtheit objektiver Umstände, aus denen sich ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wurde, und zum anderen ein subjektives Element, das in der Absicht der betroffenen Person besteht, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden. Bei einer solchen Einstufung müssen außerdem alle Tatsachen und Umstände des Einzelfalls berücksichtigt werden (vgl. i.d.S. Urt. v. 21.12.2023, BMW Bank u.a., C-38/21, C-47/21 und C-232/21, EU:C:2023:1014, Rn. 285 und 286 sowie die dort angeführte Rechtsprechung).

Rn. 37 Was als Erstes das objektive Element einer missbräuchlichen Verhaltensweise anbelangt, ist darauf hinzuweisen, dass eine betroffene Person mit Art. 15 DS-GVO vor dem Hintergrund des 63. ErwG der DS-GVO ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können soll, um sich insbesondere der Verarbeitung dieser Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können, damit sie gegebenenfalls ihre Rechte auf Berichtigung, auf Löschung und auf Einschränkung der Verarbeitung sowie ihr Widerspruchsrecht und im Schadensfall ihr Recht auf einen Rechtsbehelf ausüben kann (vgl. i.d.S. Urt. v. 12.1.2023, Österreichische Post [Informationen über die Empfänger personenbezogener Daten], C-154/21, EU:C:2023:3, Rn. 37 und 38).

Rn. 38 Im vorliegenden Fall stellte TC, wie sich aus der dem Gerichtshof vorliegenden Akte ergibt, den im Ausgangsverfahren streitigen Auskunftsantrag, nachdem er sich zum Newsletter von Brillen Rottler angemeldet und dem Unternehmen dabei bestimmte personenbezogene Daten übermittelt hatte, so dass dieser Auskunftsantrag in formaler Hinsicht eine Ausübung des Auskunftsrechts von TC im Hinblick auf die Erreichung des Ziels der Regelung darstellen könnte.

Rn. 39 In Anbetracht der oben in Rn. 36 angeführten Rechtsprechung kann jedoch der „exzessive" Charakter eines Auskunftsantrags und damit das Vorliegen eines Rechtsmissbrauchs nicht allein anhand der formalen Einhaltung der Anwendungsvoraussetzungen des Art. 15 DS-GVO ausgeschlossen werden.

Rn. 40 Was insoweit als Zweites das subjektive Element einer missbräuchlichen Vorgehensweise betrifft, so muss der Verantwortliche, um einen Auskunftsantrag als „exzessiv" im Sinne von Art. 12 Abs. 5 DS-GVO einstufen zu können, anhand aller relevanten Umstände des Einzelfalls nachweisen, dass eine Missbrauchsabsicht seitens der betroffenen Person vorliegt, wobei eine solche Absicht festgestellt werden kann, wenn diese Person den Antrag zu einem anderen Zweck stellt als dem, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, um anschließend ihre Rechte aus der DS-GVO schützen zu können (vgl. i.d.S. Urt. v. 9.1.2025, Österreichische Datenschutzbehörde [Exzessive Anfragen], C-416/23, EU:C:2025:3, Rn. 50 und 56).

Rn. 41 Somit obliegt im vorliegenden Fall unter Berücksichtigung insbesondere dessen, was sich aus Rn. 35 des vorliegenden Urteils ergibt, dem Verantwortlichen der eindeutige Nachweis, dass sich die betroffene Person mit dem Auskunftsantrag nach Art. 15 DS-GVO nicht der Datenverarbeitung bewusst werden, sondern künstlich die Voraussetzungen für die Erlangung von Schadensersatz von dem Verantwortlichen schaffen wollte.

Rn. 42 Insoweit werden sämtliche Fallumstände zu berücksichtigen sein, insbesondere der Umstand, dass die be-

troffene Person personenbezogene Daten freiwillig bereitgestellt hat, der Zweck der Bereitstellung dieser Daten, die zwischen der Datenbereitstellung und dem Auskunftsantrag verstrichene Zeit sowie das Verhalten dieser Person.

Rn. 43 Vor dem Hintergrund des bei ihm anhängigen Rechtsstreits sieht sich das vorlegende Gericht vor die Frage gestellt, ob bei der Beurteilung des Vorliegens eines Rechtsmissbrauchs öffentliche Informationen berücksichtigt werden können, die darauf hindeuten sollen, dass TC Anträge auf Auskunft über seine personenbezogenen Daten und Schadensersatzforderungen systematisch an verschiedene Verantwortliche nach einem Muster richtet, das mit dem im vorliegenden Fall angewandten vergleichbar ist. Dieser Anhaltspunkt kann zur Feststellung missbräuchlicher Absichten der betroffenen Person durchaus herangezogen werden, sofern er durch andere relevante Anhaltspunkte bestätigt wird.

Rn. 44 Mithin hat das vorlegende Gericht im vorliegenden Fall zu prüfen, ob Brillen Rottler unter Berücksichtigung aller relevanten Umstände nachgewiesen hat, dass TC mit dem betreffenden Auskunftsantrag eine missbräuchliche Absicht verfolgte.

Rn. 45 Nach alledem ist auf die Fragen 1 bis 3 und 7 zu antworten, dass Art. 12 Abs. 5 DS-GVO dahin auszulegen ist, dass ein erster von der betroffenen Person an den Verantwortlichen gerichteter Antrag nach Art. 15 DS-GVO auf Auskunft über personenbezogene Daten als „exzessiv" im Sinne dieses Art. 12 Abs. 5 angesehen werden kann, wenn der Verantwortliche in Ansehung aller relevanten Fallumstände nachweist, dass dieser Antrag trotz formaler Einhaltung der in diesen Bestimmungen vorgesehenen Bedingungen von der betroffenen Person nicht gestellt wurde, um sich der Verarbeitung dieser Daten bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, damit sie anschließend ihre Rechte aus der DS-GVO schützen kann, sondern in missbräuchlicher Absicht wie zur künstlichen Schaffung der Voraussetzungen für die Erlangung eines sich aus der DS-GVO ergebenden Vorteils. Dass die betroffene Person nach öffentlich zugänglichen Informationen etwa mehrere Anträge auf Auskunft über ihre personenbezogenen Daten, gefolgt von Schadensersatzforderungen gegenüber verschiedenen Verantwortlichen, gestellt hat, kann für die Feststellung einer solchen missbräuchlichen Absicht berücksichtigt werden.

Rn. 46 Mit seiner fünften und seiner sechsten Frage, die zusammen und als Zweites zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass er der betroffenen Person einen Anspruch auf Ersatz des aus einer Verletzung des Auskunftsrechts nach Art. 15 Abs. 1 DS-GVO entstandenen Schadens verleiht.

Rn. 47 Wie oben in Rn. 24 ausgeführt, sind nach ständiger Rechtsprechung bei der Auslegung einer Bestimmung des Unionsrechts nicht nur ihr Wortlaut, sondern auch ihr Zusammenhang und die mit ihr verfolgten Ziele zu berücksichtigen.

Rn. 48 Nach Art. 82 Abs. 1 DS-GVO hat eine Person, der „wegen eines Verstoßes gegen diese Verordnung" ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen. Es ist festzustellen, dass diese Bestimmung keine Bezugnahme auf die „Verarbeitung" enthält, so dass der Ersatzanspruch nicht auf Schäden beschränkt sein kann, die sich aus einer Verarbeitung personenbezogener Daten ergeben.

Rn. 49 Bestätigung findet diese Feststellung erstens in der systematischen Analyse dieser Bestimmung im Licht des 141. ErwG der DS-GVO, wonach jede betroffene Person das Recht haben sollte, gem. Art. 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, „wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht". Art. 82 Abs. 1 DS-GVO findet sich nämlich in deren Kapitel VIII über die Rechtsbehelfe, Haftungsregeln und Sanktionen zum Schutz dieser Rechte. Diese Rechte umfassen aber sowohl das in Art. 12 DS-GVO vorgesehene Recht einer betroffenen Person auf Information als auch ihr Auskunftsrecht nach Art. 15 Abs. 1 DS-GVO, so dass sie durch Art. 82 DS-GVO geschützt werden müssen, der somit dahin auszulegen ist, dass er auch für Schäden aus Verstößen gegen die Art. 12 und 15 DS-GVO gilt.

Rn. 50 Diese Auslegung kann nicht dadurch in Frage gestellt werden, dass zum einen ausweislich des 146. ErwG der DS-GVO der Verantwortliche Schäden ersetzen sollte, die einer Person „aufgrund einer Verarbeitung" entstehen, die mit der DS-GVO nicht im Einklang steht, und dass zum anderen in Art. 82 Abs. 2 und 4 DS-GVO von dem „durch [eine/die] Verarbeitung verursachten Schaden" die Rede ist.

Rn. 51 Wie nämlich die Kommission in ihren schriftlichen Erklärungen im Wesentlichen geltend macht, kann sich der behauptete Verstoß im Fall einer Verletzung der in den Bestimmungen des Kapitels III der DS-GVO vorgesehenen Rechte, insbesondere der Rechte auf Auskunft über die Daten und auf Berichtigung sowie der Rechte auf Löschung, auf Einschränkung der Verarbeitung und auf Übertragbarkeit, nicht aus einer tatsächlichen Verarbeitung der personenbezogenen Daten als solcher ergeben, sondern vielmehr aus der Weigerung, aufgrund des auf die Ausübung dieser Rechte bezogenen Antrags der betroffenen Person tätig zu werden. Würde der Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO vom Vorliegen von Schäden abhängig gemacht, die sich aus einer Verarbeitung als solcher ergeben, hätte dies daher den Ausschluss solcher Fälle vom Anwendungsbereich dieser Bestimmung zur Folge, deren praktische Wirksamkeit damit beeinträchtigt würde.

Rn. 52 Im Übrigen hat der Gerichtshof bereits entschieden, dass der Verstoß des Verantwortlichen gegen die Art. 26 und 30 DS-GVO, von denen der erste den Abschluss einer Vereinbarung über die jeweiligen Funktionen und Beziehungen der Verantwortlichen gegenüber betroffenen Personen und der zweite die Führung eines Verzeichnisses der Verarbeitungstätigkeiten betrifft, keine „unrechtmäßige Verarbeitung" darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht. Ein solcher Verstoß ist daher unter Rückgriff auf andere von der DS-GVO vorgesehene Maßnahmen zu heilen, u.a. durch Ersatz des vom Verantwortlichen etwaig verursachten Schadens gemäß Art. 82 DS-GVO (vgl. i.d.S. Urt. v. 4.5.2023, Bundesrepublik Deutschland [Elektronisches Gerichtsfach], C-60/22, EU:C:2023:373, Rn. 66 und 67).

Rn. 53 Zweitens findet die oben in Rn. 48 getroffene Feststellung Bestätigung in der teleologischen Auslegung von Art. 82 Abs. 1 DS-GVO, denn dieser Art. soll die Verwirklichung der Ziele der DS-GVO gewährleisten, zu denen u.a. das in deren elftem ErwG genannte Ziel gehört, die Rechte der

betroffenen Personen zu stärken und die Verpflichtungen für diejenigen zu verschärfen, die personenbezogene Daten verarbeiten und darüber entscheiden. Wie der Generalanwalt in Nr. 72 seiner Schlussanträge im Wesentlichen ausgeführt hat, würden aber diese Rechte, zu denen das Auskunftsrecht, um das es dem vorlegenden Gericht geht, gerade gehört, erheblich geschwächt, wenn Art. 82 Abs. 1 DS-GVO dahin ausgelegt werden sollte, dass er allein Schäden erfasst, die sich aus rechtswidrigen Handlungen ergeben, die eine Datenverarbeitung umfassen.

Rn. 54 Daraus folgt, dass sich die betroffene Person auch bei einem Verstoß gegen die DS-GVO, bei dem als solchem keine Datenverarbeitung impliziert ist, auf das in Art. 82 DS-GVO vorgesehene Recht auf Schadensersatz berufen kann.

Rn. 55 Demnach ist auf die fünfte und die sechste Frage zu antworten, dass Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass er der betroffenen Person einen Anspruch auf Ersatz des aus einer Verletzung des Auskunftsrechts nach Art. 15 Abs. 1 DS-GVO entstandenen Schadens verleiht.

Rn. 56 In Anbetracht der Antwort auf die fünfte und die sechste Vorlagefrage ist die vierte Frage nicht zu beantworten.

Rn. 57 Mit seiner achten Frage, die als Drittes und Letztes zu prüfen ist, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass der immaterielle Schaden der betroffenen Person den Verlust der Kontrolle über ihre personenbezogenen Daten oder ihre Ungewissheit darüber umfasst, ob diese Daten verarbeitet wurden.

Rn. 58 Da die DS-GVO für den Sinn und die Tragweite der in ihrem Art. 82 Abs. 1 enthaltenen Begriffe, insbesondere, was die Begriffe „materieller oder immaterieller Schaden" und „Schadenersatz" betrifft, nicht auf das Recht der Mitgliedstaaten verweist, sind diese Begriffe für die Zwecke der Anwendung der DS-GVO als autonome Begriffe des Unionsrechts anzusehen, die in allen Mitgliedstaaten einheitlich auszulegen sind (vgl. i.d.S. Urt. v. 4.5.2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, EU:C:2023:370, Rn. 30, und v. 4.9.2025, Quirin Privatbank,C-655/23, EU:C:2025:655, Rn. 55 und die dort angeführte Rechtsprechung).

Rn. 59 Insoweit ist darauf hinzuweisen, dass nicht davon ausgegangen werden kann, dass jeder „Verstoß" gegen die Bestimmungen der DS-GVO für sich genommen einen Schadensersatzanspruch der betroffenen Person begründet. Nach Art. 82 Abs. 1 DS-GVO hat nämlich „[j]ede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, ... Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter". Daraus geht klar hervor, dass das Vorliegen eines „Schadens", der „entstanden" ist, eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadensersatzanspruch darstellt, ebenso wie das Vorliegen eines Verstoßes gegen die DS-GVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. i.d.S. Urt. v. 4.5.2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, EU:C:2023:370, Rn. 31 bis 33, und v. 4.9.2025, Quirin Privatbank,C-655/23, EU:C:2025:655, Rn. 56 und die dort angeführte Rechtsprechung).

Rn. 60 Somit muss die Person, die auf der Grundlage von Art. 82 Abs. 1 DS-GVO Ersatz eines immateriellen Schadens fordert, nicht nur den Verstoß gegen Bestimmungen der DS-GVO nachweisen, sondern auch, dass ihr durch diesen Verstoß ein solcher Schaden entstanden ist. Ein entsprechender Schaden kann daher nicht allein deshalb vermutet werden, weil sich der Verstoß ereignet hat (Urt. v. 4.10.2024, Agentsia po vpisvaniyata,C-200/23, EU:C:2024:827, Rn. 141 und die dort angeführte Rechtsprechung).

Rn. 61 Davon abgesehen hat der Gerichtshof bereits entschieden, dass aus der im ersten Satz des 85. ErwG der DS-GVO enthaltenen beispielhaften Aufzählung der „Schäden", die den betroffenen Personen entstehen können, hervorgeht, dass der Unionsgesetzgeber unter den Schadensbegriff insbesondere auch den bloßen „Verlust der Kontrolle" über ihre eigenen personenbezogenen Daten infolge eines Verstoßes gegen die DS-GVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten erfolgt sein sollte (Urt. v. 4.10.2024, Agentsia po vpisvaniyata,C-200/23, EU:C:2024:827, Rn. 145 und die dort angeführte Rechtsprechung).

Rn. 62 Der Gerichtshof hat auch befunden, dass der Begriff „immaterieller Schaden" nicht allein auf Schäden mit einer gewissen Erheblichkeit beschränkt werden kann. Insbesondere darf eine nationale Regelung oder Praxis für einen durch einen Verstoß gegen die DS-GVO verursachten immateriellen Schaden keine „Bagatellgrenze" festlegen. Die betroffene Person muss jedoch nachweisen, dass ihr zum einen tatsächlich ein solcher Schaden – so geringfügig er auch sein mag – entstanden ist und dass zum anderen in den Folgen dieses Verstoßes, die sie erlitten zu haben behauptet, ein Schaden begründet liegt, der sich von der bloßen Verletzung der Bestimmungen der DS-GVO unterscheidet (vgl. i.d.S. Urt. v. 14.12.2023, Gemeinde Ummendorf,C-456/22, EU:C:2023:988, Rn. 22 und 23).

Rn. 63 So kann das bloße Vorbringen seitens der betroffenen Person einer durch einen Verlust der Kontrolle über ihre personenbezogenen Daten hervorgerufenen Befürchtung nicht zu Schadenersatz nach Art. 82 Abs. 1 DS-GVO führen (vgl. i.d.S. Urt. v. 20.6.2024, PS [Fehlerhafte Anschrift], C-590/22, EU:C:2024:536, Rn. 33 und 35). Beruft sich eine Person, die auf der Grundlage dieser Bestimmung Schadenersatz fordert, auf die Befürchtung, dass ihre personenbezogenen Daten etwa in Zukunft aufgrund eines Verstoßes gegen die DS-GVO missbräuchlich verwendet werden, muss daher das angerufene nationale Gericht prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. i.d.S. Urt. v. 4.10.2024, Agentsia po vpisvaniyata,C-200/23, EU:C:2024:827, Rn. 143 und die dort angeführte Rechtsprechung).

Rn. 64 Die Erwägungen in den vorstehenden Rn. 59 bis 63 gelten auch in einer Situation, in der nach Ansicht der betroffenen Person Unsicherheit darüber besteht, ob ihre personenbezogenen Daten verarbeitet wurden.

Rn. 65 Um dem vorlegenden Gericht eine zweckdienliche Antwort zu geben, ist noch darauf hinzuweisen, dass der Kausalzusammenhang zwischen dem behaupteten Verstoß und dem behaupteten Schaden durch die Handlungsweise der betroffenen Person unterbrochen werden kann, sofern

sich diese Handlungsweise als die entscheidende Ursache für den Schaden erweist. Eine entsprechende Handlung kann u. a. in einer Entscheidung der geschädigten Person bestehen, allerdings nur, sofern diese Entscheidung für sie nicht zwingend war (vgl. entsprechend Urt. v. 18.12.2025, WS u. a./Frontex [Gemeinsame Rückkehraktion], C-679/23 P, EU:C:2025:976, Rn. 151 und 152 sowie die dort angeführte Rechtsprechung).

Rn. 66 Außerdem ergibt sich aus der oben in Rn. 59 angeführten Rechtsprechung, dass das Bestehen eines Kausalzusammenhangs zwischen dem behaupteten Verstoß gegen die DS-GVO und dem Schaden, der der betroffenen Person entstanden sein soll, eine unabdingbare Voraussetzung für einen Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO ist. Folglich kann der betroffenen Person nach Art. 82 Abs. 1 DS-GVO kein Ersatz für Schäden gewährt werden, die ihr durch den Verlust der Kontrolle über ihre personenbezogenen Daten oder ihre Ungewissheit über das Vorliegen einer Verarbeitung dieser Daten entstanden sein sollen, wenn der Kausalzusammenhang aufgrund der Handlungsweise dieser Person unterbrochen wird, weil besagter Kontrollverlust oder besagte Ungewissheit durch die Entscheidung der betroffenen Person herbeigeführt wurden, dem Verantwortlichen diese Daten in der Absicht zu übermitteln, künstlich die Voraussetzungen für die Anwendung dieser Bestimmung zu schaffen.

Rn. 67 Demnach ist auf die achte Frage zu antworten, dass Art. 82 Abs. 1 DS-GVO dahin auszulegen ist, dass der immaterielle Schaden der betroffenen Person den Verlust der Kontrolle über ihre personenbezogenen Daten oder ihre Ungewissheit darüber umfasst, ob ihre Daten verarbeitet wurden, sofern insbesondere nachgewiesen wird, dass dieser Person tatsächlich ein solcher Schaden entstanden ist und dass ihr Verhalten nicht die entscheidende Ursache für diesen Schaden war.

Rn. 68 Für die Beteiligten des Ausgangsverfahrens ist das Verfahren Teil des beim vorlegenden Gericht anhängigen Verfahrens; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Fehlgeleitete Bewerbungsnachricht als Schaden

(BGH, Urt. v. 23. Juni 2026 – VI ZR 97/22 –)

1. **Zum Begriff des immateriellen Schadens i.S.v. Art. 82 DS-GVO.**
2. **Zu den Voraussetzungen eines Unterlassungsanspruchs nach nationalem Recht, der sich gegen eine erneute Übermittlung personenbezogener Daten unter Verstoß gegen die Datenschutz-Grundverordnung richtet.**

(Amtliche Leitsätze)

Aus den Gründen:

Rn. 11 Die zulässige Revision des Klägers ist begründet. Entgegen der Beurteilung des Berufungsgerichts steht dem Kläger gegen die Beklagte ein Schadensersatzanspruch gemäß Art. 82 Abs. 1 DS-GVO dem Grunde nach zu. Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die Datenschutz-Grundverordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Diese Voraussetzungen sind im Streitfall erfüllt.

[…]

Rn. 15 3. Die Beklagte hat gegen Bestimmungen der Datenschutz-Grundverordnung verstoßen. Das Berufungsgericht hat zutreffend erkannt, dass die angegriffene Verarbeitung der personenbezogenen Daten des Klägers durch die Beklagte gemäß Art. 6 Abs. 1 DS-GVO unrechtmäßig, insbesondere nicht durch eine Einwilligung des Klägers gedeckt war. Die Beklagte macht auch nicht geltend, dass die Verarbeitung nach dieser Vorschrift rechtmäßig gewesen wäre. Ob die Beklagte daneben auch – wie vom Berufungsgericht angenommen – gegen Art. 34 DS-GVO verstoßen hat, weil sie den Kläger nicht unverzüglich von der unrechtmäßigen Datenübermittlung benachrichtigt hat, kann dahinstehen. Denn der Kläger macht nicht geltend, dass er wegen der unterbliebenen bzw. verspäteten Benachrichtigung einen immateriellen Schaden erlitten hätte. Nachdem der Kläger noch am Tag der Übermittlung der Nachricht an den Dritten von diesem über den Vorgang in Kenntnis gesetzt wurde, wie sich aus dem vom Berufungsgericht in Bezug genommenen Chatverlauf ergibt, bestehen dafür auch keine Anhaltspunkte.

Rn. 16 4. Entgegen der Beurteilung des Berufungsgerichts ist auch das Vorliegen eines durch den Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung verursachten immateriellen Schadens im Sinne von Art. 82 Abs. 1 DS-GVO zu bejahen.

Rn. 17 a) Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten i.S.d. Bestimmung autonom unionsrechtlich zu definieren (st. Rspr. , vgl. nur EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 57; v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 55; Senatsurt. v. 11.11.2025 – VI ZR 396/24, GRUR 2026, 95 Rn. 25; v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 28; jeweils m.w.N.; BGH, Urt. v. 18.12.2025 – I ZR 97/25, NJW 2026, 845 Rn. 56). Dabei soll nach ErwG 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich (st. Rspr. , vgl. EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 59 f.; v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 56; Senatsurt. v. 11.11.2025 – VI ZR 396/24, GRUR 2026, 95 Rn. 25; v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 28; jeweils m.w.N.; BGH, Urt. v. 18.12.2025 – I ZR 97/25, NJW 2026, 845 Rn. 56).

Rn. 18 Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DS-GVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens i.S.d. Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (vgl. EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 62; v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 58; v. 20.6.2024 – C-590/22, DB

2024, 1676 Rn. 26; v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 36; v. 4.5.2023 – C-300/21, VersR 2023, 920 Rn. 51). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DS-GVO verpflichtet ist nachzuweisen, dass sie tatsächlich einen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die Datenschutz-Grundverordnung betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 dieser Verordnung darstellen (vgl. EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 62; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 142; v. 20.6.2024 – C-590/22, DB 2024, 1676 Rn. 27; v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 36).

Rn. 19 Unter Bezugnahme auf ErwG 85 hat der Gerichtshof zudem wiederholt darauf hingewiesen, dass der Unionsgesetzgeber unter den Begriff des Schadens auch den "bloßen Verlust der Kontrolle" über die eigenen personenbezogenen Daten dieser Personen infolge eines Verstoßes gegen die Datenschutz-Grundverordnung "fassen" wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten erfolgt sein sollte (EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 61; v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 60; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 145; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 82). Ähnlich heißt es im Urt. des Gerichtshofs v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 42, dass der 85. ErwG der DS-GVO ausdrücklich den "Verlust der Kontrolle" zu den Schäden "zählt", die durch eine Verletzung personenbezogener Daten verursacht werden können. In demselben Urteil (a.a.O.) sowie in seinem Urt. v. 20.6.2024 – C-590/22, ZD 2024, 519 Rn. 33 hat der Gerichtshof ausgeführt, dass der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DS-GVO "darstellen" (englische Fassung: "constitute", französische Fassung: "constituer") kann, der einen Schadensersatz begründet, sofern die betroffene Person den Nachweis erbringt, dass sie tatsächlich "einen solchen Schaden" – so geringfügig er auch sein mag – erlitten hat.

Rn. 20 Schließlich ist durch die Rechtsprechung des Gerichtshofs geklärt, dass die durch einen Verstoß gegen die Datenschutz-Grundverordnung ausgelöste (empfundene) Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung von Dritten missbräuchlich verwendet werden, "für sich genommen" einen immateriellen Schaden i.S.v. Art. 82 Abs. 1 DS-GVO darstellen kann, sofern diese Befürchtung samt ihrer negativen Folgen ordnungsgemäß nachgewiesen ist (vgl. EuGH, Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 61; v. 4.10.2024 – C-200/23, DB 2024, 2952 Rn. 143 f.; v. 20.6.2024 – C-590/22, ZD 2024, 519 Rn. 32, 35, 36; v. 25.1.2024 – C-687/21, CR 2024, 160 Rn. 65; Senatsurt. v. 13.5.2025 – VI ZR 186/22, CR 2025, 585 Rn. 28; vom 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 32). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (vgl. EuGH, Urt. v. 20.6.2024 – C-590/22, a.a.O. Rn. 35; v. 25.1.2024 – C-687/21, a.a.O. Rn. 68; Senatsurt. v. 13.5.2025 – VI ZR 186/22, a.a.O. Rn. 29; v. 18.11.2024 – VI ZR 10/24, a.a.O.). Die Befürchtung muss unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als "begründet" angesehen werden können (vgl. EuGH, Urt. v. 19.3.2026 – C-526/24, WRP 2026, 596 Rn. 63; v. 4.10.2024 – C-200/23, a.a.O. Rn. 143 m.w.N.; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 85; Senatsurt. v. 13.5.2025 – VI ZR 186/22, a.a.O.). Ebenso wenig wie beim Kontrollverlust ist es dagegen erforderlich, dass es zu einer missbräuchlichen Verwendung der Daten tatsächlich kommt (vgl. Senatsurt. v. 11.11.2025 – VI ZR 396/24, GRUR 2026, 95 Rn. 37). Die mit der begründeten Befürchtung einer missbräuchlichen Datenverwendung verbundenen negativen Folgen können auch negative Gefühle wie Sorge und Ärger sein, auch wenn diese Teil des allgemeinen Lebensrisikos sein können (vgl. EuGH, Urt. v. 4.9.2025 – C-655/23, a.a.O. Rn. 62, 64).

Rn. 21 b) Nach diesen Maßstäben ist vorliegend von einem immateriellen Schaden des Klägers i.S.v. Art. 82 DS-GVO spätestens ab dem Zeitpunkt auszugehen, zu dem der Dritte, an den die Beklagte die personenbezogenen Daten des Klägers unbefugt übermittelt hatte, diese zur Kenntnis und zum Anlass nahm, sich mit einer Rückfrage an den Kläger hinsichtlich dessen Bewerbung bei der Beklagten zu wenden. Denn zum einen lag darin bereits eine missbräuchliche Verwendung der Daten, so dass der mit ihrer Versendung an den Dritten verbundene Kontrollverlust für den Kläger nicht folgenlos geblieben ist. Der Rechtsprechung des Gerichtshofs lässt sich ohne Zweifel entnehmen, dass jedenfalls in einem solchen Fall ein immaterieller Schaden im Sinne von Art. 82 DS-GVO vorliegt (vgl. dazu näher Senatsurt. v. 11.11.2025 – VI ZR 396/24, GRUR 2026, 95 Rn. 32 m.w.N.). Zum anderen hat der Kläger die Befürchtung gehegt, dass der in der gleichen Branche wie er selbst tätige Dritte die in der streitgegenständlichen Nachricht enthaltenen Daten weitergegeben habe oder sich als Konkurrent auf etwaige Stellen aus der Kenntnis der übermittelten Informationen im Bewerbungsprozess habe einen Vorteil verschaffen können. Angesichts des Umstands, dass der Dritte nach Kenntnisnahme von den an ihn übermittelten personenbezogenen Daten des Klägers sich bei ihm nach seiner Bewerbung erkundigte, war diese Befürchtung auch hinreichend begründet.

Rn. 22 Auch das Rechtsmittel der Beklagten hat Erfolg.

[…]

Rn. 24 2. Die Revision der Beklagten ist auch begründet. Das Berufungsgericht hat die geltend gemachten Ansprüche auf Unterlassung und Erstattung der durch die Verfolgung des Unterlassungsanspruchs verursachten außergerichtlichen Rechtsverfolgungskosten zu Unrecht bejaht.

Rn. 25 a) Dem Kläger steht der geltend gemachte Anspruch gegen die Beklagte auf Unterlassung der Verarbeitung seiner personenbezogenen Daten nicht zu.

Rn. 26 Der Gerichtshof hat in seinem Urt. v. 4.9.2025 in der Rechtssache C-655/23 ausgeführt, die Bestimmungen der Datenschutz-Grundverordnung seien dahin auszulegen, dass sie zugunsten der von der unrechtmäßigen Verarbeitung personenbezogener Daten betroffenen Person für den Fall, dass diese Person – wie der Kläger im Streitfall – nicht die Löschung ihrer Daten beantragt, keinen gerichtlichen Rechtsbehelf vorsehen, der es ihr ermöglicht, präventiv zu erwirken, dass dem Verantwortlichen auferlegt wird, künftig eine erneute unrechtmäßige Verarbeitung zu unterlassen. Allerdings hinderten sie die Mitgliedstaaten nicht daran, einen

solchen Rechtsbehelf in ihren jeweiligen Rechtsordnungen vorzusehen (NJW 2025, 3137 Rn. 52). Damit kommt vorliegend aufgrund der gegen Art. 6 DS-GVO verstoßenden Übermittlung der personenbezogenen Daten des Klägers eine Verurteilung der Beklagten zu der beantragten Unterlassung nach nationalem Recht in entsprechender Anwendung von § 1004 Abs. 1 S. 2, § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, Art. 2 Abs. 1 GG wegen der durch die rechtswidrige Datenverarbeitung verursachten Verletzung des allgemeinen Persönlichkeitsrechts des Klägers in seiner Ausprägung als Recht auf informationelle Selbstbestimmung oder gem. § 1004 Abs. 1 S. 2 analog, § 823 Abs. 2 BGB i.V.m. Art. 6 DS-GVO (vgl. zum Unterlassungsanspruch bei einer nach § 29 BDSG a.F. unzulässigen Übermittlung Senatsurt. v. 27.2.2018 – VI ZR 489/16, BGHZ 217, 350 Rn. 42; v. 20.2.2018 – VI ZR 30/17, BGHZ 217, 340 Rn. 21 f.) in Betracht. Ob – wie die Beklagte meint – einer Verurteilung der Beklagten zur Unterlassung nach nationalem Recht entgegensteht, dass hierfür aufgrund des dem Betroffenen durch Art. 17 DS-GVO eingeräumten Anspruchs auf Löschung seiner personenbezogenen Daten kein Bedürfnis besteht, kann offen bleiben. Denn Voraussetzung für das Bestehen eines Unterlassungsanspruchs nach nationalem Recht ist in jedem Fall, dass künftig (weitere) Beeinträchtigungen der Rechte des Anspruchstellers zu besorgen sind, § 1004 Abs. 1 S. 2 BGB. Daran fehlt es hier. Das Berufungsgericht hat eine Wiederholungsgefahr bezüglich des geltend gemachten Unterlassungsbegehrens zu Unrecht bejaht.

Rn. 27 aa) Die Beurteilung, ob und inwieweit Wiederholungsgefahr für ein beanstandetes Verhalten besteht, ist im Wesentlichen tatsächlicher Natur. Sie ist im Revisionsverfahren nur beschränkt nachprüfbar darauf, ob das Berufungsgericht von richtigen rechtlichen Gesichtspunkten ausgegangen ist und keine wesentlichen Tatumstände außer Acht gelassen hat (vgl. zu § 1004 BGB Senatsurt. v. 16.11.2021 – VI ZR 1241/20, NJW 2022, 940 Rn. 33; v. 27.4.2021 – VI ZR 166/19, NJW 2021, 3334 Rn. 22; v. 4.6.2019 – VI ZR 440/18, VersR 2019, 1375 Rn. 22; v. 4.12.2018 – VI ZR 128/18, NJW 2019, 1142 Rn. 8; zu § 97 UrhG vgl. BGH, Urt. v. 22.9.2021 – I ZR 83/20, NJW 2022, 775 Rn. 34; jeweils m.w.N.).

Rn. 28 bb) Im rechtlichen Ausgangspunkt zutreffend ist das Berufungsgericht davon ausgegangen, dass dann, wenn bereits ein – hier gegebener – Verstoß erfolgt ist, eine tatsächliche Vermutung für das Vorliegen der Wiederholungsgefahr besteht. Es hat allerdings nicht hinreichend berücksichtigt, dass diese Vermutung entkräftet werden kann, wobei an die Entkräftung strenge Anforderungen zu stellen sind. Dabei kann dahinstehen, ob vorliegend bereits die von der Beklagten abgegebene strafbewehrte Unterlassungserklärung der Bejahung einer Wiederholungsgefahr entgegensteht. Denn die Widerlegung der tatsächlichen Vermutung für das Vorliegen der Wiederholungsgefahr kann ausnahmsweise auch dann angenommen werden, wenn der Verstoß durch eine einmalige Sondersituation veranlasst war (vgl. zu § 1004 BGB Senatsurt. v. 27.4.2021 – VI ZR 166/19, NJW 2021, 3334 Rn. 23; v. 4.6.2019 – VI ZR 440/18, VersR 2019, 1375 Rn. 36; v. 14.11.2017 – VI ZR 534/15, ZUM 2018, 440 Rn. 17; v. 8.2.1994 – VI ZR 286/93, VersR 1994, 570, juris Rn. 27).

Rn. 29 So liegt es hier. Der Kläger hat beantragt, die Beklagte zu verurteilen, es künftig zu unterlassen, personenbezogene Daten über den Kläger, die im Zusammenhang mit seiner Bewerbung stehen, zu verarbeiten oder verarbeiten zu lassen, wenn dies geschieht wie in der Nachricht über das Portal Xing an Herrn F. W. am 23.10.2018. Sein Unterlassungsbegehren beschränkt sich somit auf die Wiederholung der bereits begangenen Verletzungshandlung in ihrer konkreten Form, die dadurch gekennzeichnet ist, dass im Rahmen des laufenden Bewerbungsprozesses eine für den Kläger als Bewerber bestimmte und auf ihn bezogene personenbezogene Daten enthaltende Nachricht unbeabsichtigt an einen Dritten versandt wurde. Nachdem das Bewerbungsverfahren, an dem der Kläger teilgenommen hat, mittlerweile abgeschlossen ist, fehlt jedoch jede Wahrscheinlichkeit für eine Wiederholung einer derartigen Beeinträchtigung der Rechte des Klägers.

Rn. 30 cc) Einen vorbeugenden Unterlassungsanspruch, für den es auf das Bestehen einer Erstbegehungsgefahr ankäme, macht der Kläger nicht geltend. Wie bereits ausgeführt, zielt der Klageantrag – den der Senat als Revisionsgericht in freier Würdigung selbst auslegen kann (vgl. Senatsurt. v. 18.6.1996 – VI ZR 325/95, MDR 1997, 94, 95, juris Rn. 11; Senatsbeschl. v. 19.4.2005 – VI ZB 47/03, NJW-RR 2005, 955, juris Rn. 9; jeweils m.w.N.; BGH, Urt. v. 21.2.2012 – X ZR 111/09, NJW-RR 2012, 872 Rn. 24) – allein auf die Unterlassung der Wiederholung der bereits begangenen Verletzungshandlung.

Zulässigkeit der SCHUFA-Einmeldung bestrittener Forderungen und Folgenbeseitigung durch Widerruf (LS)

(BGH, Urteil vom 12. Mai 2026 – VI ZR 375/24 –)

1. **Die Meldung einer nicht titulierten, bestrittenen und nicht plausibel gemachten Forderung an eine Wirtschaftsauskunftei ist zur Wahrung berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO nicht erforderlich, weil sich aus solchen Forderungsdaten keine aussagekräftigen Indizien über Zahlungsfähigkeit oder Zahlungswillen des Betroffenen gewinnen lassen.**

2. **Werden personenbezogene Daten zu behauptet offenen Forderungen an eine Wirtschaftsauskunftei rechtswidrig übermittelt, kann dem Betroffenen gegen den Übermittelnden ein Folgenbeseitigungsanspruch in Form des Widerrufs der Einmeldung zustehen.**

3. **Ein immaterieller Schaden nach Art. 82 Abs. 1 DS-GVO liegt in der Beeinträchtigung des wirtschaftlichen Rufs, wenn die Einmeldung den Score-Wert des Betroffenen verschlechtert und dieser bei Vertragsanbahnungen tatsächlich berücksichtigt worden ist. Unter dem Gesichtspunkt des Kontrollverlusts genügt bereits, dass die Übermittlung an die Auskunftei zur Gefahr weiterer Übermittlungen an eine unbestimmte Zahl von Dritten geführt hat.**

(Nicht amtliche Leitsätze)

Lauterkeitsrechtliche Haftung für unzutreffende Facharztangaben des eigenen KI-Chatbots

(OLG Hamm, Urteil vom 12. Mai 2026 – 4 UKl 3/25 –)

1. **Die Antworten eines auf der Unternehmenswebseite implementierten KI-Chatbots sind geschäftliche Handlungen des Betreibers nach § 2 Abs. 1 Nr. 2 UWG. Dass der Chatbot autonom und im Einzelfall ungesteuert antwortet („Black-Box-Problem"), ändert daran nichts, solange der Betreiber dessen Tätigkeitsrahmen festlegen kann.**

2. **Der Chatbot ist kein Dritter im Sinne der wettbewerbsrechtlichen Verkehrspflicht. In Rede steht die Haftung für den eigenen Wettbewerbsverstoß des Betreibers. Die Störerhaftung kommt im Bereich des Verhaltensunrechts nicht mehr in Betracht.**

3. **Auch nach den Grundsätzen der Verkehrspflicht und der Störerhaftung hätte der Betreiber bereits vor der ersten Inbetriebnahme sicherstellen müssen, dass der Chatbot keine unzutreffenden Qualifikationsangaben ausgibt. Die nachträgliche Umprogrammierung belegt die Zumutbarkeit.**

4. **Halluzinierte Facharztbezeichnungen sind irreführend nach § 5 Abs. 1, Abs. 2 Nr. 3 UWG. Ein Erfahrungssatz, wonach Verbraucher KI-Antworten generell für überprüfungsbedürftig halten, besteht nicht.**

5. **Offen bleibt, ob anderes für Antworten gilt, die durch eine tendenziöse oder suggestive Fragestellung des Nutzers provoziert werden.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Rn. 52 Die zulässige Klage ist auch in vollem Umfang begründet.

Rn. 53 1.

Rn. 54 Der Kläger hat gegenüber der Beklagten gem. § 2 Abs. 1 S. 1 UKlaG i.V.m. § 3 Abs. 1, § 5 Abs. 1, Abs. 2 Nr. 3 UWG einen Anspruch darauf, die in den Unterlassungsanträgen zu Ziff. 1 lit. a) bis c) umschriebenen Handlungen zu unterlassen.

[...]

Rn. 61 Bei den vom Kläger mit dem Klageantrag zu Ziff. 1 beanstandeten Aussagen handelt es sich auch um gemäß § 3 Abs. 1 UWG unzulässige – weil nach § 5 Abs. 1, Abs. 2 Hs. 2 Nr. 3 UWG unlautere – geschäftliche Handlungen.

Rn. 62 Gem. 5 Abs. 1 UWG handelt unlauter, wer eine irreführende geschäftliche Handlung vornimmt, die geeignet ist, den Verbraucher oder sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung zu veranlassen, die er andernfalls nicht getroffen hätte. Gemäß § 5 Abs. 2 Hs. 2 Nr. 3 UWG ist eine geschäftliche Handlung unter anderem dann irreführend, wenn sie zur Täuschung geeignete Angaben über die Person oder Eigenschaften des Unternehmers wie dessen Befähigung, Status, Zulassung oder Auszeichnungen enthält.

Rn. 63 aa.

Rn. 64 Die vom Kläger beanstandeten Antworten des Chatbots stellen geschäftliche Handlungen der Beklagten dar.

Rn. 65 Nach der in § 2 Abs. 1 Nr. 2 UWG enthaltenen Legaldefinition ist eine geschäftliche Handlung jedes Verhalten einer Person zugunsten des eigenen oder eines fremden Unternehmens vor, bei oder nach einem Geschäftsabschluss, das mit der Förderung des Absatzes oder des Bezugs von Waren oder Dienstleistungen oder mit dem Abschluss oder der Durchführung eines Vertrags über Waren oder Dienstleistungen unmittelbar und objektiv zusammenhängt.

Rn. 66 (1)

Rn. 67 Zunächst einmal stehen die vom Kläger beanstandeten Angaben des auf der Webseite der Beklagten implementierten Chatbots in dem von § 2 Abs. 1 Nr. 2 UWG vorausgesetzten zeitlichen und sachlichen Zusammenhang mit dem Abs. der von der Beklagten angebotenen Dienstleistungen sowie dem Abschluss oder der Durchführung von Verträgen hierüber und wirken so zugunsten des von der Beklagten betriebenen Unternehmens.

Rn. 68 (2)

Rn. 69 Darüber hinaus stellen die Angaben des Chatbots auch jeweils ein "Verhalten" der Beklagten im Sinne von § 2 Abs. 1 Nr. 2 UWG dar.

Rn. 70 Der Begriff des Verhaltens ist weit zu fassen und erstreckt sich auf alle menschlichen Verhaltensweisen, auf positives Tun und Unterlassen, auf Äußerungen und rein tatsächliche Handlungen. Darüber hinaus wird hiervon auch der Einsatz von technischen Mitteln erfasst. So kann eine geschäftliche Handlung nach der Rechtsprechung des Bundesgerichtshof auch – etwa mit Hilfe eines von der Person entwickelten oder genutzten Computerprogramms – technisch gestützt oder automatisiert vorgenommen werden. Unerheblich ist in diesem Zusammenhang, dass die vom Nutzer des angebotenen technischen Service abgefragten Informationen nicht von dem in Anspruch genommenen Verwender persönlich, sondern von der bereitgestellten Software generiert werden. So hat der Bundesgerichtshof bereits entschieden, dass es sich bei der rein softwarebasierten Erstellung eines Vertragsdokuments um eine geschäftliche Handlung der dahinterstehenden (juristischen) Person im Sinne des § 2 Abs. 1 RDG handelt (vgl. BGH, Urt. v. 9.9.2021 – I ZR 113/20 – Vertragsdokumentengenerator, NJW 2021, 3125 Rn. 23-26, beck-online m.w.N.).

Rn. 71 Für die Antworten des von der Beklagten eingesetzten Chatbots kann im Ergebnis nichts Anderes gelten. Unstreitig war die Beklagte für den Betrieb des Chatbots auf ihrer Webseite verantwortlich und hatte dabei auch entscheidenden Einfluss darauf, wie dieser mit den angesprochenen Verkehrskreisen kommuniziert, was letztlich dadurch belegt wird, dass die Beklagte nach dem in Rede stehenden Vorfall problemlos in der Lage war, den Chatbot so umprogrammieren zu lassen, dass er keine unzutreffenden Antworten über eine vermeintlich bestehende Facharztqualifikation ihrer Geschäftsführer mehr auswarf. Die (vom Kläger mit Nichtwissen bestrittene) Behauptung der Beklagten, der Chatbot arbeite als KI-System in dem ihm gesetzten Tätigkeitsrahmen weitgehend autonom und werde nicht im Einzelnen gesteuert oder kontrolliert, kann zu keinem anderen Ergebnis führen. Zwar mag daraus – die Behauptung als nachgewiesen unterstellt – folgen, dass die Beklagte nicht in die Beant-

wortung der einzelnen Fragen durch den Chatbot eingebunden war und diese nicht kontrollierte. Allerdings bleibt auch danach unstreitig, dass die Beklagte dem Chatbot für die Beantwortung von Nutzeranfragen gezielte Vorgaben machen konnte (und auch machte), indem sie dessen "Tätigkeitsrahmen" entsprechend festlegt, was – wie soeben bereits ausgeführt – dadurch belegt wird, dass es ihr durch die Implementierung einer Prompt-Anweisung zur neutralen Antwort bei Fragen mit dem Begriff „Facharzt" sowie eines nachgelagerten Keyword-Filters zur automatischen Unterdrückung des unerwünschten Begriffs „Facharzt" gelungen ist, unzutreffende Ausgaben des Chatbots betreffend die tatsächlich nicht vorhandene Facharztqualifikation ihrer Geschäftsführer zu unterbinden. In Anbetracht dessen stellt der Chatbot (lediglich) ein technisches Mittel dar, dessen sich die Beklagte zur Kommunikation mit potenziellen Kunden/Patienten bediente und über das sie hinreichende Steuerungsgewalt besaß.

Rn. 72 Dem steht nach Auffassung des Senats auch nicht entgegen, dass der Chatbot die an ihn gerichteten Fragen gänzlich ohne menschliches Zutun und auf eine von außen nicht nachvollziehbare Weise beantwortet (sog. „Black-Box-Problem"). Zwar lässt sich deshalb die Beantwortung der einzelnen an ihn gerichteten Fragen nicht auf eine menschliche Willensentschließung im Einzelfall zurückführen. Gleichwohl unterscheidet sich der Chatbot insoweit in rechtlicher Hinsicht nicht wesentlich von dem Vertragsdokumentengenerator, über den der Bundesgerichtshof in der vorzitierten Entscheidung zu befinden hatte. Denn auch dieser generierte die betreffenden Vertragsdokumente anhand der Eingaben des Nutzers eigenständig, das heißt ohne jegliches menschliche Zutun und einen menschlichen Willensentschluss im Einzelfall. Und ebenso wie der Einsatz des Vertragsdokumentengenerators in dem vom Bundesgerichtshof entschiedenen Fall, war und ist der grundsätzliche Einsatz des Chatbots auf der Webseite der Beklagten in seiner konkreten Ausgestaltung von der Willensentschließung der Beklagten und des in ihrem Auftrag tätigen IT-Dienstleisters (§ 8 Abs. 2 UWG) getragen.

Rn. 73 Dabei verkennt der Senat nicht, dass der Vertragsdokumentengenerator bei der Bearbeitung der an ihn gerichteten Nutzeranfragen – evtl. anders als der Chatbot im Streitfall – auf zuvor durch Menschenhand erstellte und in einer Datenbank hinterlegte Textbausteine zurückgriff, die er entsprechend den Kundenbedürfnissen zu einem Vertragstext zusammenfügte, der evtl. noch durch weitere Kundeneingaben ergänzt wurde. Jedoch ändert dies nichts daran, dass der konkrete Abfragevorgang von der Software – ebenso wie bei dem von der Beklagten eingesetzten Chatbot – gänzlich autonom bearbeitet und beantwortet wurde. Hinzu kommt, dass auch der von der Beklagten eingesetzte Chatbot, bei dem es sich letztlich (nur) um ein im Wesentlichen auf Wahrscheinlichkeitsberechnungen basierenden Algorithmus handelt, zur „Beantwortung" der an ihn herangetragenen Kundenfragen insbesondere auf dasjenige Datenmaterial zurückgriff, das ihm hierfür zur Verfügung gestellt wurde.

Rn. 74 Nach alldem handelt es sich nach zutreffender Auffassung, der der Senat folgt, auch bei dem Einsatz von Künstlicher Intelligenz (KI), wie etwa bei „Erklärungen" eines lernfähigen Algorithmus und dem Verhalten von Chatbots und Socialbots, um geschäftliche Handlungen seines Betreibers, weil dieser hinreichenden Einfluss auf das System hat und es in Gang setzt. Diese Auslegung entspricht auch den Vorgaben des Art. 2 lit. d) UGP-RL, die unter Geschäftspraktiken „jede Handlung, Unterlassung, Verhaltensweise oder Erklärung, kommerzielle Mitteilung einschließlich Werbung und Marketing" erfasst (vgl. Köhler/Feddersen/Köhler, 44. Aufl. 2026, UWG § 2 Rn. 2.13, beck-online; BeckOK UWG/Alexander, 31. Ed. 1.2.2026, UWG § 2 Rn. 71, beck-online; Dornis: Lauterkeitsrecht im KI-Zeitalter – Grundlagen, Strukturen und Fallgruppen (Teil 1), GRUR 2023, 1729 [1733], beck-online).

[...]

Rn. 76 Soweit die Beklagte in diesem Zusammenhang Ausführungen zur sog. wettbewerbsrechtlichen Verkehrspflicht (Sorgfaltspflicht) macht und im Rahmen dessen insbesondere unter Verweis auf höchstrichterliche Rechtsprechung geltend macht, deren Verletzung setze zunächst das Bestehen von Prüf-, Überwachungs- und Verhinderungspflichten auf Seiten des vermeintlichen Verletzters voraus, die vorliegend schon nicht bestünden, weil die unzutreffenden Angaben des Chatbots für sie nicht voraussehbar gewesen seien, verfängt dies nicht.

Rn. 77 Die Beklagte verkennt dabei, dass die wettbewerbsrechtliche Verkehrspflicht bzw. unternehmerische Sorgfaltspflicht nur dann greift, wenn der Verletzer durch sein Handeln im geschäftlichen Verkehr die ernsthafte Gefahr begründet, dass Dritte durch das Wettbewerbsrecht geschützte Interessen von Marktteilnehmern verletzen. Demnach muss in diesen Fällen die Erstbegehungs- oder Wiederholungsgefahr eines Wettbewerbsverstoßes in der Person des Dritten bestehen. Hiervon erfasst ist insbesondere das Betreiben einer Einrichtung (etwa eines Online-Marktplatzes), die von Dritten gegen Entgelt dazu benutzt werden kann, Waren oder Dienstleistungen an Verbraucher abzusetzen. In solchen Fällen ist der Verletzer auf Grund einer wettbewerbsrechtlichen Verkehrspflicht dazu verpflichtet, diese Gefahr im Rahmen des Möglichen und Zumutbaren zu begrenzen (vgl. Köhler/Feddersen/Köhler/Feddersen, 44. Aufl. 2026, UWG § 8 Rn. 2.6, 2.10, beck-online unter Verweis auf BGH GRUR 2007, 890 Rn. 38 – Jugendgefährdende Medien bei eBay; GRUR 2018, 203 Rn. 37 – Betriebspsychologe).

Rn. 78 Damit umfasst die wettbewerbsrechtliche Verkehrspflicht nur Sachverhalte, die von dem zur Entscheidung vorliegenden Sachverhalt maßgeblich abweichen. Denn im Streitfall steht nicht die (täterschaftliche) Haftung aufgrund eigener Sorgfaltspflichtverletzung der Beklagten für einen von dritter Seite begangenen Wettbewerbsverstoß in Rede – insbesondere handelt es sich bei dem von der Beklagten eingesetzten KI-Chatbot nicht um einen Dritten in diesem Sinne -, sondern die Haftung der Beklagten für den von ihr selbst begangenen Wettbewerbsverstoß.

[...]

Rn. 80 Schließlich bleibt auch der Verweis der Beklagten auf die sog. Autocomplete-Entscheidung des Bundesgerichtshofs (BGH, Urt. v. 14.5.2013 – VI ZR 269/12 – Autocomplete-Funktion, BGHZ 197, 213-224) ohne Erfolg.

Rn. 81 Insoweit verkennt die Beklagte, dass sich der Bundesgerichtshof in jener Entscheidung (lediglich) damit auseinandergesetzt hat, unter welchen Voraussetzungen der Betreiber einer Internet-Suchmaschine als Störer für persönlichkeitsrechtsverletzende Suchergänzungsvorschläge

haftet. Eine derartige Störerhaftung kommt jedoch nach der inzwischen gefestigten Rechtsprechung des Bundesgerichtshofs im – auch hier einschlägigen – Bereich des Verhaltensunrechts nicht (mehr) in Betracht (vgl. etwa BGH, Urt. v. 12.7.2012 – I ZR 54/11 – Solarinitiative, GRUR 2013, 301 Rn. 49, beck-online m.w.N.; Urt. v. 22.7.2010 – I ZR 139/08 -Kinderhochstühle im Internet, GRUR 2011, 152 Rn. 48, beck-online m.w.N.; Köhler/Feddersen/Köhler/Feddersen, 44. Aufl. 2026, UWG § 8 Rn. 2.2c, beck-online m.w.N.; Fezer/Büscher/Obergfell/Büscher, 3. Aufl. 2016, UWG § 8 Rn. 130, beck-online m.w.N.).

[…]

Rn. 83 Doch selbst, wenn man – der unzutreffenden Ansicht der Beklagten folgend – von einer Anwendbarkeit der zur wettbewerbsrechtlichen Verkehrspflicht und/oder zur Störerhaftung entwickelten Grundsätze ausgehen wollte, würde dies zu keinem anderen Ergebnis in der Sache führen. Denn auch danach hätte die Beklagte jeweils für die unzutreffenden Antworten des Chatbots einzustehen.

Rn. 84 (a)

Rn. 85 Die wettbewerbsrechtliche Verkehrspflicht (Sorgfaltspflicht) ist ihrem Inhalt nach darauf gerichtet, den wettbewerbswidrigen Erfolg, also die Zuwiderhandlung eines Dritten , abzuwenden. Was im Einzelnen geschuldet ist, hängt von den Umständen des Einzelfalls ab. Es kann sich insbesondere um Prüfungs-, Überwachungs- und Eingreifpflichten handeln. Dabei sind nur solche Gefahrabwendungsmaßnahmen geschuldet, deren Erfüllung dem Handelnden möglich und zumutbar ist. Die Zumutbarkeit hängt wiederum einerseits davon ab, wie groß die vom Dritten ausgehende Verletzungsgefahr und wie gewichtig das verletzte Interesse ist, andererseits davon, welches wirtschaftliche Eigeninteresse der Verpflichtete hat und welcher Aufwand für die Gefahrenabwehr erforderlich ist (vgl. statt vieler Köhler/Feddersen/Köhler/Feddersen, 44. Aufl. 2026, UWG § 8 Rn. 2.10, beck-online unter Verweis auf BGH WRP 2014, 1050 Rn. 21 – Geschäftsführerhaftung; GRUR 2016, 209 Rn. 23 – Haftung für Hyperlink; GRUR 2021, 1534 Rn. 68 f. – Rundfunkhaftung I; GRUR 2011, 152 Rn. 36 – Kinderhochstühle im Internet I; GRUR 2010, 633 Rn. 13 – Sommer unseres Lebens).

Rn. 86 (b)

Rn. 87 Als Störer im Sinne von § 1004 BGB ist hingegen – ohne Rücksicht darauf, ob ihn ein Verschulden trifft – jeder anzusehen, der die Störung herbeigeführt hat oder dessen Verhalten eine Beeinträchtigung befürchten lässt. Sind bei einer Beeinträchtigung mehrere Personen beteiligt, so kommt es für die Frage, ob ein Unterlassungsanspruch gegeben ist, grundsätzlich nicht auf Art und Umfang des Tatbeitrags oder auf das Interesse des einzelnen Beteiligten an der Verwirklichung der Störung an. Im Allgemeinen ist ohne Belang, ob er sonst nach der Art seines Tatbeitrags als Täter oder Gehilfe anzusehen wäre. Als (Mit-)Störer kann auch jeder haften, der in irgendeiner Weise willentlich und adäquat kausal an der Herbeiführung der rechtswidrigen Beeinträchtigung mitgewirkt hat, sofern der in Anspruch Genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte. Dem negatorischen Unterlassungsbegehren steht nicht entgegen, dass dem in Anspruch Genommenen die Kenntnis der die Tatbestandsmäßigkeit und die Rechtswidrigkeit begründenden Umstände fehlt. Ebenso ist Verschulden nicht erforderlich (vgl. BGH, Urt. v. 14.5.2013 – VI ZR 269/12 – Autocomplete-Funktion, BGHZ 197, 213-224, Rn. 24 m.w.N.).

Rn. 88 Auch die Verantwortlichkeit des (unterlassenden) Störers wird – ebenso wie diejenige des sorgfaltswidrig Handelnden Täters (s.o.) – durch die Kriterien der Möglichkeit und Zumutbarkeit der Erfolgsverhinderung begrenzt. Dabei kann sich die Möglichkeit der Beseitigung einer Beeinträchtigung daraus ergeben, dass der Betroffene die Quelle der Störung beherrscht oder Einfluss auf jemanden nehmen kann, der zur Beendigung der Beeinträchtigung in der Lage ist. Ist dies der Fall, kann für die Zumutbarkeit der Beseitigung der Beeinträchtigung eine dem Betroffenen obliegende Überwachungspflicht von Bedeutung sein. Voraussetzung einer Haftung des Betreibers einer entsprechenden Software ist daher eine Verletzung von Prüfungspflichten. Deren Bestehen wie deren Umfang richtet sich im Einzelfall nach einer Abwägung aller betroffenen Interessen und relevanten rechtlichen Wertungen. Überspannte Anforderungen dürfen im Hinblick darauf, dass es sich um eine erlaubte Teilnahme am geschäftlichen Verkehr handelt, nicht gestellt werden. Daher kommt es entscheidend darauf an, ob und inwieweit dem in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist (vgl. BGH, a.a.O., Rn. 27 – 29, juris m.w.N.).

Rn. 89 (c)

Rn. 90 Nach diesen Maßgaben wäre die Beklagte sowohl im Rahmen der wettbewerbsrechtlichen Verkehrspflicht, als auch nach den zur Störerhaftung entwickelten Grundsätzen gehalten gewesen, die vom Kläger beanstandeten Angaben des von ihr eingesetzten Chatbots zu unterbinden.

Rn. 91 Zunächst einmal war und ist die Tätigkeit der Beklagten in Bezug auf den Einsatz des Chatbots nicht nur rein technischer, automatischer und passiver Art. Vielmehr verarbeitet die Beklagte die Abfragedaten der Nutzer in einem eigenen Programm – dem Chatbot –, das (vermeintlich) passende Antworten generiert. Für deren Ausgabe in Form eigener Antworten auf Nutzerfragen ist die Beklagte grundsätzlich aufgrund der ihr zuzurechnenden Erarbeitung verantwortlich. Der Beklagten könnte deshalb grundsätzlich vorgeworfen werden, keine hinreichenden Vorkehrungen getroffen zu haben, um zu verhindern, dass die von dem Chatbot generierten Antworten keine Wettbewerbsverletzungen beinhalten (vgl. BGH, a.a.O., Rn. 26, juris).

Rn. 92 Zudem war es der Beklagten – entgegen ihrer Ansicht – auch zumutbar, bereits vor der ersten Inbetriebnahme des Chatbots sicherzustellen, dass dieser keine unzutreffenden Auskünfte zu der Facharztqualifikation der bei ihr tätigen Ärzte, insbesondere ihrer Geschäftsführer, gibt.

Rn. 93 Zunächst einmal liegt es auf der Hand, dass ein wesentlicher Teil der von der Beklagten angesprochenen Verbraucher – das sind diejenigen Personen, die sich ernsthaft für schönheitsoperative Eingriffe im weitesten Sinn interessieren – ein gesteigertes Interesse daran haben, zu erfahren, ob und ggf. welche der bei der Beklagten tätigen Mediziner über einen Facharzttitel auf ihrem Tätigkeitsgebiet verfügen. Dies nicht zuletzt auch deshalb, weil – dies ist allgemein bekannt – missglückte und handwerklich unzureichend ausgeführte Schönheitseingriffe seit vielen Jahren eine breite mediale Berichterstattung erfahren und für die Betroffenen weitreichende Folgen haben. Vor diesem Hintergrund haben diejenigen Personen, die sich ernsthaft mit der Vornahme entsprechender Eingriffe auseinandersetzen, bei der Wahl des Behandlers ein besonders großes Interesse daran, dessen fachliche Qualifikation zuverlässig einschätzen zu kön-

nen, wozu nach dem allgemeinen Verkehrsverständnis insbesondere auch darauf abgestellt werden kann, ob der Arzt der Wahl über einen entsprechenden Facharzttitel verfügt. Dass dies grundsätzlich auch der Beklagten bewusst ist, belegt der Umstand, dass sie hinsichtlich der bei ihr tätigen und entsprechend ausgebildeten Ärzte auf ihrer Webseite mit der vorhandenen Facharztqualifikation wirbt. Soweit die Beklagte dies im Rahmen ihrer Klageerwiderung vom 29.7.2025 noch in Abrede gestellt hatte, hat sie diesen Umstand mit ihrer Duplik vom 4.5.2026 inzwischen eingeräumt.

Rn. 94 Hinzu kommt, dass im Bereich des Gesundheitsschutzes und des Gesundheitswesens aufgrund der weitreichenden Folgen für die angesprochenen Verkehrskreise grundsätzlich besonders strenge Anforderungen an das Marktverhalten der handelnden Akteure zu stellen sind. Folglich hätte die Beklagte bei gehöriger Anstrengung – d.h. als umsichtiger und gewissenhafter Marktakteur – antizipieren können und müssen , dass sich potenzielle Kunden/Patienten mit der Frage nach der Facharztqualifikation der bei ihr tätigen Behandler an den von ihr bereitgestellten Chatbot wenden.

Rn. 95 Nach alledem musste für die Beklagte bzw. ihren bei der Programmierung und Inbetriebsetzung des Chatbots zum Einsatz kommenden Beauftragten, für den die Beklagte gemäß § 8 Abs. 2 UWG einzustehen hat, bei gewissenhaftem und umsichtigem Vorgehen auf der Hand liegen, dass der Chatbot auf die naheliegende Frage nach der (tatsächlich nicht vorhandenen) Facharztqualifikation ihrer medial bekannten Geschäftsführer unzutreffende Antworten halluzinieren könnte, was er letztlich auch tat.

Rn. 96 Da es ihr zudem ein Leichtes gewesen ist – dies belegt der Geschehensablauf nach der Kenntniserlangung von der Verletzung –, den Chatbot derart umzuprogrammieren, dass dieser keine unzutreffenden Antworten über die Facharztqualifikation der bei ihr tätigen Behandler mehr ausgibt, war es ihr im Ergebnis auch zumutbar, dies bereits vor der ersten Inbetriebnahme sicherzustellen.

Rn. 97 Dabei muss sich der Senat nicht mit der Frage befassen, ob etwas anderes für solche fehlerhaften „Antworten" eines KI-Sprachmodells oder KI-Chatbots gilt, die durch eine tendenziöse Fragestellung des Nutzers provoziert werden. Denn im Streitfall waren die an den Chatbot gerichteten Fragestellungen weder tendenziös, noch suggestiv.

[…]

Rn. 99 Die danach in Rede stehenden geschäftlichen Handlungen der Beklagten sind auch irreführend, weil sie zur Täuschung geeignete Angaben über die fachliche Befähigung ihrer Geschäftsführer enthalten.

Rn. 100 Eine Irreführung liegt vor, wenn das Verständnis, das eine Angabe bei den Verkehrskreisen erweckt, an die sie sich richtet, mit den tatsächlichen Verhältnissen nicht übereinstimmt (vgl. BGH, Urt. v. 29.7.2021 – I ZR 114/20 – Kieferorthopädie, NJW-RR 2021, 1491 Rn. 12, beck-online m.w.N.). Dabei ist im Ausgangspunkt auf die Sicht eines durchschnittlich informierten, aufmerksamen und verständigen Verbrauchers in seiner Rolle als (potenzieller) Patient einer Arztpraxis für minimalinvasive Schönheitsbehandlungen abzustellen, wobei der Senat aufgrund eigener Sachkunde beurteilen kann, wie die Verbraucher die vom Kläger angegriffenen Angaben verstehen, weil seine Mitglieder selbst zu den angesprochenen Verkehrskreisen gehören (st. Rspr, vgl. nur BGH a.a.O., Rn. 18, beck-online m.w.N.).

Rn. 101 Wie der Bundesgerichtshof bereits entschieden hat, sind dem Durchschnittsverbraucher Facharztbezeichnungen nicht fremd. Zwar macht er sich in der Regel keine vertieften Gedanken zur Dauer und zum Inhalt einer Facharztausbildung. Jedoch stellt er sich unter einem Facharzt entsprechend der geltenden Rechtslage einen Arzt vor, der eine von der zuständigen Berufsaufsicht anerkannte Weiterbildung in dem betreffenden Fachgebiet mit bestandener Prüfung absolviert hat (vgl. BGH a.a.O., Rn. 28, beck-online; so auch Senatsurt. v. 24.7.2008 – 4 U 82/08 – Männerarzt, GRUR-RR 2008, 434, beck-online; OLG Oldenburg, Urt. v. 30.4.2021 – 6 U 263/20, Rn. 49, juris).

Rn. 102 Demgemäß hegt der angesprochene Durchschnittsverbraucher bei den in Rede stehenden Bezeichnungen (Facharzt für plastische und ästhetische Chirurgie, Facharzt für ästhetische Medizin und Facharzt für ästhetische Behandlungen) die fehlerhafte Erwartung, dass die Geschäftsführer der Beklagten erfolgreich eine Weiterbildung zum Facharzt für plastische und ästhetische Chirurgie bzw. zum Facharzt für plastische, rekonstruktive und ästhetische Chirurgie absolviert haben.

Rn. 103 cc.

Rn. 104 Dass die so hervorgerufene Fehlvorstellung über die fachliche Qualifikation der bei der Beklagten tätigen Ärzte, bei denen es sich zugleich auch noch um ihre Geschäftsführer und ihre medialen „Aushängeschilder" handelt, die von § 5 UWG geforderte geschäftliche Relevanz besitzt, steht außer Frage.

Rn. 105 Die Beklagte geht fehl in der Annahme, an der geschäftlichen Relevanz fehle es deshalb, weil der angesprochene Verbraucher um die Fehleranfälligkeiten von KI-Chatbots und deren „Antworten" wisse und sich deshalb bewusst sei, dass die von diesem ausgegebenen Informationen stets eines Faktenchecks bedürfen, um als belastbar angesehen zu werden. Dahingehende Erfahrungssätze zeigt die Beklagte nicht auf und existieren auch nicht. Vielmehr trifft es zu, dass ein Großteil der angesprochenen Verbraucher in besonderer Weise auf die Richtigkeit der computergenerierten Antwort vertraut, da Maschinen im Allgemeinen als weniger fehleranfällig als der Mensch wahrgenommen werden. Andernfalls – d.h. bei einem grds. bestehenden Misstrauen der potenziellen Kunden gegenüber der durch die KI-Anwendung generierten Antworten – hätte sich die Beklagte sicherlich auch nicht dazu entschieden, auf ihrer Webseite einen KI-Chatbot zur Kommunikation mit den Kunden zu implementieren.

[…]

Rn. 107 Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr wird durch die jeweilige Verletzungshandlung indiziert. Anhaltspunkte dafür, dass diese entfallen sein könnte, sind weder vorgebracht noch anderweitig ersichtlich. Insbesondere hat die Beklagte keine strafbewehrte Unterlassungserklärung abgegeben, die hierfür in der Regel erforderlich ist.

[…]

Rn. 119 Der Senat lässt die Revision gemäß § 6 Abs. 2 UKlaG i.V.m. § 543 Abs. 1 Nr. 1, Abs. 2 S. 1 Nr. 1 ZPO wegen grundsätzlicher Bedeutung zu.

Die Datenkopie muss nicht maschinenlesbar sein

(OLG Brandenburg, Beschluss vom 15. April 2026 – 3 U 31/25 –)

1. **Art. 15 Abs. 3 S. 3 DS-GVO verlangt ein gängiges elektronisches Format. Das ist nicht das strukturierte, gängige und maschinenlesbare Format des Art. 20 Abs. 1 DS-GVO. Bei der Auskunft stehen Menschenlesbarkeit und leichter Zugang im Vordergrund.**
2. **Ein Anspruch auf Erleichterungen bei der Durchsetzung datenschutzfremder Zwecke folgt aus der DS-GVO nicht.**

(Nicht amtliche Leitsätze)

Aus den Gründen (Rn. sind redaktionell gesetzt):

Rn. 4 1. Die erhobene Stufenklage ist unzulässig.

Rn. 5 Entgegen der Ansicht des Klägers ist die vom Senat zitierte Entscheidung des OLG Köln vom 26.7.2019 – 20 U 75/18 – nicht durch die später ergangene Rechtsprechung des Europäischen Gerichtshofs überholt. Soweit der Kläger insoweit auf das Urteil des EuGH vom 26.10.2023 – C-307/22 – Bezug nimmt, ergibt sich daraus nur, dass die betroffene Person ihren Antrag auf Auskunft nicht begründen muss, weil der Auskunftsanspruch nicht vom Verwendungszweck der begehrten Daten abhängt. Dass die betroffene Person mit der Verfolgung ihres Auskunftsanspruchs unter Umständen einen dem Datenschutzrecht fremden Zweck verfolgt, steht der Verpflichtung zur Auskunft nach Art. 15 DS-GVO zwar nicht entgegen (EuGH, a.a.O., Rn. 38, 51 f.; BGH, Urt. v. 5.3.2024, VI ZR 330/21, Rn. 20). Daraus lässt sich aber nicht der Schluss ziehen, dass der allgemeine Auskunftsanspruch nach Art. 15 DS-GVO in der ersten Stufe mit einem unbezifferten Zahlungsantrag in zweiter Stufe mittels einer Stufenklage verbunden werden kann. Die Zulässigkeit der Stufenklage richtet sich nach § 254 ZPO und nicht nach Art. 15 DS-GVO, der allein die materiellrechtlichen Voraussetzungen des Auskunftsanspruchs definiert.

Rn. 6 Da der Auskunftsanspruch nach Art. 15 DS-GVO nicht der Bestimmbarkeit von Bereicherungsansprüchen aus rechtswidrigen Glücksspielverträgen dient, kann er nicht mittels einer Stufenklage mit einem unbezifferten Leistungsantrag verknüpft werden (OLG Frankfurt, Beschluss vom 22.9.2025 – 6 U 323/24, BeckRS 2025, 37555 Rn. 15).

Rn. 7 Aus der im klägerischen Schriftsatz vom 29.1.2026 zitierten Entscheidung des OLG Düsseldorf ergibt sich nichts anderes. Zwar hat das OLG Düsseldorf in einem vergleichbaren Fall die Stufenklage für zulässig gehalten (Beschl. v. 2.12.2024 – I-16 W 93/23, Rn. 27, juris). Das OLG Düsseldorf begründet die Zulässigkeit der Stufenklage aber allein damit, dass für deren erste Stufe über den Wortlaut des § 254 ZPO hinaus jegliche Auskunftsbegehren in Betracht kämen. Nicht geprüft hat das OLG Düsseldorf hingegen, ob der erforderliche Zusammenhang zwischen dem Auskunfts- und Leistungsbegehren gegeben ist. Aus der einzigen, von dem OLG Düsseldorf im Zusammenhang mit der Zulässigkeit der Stufenklage nach § 254 ZPO zitierten Fundstelle ergibt sich nämlich, dass bei einer Klage auf Erteilung einer Datenauskunft gemäß Art. 15 DS-GVO es in der Regel an dem erforderlichen Zusammenhang fehlt (BeckOK/Bacher, ZPO, 60. Ed., Stand: 1.3.2026, § 254 Rn. 4.5).

Rn. 8 Selbst wenn man es für die Zulässigkeit der Stufenklage genügen lässt, wenn das Auskunftsbegehren nach Art. 15 DS-GVO nicht nur auf die zur Bezifferung des Leistungsanspruchs erforderlichen Auskünfte, sondern zusätzlich auf weitere Informationen gerichtet ist, solange die begehrte Information zumindest auch der Bestimmung der beanspruchten Leistung dienen soll (so das OLG Saarbrücken, NJW-RR 2024, 241 Rn. 15), ist die Stufenklage hier nicht zulässig. Denn die Stufenklage steht auch nicht zur Verfügung, wenn der Kläger zur genauen Bestimmung seines Hauptanspruches der Auskunft nicht bedarf. Auch dann steht die erstrebte Auskunft nicht mit der (gegebenen) Bestimmbarkeit des Hauptanspruches im Zusammenhang (Stein/Roth, ZPO, 24. Aufl., § 254 Rn. 2). So liegt der Fall hier. Denn der Kläger verfügt bereits über sämtliche Informationen, die er zur Bezifferung seines Anspruchs benötigt. Er kann sowohl anhand seiner eigenen Bankunterlagen (vgl. insoweit OLG Brandenburg, Urt. v. 26.6.2025 – 12 U 122/24) als auch der ihm bereits vorprozessual erteilten Auskunft seine Spieleinsätze nachvollziehen.

Rn. 9 2. Der gleichwohl im Wege der objektiven Klagehäufung zulässige Auskunftsantrag ist unbegründet. Der ursprünglich nach Art. 15 DS-GVO bestehende Auskunftsanspruch des Klägers ist bereits vorgerichtlich durch Erfüllung gemäß § 362 BGB erloschen. Insoweit wird auf die ausführliche Begründung des Hinweisbeschlusses Bezug genommen.

Rn. 10 Weder hat der Kläger Anspruch auf eine Zurverfügungstellung der unveränderten Rohdaten (weshalb auch nicht von einer „technischen Manipulation" die Rede sein kann), noch muss die Datenkopie maschinenlesbar sein. Der Senat hat in seinem vorangegangenen Hinweisbeschluss bereits Fundstellen aus der datenschutzrechtlichen Kommentierung genannt, wonach kein Anspruch des Betroffenen auf eine Maschinenlesbarkeit der Datenkopie nach Art. 15 DS-GVO besteht.

Rn. 11 Das steht auch mit der obergerichtlichen Rechtsprechung in Einklang. Umfang und Inhalt des Auskunftsanspruchs aus Art. 15 Abs. 1 lit. h) DS-GVO werden maßgeblich durch das Transparenzgebot gem. Art. 12 Abs. 1 DS-GVO sowie seine teleologische Auslegung im Lichte der Betroffenenrechte nach Art. 22 Abs. 3 DS-GVO bestimmt. Zum einen verpflichtet Art. 12 Abs. 1 DS-GVO den Verantwortlichen, der betroffenen Person die relevanten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zur Verfügung zu stellen (EuGH, Urt. v. 27.2.2025, C-203/22, Rn. 49, CR 2025, 302 ff). Zum anderen soll das Auskunftsrecht der betroffenen Person ermöglichen, ihre datenschutzrechtlichen Ansprüche effektiv geltend machen zu können (OLG Dresden, Urt. v. 7.10.2025 – 4 U 884/24, juris Rz. 34). Sinn und Zweck des Auskunftsanspruchs ist es also, der betroffenen Person problemlos und in angemessenen Abständen zu ermöglichen, sich der Verarbeitung der sie betreffenden personenbezogenen Daten bewusst zu werden und die Rechtmäßigkeit dieser Verarbeitung überprüfen zu können. Zwar fördert die

Bereitstellung der Auskunft in einem maschinenlesbaren Dateiformat die effektive Wahrnehmung der Rechte aus Art. 15 Abs. 1 DS-GVO und steht im Einklang mit dem Transparenzgrundsatz aus Art. 12 Abs. 1 DS-GVO. Ein zwingender Anspruch auf Erteilung einer maschinenlesbaren Auskunft folgt hieraus allerdings nicht (OLG Dresden Urt. v. 18.11.2025 – 4 U 543/25, BeckRS 2025, 40398 Rn. 38).

Rn. 12 Ein solcher einklagbarer Anspruch auf Übermittlung in maschinenlesbarer Form folgt zunächst nicht aus Art. 12 DS-GVO, denn dort ist nur von „geeigneten" Maßnahmen die Rede, die dem eingangs skizzierten Zweck der Auskunftserteilung Genüge tun. Anders als bei Art. 20 DS-GVO stehen hier nicht die Maschinenlesbarkeit, sondern die Menschenlesbarkeit und der leichte Zugang im Vordergrund. Stellt die betroffene Person bereits den Antrag auf elektronischem Wege, ist gemäß Abs. 3 S. 3 DS-GVO ein gängiges elektronisches Format für die Auskunftserteilung zu verwenden, sofern nichts anderes angegeben wird. Dieses gängige elektronische Format ist aber nicht zu verwechseln mit dem strukturierten, gängigen und maschinenlesbaren Format des Art. 20 Abs. 1 DS-GVO. Letzterer findet direkte Anwendung nur beim Recht auf Bearbeitung und Löschung, also auf dem Gebiet der Datenbearbeitung, um die es bei der Auskunft (zunächst) nicht geht. Anders als beim Recht auf Datenübertragbarkeit (Art. 20 Abs. 1) muss daher die Kopie nach Art. 15 Abs. 3 S. 3 DS-GVO nicht maschinenlesbar sein (OLG Dresden, a. a. O., Rn. 39).

Rn. 13 Der vorrangige Zweck des Auskunftsanspruchs – nämlich dem Betroffenen die Rechtmäßigkeit der Verarbeitung seiner Daten und die effektive Kontrolle über diese zu ermöglichen – gebietet es nicht, in Anwendung der Grundsätze des Art. 20 DS-GVO die Datenauskunft in maschinenlesbarer Form zu erteilen. Entscheidend ist hierbei, dass die Auskunftserteilung nach der DS-GVO – anders als die Auskunftserteilung etwa nach bürgerlichem Recht – dem Zweck dient, dem Betroffenen die Ausübung seiner Persönlichkeitsrechte in der Form der Kontrolle über die über ihn erhobenen Daten zu ermöglichen. Sie hat nicht in erster Linie der Durchsetzung anderer, datenschutzfremder Rechte, wie Rückzahlungs- oder Schadensersatzansprüchen zu dienen. Allein hierfür wäre eine maschinenlesbare Form eine Erleichterung für den Kläger, denn dann könnte er beispielsweise seine Ausgaben und Wett- und Spielgewinne in Tabellenform zusammenfassen und automatisiert auswerten, ohne die erteilten Auskünfte händisch einzeln in eine maschinell auswertbare Tabelle zu übertragen. Einen Anspruch auf derartige Erleichterungen bei der Durchsetzung datenschutzfremder Zwecke gewährt die DS-GVO allerdings nicht (OLG Dresden, a.a.O., Rn. 40).

Rn. 14 Die von der Beklagten dem Kläger übersandte Datenkopie ist unstreitig für das menschliche Auge lesbar. Damit ist der Verständlichkeit und Transparenz Genüge getan. Nur ergänzend sei daran erinnert, dass die Beklagte dem Kläger mit Schriftsatz vom 2.2.2026 einen Weg aufgezeigt hat, wie er eine maschinelle Weiterverarbeitungsmöglichkeit der Datenkopie herstellen kann.

Rn. 15 Soweit der Kläger auf das Urteil des OLG Brandenburg vom 26.6.2025 – 12 U 122/24 – Bezug nimmt, trifft es zwar zu, dass die dortige Beklagte zur Auskunftserteilung nach Art. 15 DS-GVO durch Zurverfügungstellung einer maschinenlesbaren Excel-Datei verurteilt wurde. Ausweislich der Entscheidungsgründe hatte die dortige Beklagte aber keine Einwände gegen dieses Format. Die Parteien können sich auf ein bestimmtes Format einigen. Liegt eine solche Einigung nicht vor, kann der Verantwortliche nach dem Gesetzeswortlaut des Art. 15 DS-GVO die Datenkopie in einem gängigen elektronischen Format zur Verfügung stellen, was hier durch Übermittlung eines als gängig anerkannten PDF-Dokuments erfolgt ist.

Rn. 16 Welcher Sachverhalt dem Versäumnisurteil des OLG Frankfurt a.M. vom 29.8.2024 – 6 S 45/24 zugrunde lag, lässt sich den Entscheidungsgründen nicht entnehmen, so dass daraus keine über den dort entschiedenen Einzelfall hinausgehenden Schlüsse gezogen werden können.

Rn. 17 3. Der unbezifferte Zahlungsantrag ist mangels hinreichender Bestimmtheit unzulässig. Insofern kommt es weder auf die im Hinweisbeschluss erwähnte Entscheidung des BGH vom 22.3.2024 – I ZR 88/23 – noch auf die Verjährungseinrede an.

Rn. 18 4. Eine Vorlagepflicht des Senats besteht nicht, weshalb der Aussetzungsantrag des Klägers zurückgewiesen wird.

Rn. 19 Die Durchführung eines Vorabentscheidungsverfahrens nach Art. 267 AEUV zur Klärung einer der geprüften und festgestellten Gesichtspunkte ist nicht geboten. Die Auslegung der maßgeblichen unionsrechtlichen Begriffe ist durch die Rechtsprechung des Europäischen Gerichtshofs eindeutig geklärt.

Rn. 20 Nach der Rechtsprechung des Gerichtshofs der Europäischen Union muss ein nationales letztinstanzliches Gericht – wie hier der Senat – seiner Vorlagepflicht nachkommen, wenn sich in einem bei ihm schwebenden Verfahren eine Frage des Unionsrechts stellt, es sei denn, das Gericht hat festgestellt, dass die gestellte Frage nicht entscheidungserheblich ist, dass die betreffende unionsrechtliche Bestimmung bereits Gegenstand einer Auslegung durch den Gerichtshof war – acte éclairé – oder dass die richtige Anwendung des Unionsrechts derart offenkundig ist, dass für einen vernünftigen Zweifel keinerlei Raum bleibt – acte clair – (BVerfG, NJW 2021, 1005 Rn. 10).

Rn. 21 Die Auslegung des Art. 15 DS-GVO im Hinblick auf die von dem datenschutzrechtlich Verantwortlichen zur Verfügung zu stellenden Datenkopie ist durch die im vorangegangenen Hinweisbeschluss des Senats zitierte Entscheidung des EuGH vom 4.5.2023 – C-487/21 – hinreichend geklärt. Danach verlangt der Grundsatz der Transparenz, auf den im 58. ErwG der DS-GVO Bezug genommen wird und der in Art. 12 Abs. 1 DS-GVO ausdrücklich verankert ist, eine für die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abzufassen. Aus dieser Bestimmung ergibt sich, dass der Verantwortliche geeignete Maßnahmen zu treffen hat, um der betroffenen Person alle in Art. 15 DS-GVO genannten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, und dass die Übermittlung der Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch zu erfolgen hat, es sei denn, die betroffene Person verlangt, dass diese mündlich erteilt werden. Diese Bestimmung, die Ausdruck des

Transparenzgrundsatzes ist, soll gewährleisten, dass die betroffene Person in die Lage versetzt wird, die an sie gerichteten Informationen in vollem Umfang zu verstehen (EuGH, EuZW 2023, 575 Rn. 38). Nach der Rechtsprechung des EuGH ist mithin keine Zurverfügungstellung der Datenkopie in maschinenlesbarer Form erforderlich.

KI-Nachschärfung von Luftbildaufnahmen begründet keinen intensiveren Grundrechtseingriff (LS)

(OVG NRW, Beschluss vom 22. Juni 2026 – 16 B 169/25 –)

Die Möglichkeit, Luftbildaufnahmen eines Grundstücks mit Hilfe von Künstlicher Intelligenz zu verarbeiten, um bestehende Unschärfen nachträglich auszugleichen, führt nicht ohne Weiteres dazu, dass das Anfertigen solcher Luftbildaufnahmen und deren Verwendung im Rahmen der Festsetzung von Niederschlagswassergebühren einen Grundrechtseingriff mit mehr als geringer Eingriffsintensität darstellt.

(Amtlicher Leitsatz)

Angemessener Untersuchungsumfang einer Datenschutzbeschwerde durch die Aufsichtsbehörde (LS)

(VG Düsseldorf, Urteil vom 22. Juni 2026 – 29 K 3490/24 –)

1. **Welchen Umfang die Untersuchung einer Beschwerde nach Art. 57 Abs. 1 lit. f) DS-GVO haben muss, richtet sich insbesondere nach der individuellen Bedeutung der Sache und der Schwere des in Rede stehenden Verstoßes. Insoweit steht der Aufsichtsbehörde ein Ermessen zu, dessen Ausübung gerichtlich nur eingeschränkt überprüfbar ist.**
2. **Liegen keine konkreten Anhaltspunkte für eine weitere Aufklärungsbedürftigkeit des Sachverhalts vor, muss die Aufsichtsbehörde Ermittlungen ins Blaue hinein auch auf Antrag der Beschwerdeführer nicht einleiten.**

(Nicht amtliche Leitsätze)

Vervielfältigung geschützter Musikwerke beim Training und im Modell eines KI-Musikgenerators (LS)

(LG München I, Endurteil vom 31. Juli 2026 – 42 O 763/25 –)

1. **Werden geschützte Musikwerke beim Training eines generativen KI-Modells so in dessen Parametern festgelegt, dass das Modell sie auf einfache, ergebnisoffene Prompts hin wiedererkennbar wiedergibt (Memorisierung), liegt darin eine Vervielfältigung nach § 16 Abs. 1 UrhG, Art. 2 InfoSoc-RL.**
2. **Die Text-und-Data-Mining-Schranke (§ 44b UrhG, Art. 4 DSM-RL) deckt Vervielfältigungen zur Erstellung des Trainingskorpus, nicht die Vervielfältigung im Modell.**
3. **Wer sich Trainingsdaten unter Umgehung des Rolling Cipher verschafft, hat keinen rechtmäßigen Zugang im Sinne des § 44b Abs. 2 UrhG.**
4. **Art. 53 Abs. 1 lit. c) und d) KI-VO legt den Anwendungsbereich der DSM-RL nicht fest. Urheberrechts-Strategie und Trainingsdaten-Zusammenfassung ersetzen keine Lizenzierung.**
5. **§ 131 Abs. 2 VGG ist doppelfunktional anzuwenden und begründet die internationale Zuständigkeit auch für Verletzungshandlungen im Ausland.**
6. **Das Angebot des Musikgenerators ist unmittelbare öffentliche Wiedergabe der memorisierten Werke (§ 15 Abs. 2 S. 1 UrhG). Eine öffentliche Zugänglichmachung nach § 19a UrhG scheidet aus, wenn der Abruf nicht verlässlich zu Zeiten der Wahl möglich ist.**
7. **Das Training mit Werken, die als wesentlich ähnliche Outputs ausgegeben werden, ist nicht transformativ und nicht von fair use (17 U.S.C. § 107) gedeckt (Abgrenzung zu Bartz v. Anthropic und Kadrey v. Meta).**

(Nicht amtliche Leitsätze)

Exzessiver erster Auskunftsantrag nach Brillen Rottler (LS)

(AG Arnsberg, Urteil vom 1. Juli 2026 – 42 C 434/23 –)

1. **Auch ein erster Auskunftsantrag kann exzessiv im Sinne von Art. 12 Abs. 5 lit. b) DS-GVO sein. Der Nachweis der Missbrauchsabsicht folgt den Kriterien von EuGH C-526/24 aus einer Gesamtwürdigung aller Umstände, etwa der freiwilligen Datenpreisgabe, dem fehlenden Interesse am Dienst, der kurzen Zeitspanne zwischen Anmeldung und Antrag und öffentlich zugänglichen Berichten über das Vorgehen des Antragstellers.**
2. **Ein Anspruch aus Art. 82 Abs. 1 DS-GVO scheitert jedenfalls am unterbrochenen Kausalzusammenhang, wenn das eigene Verhalten des Antragstellers den behaupteten Kontrollverlust ausgelöst hat.**

(Nicht amtliche Leitsätze)

Schulungs-pflicht einfach erfüllen

Beschäftigte wirksam für Datenschutz sensibilisieren

Interaktive E-Learning-Kurse mit echter Moderation statt KI-Stimme

- ✓ Kurse für Beschäftigte und Führungskräfte, entwickelt von RA Thomas Müthlein (GDD-Vorstandsmitglied)
- ✓ Abschlussquiz und interaktive Lerneinheiten
- ✓ Barrierefrei nach BFSG
- ✓ Flexibel nutzbar in unserem Experten-LMS oder per SCORM/xAPI in Ihrer Lernplattform
- ✓ Im Experten LMS inklusive: Onboarding, Reporting, Zertifikate und Support

Jetzt kostenfrei testen: **www.datakontext.com/elearning**

UNIVADO

DATAKONTEXT

BERICHT AUS BRÜSSEL

Axel Voss/Lucia Burkhardt*

Anonymisierung, neu vermessen

Der EDSA hat am 7.7.2026 in seiner Juli-Plenarsitzung die Leitlinien 02/2026 zur Anonymisierung angenommen. Die Leitlinien stehen bis zum 30.10.2026 zur öffentlichen Konsultation bereit.[1] Sie lösen die Stellungnahme 05/2014 der Artikel-29-Datenschutzgruppe ab, also eine zwölf Jahre alte Stellungnahme und damit ein Papier, das älter ist als die DS-GVO selbst. Das Timing ist besonders deswegen interessant, weil seit November 2025 im Streit um den Digitalen Omnibus auch über die Neudefinition der personenbezogenen Daten gerungen wird. Das war Thema der vorausgehenden Ausgabe dieses Berichts.[2] Nun legt der EDSA seine Meinung zu dem Thema vor, und die enthält einige spannende Passagen.

Ein Maßstab von 2014 und vier Urteile

Der EDSA begründet die Neufassung mit der Entwicklung der Technik und des Rechts seit 2014.[3] Grundlage hierfür ist vor allem der Fortschritt im Bereich der Künstlichen Intelligenz und die umfangreiche EuGH-Rechtsprechung zum Personenbezug. Zentral sind vier Urteile, namentlich Breyer,[4] Scania,[5] OC[6] und zuletzt EDSB/SRB.[7] Die Kernfolgerung aus all diesen Urteilen ist der relative Personenbezug, der sich mittlerweile etabliert hat und der auch den neuen Leitlinien zugrunde liegt. Ausgangspunkt für die Bewertung des Personenbezugs und der Anonymisierung ist damit die Perspektive der jeweiligen Stelle.[8] Das heißt, bevor man den Personenbezug ermittelt, ist zu bestimmen, für wen er ermittelt wird.[9] Erst dann ist zu prüfen, welche Mittel von der betreffenden Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die betroffen Person zu identifizieren.

Viel Wind um die Auftragsverarbeiter

Ein zentraler Kritikpunkt aus der Praxis ist die Bestimmung der maßgeblichen Perspektive bei der Auftragsverarbeitung. Im Falle einer Auftragsverarbeitung, also einer weisungsabhängigen Datenverarbeitung für einen anderen, kommt es nach den Leitlinien nicht mehr auf die Perspektive des Dienstleisters an, sondern auf die des Auftraggebers. Es zählt allein, ob die Daten für den Auftraggeber personenbezogen sind. So gelesen ist es nicht mehr möglich, einen weisungsgebundenen Dienstleister aus der DS-GVO herauszuhalten, indem man die Daten anonymisiert, bevor man sie an ihn weitergibt. Sie bleiben für ihn personenbezogen, auch wenn er sie mit eigenen Mitteln niemandem zuordnen kann.[10] Der EDSA begründet das teleologisch. Er möchte verhindern, dass das Konzept der Auftragsverarbeitung zur Pflichtenflucht führt und die Pflichten der DS-GVO im Ergebnis über eine Auslagerung unterlaufen werden.[11]

Die Folge für die Praxis ist vor allem eines: Aufwand. Auch bei anonymisierten Daten muss mit dem Auftragsverarbeiter ein Vertrag nach Art. 28 DS-GVO geschlossen werden. Außerdem gelten die Sicherheits- und Meldepflichten, und bei Drittlandbezug unterliegen die Daten dem Kapitel V der DS-GVO.[12] Nicht zuletzt deswegen ist die Beurteilung der Auftragsverarbeitung des EDSA in der Praxis auf erhebliche Kritik gestoßen.

Eingewandt wird zudem, dass die relative Betrachtung so für die gesamte Auftragskette faktisch einkassiert werde. Die Behandlung der Auftragsverarbeitung war bereits bei der Stakeholder-Anhörung umstritten, und er dürfte auch in der Konsultation zu den größten Klärungsbedarfen gehören.

Über die rechtliche Tragweite ist allerdings auch dann noch nichts gesagt, wenn der EDSA bei seiner Linie bleibt. Der EDSA ist eine Einrichtung der Union mit eigener Rechtspersönlichkeit, in der die Leiter der nationalen Aufsichtsbehörden und der EDSB zusammenwirken[13] und die eine einheitliche Anwendung der DS-GVO sichern soll.[14] Verbindliches Recht setzen seine Leitlinien nicht. Zu erwarten ist zwar, dass die Behörden ihre Prüfpraxis daran ausrichten und sich auch die Gerichte daran orientieren, das letzte Wort hat aber der EuGH.

Auf welche Mittel kommt es an?

Steht fest, auf wessen Perspektive es ankommt, ist zu prüfen, ob die jeweilige Stelle die betroffene Person mit Mitteln identifizieren kann, die nach allgemeinem Ermessen wahrscheinlich genutzt werden (ErwG 26 DS-GVO). Diesen Maßstab hat der EuGH seit Breyer konkretisiert. Die Leitlinie legt ihn streng aus.

* Axel Voss ist Mitglied des Europäischen Parlaments für die EVP. Er ist Berichterstatter des hier besprochenen Initiativberichts. Lucia Burkhardt ist wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln.

1 EDSA, Guidelines 02/2026 on Anonymisation, Version 1.0, angenommen am 7.7.2026 zur öffentlichen Konsultation, https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf (zuletzt abgerufen am 4.8.2026).

2 Dazu die vorausgehende Ausgabe des Berichts aus Brüssel, RDV 2026.

3 EDSA, Guidelines 02/2026, Rn. 2.

4 EuGH, Urt. v. 19.10.2016 – C-582/14.

5 EuGH, Urt. v. 9.11.2023 – C-319/22.

6 EuGH, Urt. v. 7.3.2024 – C-479/22 P.

7 EuGH, Urt. v. 4.9.2025 – C-413/23 P, RDV 2026, 39.

8 EDSA, Guidelines 02/2026, Rn. 6 f.

9 EDSA, Guidelines 02/2026, Rn. 11 f.

10 EDSA, Guidelines 02/2026, Rn. 15.

11 EDSA, Guidelines 02/2026, Rn. 15.

12 EDSA, Guidelines 02/2026, Fn. 12: genannt werden u.a. Art. 27, 28, 29, 30 Abs. 2, 31, 32, 33 Abs. 2, 37, 38, 44, 46, 48 und 49 Abs. 6 DS-GVO.

13 Art. 68 Abs. 1 und 3 DS-GVO.

14 Art. 70 Abs. 1 lit. e DS-GVO.

Klargestellt wird in der Stellungnahme unter anderem, dass in die Prüfung die Mittel aller, die zur Identifizierung beitragen könnten, mit einzubeziehen sind.[15] Ein Bruch mit dem relativen Ansatz ist das nicht, denn geprüft wird nach wie vor die Identifizierungsmöglichkeit ausgehend von der datenverarbeitenden Stelle. Die Einbeziehung Dritter bedeutet zunächst, dass auch das Wissen derjenigen zu berücksichtigen ist, derer Hilfe sich die ausgehende Stelle bei der Identifizierung bedienen könnte. Bedacht werden aber nicht nur Dritte, die dem Verantwortlichen bei dessen Identifizierung unterstützen, sondern auch Empfänger, die die Daten eigenständig einer Person zuordnen können. Ausreichend ist, dass sie die Daten vom Verantwortlichen erlangen. Sind die Empfänger in der Lage, die Daten einer Person zuzuordnen, sind die Daten nicht nur für diese personenbezogen, sondern mittelbar auch für den verantwortlichen Übermittler. Dem EDSA zufolge sind hierbei nicht nur Dritte zu berücksichtigen, die die Daten durch aktive Weitergabe erlangen, sondern auch Dritte, die die Daten durch Leck oder unbefugten Zugriff, etwa illoyaler Beschäftigter, fremder Nachrichtendienste oder Cyberkrimineller erhalten.[16] Der Kreis der nach dem EDSA zu berücksichtigen Dritten ist damit denkbar weit gezogen. Begrenzt wird er allein durch die Wahrscheinlichkeit: Wer die Daten realistisch weder erlangen noch von anderen erhalten kann, bleibt außer Betracht.[17]

Als Mittel zählt sodann alles vom einfachen Lesen über die Websuche bis zur komplexen Analyse.[18] Prinzipiell ausgeschlossen wird nur, was unmöglich ist, unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft verlangt oder gesetzlich verboten ist.[19] Ob der Einsatz eines Mittels wahrscheinlich ist, bemisst sich hierbei nach objektiven Faktoren: den Eigenschaften der Daten, den Zugangsbeschränkungen, den verfügbaren Zusatzinformationen, dem Aufwand ihrer Beschaffung und der verfügbaren Technik einschließlich absehbarer Entwicklungen.[20] Abraten tut der EDSA hingegen von der fehlenden Motivation zur Re-Identifizierung als Prüffaktor. Motive ließen sich objektiv kaum feststellen und würden sich ändern. Identifiziert werden könne auch aus Versehen, aus Nachlässigkeit oder weil äußere Umstände die Stelle dazu zwingen. Stattdessen sollen als objektive Kriterien der Wert, den die re-identifizierten Daten für die jeweilige Stelle hätten, und das Risiko, das sie mit der Re-Identifizierung selbst eingeht, berücksichtigt werden.[21]

Der Ausschluss gesetzlich verbotener Mittel steht dabei für den EDSA unter einem Vorbehalt. Er beruht auf der Annahme, dass sich die Beteiligten an das Recht halten, und diese Annahme ist widerleglich. Wird ein Verbot kaum durchgesetzt, übersteigt der Gewinn den Aufwand oder wurde es in vergleichbaren Lagen schon gebrochen, zählen auch rechtswidrige Mittel.[22] Deswegen kommen als Empfänger auch Cyberkriminelle prinzipiell in Betracht. Ob diese Lesart Bestand hat, ist genauso offen wie die zur Auftraggeber-Perspektive. Der EuGH hat bisher schlicht festgehalten, dass ein Mittel nicht vernünftigerweise wahrscheinlich genutzt wird, wenn die Identifizierung gesetzlich verboten oder praktisch nicht durchführbar ist.[23] Ob diese Annahme widerlegt werden kann, wenn das Verbot faktisch nicht abhält, hat er bislang nicht entschieden.

Praktisch entscheidend ist darüber hinaus ein Satz zur Technik. Die dokumentierten Verfahren zur Re-Identifizierung seien zunehmend zugänglich, verlangten überschaubare Mittel und liefen auf handelsüblicher Hardware, und die Entwicklung agentischer KI werde Zeit- und Kostenaufwand weiter senken.[24] Der EDSA macht hier deutlich, dass sich die Schwelle des unverhältnismäßigen Aufwands, die der EuGH in Breyer gezogen hat, mit der technischen Fortentwicklung stetig weiter nach unten verschiebt.

Fazit

Die Leitlinien beenden zwölf Jahre Stillstand bei einer Frage, die über den Anwendungsbereich des gesamten Datenschutzrechts entscheidet. Fest steht nach vier zentralen Urteilen des EuGH, ob Daten anonym sind, hängt von der Perspektive der jeweiligen Stelle und den von ihr wahrscheinlich genutzten Mitteln ab. Wie eng der Ausschuss dieses Programm führt, zeigen die beiden dargestellten Weichenstellungen: die Auftraggeber-Perspektive, die Auftragsverarbeitern den Weg aus der DS-GVO versperrt, und die Einbeziehung rechtswidriger Mittel, mit der er über die bisherige Linie des EuGH hinausgeht. Beides steht unter einem Vorbehalt, denn Rechtsbindung erzeugen die Leitlinien nicht. Ob der Gerichtshof folgt, ist offen.

15 EDSA, Guidelines 02/2026, Rn. 30; zum Begriff der relevanten Stelle auch das Glossar der Leitlinien (Abschnitt 4).

16 EDSA, Guidelines 02/2026, Rn. 30.

17 EDSA, Guidelines 02/2026, Rn. 9; veranschaulichend Rn. 94 (Beispiel 22).

18 EDSA, Guidelines 02/2026, Rn. 28.

19 EDSA, Guidelines 02/2026, Rn. 26, unter Verweis auf EuGH, Urt. v. 4.9.2025 – C-413/23 P.

20 EDSA, Guidelines 02/2026, Rn. 29.

21 EDSA, Guidelines 02/2026, Rn. 31.

22 EDSA, Guidelines 02/2026, Rn. 32 f.

23 EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 46; ferner EuGH, Urt. v. 7.3.2024 – C-479/22 P, Rn. 51; EuGH, Urt. v. 4.9.2025 – C-413/23 P, Rn. 82.

24 EDSA, Guidelines 02/2026, Rn. 92.

BUCHBESPRECHUNG

Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz

C.H. Beck, München, 4. Aufl. 2026, 1744 S., 155,00 €, ISBN: 978-3-406-81271-2

Der Kommentar zur DS-GVO und zum BDSG von Paal/Pauly wird nach fünf Jahren neu aufgelegt. Seit der letzten Auflage ist viel passiert. Der EuGH hat zahlreiche das Datenrecht prägende Entscheidungen getroffen, u.a. die SCHUFA-Entscheidung und eine Vielzahl an Urteilen zu Art. 82 DS-GVO. Zudem wurde die KI-VO erlassen, die stufenweise Geltung erlangt und an vielen Stellen in das Datenschutzrecht hineinwirkt. Dementsprechend hoch war der Aktualisierungsbedarf.

Die Neuauflage wird dieser Herausforderung mehr als gerecht. Für 155,00 € bekommt die Leserschaft eine 1.744 Seiten starke Kommentierung, die es schafft, trotz des umfangreichen Sachstandes einen präzisen Überblick zu geben. Dem Kommentar gelingt dabei in bemerkenswerter Weise der Spagat zwischen dogmatischer Tiefe und handlicher Praxishilfe. Die Herausgeber Boris P. Paal (Juraprofessor an der Technischen Universität München) und Daniel A. Pauly (Rechtsanwalt und Partner einer internationalen Großkanzlei) verkörpern dabei selbst die Verbindung von Wissenschaft und Beratungspraxis, die das gesamte Werk ausmacht. Neben ihnen waren zahlreiche weitere Bearbeiter beteiligt, die die gesamte Bandbreite juristischer Perspektiven abdecken. Sie kommen aus Wissenschaft, Beratungspraxis, Unternehmen und Aufsicht. Hierdurch erhält der Leser einen fundierten Gesamtüberblick und das Werk seine Tiefe.

Dass die Neuauflage hält, was sie verspricht, wird vor allem an den Stellen deutlich, an denen sich in den letzten fünf Jahren am meisten getan hat. Eine dieser Stellen ist der Art. 22 DS-GVO, auf den daher im Folgenden exemplarisch eingegangen wird. Die automatisierte Entscheidung, die in Art. 22 DS-GVO reglementiert ist, spielte vor fünf Jahren noch eher eine randständige Rolle. Ihr Anwendungsbereich war klein und wies eher in die Richtung zukünftiger Entwicklung als in die Realität. Das ist mittlerweile anders. In einer Gesellschaft, in der quasi jeder Akteur, sei es aus Wirtschaft, Justiz oder Politik, KI-Systeme in der ein oder anderen Form nutzt, und sich auch die gesellschaftlichen Debatten zentral um die Möglichkeiten und Grenzen von künstlicher Intelligenz drehen, rückt Art. 22 ins Zentrum vieler juristischer Diskussionen. Dass die Neuauflage hier entsprechend aufgerüstet hat, zeigt sich bereits an den zahlreichen Einschub-Randnummern (etwa Rn. 7a–7g, 20a–20i oder 39a–39i). Hierbei nimmt der Kommentar nicht nur die DS-GVO selbst, sondern auch Parallelregelungen in den Blick. Das ist bei einem Rechtsgebiet wie dem Datenrecht, das durch zahlreiche nationale wie internationale Regime geprägt wird, keine Kür. Spannend sind insbesondere die Abschnitte zum Verhältnis der DS-GVO zur KI-VO (Rn. 7c ff.), denn die Kommentierung beschränkt sich nicht auf den Hinweis, die Gesetze seien nebeneinander anwendbar. Sie geht stattdessen auf tatsächliche Zusammenhänge ein. So wird die menschliche Aufsicht des Art. 14 KI-VO als Verwandte der Schutzmaßnahmen des Art. 22 Abs. 3 beschrieben (Rn. 7d) und der Erläuterungsanspruch aus Art. 86 KI-VO neben Art. 15 Abs. 1 lit. h) DS-GVO gestellt. Beide Regelwerke wollen, wie die Kommentierung anschaulich formuliert, den Einzelnen vor einer „Computer-says-no-Dystopie" bewahren (Rn. 7d).

Die Kommentierung beleuchtet nicht nur parallele europäische Regelungen, sondern auch das nationale Recht und führt zahlreiche verstreute Regelungen zusammen (Rn. 42 ff.): die Sondernormen für den voll automatisierten Erlass von Verwaltungsakten, Sozialverwaltungsakten und Steuerbescheiden (§ 35a VwVfG, § 31a SGB X, § 155 Abs. 4 AO), die Ausnahme für automatisierte Entscheidungen über Versicherungsleistungen bei Heilbehandlungen (§ 37 BDSG) sowie die auf Art. 23 DS-GVO gestützten Beschränkungen in § 22b Abs. 1 S. 2 BörsG und § 51a Abs. 2 S. 1 GwG (Rn. 43c). Gleichzeitig wird der eng begrenzte nationale Handlungsspielraum dargestellt, der sich im Wesentlichen auf die Öffnungsklauseln des Art. 22 Abs. 2 lit. b) und des Art. 23 DS-GVO beschränkt (Rn. 43). Die Leserschaft bekommt daher einen umfassenden Überblick über den Rechtsrahmen, der national wie international tatsächlich gilt, ohne verschiedene Kommentierungen bemühen zu müssen.

Die Kommentierung schafft einen echten Mehrwert aber nicht nur beim Gesamtüberblick, sondern auch im Herzen einer jeden Kommentierung, der Arbeit am Tatbestand. Die Anwendungsfelder des Art. 22 DS-GVO strukturiert darzustellen, fordert heraus, da die Norm in praktisch jeden Lebensbereich hineinreicht, von der Werbung über die Personalauswahl bis zu Online-Shops und Zahlungsdienstleistern (Rn. 8). Der Text wird dieser Herausforderung gerecht, indem er das Verbot in Unterprobleme zerlegt und jede Konstellation präzise durchprüft. So entsteht die rechtliche Einordnung anhand tatsächlicher Problemfelder und hängt nicht im luftleeren Raum. Der Kommentierung liegt hierbei erkennbar fundiertes Wissen zu den tatsächlichen Einsatzfeldern automatisierter Entscheidungen und entscheidungsvorbereitender Systeme zugrunde. Die Betrugsprävention der niederländischen Sozialverwaltung (Rn. 16a), polizeiliche Analyseplattformen (Rn. 20c f.) und die Personalisierung von Preisen anhand des Klickverhaltens der Verbraucher (Rn. 27a ff.) sind nur einige der im Kommentar bearbeiteten Praxisbereiche. Das ermöglicht es der Leserschaft, der Komplexität des Themas leichtfüßig Herr zu werden. Die tatsächliche Rückkopplung wird zudem dadurch deutlich, dass der Autor das Phänomen des Automation Bias, der die Letztentscheidung faktisch entwertet, nicht unbedacht lässt (Rn. 20g). Leiden tut die dogmatische Tiefe trotz des Praxisbezugs an keiner Stelle. Auch die dogmatisch nach wie vor umstrittenen Problemfelder, wie die Konturierung des Begriffs der ausschließlich automatisierten Entscheidung (Rn. 16 ff.), bearbeitet der Kommentar pointiert. Unter anderem durch die Rückbindung an den Zweck der Norm (Rn. 24b) bringt der Text die Norm konsequent so zur Anwendung, wie es ihrer Zielvorstellung entspricht.

Die Kommentierung bietet einen konkreten Nutzen für Akteure aus Wissenschaft und Praxis. Der Griff zum neuen Paal/Pauly kann daher jedem, der sich einen Überblick über die aktuelle Rechtslage verschaffen möchte, nach wie vor ans Herz gelegt werden.

Professor Dr. Rolf Schwartmann, Köln

Sofortmaßnahme „KI-Seepferdchen“

Die Kommission zum Jugendschutz der Bundesregierung will Grundschüler auf das Leben mit KI vorbereiten

Die Kommission zum Kinder- und Jugendschutz in der digitalen Welt, der ich angehöre, hat im Juni Handlungsempfehlungen vorgelegt. Sie muss sich insbesondere an konkreten und sofort umsetzbaren Maßnahmen messen lassen. Dazu haben wir uns für die Empfehlung einer flächendeckend und zentral organisierten Sofortmaßnahme für Kinder im Grundschulalter entschieden. Dazu dient das „KI-Seepferdchen“, das nötig ist, um beim Einsatz von KI den Kopf über Wasser zu halten. Wer sich bei der Nutzung von KI treiben lässt, wie auf einem Floß in einem Strom, der muss lernen, wie man es anstellt nicht an gefährliche Stellen getragen zu werden oder gar unterzugehen. Die Kommission schlägt ein konkretes Verfahren vor. So soll bei einer Bundesbehörde, naheliegend wäre etwa die in Bonn ansässige Bundeszentrale für Kinder- und Jugendmedienschutz (BzKJ), für alle Grundschulen in Deutschland ein online zu erwerbendes Zertifikat zu den Möglichkeiten und Risiken des KI-Einsatzes erworben werden, das „KI-Seepferdchen“. Die Maßnahme soll über einen zentralen Anschubservice des Bundes organisiert und getragen werden. Ein „Expertenrat Kinder und KI“ soll auf Bundesebene die Inhalte fortlaufend anpassen und die Bundesregierung beraten. Die daran anknüpfende und weitergehende Algorithmen- und KI-Kompetenz im Bildungskontext soll darauf aufbauen. Insbesondere in den Sekundarstufen I und II sollen die Schülerinnen und Schüler zu einem reflektierten, kritischen und verantwortungsvollen Umgang mit KI befähigt werden. Die Auseinandersetzung mit algorithmischen Empfehlungssystemen und generativen KI-Anwendungen, wie Chatbots soll in den Lehrplänen verankert werden. All das soll durch eine entsprechende Fortbildung der Lehrkräfte begleitet werden.

Bild: Prostock-studio – stock.adobe.com

Zertifizierung zum Datenschutzbeauftragten GDDcert. EU

Starten Sie jetzt Ihre Ausbildung!

30.11.–01.12. + 03.12.–04.12. + 08.12.2026 | online
22.02.–23.02. + 25.02.–26.02. + 02.03.2027 | online

- über 30 Jahre Erfahrung und mehr als 12.000 Absolventen
- von Experten entwickeltes 10-tägiges Schulungskonzept
- renommierter Kompetenznachweis gegenüber Behörden, Kunden und Partnern
- Ausbildung durch die größte deutsche Datenschutzvereinigung

Jetzt anmelden: **www.datakontext.com/GDDcert-EU**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

powered by GDD

Foto: peshkova, Adobe Stock

NEU: Version 2.0 mit KI-Assistenten:

- ✓ DSGVO-FAQ-Assistent
- ✓ Verfahren-Generator
- ✓ Onboarding-Assistent

DATA AGENDA Datenschutz Manager

Datenschutz einfach organisiert

- ✓ webbasiertes Management System
- ✓ professionelle Schritt-für-Schritt Anleitung mit vielen Vorlagen
- ✓ einfaches Erfassen und Dokumentieren aller Datenschutzmaßnahmen
- ✓ effektive Zusammenarbeit aller verantwortlichen Stellen
- ✓ besonders für externe DSBs geeignet: Alle Mandanten in einem System

Jetzt einfach Demotermin vereinbaren:
www.DataAgenda.de/datenschutzmanager

DATAKONTEXT