1 | 2025 1. Jahrgang | Seiten 1–64 EuDIR.nomos.de

EuDIR

Zeitschrift für Europäisches Daten- und Informationsrecht

Aus dem Inhalt

Nomos

Nomos

JETZT ANMELDEN

NomosWebinar

DAS RECHT DER KÜNSTLICHEN INTELLIGENZ UPDATE

21.02.2025 | 10.30 – 13 UHR

Am 1. August 2024 ist der **AI Act in Kraft** getreten. Sein horizontaler und risikobasierter Regulierungsansatz löst vor allem für Anbieter und Betreiber von KI-Systemen umfangreiche **Compliance-Pflichten** aus. Der AI Act legt zudem die Grundlage für ein neues **Aufsichtsregime** und harmonisierte Standards. Dadurch entsteht ein komplexes Regelsystem, das sich in nahezu allen Wirtschaftssektoren und Gesellschaftsbereichen auswirkt. Hinzu kommt, dass **Anbieter und Betreiber** eine **KI-Kompetenz** sicherstellen müssen.

Das Webinar vermittelt Ihnen einen praxisbezogenen Überblick über das Regelwerk, inklusive seiner Ausstrahlungen auf das Informationstechnologierecht.

SPEAKER:IN

Prof. Dr. Janine Wendt
ist Leiterin des Fachgebietes für Bürgerliches Recht und Unternehmensrecht an der Technischen Universität Darmstadt.

Prof. Dr. Domenik Wendt, LL.M.
hält die Professur für Bürgerliches Recht, Europäisches Wirtschaftsrecht und Europarecht an der Frankfurt University of Applied Sciences und ist Direktor des ReLLaTe.

Teilnahmegebühr: 149,– €*
Inkl. instruktiver Präsentation und Teilnahmebescheinigung.

*(zzgl. MwSt.)

QR-Code scannen und anmelden.

Inhalt 1/2025

Rezensionen

Impressum

Zeitschrift für Europäisches Daten- und Informationsrecht (EuDIR)
ISSN 2944-456X

Schriftleitung:
Prof. Dr. Rolf Schwartmann (V.i.S.d.P.)
RiVG Kristin Benedikt
E-Mail: Schriftleitung-EuDIR@nomos-journals.de

Redaktion:
Lucia Burkhardt
Moritz Köhler
E-Mail: EuDIR@nomos-journals.de
www.EuDIR.nomos.de

Manuskripte und andere Einsendungen:
Alle Einsendungen sind an die o. g. Adresse zu richten. Es besteht keine Haftung für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss in Textform erfolgen. Mit der Annahme zur Veröffentlichung überträgt die Autorin/der Autor der Nomos Verlagsgesellschaft mbH & Co.KG an ihrem/seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in §38 Abs.4 UrhG niedergelegte zwingende Zweitverwertungsrecht der Autorin/des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt. Eine eventuelle, dem einzelnen Beitrag oder der jeweiligen Ausgabe beigefügte Creative Commons-Lizenz hat im Zweifel Vorrang. Zum Urheberrecht vgl. auch die allgemeinen Hinweise unter www.nomos.de/urheberrecht. Unverlangt eingesandte Manuskripte – für die keine Haftung übernommen wird – gelten als Veröffentlichungsvorschlag zu den Bedingungen des Verlages. Es werden nur unveröffentlichte Originalarbeiten angenommen. Die Verfasser erklären sich mit einer nicht sinnentstellenden redaktionellen Bearbeitung einverstanden.

Redaktionsrichtlinie:
Diese Zeitschrift ist auch in der Datenbank BeckOnline verfügbar. Um die Funktionen dieser Datenbank optimal zu nutzen (insbesondere die Verlinkungsfunktion), empfehlen wir dringend die Beachtung der C.H.BECK-Redaktionsrichtlinien und Werkabkürzungen. Diese finden Sie im Zitierportal des Verlags C.H.BECK www.zitierportal.de

Anzeigen:
Verlag C.H. BECK
Anzeigenabteilung
Dr. Jiri Pawelka
Wilhelmstraße 9
80801 München
Media-Sales:
Tel: (089) 381 89-687 687
mediaberatung@beck.de

Verlag und Gesamtverantwortung für Druck und Herstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestr. 3-5
76530 Baden-Baden
Telefon: 07221/2104-0
Telefax: 07221/2104-27
www.nomos.de

Geschäftsführer: Thomas Gottlöber
HRA 200026, Mannheim

Sparkasse Baden-Baden Gaggenau
IBAN DE05662500300005002266
(BIC SOLADES1BAD)

Erscheinungsweise: zweimonatlich

Preise:
Individualkunden: Jahresabo € 199,00
Alle Abopreise inklusive Zugang zur digitalen Ausgabe in beck-online für einen Nutzer/eine Nutzerin.
Die Abopreise verstehen sich einschließlich der gesetzlichen Umsatzsteuer und zuzüglich Vertriebskostenanteil € 18,00, sowie Direktbeorderungsgebühr € 3,50, (Inland); Einzelheft: € 35,00.

Bestellungen über jede Buchhandlung und beim Verlag.

Kundenservice:
Telefon: +49-7221-2104-222
Telefax: +49-7221-2104-285
E-Mail: service@nomos.de
Hier erhalten Sie unter Angabe Ihrer Abo-Nummer auch die Zugangsdaten für die Online-Nutzung.

Kündigung:
Abbestellungen mit einer Frist von sechs Wochen zum Kalenderjahresende.

Adressenänderungen:
Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.
Hinweis gemäß Art. 21 Abs. 1 DSGVO: Bei Anschriftenänderung kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeauftrag gestellt ist. Hiergegen kann jederzeit mit Wirkung für die Zukunft Widerspruch bei der Post AG eingelegt werden.

EuDIR

Zeitschrift für Europäisches Daten- und Informationsrecht
1/2025 | Seiten 1–64

Grußwort der Schriftleitung und des Verlages

Für ein faires, konsistentes und zeitgemäßes Europäisches Daten- und Informationsrecht

Menschen und Unternehmen in Europa sind auf einen wirtschaftlich und rechtlich tragfähigen Rahmen für eine Datenwirtschaft angewiesen, in dem die Grundrechte mit den Interessen der Unternehmen und dem Sicherheitsbedürfnis des Staates in einen fairen Ausgleich gebracht werden. Das ehrgeizige Ziel ist es, einen „Brüssel-Effekt" auszulösen, um weltweit die Standards für die Digitalisierung zu setzen, die mittel- und langfristig die richtigen sind. Dabei geht es längst nicht mehr nur um Datenschutz. Im Jahr 2025 gibt es Regeln, die einen rechtlichen Rahmen für die Strukturen des Datenaustauschs, für das Teilen von Daten zu wirtschaftlichen Zwecken für Nutzer und Unternehmen, für die Sicherung des Wettbewerbs im EU-Binnenmarkt gegenüber internationalen „Tech-Giganten" und für den Schutz der Meinungsfreiheit und die Bekämpfung von „Hasskriminalität" auf Plattformen wie sozialen Netzwerken setzen. Mit der KI-Verordnung, die ein spezielles Produktrecht für die Entwicklung und den Betrieb von KI-Systemen und KI-Modellen enthält, hat die EU weltweit Aufmerksamkeit erregt. Die Rechtsakte sind vielfältig, unübersichtlich und komplex. Sie überschneiden sich inhaltlich und werden von einer Vielzahl von Behörden vollzogen.

Ein wesentliches Manko des Datenrechts ist dessen fehlende Konsistenz. Die Zeitschrift für Europäisches Daten- und Informationsrecht (EuDIR) will einen Beitrag zu seiner Systematisierung leisten. Dazu hat sich ein Kreis von Digital- und Daten(rechts)expertinnen und -experten zusammengefunden. Zu diesem Kreis gehören in den Reihen der Herausgeber, des Beirats und der Redaktion Mitwirkende aus Wissenschaft, Justiz, Anwaltschaft, Aufsichtsbehörden, Medienwissenschaft und Informatik. Unser Ziel ist es, dem ausufernden und in verschiedene Richtungen wachsenden Rechtsgebiet des Datenrechts Struktur zu geben. Das **Datenwirtschaftsrecht** und **Datenschutzrecht** sind dabei ebenso relevant wie das **Recht der Datensicherheit** und der **Künstlichen Intelligenz**. Es reicht vom digitalen Vertragsrecht über das Onlinestrafrecht und das Wettbewerbsrecht bis in den Kern der Wahrung der demokratischen Voraussetzungen der EU, die durch die Vermischung staatlicher und privater Meinungsmacht auf Plattformen in den USA und China existentiell herausgefordert sind. Wir wollen die Herausforderungen benennen und Lösungen anbieten. Insofern versteht sich die EuDIR als Forum für einen praxisorientierten und wissenschaftlich fundierten Diskurs in einem thematisch denkbar breiten Feld. Zugleich können die hier auftretenden Probleme nicht isoliert gelöst werden.

Damit wir und alle, die hier schreiben, diesen Herausforderungen konstruktiv begegnen können, haben das Team der EuDIR und der Nomos Verlag die neue Zeitschrift ins Leben gerufen, die auf beck-online in den Modulen **NomosOnline Premium** und **NomosOnline Daten- und Informationsrecht** abrufbar ist. Jede der zweimonatlich erscheinenden Ausgaben wird von zwei Personen aus dem Kreis der Herausgebenden betreut. Darüber hinaus sind die geschäftsführenden Herausgeber in Zusammenarbeit mit der Redaktion für die Einhaltung des Gesamtkonzepts verantwortlich. Der Herausgeberbeirat gibt Impulse aus übergeordneter Perspektive.

Jede Ausgabe beginnt mit einem **Editorial**, in dem Persönlichkeiten aus dem Bereich des Datenschutzes zu Wort kommen. Es folgen **Aufsätze** und **Urteilsbesprechungen**. Besondere Zuständigkeiten im Herausgeberkreis bestehen für die **Rechtsprechung** und die Rubrik „**Brüssel Inside**". Mit letzterer wollen wir Impulse aus Kommission und EU-Parlament an der Quelle aufgreifen und in den Kontext der EuDIR setzen. Darüber hinaus ist der im Datenrecht faktisch sehr relevanten **Vollzugspraxis** eine eigene Rubrik gewidmet. Unser Augenmerk gilt in jeder Ausgabe auch einer Auswahl von Publikationen, die wir einordnen.

Wir danken allen Leserinnen und Lesern der EuDIR für ihr Interesse und hoffen, mit ihr einen Beitrag zu einem fairen, konsistenten und zeitgemäßen Datenrecht leisten zu können.

Rolf Schwartmann
Schriftleiter

Kristin Benedikt
Schriftleiterin

Thomas Gottlöber
Nomos Verlag, Verlagsleiter

Marco Ganzhorn
Nomos Verlag, Lektoratsleitung

Das verflixte siebte Jahr: Die DS-GVO zwischen Datenschutz und Datenwirtschaft

Für uns beide ist das junge Datenschutzrecht der Europäischen Union schon fast 15 Jahre alt. So lange ist es her, dass die Arbeiten der EU-Institutionen dafür begonnen. Der Vertrag von Lissabon, der damals in Kraft trat, sah mit der Grundrechtecharta endlich ein verbindliches und ausdrückliches Grundrecht auf Datenschutz vor und gab selbst durch Artikel 16 AEUV dem EU-Gesetzgeber eine umfassende Gesetzgebungskompetenz für dessen Schutz und den freien Datenverkehr im Europäischen Markt. Tatsächlich zur Anwendung kommt die daraus hervorgegangene Datenschutz-Grundverordnung nun seit dem 25. Mai 2018. Für ein EU-Gesetz ist es nicht nur in überragender Weise zu einer allseits geläufigen Regelung im Zusammenleben und Wirtschaften auf diesem Kontinent geworden, es ist auch ein regulativer Exportschlager der EU – die Standards der DS-GVO sind heute weltweit bekannt und maßgeblich.

Doch wir alle wissen: Das war auch mit Zumutungen verbunden, viele Menschen stöhnen noch immer auf, wenn es um das Datenschutzgesetz made in Brüssel geht. Es ist eine ambivalente Beziehung, die nun in ihrem siebten Jahr ist. Doch vielleicht lässt sich in diesem verflixten siebten Jahr auch ein gemeinsamer Neustart finden, der die Beziehung zwischen Gesetz, Mensch und einer datenbestimmten Welt ein wenig normalisiert. Das gemeinsame EU-weite Recht hat durchaus zu Vertrauen und Rechtssicherheit bei den Menschen beigetragen, viele Unkenrufe bezüglich ihrer Wirkung sind nicht eingetreten, doch erleichtert sie andererseits die Datennutzung auch nicht besonders. Jene, die anführen, dass es Deutschland beim Datenschutz übertreibe und dann auf Länder wie Estland, Dänemark oder die Niederlande verweisen, können ihre kritische Analyse offenbar nicht auf die DS-GVO beziehen, denn diese gilt in jenen Ländern gleichermaßen direkt.

Zugleich ist auch deutlich: Statt die DS-GVO als zentrale Leitlinie für den Datenschutz zu betrachten und diese einheitlich europaweit auszulegen gibt es in den 27 EU-Ländern und hierzulande in 16 Bundesländern noch sehr viele Sonderregeln zum Datenschutz, die Regeln werden mitunter noch sehr ambitioniert unterschiedlich angewandt. Hier muss in Zukunft mehr Gemeinsamkeit und Klarheit die Leitlinie sein. Die Energie sollte statt in Sonderregelungen z.B. in die Erarbeitung etwa einfach verständlicher Symbole zu Datenschutzpräferenzen oder die Harmonisierung von ePrivacy-Vorschriften gesteckt werden, die noch immer in 27 nationale Rechtsrahmen umgesetzt wird. Und der Blick derer Wirtschaftsakteure, die über die DS-GVO stöhnen, könnte auch einmal auf die vielen Möglichkeiten gelenkt werden, die diese für die Verarbeitung von Daten schafft – nicht zuletzt dann, wenn es gar um anonyme Informationen geht. Deren Datenschatz bleibt mithin von der DS-GVO gänzlich unberührt. Die Datenschutz-Grundverordnung ist eigentlich viel besser als ihr Ruf doch ihre Wirkung hinsichtlich eines einheitlichen Datenmarktes in der Europäischen Union bleibt hinter den Erwartungen noch zurück.

Im siebten Jahr ihres Bestehens ist die DS-GVO nicht mehr das einzige Instrument des europäischen Datenrechts. Sie reiht sich ein in ein Orchester aus Rechtsakten, die den Datenschutz ebenso wie die Datenwirtschaft in den Blick nehmen. Damit deren Zusammenspiel nicht in eine Kakofonie ausartet, muss die Anwendung der EU-Gesetze dirigiert werden. Speziell in Deutschland fehlt es bisweilen aber an einer Koordination der zahlreichen Aufsichtsbehörden. Die DS-GVO wird hierzulande ergänzt durch das Bundesdatenschutzgesetz sowie 16 Landesdatenschutzgesetze. Deren Durchführung obliegt insgesamt 18 Behörden. Die Konferenz der Datenschutzbeauftragten ist eine wichtige Kommunikationsplattform, doch auch sie kann nicht immer eine einheitliche Auslegung gewährleisten und erreicht eine Detailtiefe, die so nicht angelegt war. Hinzu kommt, dass sich die Bundesnetzagentur anschickt, den Datenschutzbehörden ihre Position als erste Geige streitig zu machen. Sie beaufsichtigt die Durchführung des Digital Services Acts und wird wohl auch die Kompetenzen der Marktaufsichtsbehörde nach der KI-Verordnung erhalten. Die enge Verflechtung zwischen Digitalwirtschaft, Künstlicher Intelligenz und Datenrecht ist offenkundig. Die Datenschutzbehörden berufen sich deshalb auf ihre Sachnähe und reklamieren die Marktüberwachung nach der KI-Verordnung für sich; ein Vorgeschmack auf unliebsame Dissonanzen?

Im verflixten siebten Jahr der Ehe von Datenschutz und Datenwirtschaft hat sich die Welt der Daten, ihre wirtschaftlichen Rahmenbedingungen, ihr rechtlicher Kontext und das politische Umfeld verändert. Eine Modernisierung oder Anpassung auch an neue Technologien wird dringend erforderlich. Aus dem Rausch der Daten müsste ein nüchterner Umgang mit den Erforderlichkeiten und eine verlässliche Partnerschaft werden, die für die Stürme der Zukunft gerüstet ist. Nun muss es ein gutes Jahr werden und die noch junge EU-Kommission und das neugewählte EU-Parlament müssen dafür ebenso klug und umsichtig handeln, wie die kommende Bundesregierung in Deutschland. Sie muss vor allem die Koordinierung angehen und die Digitalisierung im Einklang mit nationalen und europäischen Gesetzen orchestrieren. Allenthalben wird gefordert, die Vereinheitlichung und Systematisierung des Datenrechts zentral bei einem neu zu schaffenden Digitalministerium anzusiedeln. Dass der bisher verfolgte dezentrale Weg der Digitalisierung mit zahlreichen Hürden einhergeht, haben die vergangenen Jahre gezeigt. Wahrscheinlich würde ein Querschnittsministerium eine effektive Digitalisierung besser und effizienter vorantreiben können.

Bis dahin freuen wir uns, dass mit der EuDIR schon jetzt und zugleich endlich eine Zeitschrift existiert, die das europäische Daten- und Informationsrecht ganzheitlich in den Blick nimmt. Alle Mitwirkenden leisten einen wichtigen Beitrag zur Entwicklung einer digitalen Gesellschaft, die die Bedürfnisse von Bürgern und Wirtschaftsunternehmen gleichermaßen berücksichtigt. Wir haben die Lektüre des ersten Hefts genossen und wünschen auch Ihnen viel Freude mit dieser und allen weiteren Ausgaben.

Jan Philipp Albrecht, heute Vorstand der Grünen-nahen Heinrich-Böll-Stiftung, war Berichterstatter des Europäischen Parlaments zur Datenschutz-Grundverordnung

und

Axel Voss, Mitglied des Europäischen Parlaments für die EVP, war Berichterstatter seiner Fraktion für die Datenschutz-Grundverordnung

Prof. Dr. Rolf Schwartmann/Kai Zenner*

GPAI-Anwendungen auf dem Prüfstand: Die Regulierung der KI-VO entlang der Wertschöpfungskette

GPAI-Anwendungen reiten vorne auf der aktuellen KI-Welle. Die Wirtschaft hat in ihnen ein beträchtliches Potenzial erkannt. Derzeit werden die Anwendungen in Unternehmen allerdings oftmals unter privaten Lizenzen eingesetzt: Laut einer Umfrage des Digitalverbandes BITKOM wird in jedem dritten Unternehmen private KI genutzt. In einem weiteren Viertel der Unternehmen weiß man es zwar nicht genau, geht aber davon aus, dass private KI genutzt wird. Die KI-VO adressiert die Anbieter und Betreiber von GPAI-Anwendungen indes ungeachtet der gewählten Lizenzen und reguliert auch die sogenannte Schatten-KI. Der vorliegende Beitrag beschäftigt sich daher mit der Frage, welche Pflichten Unternehmen erfüllen müssen, in denen GPAI-Anwendungen eingesetzt werden.

I. GPAI-Anwendungen im Regelungskontext der KI-VO

1 Künstliche Intelligenz (KI) ist mehr als nur Chatbots. Der KI-Begriff umfasst eine große Zahl unterschiedlicher Technologien in verschiedenen Sektoren und für verschiedene Anwendungsfälle und vom unspezifischen Basismodel bis zum KI-System mit konkreter Zweckbestimmung.[1] Zur Wahrheit gehört aber auch, dass die Wirtschaft gerade bei KI-Anwendungen wie Chatbots ein beträchtliches Potenzial erkannt hat und sie deshalb zunehmend in Unternehmensabläufe integriert werden.[2] Ihr besonderes Potenzial entspringt ihrer Vielseitigkeit: Durch ihre Fähigkeit, Inhalte und insbesondere Sprache zu verarbeiten, sind sie für eine Vielzahl von Zwecken einsetzbar. Sie werden in der KI-Verordnung[3] dementsprechend als KI mit allgemeinem Verwendungszweck (engl.: general purpose artificial intelligence, kurz: GPAI) bezeichnet. Ein sogenanntes GPAI-System kann etwa die Gestalt eines KI-Chatbots annehmen, der dem Anwender als Suchmaschine dient; sei es für Suchen im Web oder in einer unternehmensinternen Wissensdatenbank. Es kann aber auch in Textverarbeitungs- oder Tabellenkalkulationsprogramme integriert werden und die menschlichen Sachbearbeiter bei der Bearbeitung der dort jeweils anfallenden Aufgaben als sogenannter Copilot unterstützen.

2 Die vielseitige Einsatzfähigkeit von GPAI hat den europäischen Gesetzgeber bei der Schaffung der KI-VO vor erhebliche Probleme gestellt: Im Kommissionsentwurf[4] aus dem Jahre 2021 wurde zunächst ein streng risikobasiertes Regulierungskonzept für KI-Systeme mit einer festen Zweckbestimmung aufgestellt, das in weiten Teilen auch der finalen KI-VO entspricht. Zentrale Grundlage der Risikoklassifizierung ist in diesem Konzept die Zweckbestimmung. Ist der Zweck, den ein KI-System erfüllen soll, einem hochriskanten Lebensbereich zuzuordnen (Art. 6 Abs. 2 i.V.m. Anhang III KI-VO) oder aufgrund produktsicherheitsrechtlicher Erwägungen inhärent hochriskant (Art. 6 Abs. 1 i.V.m. Anhang I KI-VO), so gilt auch das KI-System als Hochrisiko-KI-System im Sinne der KI-VO. Als solches muss es spezifische Anforderungen erfüllen, die in Art. 8 ff. KI-VO festgelegt sind. Die Akteure (Art. 3 Nr. 8 KI-VO) entlang der Wertschöpfungskette des Hochrisiko-KI-Systems treffen zudem besondere Pflichten. Dieser Regelungsansatz wird durch GPAI-Anwendungen strapaziert:[5] Wie gesehen, können diese *per definitionem* für eine Vielzahl von Zwecken eingesetzt werden. Darunter fallen auch hochriskante Zwecke, wie das Beispiel des kolumbianischen Richters zeigt, der bereits im Frühjahr 2023 eine Entscheidung unter anderem auf Ausführungen von ChatGPT stützte.[6]

II. Die Regulierung von GPAI-Anwendungen in der KI-VO

3 GPAI-Anwendungen passen also nicht unmittelbar in das ursprünglich gewählte Regulierungskonzept der KI-VO.[7] Wie der europäische Gesetzgeber diese Friktion aufzulösen

* Der erstgenannte Autor ist Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln. Außerdem ist er Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) eV. Der zweitgenannte Autor ist Büroleiter des Europaabgeordneten Axel Voss. Alle geäußerten Ansichten sind persönlicher Natur und stellen weder die Position des Europäischen Parlaments noch die der EVP-Fraktion dar. Die Autoren danken Moritz Köhler für die wertvolle Unterstützung bei der Erstellung des Beitrages.

1 Schwartmann/Keber/Zenner/Schwartmann/Mühlenbeck, 2. Aufl. 2024, KI-VO, 1. Teil 4. Kap. Rn. 11 ff.

2 Bitkom, Erstmals beschäftigt sich mehr als die Hälfte der Unternehmen mit KI, 16.10.2024, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Erstmals-beschaeftigt-Haelfte-Unternehmen-KI.

3 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024, im Folgenden: KI-VO.

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

5 Dazu bereits Zenner RDV 2023, 204.

6 Gutiérrez, ChatGPT in Colombian Courts, 23.2.2023, abrufbar unter https://verfassungsblog.de/colombian-chatgpt/. Zur Hochrisiko-Klassifizierung solcher Zwecke vgl. Anhang III Nr. 8 Buchst. a KI-VO.

7 Schwartmann/Zenner, DataAgenda Datenschutz Podcast, Episode 62: Update KI-VO Herbst 2024, abrufbar unter https://dataagenda.podigee.io/70-kai-zenner, ab Minute 22:25.

versucht hat, soll im Folgenden dargestellt werden. Dazu werden die verschiedenen Akteure entlang der Wertschöpfungskette gemeinsam mit ihren jeweiligen Pflichten beleuchtet.

1. Anbieter eines GPAI-Modells

4 GPAI-Systeme (z.B. ChatGPT von OpenAI) sind in Art. 3 Nr. 66 KI-VO legaldefiniert als KI-Systeme, die in der Lage sind, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen und die auf einem GPAI-Modell beruhen. Dabei handelt es sich gem. Art. 3 Nr. 63 KI-VO wiederum um ein KI-Modell (z.B. GPT-4 von OpenAI), das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen. Es kann in eine Vielzahl nachgelagerter Systeme integriert und in zahlreichen Anwendungsfällen genutzt werden. Bei GPAI-Modellen handelt es sich üblicherweise um künstliche neuronale Netze. Sie werden in der Regel mit großen Datenmengen trainiert, wobei verschiedene Methoden, wie überwachtes, unüberwachtes und bestärkendes Lernen zur Anwendung kommen, ErwG 97 S. 3 KI-VO.

a) Technische und rechtliche Grundlagen

5 Bekannte und viel diskutierte GPAI-Modelle sind die sogenannten Large Language Models (LLMs). Die einzelnen Knotenpunkte dieser künstlichen neuronalen Netze bestehen aus kurzen Wörtern oder Wortbestandteilen, den sogenannten Tokens.[8] In der Trainingsphase des Modells wird eine große Zahl von Texten analysiert, wobei sich im Rahmen der Analyse Wahrscheinlichkeiten für typische Tokenfolgen herausbilden.[9] Bei Texten, die in der Anwendungsphase unter Heranziehung eines LLMs ausgegeben werden, handelt es sich um Neuschaffungen, die sich in den Trainingsdaten nicht unmittelbar wiederfinden. Daher wird auch von generativen KI-Systemen gesprochen. Da GPAI-Modelle als Grundlage für eine Vielzahl von KI-Systemen herangezogen werden können, wurden sie in der Vergangenheit bisweilen auch als Foundation Models bezeichnet.[10] Der europäische Gesetzgeber hat sich in der KI-VO allerdings für den weiteren Begriff des GPAI-Modells entschieden, um die Verordnung technologieoffener zu gestalten und besser für künftige Entwicklungen zu rüsten.

6 In technischer und vor allem rechtlicher Hinsicht ist die Differenzierung zwischen GPAI-Modellen und GPAI-Systemen entscheidend. GPAI-Modelle stellen für sich genommen keine Systeme im Sinne der KI-VO dar, ErwG 97 S. 6 KI-VO. In der Folge unterliegen sie nicht der Regulierung von (Hochrisiko-)KI-Systemen. Die KI-VO verhält sich zur Abgrenzung von KI-Modell und KI-System äußerst zurückhaltend. Der Normtext enthält hierzu kaum Anhaltspunkte. Allenfalls kann aus den Legaldefinitionen von GPAI-Modell und GPAI-System abgeleitet werden, dass ein KI-Modell Teil eines KI-Systems ist. Das lässt die Folgerung zu, dass ein GPAI-Modell durch eine technische Weiterentwicklung sowie eine Verknüpfung mit weiteren Komponenten zu einem KI-System werden kann. Diesen Befund bestätigt ErwG 97 S. 7 KI-VO ausdrücklich und nennt die Nutzerschnittstelle beispielhaft als eine dieser Komponenten. Ob die Integration einer Nutzerschnittstelle ausreicht und welche Komponenten andernfalls für den Übergang von GPAI-Modell zu GPAI-System erforderlich sind, bleibt allerdings offen. Fest steht, dass das GPAI-Modell insbesondere mit Blick auf seine Zweckbestimmungen durch die Wandlung in ein GPAI-System wesentlich spezifischer wird, der Grad seiner allgemeinen Verwendbarkeit wird erheblich reduziert. Gleichwohl hat auch ein GPAI-System noch eine Vielzahl von Verwendungen, im Gegensatz zu einem KI-System, welches nur noch eine Zweckbestimmung hat. In Anbetracht der grundlegenden Bedeutung der Abgrenzung von GPAI-Modell und GPAI-System wäre es sinnvoll, wenn die Kommission dazu bereits in der ersten Leitlinie zur praktischen Umsetzung der KI-VO Stellung beziehen würde, die auf Basis von Art. 96 Abs. 1 lit. f KI-VO im Februar 2025 zur Definition von KI herausgegeben werden soll.[11] Darüber hinaus könnte es sein, dass das Spannungsverhältnis zwischen GPAI-Modell, GPAI-System und KI-System auch im GPAI-Praxisleitfaden aufgegriffen wird, welcher gerade von den GPAI-Modell-Anbietern und der Kommission nach Art. 56 KI-VO entwickelt wird und gem. Art. 56 Abs. 9 Satz 1 KI-VO spätestens am 2.5.2025 vorliegen muss. Im ersten Entwurf des Praxisleitfadens finden ich hierzu allerdings keine Anhaltspunkte.[12]

b) Die Regulierung von GPAI-Modellen in der KI-VO

7 Die Anbieter von GPAI-Modellen unterfallen in der KI-VO einer spezifischen Regulierung.[13] Anbieter ist in diesem Zusammenhang nach der Begriffsdefinition in Art. 3 Nr. 3 KI-VO jede natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein GPAI-Modell entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt, sei es entgeltlich oder unentgeltlich. Ist der Anbieter eines GPAI-Modells, das auf dem Unionsmarkt in Verkehr gebracht werden soll, in einem Drittland niedergelassen, so hat er gem. Art. 54 Abs. 1 KI-VO zunächst einen Bevollmächtigten zu benennen. Dieser hat unter anderem zu überprüfen, ob die Pflichten der KI-VO eingehalten werden, Art. 54 Abs. 3 Satz 3 Buchst. a KI-VO.

8 GPAI-Modelle werden nach einem zweistufigen Ansatz reguliert.[14] Die Pflichten der Anbieter hängen von der Einstufung des in Frage stehenden Modells ab. So statuiert

8 Vaswani u.a., Attention is All You Need, abrufbar unter https://arxiv.org/pdf/1706.03762, S. 7.
9 Schwartmann/Keber/Zenner/Meding KI-VO, 1. Teil 4. Kap. Rn. 5 ff.
10 Vgl. etwa Bommasani u. a., On the Opportunities and Risks of Foundation Models, abrufbar unter https://arxiv.org/pdf/2108.07258.
11 Schwartmann/Zenner, Fn. 6, ab Minute 6:06.
12 First Draft General Purpose AI Code of Practice, abrufbar unter: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice
13 Zu den in den Trilog-Verhandlungen vorgeschlagenen Regulierungsansätzen vgl. Schwartmann/Köhler RDV 2024, 27 (28).

Art. 53 KI-VO Pflichten für alle Anbieter von GPAI-Modellen, während Art. 55 KI-VO besondere Pflichten für die Anbieter von GPAI-Modellen mit systemischem Risiko vorsieht. Die erforderliche Einstufung von GPAI-Modellen regelt Art. 51 KI-VO. Das Verfahren zur Einstufung orientiert sich stark an den Verfahren des Digital Services Acts[15] zur Bestimmung von „Very Large Online Platforms" und „Very Large Online Search Engines".[16] Ein systemisches Risiko ist grundsätzlich anzunehmen, wenn das GPAI-Modell Fähigkeiten mit hohem Wirkungsgrad aufweist (Abs. 1 Buchst. a) oder eine entsprechende Entscheidung der Kommission vorliegt (Abs. 1 Buchst. b). Fähigkeiten mit hohem Wirkungsgrad werden vermutet, wenn das GPAI-Modell für sein Training mindestens eine Rechenleistung von 10^25 Gleitkommaoperationen (engl.: Floating Point Operations Per Second, kurz: FLOPs) benötigt hat. Um den Grenzwert hatten das Europäische Parlament und die Mitgliedstaaten im Gesetzgebungsverfahren lange gerungen. Bei der schließlich festgelegten Zahl handelt es sich um einen politischen Kompromiss, der einer technischen Grundlage weitgehend entbehrt.[17]

9 Alle Anbieter von GPAI-Modellen müssen gem. Art. 53 Abs. 1 KI-VO Informations- und Dokumentationspflichten erfüllen. Dazu gehört insbesondere die Erstellung und Aktualisierung einer technischen Dokumentation, die mindestens die in Anhang XI KI-VO aufgeführten Informationen enthält. Nur für GPAI-Modelle mit systemischem Risiko gelten dabei die Informationspflichten, die sich aus Anhang XI Abschnitt 2 KI-VO ergeben. Eine weitere dieser Pflichten besteht etwa in der Dokumentation von Fähigkeiten und Grenzen des GPAI-Modells, um diese gegebenenfalls an Anbieter von KI-Systemen weiterzugeben, die das GPAI-Modell in ihr System integrieren wollen.[18] Die Anbieter von GPAI-Modellen mit systemischem Risiko haben darüber hinaus die spezifischen Pflichten des Art. 55 KI-VO zu erfüllen. Dazu zählen eine umfangreiche Evaluierung des GPAI-Modells, eine Untersuchung der systemischen Risiken, die Beobachtung und Dokumentation gravierender Vorfälle sowie deren Meldung an das Büro für Künstliche Intelligenz und die Gewährleistung eines adäquaten Levels an Cybersicherheit und physischer Infrastruktur.[19] Die Einhaltung der Pflichten aus Art. 55 KI-VO können die Anbieter von GPAI-Modellen, jedenfalls bis harmonisierte Normen i.S.v. Art. 40 Abs. 1 KI-VO vorliegen, auch durch eine Selbstverpflichtung in Form von den schon erwähnten Praxisleitfäden nach Art. 56 KI-VO sicherstellen, die sie gemeinsam mit dem Büro für Künstliche Intelligenz entwickeln, Art. 55 Abs. 2 Satz 1 KI-VO. So können sie die Rechtsunsicherheit verringern, der sie sich ansonsten auf der Suche nach adäquaten Maßnahmen ausgesetzt sehen.[20]

2. Fine-Tuner eines GPAI-Modells

10 GPAI-Modelle geben Wahrscheinlichkeiten wieder. Diese können in unterschiedlichen Situationen allerdings divergieren, sodass sie das gewünschte Ergebnis mal mehr und mal weniger korrekt abbilden. Ein plastisches Beispiel bilden sogenannte Teekesselchen: Die „Bank" hat in der Stadtplanung (z.B. Sitzmöglichkeit in einer Fußgängerzone) eine andere Bedeutung als im Finanzsektor, wo der Begriff einem Kreditinstitut entspricht. Damit ein GPAI-Modell die gewünschte Bedeutung eines Wortes und damit das gewünschte Ergebnis möglichst präzise ermittelt, kann es hilfreich sein, seinen Kontext bewusst auf spezifische Anwendungsszenarien zu verengen. Das technische und wirtschaftliche Bedürfnis nach einem solchen Finetuning von GPAI-Modellen hat der europäische Gesetzgeber erkannt: GPAI-Modelle können laut ErwG 97 S. 5 KI-VO „weiter geändert oder zu neuen Modellen verfeinert werden". Die Rechtslage bleibt dennoch unklar.

11 So stellt sich aus der Perspektive der KI-VO die Frage, welche Pflichten die Anbieter von derart verfeinerten GPAI-Modellen treffen und ab wann sich ein GPAI-Modell dabei in ein GPAI-System weiterentwickelt hat. Aus dem Normtext selbst ergeben sich hierzu über den ErwG 100 hinaus keine Anhaltspunkte. Unklar ist bereits, inwieweit ein verfeinertes Modell mit reduzierter Verwendbarkeit noch „eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen" (Art. 3 Nr. 63 KI-VO). Laut ErwG 109 S. 3 KI-VO sollen im Falle einer Änderung oder Feinabstimmung die Pflichten der Anbieter von GPAI-Modellen „auf diese Änderung oder Feinabstimmung beschränkt sein, indem beispielsweise die bereits vorhandene technische Dokumentation um Informationen über die Änderungen, einschließlich neuer Trainingsdatenquellen, ergänzt wird, um die in dieser Verordnung festgelegten Pflichten in der Wertschöpfungskette zu erfüllen".

12 Die in dem Erwägungsgrund geforderte Begrenzung der Anbieterpflichten ist nachvollziehbar, setzt allerdings deren grundsätzliche Geltung voraus. Da die Art. 51 ff. KI-VO ausschließlich auf die Anbieter von GPAI-Modellen anwendbar sind, müsste auch das verfeinerte GPAI-Modell mit reduzierter Verwendbarkeit der Definition des Art. 3 Nr. 63 KI-VO unterfallen. Bei einer engen Auslegung des Begriffs der allgemeinen Verwendbarkeit wäre das nicht der Fall, sodass den Anbieter eines verfeinerten GPAI-Modells mit reduzierter Verwendbarkeit keine Pflichten treffen würden. Dies entspräche analog dem Willen des EU-Gesetzgebers, welcher in der Folgenabschätzung der KI-VO[21] unterstrich,

14 Buchalik/Gehrmann CR 2024, 145 (150).
15 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277 S. 1, ber. 2022 ABl. L 310 S. 17, im Folgenden: DSA.
16 Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen KI-VO, 2. Teil, 1. Kap. Rn. 493.
17 Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen KI-VO, 2. Teil, 1. Kap. Rn. 494.
18 Ausführlich zu den Pflichten Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen, KI-VO, 2. Teil, 1. Kap. Rn. 502-509.
19 Ausführlich zu den Pflichten Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen, KI-VO, 2. Teil, 1. Kap. Rn. 497.
20 Schwartmann/Keber/Zenner/Zenner/Schwartmann/Hansen, KI-VO, 2. Teil, 1. Kap. Rn. 498.

dass die KI-VO insbesondere die Anbieter von KI-Systemen (mehrheitlich US-Unternehmen) und weniger deren Betreiber (mehrheitlich EU-Unternehmen) treffen sollte. Bei einer systematischen Auslegung der KI-VO wird dies im Rechtstext auch bei einem Vergleich der Hochrisiko-Pflichten aus Art 16 und 26 KI-VO deutlich. Auf Modellebene übertragen wären europäische Unternehmen wohl vor allem Fine-Tuner, nicht aber Anbieter der ursprünglichen GPAI-Modelle. Um dieses politische Ziel zu erreichen, könnte die Kommission sich im Rahmen der weiteren Rechtauslegung (z.B. Praxisleitfäden nach Art. 56 KI-VO oder Leitfäden nach Art 96 KI-VO) entscheiden, den Übergang von GPAI-Modell zu GPAI-System im Sinne des ErwG. 100 relativ früh zu bejahen. Im Ergebnis wäre der Fine-Tuner als Anbieter eines GPAI-Systems kaum rechtlichen Vorgaben ausgesetzt.

13 Angesichts der außergewöhnlichen Fähigkeiten neuester GPAI-Modelle und der potentiell gravierenden Regelungslücken, spricht allerdings auch viel dafür unter Verweis auf ErwG 109 S. 3 KI-VO ein weites Begriffsverständnis zugrunde zu legen und die Anwendbarkeit der Art. 51 ff. KI-VO auf verfeinerte Modelle im Grundsatz anzunehmen. Unterstützend ließe sich argumentieren, dass der Fine-Tuner die eigentliche Kontrolle über das veränderte GPAI-Modell inne hat und der vorherige Anbieter nicht länger die Hauptverantwortung tragen darf, wenn sein GPAI-Modell signifikant weiterentwickelt wurde. Es stellt sich allerdings dann die Frage, welches Maß an Veränderung des ursprünglichen Modells eigene Transparenzpflichten auslöst.[22]

14 Überzeugend erscheint daher vermittelnd, die Pflichten im Sinne des ErwG 109 S. 3 KI-VO gegen den Fine-Tuner dann gelten zu lassen, wenn die Veränderungen im Sinne des Art. 3 Nr. 23 KI-VO analog als 'wesentlich' zu betrachten sind. Selbst dann sollten sich die Pflichten aber sowohl am Maße der Veränderung als auch an den technischen Fähigkeiten und Kenntnissen des Fine-Tuners orientieren. Zu beobachten sind daher die Veröffentlichungen des GPAI-Praxisleitfadena nach Art. 56 KI-VO am 2.5.2025 bzw. der Leitfäden nach Art. 96 KI-VO. Es bleibt zu hoffen, dass die Leitfäden eine technisch korrekte Unterscheidung vornehmen und dabei auch 'wesentlich' genauer auslegen, um Rechtsunsicherheit auf dem Markt zu vermeiden.

3. Anbieter eines GPAI-Systems

15 Fügt ein Akteur zu einem GPAI-Modell weitere Komponenten hinzu, wird er, wie bereits dargestellt, zum Anbieter eines GPAI- bzw. KI-Systems, vgl. ErwG 97 S. 7 KI-VO.[23] Welche Vorschriften der KI-VO auf das so entwickelte System anzuwenden sind, hängt von den Zweckbestimmungen und deren Risikoklassifizierungen ab. Besondere Anforderungen und Pflichten gelten nur für Hochrisiko-KI-Systeme.

a) Hochriskante Zweckbestimmung durch den Anbieter

16 Entscheidend für die Risikoklassifizierung eines KI-Systems ist seine Zweckbestimmung.[24] Darunter ist entsprechend der Legaldefinition in Art. 3 Nr. 12 KI-VO die Verwendung zu verstehen, für die ein KI-System laut Anbieter bestimmt ist. Bei der Konkretisierung der Zweckbestimmung sind die besonderen Umstände und Bedingungen für die Verwendung zu berücksichtigen, wie sie sich aus den vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation ergeben. Wirbt ein Anbieter beispielsweise damit, dass sich ein KI-System besonders gut für das Sichten und Filtern von Bewerbungen eignet (vgl. Anhang III Nr. 4 Buchst. a KI-VO), handelt es sich bei dem beworbenen System regelmäßig um ein Hochrisiko-KI-System, das den Anforderungen der Art. 8 ff. KI-VO genügen muss. Der Anbieter muss die Pflichten der Art. 16 ff. KI-VO, der Betreiber die der Art. 26 f. KI-VO erfüllen. Dieser Grundsatz gilt auch für KI-Systeme, die auf GPAI-Modellen aufsetzen und bei denen die allgemeine Verwendbarkeit auf eine Zweckbestimmung reduziert wurde: Ist ein KI-System beispielsweise nach den Kategorien des Art. 3 Nr. 12 i.V.m. Art. 6 Abs. 1 und 2 KI-VO als Hochrisiko-KI-System zu klassifizieren, ändert die ursprüngliche allgemeine Verwendbarkeit des zugrundeliegenden Modells nichts an der entsprechenden Einordnung. Die Kommission hätte mit ihrem ursprünglichem Gesetzesvorschlag aus dem Jahr 2021 nur solche KI-Systeme, die eine singuläre Zweckbestimmung nach Art. 3 Nr. 12 KI-VO aufweisen, unter Anhang III subsumiert.[25] KI-Modelle bzw. -Systeme mit allgemeiner Verwendbarkeit waren konzeptionell nicht vorgesehen; ein Umstand, der mit Blick auf den KI-Markt im Jahr 2025 realitätsfern wirkt.

b) Risikoklassifizierung von GPAI-Systemen

17 Die Ko-Gesetzgeber entschieden sich daher am Ende der Trilogverhandlungen, das Konzept des GPAI-Systems im finalen Rechtstext aufzunehmen. Diese späte systematische Umstellung der KI-VO macht die Risikoklassifizierung von GPAI-Systemen äußerst komplex, auch da das restliche Gesetz nicht konsequent an die Einfügungen angepasst wurde. Daraus entstehende Unklarheiten und Regelungslücken wurden aufgrund des Zeitdrucks Ende 2023[26] bewusst in Kauf genommen.[27] So stellt sich jetzt die Frage, ob ein KI-System, das bestimmungsgemäß für eine Vielzahl von Zwecken eingesetzt werden kann, als Hochrisiko-KI-System

21 Europäische Kommission, Folgenabschätzung zur Verordnung über künstliche Intelligenz, 21.4.2021, abrufbar unter https://digital-strategy.ec.europa.eu/de/library/impact-assessment-regulation-artificial-intelligence.
22 Buchalik/Gehrmann CR 2024, 145 (153).
23 Zur Frage, welche Komponenten erforderlich sind, s.o. 1. a).
24 S.o., I.
25 Europäische Kommission, Fn. 19; Mazzini/Scalzo, The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts, 16.5.2022, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4098809.
26 Dazu Zenner RDV 2023, 340.
27 Schwartmann/Zenner, Fn. 6, ab Minute 24:39.

im Sinne der KI-VO gilt, wenn zu den denkbaren Einsatzzwecken auch hochriskante zählen.

18 In diese Richtung deutet der Wortlaut der ErwG 85 und 100 sowie des Art. 75 Abs. 2 KI-VO. Demnach müssen GPAI-Systeme, die vom Betreiber direkt für mindestens einen hochriskanten Zweck im Sinne der KI-VO verwendet werden können, den Anforderungen der KI-VO genügen. Zwar bezieht sich die Vorschrift nicht ausdrücklich auf die Anforderungen an Hochrisiko-KI-Systeme. Durch die gleichzeitige Bezugnahme auf hochriskante Zwecke wird eine solche Verbindung aber hergestellt. Bei einer strengen Auslegung der Vorschrift wäre damit jedes GPAI-System, das die Eingabe grundsätzlich offener Prompts gestattet, hochriskant, da es direkt für mindestens einen hochriskanten Zweck im Sinne der KI-VO verwendet werden kann. Betroffen wären praktisch alle GPAI-Systeme. Einem solchen Verständnis steht allerdings zunächst die Systematik der KI-VO entgegen, die an mehreren Stellen zwischen GPAI-Systemen auf der einen und Hochrisiko-KI-Systemen auf der anderen Seite differenziert, so etwa in ErwG 85 S. 1 KI-VO oder in Art. 25 Abs. 1 lit. c KI-VO. Hinzu kommt, dass dieses Verständnis dazu führen würde, dass die Anbieter von GPAI-Systemen Vorkehrungen für Einsatzzwecke treffen müssen, die sie nicht absehen können. Bei der Erfüllung der Anforderungen an Hochrisiko-KI-Systeme ist gem. Art. 8 Abs. 1 KI-VO der Zweckbestimmung des konkreten Systems Rechnung zu tragen. So soll beispielsweise sichergestellt werden, dass die Trainingsdaten geeignete statistische Merkmale für den späteren Verwendungszweck aufweisen, Art. 10 Abs. 3 Satz 2 KI-VO. Erlaubt ein KI-System eine offene Prompteingabe, ist der spätere Verwendungszweck aus Anbieterperspektive aber kaum absehbar. Der Anbieter müsste das KI-System also für Verwendungen entwickeln, die er in der Entwicklung noch nicht kennt. Eine derart enge Auslegung von Art. 75 Abs. 2 KI-VO ist also kaum praktikabel und auch die Ko-Gesetzgeber hatten sich während der Verhandlungen im Sinne der Innovation in KI explizit dagegen ausgesprochen.

c) Willkürfreier Ausschluss einer hochriskanten Verwendung

19 Eine andere Auslegung von Art. 75 Abs. 2 KI-VO ist unter Berücksichtigung der Erkenntnis möglich, dass das GPAI-System die Anforderungen an Hochrisiko-KI-Systeme nur erfüllen muss, wenn es „direkt" für mindestens einen hochriskanten Zweck im Sinne der KI-VO verwendet werden kann bzw. entwickelt worden ist. Das Tatbestandsmerkmal der direkten Verwendbarkeit dürfte als Rückkopplung an die Zweckbestimmung zu verstehen sein: Eine direkte Verwendung zu hochriskanten Zwecken ist nur möglich, wenn diese im Rahmen der Zweckbestimmung durch den Anbieter vorgesehen ist. Entscheidend sind damit die Kriterien des Art. 3 Nr. 12 KI-VO, namentlich die vom Anbieter bereitgestellten Informationen in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation. Sieht der Anbieter den Einsatz des GPAI-Systems darin zu jedem denkbaren Zweck vor, muss er auch die Verwendung zu hochriskanten Zwecken antizipieren und seine entsprechenden Pflichten erfüllen.

20 Daran anknüpfend stellt sich die Frage, ob sich der Anbieter dieser Verantwortung durch einen pauschalen Ausschluss des Einsatzes seines GPAI-Systems zu hochriskanten Zwecken entziehen kann. Dafür spricht, dass die Ko-Gesetzgeber im Dezember 2023 kurzzeitig einen neuen Artikel für GPAI-Systeme diskutierten, welcher eine solche explizite Ausschlussmöglichkeit enthielt. Aufgrund des Zeitdrucks schaffte man es allerdings nicht mehr, den Artikel rechtzeitig zum Verhandlungsschluss zu finalisieren. Einen Anknüpfungspunkt zur Möglichkeit eines Ausschlusses liefert die Rechtsprechung des BGH zur anbieterseitigen Zweckbestimmung im Medizinproduktrecht:[28] Demnach ist eine Einschränkung der Zweckbestimmung zulässig, solange sie nicht willkürlich erscheint.[29] Vor dem Hintergrund von Art. 75 Abs. 2 KI-VO und den oben angesprochenen Problemen dürfte der Ausschluss des Einsatzes eines GPAI-Systems zu hochriskanten Zwecken jedenfalls dann nicht willkürlich erscheinen, wenn der Einsatz des GPAI-Systems zu anderen Zwecken ohne Weiteres denkbar ist. Daher sollten Anbieter von GPAI-Systemen einer Verpflichtung nach Art. 16 ff. KI-VO entgehen, wenn sie Maßnahmen ergreifen, um die Verwendung zu hochriskanten Zwecken technisch auszuschließen und in den Betriebsanleitungen, im Werbe- oder Verkaufsmaterial und in diesbezüglichen Erklärungen sowie in der technischen Dokumentation keine gegenteiligen Angaben machen. Schließen die Anbieter pauschal alle Hochrisiko-Anwendungsfälle im Sinne von Ahang III aus, dürfte erforderlich sein, dass die technischen Maßnahmen sowie Erklärungen auch auf jeden im Anhang erwähnten Anwendungsfall gesondert eingehen.

4. Betreiber und Anwender eines GPAI-Systems

21 Sofern der Anbieter eines GPAI-Systems den Einsatz zu hochriskanten Zwecken willkürfrei ausschließt, gilt das System nach der hier vertretenen Ansicht nicht als Hochrisiko-KI-System im Sinne der KI-VO. Damit muss das System die Anforderungen der Art. 8 ff. KI-VO nicht erfüllen und auch die spezifischen Pflichten der Akteure im Umgang mit hochriskanter KI greifen nicht. Praktisch können GPAI-Systeme, die die Eingabe offener Prompts ermöglichen, allerdings trotzdem für hochriskante Zwecke eingesetzt werden. Deshalb stellt sich die Frage, wie die KI-VO den Betrieb eines auf Ebene des Anbieters nicht spezifisch regulierten GPAI-Systems zu hochriskanten Zwecken reguliert.

22 Als verwendenden Akteur adressiert die KI-VO den Betreiber des KI-Systems. Das ist gem. Art. 3 Nr. 4 KI-VO jede natürliche oder juristische Person, Behörde, Einrichtung oder

28 Zu diesem Vorschlag bereits Linardatos ZIP 2024, 2497 (2502 ff.); Ebers/Streitbörger RDi 2024, 393 Rn. 11.

29 BGH 18.4.2013 – I ZR 53/09, Rn. 12, NJW-RR 2014, 46.

sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Von der Betreiberrolle ausgenommen ist der Anwender, der das KI-System im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet. Unternehmen sind auch dann Betreiber im Sinne der KI-VO, wenn sie ein GPAI-System nicht lizenzieren, dessen Einsatz mit privaten Accounts aber dulden oder gar genehmigen. Die Verantwortlichkeit des Arbeitgebers für private, aber geduldete oder gebilligte Arbeitsmittel ist im deutschen Recht aus § 5 Abs. 4 BetrSichV bekannt.[30] Dessen Gedanke lässt sich auf die KI-VO übertragen: Lässt ein Unternehmen den Einsatz eines KI-Systems zu beruflichen Zwecken zu, hat es für die Erfüllung der Pflichten aus der KI-VO auch dann einzustehen, wenn der Einsatz ausschließlich auf privaten Lizenzen beruht.

a) Die Zweckänderung im Sinne von Art. 25 Abs. 1 lit. c KI-VO

23 Originär treffen den Betreiber eines GPAI-Systems keine besonderen Pflichten aus der KI-VO. Ob der Einsatz eines GPAI-Systems zu hochriskanten Zwecken damit auch ohne Beachtung der Vorgaben für Hochrisiko-KI-Systeme zulässig ist, hängt von der Auslegung des Art. 25 Abs. 1 lit. c KI-VO ab. Die Vorschrift besagt, dass Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KI-Systems gelten und den Anbieterpflichten gem. Art. 16 KI-VO unterliegen, „wenn sie die Zweckbestimmung eines KI-Systems, einschließlich eines GPAI-Systems, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Art. 6 KI-VO wird". Unklar ist, wie der Begriff der Zweckänderung zu verstehen ist. Der Wortlaut der Vorschrift lässt grundsätzlich zwei Auslegungen zu: Entweder ist eine Zweckänderung mit jedem Prompt möglich oder es ist eine technische oder organisatorische Limitierung des GPAI-Systems auf einen hochriskanten Zweck erforderlich. Ausdrücklich verlangt Art. 25 Abs. 1 lit. c KI-VO eine Änderung der Zweckbestimmung. Es scheint daher naheliegend für die Qualifikation einer Zweckänderung auf die Kategorien des Art. 3 Nr. 12 KI-VO zurückzugreifen. Dieser Ansatz erweist sich allerdings schnell als untauglich, da der Betreiber typischerweise weder Betriebsanleitungen noch Werbe- oder Verkaufsmaterial oder eine technische Dokumentation erstellt. Daher ist eine eigenständige Auslegung des Begriffs zu vorzunehmen.

24 So ließe sich vertreten, dass die Zweckbestimmung des Anbieters in den aufgezeigten Willkürgrenzen maßgeblich bleibt, auch wenn die Eingabedaten des Betreibers auf eine Verwendung zu hochriskanten Zwecken schließen lassen. Eine Änderung der Risikoklassifizierung gem. Art. 25 Abs. 1 lit. c KI-VO käme demnach nur in Betracht, wenn der Betreiber die Eigenschaften und Parameter des GPAI-Systems verändert, indem er in die Architektur oder in den Programmcode eingreift. Eine derart enge Auslegung des Begriffs der Zweckänderung mag zwar ökonomische Vorteile mit sich bringen, hinterlässt aber eine beachtliche Regelungslücke: Die Vorgaben der KI-VO zu Hochrisiko-KI-Systemen ließen sich umgehen, indem hochriskante Zwecke mit GPAI-Systemen verfolgt werden. Diese Regelungslücke würde durch eine weite Auslegung des Begriffs der allgemeinen Verwendbarkeit weiter verschärft.[31] Zur Schließung der Lücke kann der Verweis auf die Rechtspflicht aus Art. 26 Abs. 4 KI-VO nicht ausreichen. Demnach sind die Betreiber von Hochrisiko-KI-Systemen verpflichtet, dafür zu sorgen, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind. Für eine Ausweitung des Adressatenkreises der Norm auf die Betreiber von GPAI-Systemen bietet der Wortlaut der KI-VO keine Anhaltspunkte.[32]

25 Art. 25 Abs. 1 lit. c KI-VO ließe sich nach dem Gesagten auch dahingehend auslegen, dass eine Änderung der Zweckbestimmung mit jedem Prompt vorgenommen werden kann.[33] Hiergegen spricht allerdings bereits die fehlende Reversibilität des Rollenwechsels. Gilt ein Betreiber gem. Art. 25 Abs. 1 lit. c KI-VO einmal als Anbieter eines Hochrisiko-KI-Systems, bleibt er in dieser Rolle, auch wenn das GPAI-System im Anschluss an den Rollenwechsel nur noch für Zwecke ohne hohes Risiko verwendet wird.[34] Auch die Konzeption des Art. 25 Abs. 2 KI-VO spricht gegen einen Rollenwechsel durch einfachen Prompt.[35]

26 Bei der Bestimmung der Voraussetzungen einer Zweckänderung ist zu berücksichtigen, dass der Gesetzgeber die Zweckänderung als Unterfall der in Art. 25 Abs. 1 lit. b KI-VO adressierten 'wesentlichen Veränderung' eines KI-Systems verstanden hatte, wenn auch insbesondere für solche, die bisher kein hohes Risiko bergen.[36] Dieses Verständnis kommt weiterhin in der Begriffsbestimmung der „wesentlichen Veränderung" in Art. 3 Nr. 23 KI-VO und hier vor allem in der zweiten Fallgruppe zum Ausdruck. Unter Berücksichtigung der vorstehenden teleologischen und systematischen Erwägungen scheint es gerechtfertigt, eine Zweckänderung im Sinne von Art. 25 Abs. 1 lit. c KI-VO anzunehmen, wenn die Eingabedaten ein Maß an Komplexität aufweisen, das eine Konkretisierung des GPAI-Systems im Sinne einer wesentlichen Veränderung hervorruft.

27 Der Wechsel in die Anbieterrolle befreit nicht von der Einhaltung der Betreiberpflichten. Vielmehr sind Anbieter- und Betreiberpflichten im Falle einer Zweckänderung im Sinne von Art. 25 Abs. 1 lit. c kumulativ zu erfüllen. Das gilt ausnahmsweise nicht, wenn der Einsatz des GPAI-Systems entsprechend den Vorgaben des Art. 6 Abs. 3 KI-VO erfolgt und die Entscheidungsfindung daher nicht wesentlich be-

30 Vgl. Kollmer/Klindt/Schucht/Wink, 4. Aufl. 2021, BetrSichV § 5 Rn. 3. Zur Qualifikation von KI-Systemen als Arbeitsmittel vgl. ArbG Hamburg, 16.1.2024 – 24 BVGa 1/24, Rn. 25, ZD 2024, 354.
31 S.o., 2.
32 So aber Linardatos ZIP 2024, 2497 (2503).
33 Ebers/Streitbörger RDi 2024, 393 (399); Borges CR 2024, 565 (573).
34 Linardatos ZIP 2024, 2497 (2505).
35 Dazu ausführlich Linardatos ZIP 2024, 2497 (2503 f.).
36 Vgl. Martini/Wendehorst/Gössl, 2024, KI-VO, Art. 25 Rn. 21 f.

einflusst. Art. 25 Abs. 1 lit. c KI-VO verweist ausdrücklich auf den gesamten Art. 6 KI-VO und damit auch auf die Ausnahmevorschrift des Abs. 3.

b) Exkulpation des Betreibers

28 Anknüpfend an die hier vertretene Auslegung von Art. 25 Abs. 1 lit. c KI-VO stellt sich die Frage, ob der Betreiber eines GPAI-Systems auch dann als Anbieter eines Hochrisiko-KI-Systems gilt, wenn ein Mitarbeiter das bereitgestellte GPAI-System im Sinne einer wesentlichen Veränderung zu hochriskanten Zwecken einsetzt. Dogmatisch ist dabei zu berücksichtigen, dass Art. 25 Abs. 1 KI-VO unter anderem zwischen dem „Betreiber" und dem „sonstigen Dritten" differenziert, sodass es sich bei dem sonstigen Dritten um eine Person handeln muss, deren Verhalten dem Betreiber nicht zugerechnet werden kann. Dass es sich bei dem sonstigen Dritten nicht lediglich um einen privaten Nutzer handeln kann, verdeutlicht Art. 2 Abs. 10 KI-VO, der die Anwendung der KI-VO auf die Verwendung im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit ausschließt.

29 Hinsichtlich der Zurechnung des Verhaltens eines Mitarbeiters könnte daher auf die Exkulpationsregeln zurückzugreifen sein, wie sie sich aus der Rechtsprechung des EuGH zu Art. 82 Abs. 3 DS-GVO ergeben.[37] Bei analoger Anwendung dieser Rechtsprechung ist für eine Exkulpation grundsätzlich erforderlich, aber allein nicht ausreichend, dass der Betreiber den ihm unterstellten Personen, die Zugriff auf das betriebene GPAI-System haben, Weisungen erteilt hat. Darüber hinaus dürften technisch-organisatorische Maßnahmen erforderlich sein, um die Einhaltung dieser Weisungen zu überwachen.

III. Fazit

30 1. Die Abgrenzung zwischen GPAI-Modell und GPAI-System ist von großer Relevanz für die Geltung der Anforderungen und Pflichten der KI-VO. Trotzdem ist sie in der KI-VO nicht ausdrücklich geregelt und wirft Fragen auf. Es ist auf eine Konkretisierung in der ersten Leitlinie zur praktischen Umsetzung der KI-VO oder in dem GPAI-Praxisleitfaden zu hoffen.

2. Das Fine-Tuning eines GPAI-Models kann bei Hinzufügung weiterer Komponenten zur Erschaffung eines GPAI-Systems führen, welches durch die KI-VO kaum direkt mit Verpflichtungen adressiert wird. Davon unabhängig können für den Fine-Tuner aber Pflichten aus ErwG 109 S. 3 KI-VO entstehen.
3. Ein GPAI-System wird zwar nicht direkt reguliert, muss grundsätzlich aber die Anforderungen der KI-VO an Hochrisiko-KI-Systeme erfüllen, wenn es direkt hierfür eingesetzt werden kann. Der Anbieter eines GPAI-Systems kann den Einsatz zu hochriskanten Zwecken ausschließen, sofern der Ausschluss nicht willkürlich erfolgt.
4. Die Zweckbestimmung eines GPAI-Systems kann durch seine Verwendung im Sinne von Art. 25 Abs. 1 lit. c KI-VO vom Betreiber geändert und dieser dadurch zum Anbieter eines Hochrisiko-KI-Systems werden, wenn der bisherige Anbieter des GPAI-Systems die hochriskante Verwendung willkürfrei ausgeschlossen hat und die Änderung vom Betreiber wesentlich war. Eine wesentliche Veränderung kann grundsätzlich auch durch einen Prompt erreicht werden, sofern dieser Prompt ein hinreichendes Maß an Komplexität und Konkretisierung aufweist.
5. Der Betreiber wird nicht per Zweckänderung eines Mitarbeiters zum Anbieter eines Hochrisiko-KI-Systems, wenn er seinen Mitarbeitern den Einsatz zu hochriskanten Zwecken untersagt und die Einhaltung dieser Vorgabe im Rahmen seiner Möglichkeiten überwacht hat (vgl. Exkulpationsregeln im Rahmen der DS-GVO).
6. Hat sich der Betreiber erfolgreich exkulpiert, kann der Mitarbeiter als sonstiger Dritter in die Anbieterrolle rutschen, wenn er sich entgegen den Vorgaben dazu entschließt, ein zur Verfügung gestelltes GPAI-System zu hochriskanten Zwecken einzusetzen und eine wesentliche Änderung vornimmt (z.B. umfangreicher Prompt, der Schutzmaßnahmen des GPAI-Anbieters und des Betreibers aushebelt).

37 EuGH 11.4.2024 – C-741/21, Rn. 52, ZD 2024, 381 (383).

Tristan Rohner*

Datenherrschaft: Property Rights im Data Act

Der Data Act wird versuchen, die Datenherrschaft der bisherigen Dateninhaber aufzubrechen. Effiziente Datennutzung und Zugang zu Daten sind die zentralen Ziele der Verordnung. Eine Analyse der Regelungen unter Zuhilfenahme der Property Rights Theory zeigt, dass diese Ziele nur teilweise erreicht werden. Der Datenherrschaft der Inhaber werden Rechtspositionen der Nutzer entgegengesetzt. Diese sind allerdings zersplittert und können zu hohen Transaktionskosten führen, die ein Hindernis für die effiziente Datennutzung darstellen. Zugangssuchende Dritte erhalten keinen eigenen Zugangsanspruch. Es fehlt an Zugangsregeln. Diese Defizite können im Rahmen sektorspezifischer Regeln sowie bei der Auslegung unbestimmter Rechtsbegriffe und Generalklauseln berücksichtigt werden.

A. Datenherrschaft

1 Der ab dem 12. September 2025 geltende Data Act[1] wird die Datenherrschaft der bisherigen Dateninhaber von Industriedaten in Frage stellen. Die Daten[2] aus einer Fabrik 4.0, in der die Maschinen mit Sensoren ausgestattet sind und miteinander kommunizieren, beinhalten eine Vielzahl von Informationen. Diese betreffen beispielsweise Stückzahlen, Fehlerquote, Abnutzung, Wartezeiten, Temperatur und Energieverbrauch. In Deutschland ist der Markt in diesem Internet of Things 2024 auf ein Volumen von ca. 30 Mrd. € gewachsen, in der Europäischen Union sind es 177 Mrd. €.[3] In Deutschland dominiert das Industrial Internet of Things mit ungefähr einem Drittel des Marktvolumens.[4] Daneben besteht aber auch eine Vielzahl von Anwendungen außerhalb der Industrie, wie beispielsweise Sprachassistenten und Haushaltsgeräte.

2 In der Fabrik 4.0 hat das Unternehmen, das die Fabrik betreibt, die Maschinen erworben hat und zur Produktion nutzt, nicht immer uneingeschränkten Zugriff auf diese Daten. Es könnte die Daten aber nutzen, um die Wartung zu verbessern, neue Produkte zu entwickeln oder an andere Dienstleister weiterzugeben. Stattdessen sind die Unternehmen Dateninhaber, die die Maschine und die damit verbundene Software hergestellt haben. Sie profitieren von der tatsächlichen Zugriffs- und Nutzungsmöglichkeit, die sie sich durch die technische Gestaltung ihrer Produkte sichern können. Vertragliche Klauseln sichern Zugriff- und Nutzungsmöglichkeiten der Dateninhaber weiter ab.[5]

3 Diese Datenherrschaft[6] verhindert den Zugang zu diesen Daten, Wettbewerb, Innovation und eine effiziente Datennutzung. Nutzer und Dritte erhalten nur Zugang zu den Daten, wenn die Inhaber sie freiwillig herausgeben. Diese können ihre datengestützten Wettbewerbsvorteile ausnutzen. Nutzer und Dritte können die Daten selbst nicht nutzen, um Produktionsprozesse zu optimieren, bessere Produkte herzustellen oder Aftermarket-Leistungen wie Wartung und Reparatur anzubieten. Das verhindert Wettbewerb und Innovation. Das große wirtschaftliche Potential der Daten bleibt ungenutzt. Der Data Act hat sich zum Ziel gesetzt, diese Probleme zu adressieren. Es stellt sich deswegen folgende Forschungsfrage:

4 Kann der Data Act die Ziele der effizienten Datennutzung und des Datenzugangs erreichen?

5 Methodisch wird nach einer kurzen Darstellung seiner Ziele und Regelungen (dazu B.) der Data Act mit den Analysewerkzeugen der Property Rights Theory (dazu C.) daraufhin untersucht, ob er die selbst gesteckten Ziele erreicht (dazu D.). Die Erkenntnisse und mögliche Defizite können dann im Rahmen der Konkretisierung und Auslegung des Rechts berücksichtigt werden (dazu E.). Der Beitrag schließt mit einem Ausblick und Fazit (dazu F.) Im Ergebnis wird gezeigt, dass der Data Act Property Rights der Nutzer enthält, die zwar die faktischen Property Rights der Inhaber abschwächen, aber selbst Transaktionskosten erhöhen und den Zugang Dritter hindern. Die Defizite sollten Anlass sein für sektorspezifische Regeln und können im Rahmen der Auslegung und Klauselkontrolle teilweise korrigiert werden.

B. Der Data Act

6 Der Data Act regelt die Beziehungen zwischen Dateninhabern, Nutzern und zugangssuchenden Dritten. Dies soll den Zugang zu Daten ermöglichen und eine optimale Datenverteilung unter Aufrechterhaltung der Innovationsanreize erreichen.

I. Ziele

7 Der Data Act umfasst verschiedene Regelungskomplexe.[7] Aus den Erwägungsgründen kann abgeleitet werden, dass die Regelungen insbesondere die Art. 3 ff. DA primär der

* Prof. Dr. Tristan Rohner ist Juniorprofessor für Bürgerliches Recht und Wirtschaftsrecht in der digitalen Gesellschaft an der Bucerius Law School in Hamburg.

1 Auch „Datenverordnung“ (zitiert als „DA“), Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828.

2 Umfassend zum Datenbegriff Zech, Information als Schutzgegenstand, 2012, 32, 55 ff.

3 Statista, Market Insights Internet der Dinge, abrufbar unter: https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland und https://www.statista.com/outlook/tmo/internet-of-things/europe.

4 Statista, Market Insights Internet der Dinge, abrufbar unter: https://de.statista.com/outlook/tmo/internet-der-dinge/deutschland.

5 Vgl. Zech in Sattler/Zech, The Data Act: First Assessments, 2024, S. 57.

6 Umfassend dazu Deuring, Datenmacht, 2021; Becker FS Fezer, 2016, 815 (824); vgl. Zech CR 2015, 137 (145); Hofmann in Pertot, Rechte an Daten, 2020, S. 30 f.

7 Im Überblick Hennemann/Steinrötter NJW 2024, 1.

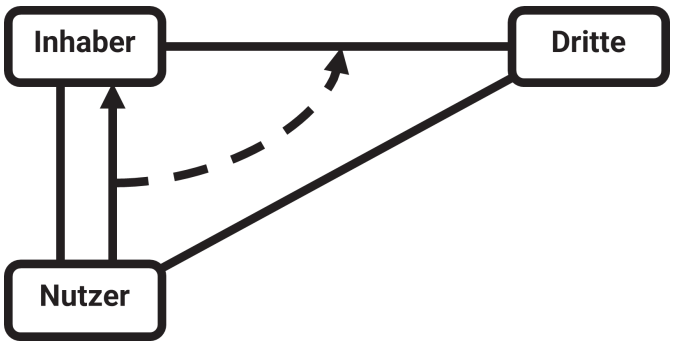
optimalen Datenverteilung und Aufrechterhaltung der Innovationsanreize und des Datenzugangs dienen.

8 Eine optimale Datenverteilung wird einleitend als wichtiges Ziel der Regelungen deklariert.[8] Die fehlende Weitergabe der Daten durch die Dateninhaber wird als Grund für eine gesamtgesellschaftliche suboptimale Allokation der Daten gesehen. Diese statische Allokationseffizienz wird um eine dynamische Komponente, die Innovationseffizienz, ergänzt.[9] Es sollen auch weiterhin neue innovative Produkte entwickelt und Anreize für Investitionen in vernetzte Produkte und deren Entwicklung aufrechterhalten werden.

9 Als zentrales Problem wird die Datenherrschaft der Inhaber angeführt, die als einzige Akteure die Daten kontrollieren.[10] Diese soll aufgebrochen werden, indem die Nutzer eines vernetzten Produkts zeitnah auf die Daten zugreifen können, die sie selbst durch die Nutzung generieren.[11] Gleichzeitig sollen sie befähigt werden, diese Daten auch an Dritte weiterzugeben. Sie sollen den Nutzen aus den Daten ziehen.[12]

II. Regelungsansatz

10 Zentrales Regelungsinstrument zum Erreichen dieser Ziele ist die Regelung der Beziehungen zwischen Dateninhaber, Nutzer und Dritten.[13] Im Mittelpunkt stehen dabei die Nutzer, die maßgeblich über die Datenerhebung, Datennutzung und Datenweitergabe bestimmen können sollen. Nutzer sind nach Art. 2 Nr. 12 DA die Personen, die vernetzte Produkte und verbundene Dienste in Anspruch nehmen.



11 Der Data Act wählt damit bewusst einen relativen Regelungsansatz.[14] Zwischen Dateninhaber und Nutzer sind die Modalitäten der Datenerhebung und Datennutzung geregelt. Möchten Nutzer die Daten weitergeben, können Sie mit interessierten Dritten Weitergabevereinbarungen abschließen. Erfolgt die Weitergabe direkt durch die Inhaber, die den direkten Zugriff auf diese haben, müssen diese auf Veranlassung des Nutzers mit den Dritten einen Vertrag schließen, in dem die Modalitäten der Datenweitergabe geregelt sind.

III. Verhältnis zur DS-GVO

12 Der Data Act betrifft alle Arten von Daten und somit auch personenbezogene Daten nach Art. 4 Nr. 1 DS-GVO. Die DS-GVO soll gem. Art. 1 Abs. 5 Satz 1 DA nicht eingeschränkt werden und bleibt parallel anwendbar.[15] Die DS-GVO enthält oftmals strengere Vorgaben, ändert aber an den Grundzügen des dargestellten Regelungsansatzes zumindest dann nichts, wenn es um die Daten der Nutzer geht und nicht um Daten anderer Personen. In den meisten Fällen werden die Nutzer auch betroffene Person i.S.v. Art. 4 Nr. 1 DS-GVO sein und die Inhaber Verantwortliche nach Art. 4 Nr. 7 DS-GVO. Dann ergänzt der Data Act gem. Art. 1 Abs 5 Satz 2 die DS-GVO. Wenn allerdings die datenschutzrechtlichen Betroffenen nicht auch Nutzer im Sinne des Data Acts sind, divergieren die Regelungen und die der DS-GVO genießen gem. Art. 1 Abs. 5 Satz 3 DA Vorrang.

C. Die Property Rights Theory

13 Die Property Rights Theory ermöglicht als Analysewerkzeug eine Untersuchung des Data Acts darauf, welche Art von Verfügungsrechten dieser enthält und welche Wirkungen diese haben.

I. Methodische Einbettung

14 Die Property Rights Theory ist ein Teilgebiet der Ökonomischen Analyse des Rechts (oder „Law and Economics"). Die Ursprünge werden auf Ronald Coase und seinen Beitrag „The Problem of Social Cost" zurückgeführt.[16] Hierin beschreibt Coase, dass bei Abwesenheit von Transaktionskosten klar definierte Verfügungsrechte zu einer optimalen Ressourcenallokation führen, unabhängig davon, wem sie zunächst zugewiesen werden. Seitdem hat sich die Property Rights Theory beständig weiterentwickelt. Wegweisende Beiträge stammen nicht nur von Coase, sondern auch von Arrow[17], Demsetz[18], Calabresi/Melamed[19] und Ostrom[20].

15 Die Property Rights Theory beschreibt und dekonstruiert Rechtpositionen an Ressourcen und untersucht, wie diese zugewiesen und ausgestaltet werden sollten, um effiziente Ergebnisse zu erzielen. Sie kann also zwei Zwecke erfüllen. Zunächst ist sie ein Analysewerkzeug, um bestehende Rechtpositionen genauer zu beschreiben. Dabei fungiert

8 ErwGr 2, umfassend Podszun/Offergeld, The EU Data Act and the Access to Secondary Markets, 2022.
9 ErwGr 32, vgl. Schweitzer/Metzger GRUR Int. 2023, 337.
10 ErwGr 3.
11 ErwGr 5.
12 ErwGr 18.
13 Vgl. Schmidt-Kessel MMR 2024, 75; Schreiber/Pommerening/Schoel, Der neue Data Act, 2024, S. 40 ff.; Hartmann/McGuire/SchulteNölke RDi 2023, 49.
14 Grundlegend zur Regulierung der Datenwirtschaft durch Verträge: Wunner, Ein regulatives Vertragsrecht für die Datenwirtschaft, 2022, S. 44 ff.; Grünberger in Bundesministerium der Justiz und für Verbraucherschutz/Max-Planck-Institut für Innovation und Wettbewerb, Data Access, Consumer Interests and Public Welfare, 2021, S. 255.
15 Umfassend Steinrötter, GRUR 2023, 216 (216 ff.); Sattler in Sattler/Zech, The Data Act: First Assessments, 2024, S. 103; Richter MMR 2023, 163.
16 Coase, Journal of Law and Economics, 1960, 1.
17 Arrow in National Bureau of Economic Research, The Rate and Direction of Inventive Activity, 1962, S. 609.
18 Demsetz The American Economic Review 1967, 347.
19 Calabresi/Melamed Harvard Law Review 1972, 1089.
20 Ostrom, Governing the Commons, 1990.

sie rein deskriptiv. Sie kann aber auch untersuchen, wie Rechtspositionen zum Erreichen verschiedener Ziele eingesetzt werden können und wie diese zur optimalen Zielerreichung ausgestaltet und zugewiesen werden sollten. Dieser Ansatz beschreibt nicht nur bestehende Regelungen, sondern kann die Regelsetzung informieren. Beide Ansätze lassen sich für eine juristische Untersuchung methodisch fruchtbar machen. Der deskriptive Ansatz unterstützt dabei, bestehende Gesetze zielgerichtet und intersubjektiv nachvollziehbar daraufhin zu untersuchen, welche Arten von Befugnissen Rechteinhabern eingeräumt werden und welchen Zielen diese dienen können. Der normative Ansatz ermöglicht die Bewertung bestehender Gesetze im Hinblick auf die Erreichung primär ökonomischer Ziele und kann bei Setzung neuer Regeln herangezogen werden.

II. Bündel von Rechten

16 Die Property Rights Theory als deskriptives Analysewerkzeug betrachtet Ressourcen und fragt danach, welche Rechtspositionen an diesen bestehen.[21] Wichtige Voraussetzung ist dabei die Erkenntnis, dass Property Rights aus einem Bündel von Rechten bestehen, die untersucht werden müssen.[22] So ist beispielsweise das Eigentum darüber zu definieren, welche Rechte es (nicht) enthält. Das Eigentum ist ein umfassendes Property Right, da es bezogen auf eine Sache als Ressource eine Vielzahl aller denkbaren Rechte umfasst.[23] Die Rechte lassen sich in verschiedene Gruppen einteilen: die Nutzung der Sache, die Fruchtziehung und der Verbrauch.[24] Nach einer ökonomischen Lesart umfasst der Verbrauch dabei nicht nur die Zerstörung und Aufgabe, sondern auch die Übertragung der Ressource. Die Property Rights Theory führt zu einer differenzierten Analyse, die genau die einzelnen zugewiesenen Rechte in den Blick nimmt. Property Rights bestehen auch, wenn rechtlich nur einzelne Rechtspositionen zugewiesen werden, ohne dass diese unter einem einheitlichen Recht zusammengefasst werden.

17 Die einzelnen Rechtspositionen müssen keine absolute Wirkung haben. Auch relative Rechte werden einbezogen. Das ist deswegen konsequent, da die Wirkungsweise der Rechte und nicht die juristische Konstruktion im Vordergrund steht. Ein relatives Recht kann faktisch ähnliche Wirkungen entfalten wie ein absolutes Recht. Die Property Rights Theory geht noch einen Schritt weiter und bezieht auch rein tatsächliche Machtpositionen in die Analyse ein.[25] Selbst wenn weder ein absolutes noch ein relatives Recht an einer Ressource besteht, kann die tatsächliche Position ähnliche Wirkungen entfalten. Demnach lässt sich aus ökonomischer Sicht in missverständlicher Weise auch von Property Rights sprechen, wenn gar keine Rechte existieren.[26] Im Ergebnis liefert die Property Rights Theory damit ein Analysetool, das einer juristischen Analyse eng verwandt ist, diese aber weiter ausdifferenziert und ergänzt.

III. Zielerreichung

18 Die Property Rights Theory ermöglicht ebenfalls eine Analyse, welche Ziele durch einzelne Rechtspositionen erreicht werden.[27] Der Data Act setzt sich selbst das Ziel einer optimalen Datenverteilung unter Aufrechterhaltung von Innovationsanreizen. Dies ist in Form von statischer und dynamischer Effizienz Teil des klassischen Untersuchungsgegenstands der Property Rights Theory.

19 Ausgangspunkt der Property Rights Theory ist dabei, dass möglichst umfassende und klar definierte Verfügungsrechte bei niedrigen Transaktionskosten zu einer effizienten Ressourcenallokation führen, indem sie Ressourcen handelbar machen und damit über den Preismechanismus am Markt eine optimale Verteilung herbeiführen. Auch bei nicht-rivalen Gütern wie Daten können Property Rights nötig sein, um den Handel überhaupt zu ermöglichen.[28] Daneben können Property Rights auch Innovation fördern. Dem liegt der Gedanke zu Grunde, dass kein Anreiz besteht, Güter bereitzustellen, wenn diese von anderen Personen genutzt werden können. Wenn diese Güter trotzdem privatwirtschaftlich bereitgestellt werden sollen, können Verfügungsrechte als Form künstlicher Verknappung einen entsprechenden Anreiz setzen.[29] Die Person, die die Daten sammelt, kann das Verfügungsrecht nutzen oder vermarkten und so Kosten kompensieren.

D. Property Rights im Data Act

20 Die Analyse zeigt, dass der Data Act einem faktischen Property Right der Inhaber Property Rights der Nutzer entgegensetzt. Die gesetzten Ziele kann dieser Regelungsansatz allerdings nur teilweise erreichen.

I. Ausgangslage

21 Die Property Rights Theory hilft dabei die Ausgangslage besser zu beschreiben, auf die der Regelungsansatz des Data Acts trifft. Die Rechteinhaber haben aufgrund technischer und vertraglich abgesicherter Zugriffsmöglichleiten auf die Daten ein faktisches Property Right an diesen. Sie können – auch ohne entsprechende Rechtsposition – allein über die Daten verfügen und andere von der Nutzung ausschließen. Dies kann in den Wirkungen der Position eines Rechteinhabers gleichkommen.[30] Diese Situation ist ineffizient. Es besteht zumindest ein starker Anreiz der In-

21 Zech in Sattler/Zech, The Data Act: First Assessments, 2024, S. 54.
22 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 5.
23 Vgl. zur daraus resultierenden „Stufenleiter der Güterzuordnung“: Zech, Information als Schutzgegenstand, 2012, S. 85 ff.
24 Diese Kategorien werden uneinheitlich verwendet.
25 Barzel/Allen, Economic Analysis of Property Rights, 3. Auflage 2023, S. 15 ff.
26 Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 23; Skaperdas, The American Economic Review, 1992, 720.
27 Spezifisch zu Rechten an Daten vgl. Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 25 ff.; Kerber GRUR Int. 2016, 989.
28 Vgl. grundlegend Arrow in National Bureau of Economic Research, The Rate and Direction of Inventive Activity, 1962, S. 609; Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 36 ff.; Zech in Sattler/Zech, The Data Act: First Assessments, S. 54 ff.
29 Grundlegend Arrow in National Bureau of Economic Research, The Rate and Direction of Inventive Activity, 1962, S. 609.
30 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 6 f.

haber, die Daten zu sammeln. Die Daten werden aber nicht optimal allokiert. Die Inhaber werden die Daten nicht offenlegen, da sie dann von allen genutzt werden könnten. Wettbewerb und Innovation bleiben auf der Strecke.[31]

22 Diese Situation ist ebenfalls zugangsfeindlich. Das faktische Property Right ermöglicht nicht den Ausgleich zwischen den Interessen der Rechteinhaber und der Zugangssuchenden. Dies würde eine Zugangsregel[32] voraussetzen, die bei dem faktischen Property Right fehlt.

II. Der Data Act

23 Dem setzt der Data Act ein System der Verfügungsrechte in Form eines Property Rights der Nutzer entgegen. Dieses ergibt sich als Bündel aus mehreren im Data Act verankerten Rechten.

1. Nutzung

24 Die Nutzung der Daten wird durch den Data Act entgegen der faktischen Kontrolle der Inhaber weitgehend dem Nutzer des vernetzten Produkts zugewiesen. Dies geschieht über die Zugangsregeln in Art. 3 Abs. 1 DA, Art. 4 Abs. 1 DA und die Ausschlussmöglichkeit des Dateninhabers nach Art. 4 Abs. 13 DA. Der Nutzer erhält entweder durch die nach Art. 3 Abs. 1 DA vorgegebene technische Gestaltung des Produkts Zugang zu den Daten („access by design") oder kann Zugang vom Dateninhaber nach Art. 4 Abs. 1 DA verlangen. Eine maßgebliche Ausnahme findet sich in Art. 4 Abs. 10 Alt. 1 DA. Danach umfasst das Recht zur Nutzung nicht die Entwicklung eines vernetzten Produkts, das mit dem genutzten Produkt im Wettbewerb steht. Weitere eher partielle Ausnahmen betreffen beispielsweise die Weitergabe von Geschäftsgeheimnissen in Art. 4 Abs. 6 DA und Daten über die wirtschaftliche Lage, die Vermögenswerte und die Produktionsmethoden des Dateninhabers in Art. 4 Abs. 10 Alt. 2 DA.[33]

25 Das Recht ist gegenüber den Dateninhabern auch exklusiv, da dieser nach Art. 4 Abs. 13 DA die ohne Weiteres verfügbaren nicht-personenbezogenen Daten nur auf der Grundlage eines Vertrags mit dem Nutzer nutzen und nach Art. 14 DA nicht-personenbezogene Produktdaten auch nur auf dieser Grundlage an Dritte herausgeben darf. Dritte, die so Daten erhalten, dürfen diese nach Art. 6 Abs. 1 DA nur auf Grundlage einer Vereinbarung mit dem Nutzer verarbeiten.

2. Früchte

26 Der Data Act weist dem Nutzer damit auch das Recht zur Fruchtziehung zu. Während die Property Rights Theory zwischen Nutzung und Fruchtziehung differenziert, umfasst die Nutzung nach dem Data Act auch die Fruchtziehung. Das wichtigste Fruchtziehungsrecht ist die Möglichkeit der „user innovation". Die Nutzer dürfen auf Grundlage der Daten neue Produkte und Dienstleistungen entwickeln und anbieten. Dieses ergibt sich schon aus einem Umkehrschluss aus Art. 4 Abs. 10 DA, in dem das Recht wiederum seine Grenze findet.

3. Übertragung

27 Zuletzt ist dem Nutzer auch das Recht zur Übertragung der Daten an Dritte zugewiesen. Soweit die Daten den Nutzern aufgrund des Zugangs nach Art. 3 Abs. 1 DA und Art. 4 Abs. 1 DA schon vorliegen, können sie diese einfach an Dritte weitergeben. Deutlich relevanter dürfte aber der Anspruch der Nutzer gegen die Inhaber auf Weitergabe der Daten an Dritte gem. Art. 5 Abs. 1 DA sein, wenn nur die Inhaber über die Infrastruktur zur Speicherung und Weitergabe verfügen. Für die Datenwirtschaft und die effiziente Datenallokation ist dieses Recht zentral. Es erfährt jedoch eine Reihe von Einschränkungen. Die Bereitstellung erfolgt zwar für den Nutzer unentgeltlich, mit dem Dritten schließt der Inhaber allerdings einen separaten Übertragungsvertrag und wird versuchen, in diesem ein möglichst hohes Entgelt für die Daten zu erzielen. Der Data Act enthält deswegen Vorgaben, welchen Inhalt dieser Vertrag haben darf und legt in Art. 8 Abs. 1 DA fest, dass die Bereitstellung zu FRAND-Bedingungen erfolgen soll und präzisiert dies für die Gegenleistung in Art. 9 DA, die auf Grundlage der Kosten und Investitionen des Dateninhabers verhandelt werden soll. Lediglich gegenüber kleinen und mittleren Unternehmen und gemeinnützigen Forschungseinrichtungen darf die Gegenleistung die Kosten des Dateninhabers nicht übersteigen.

28 Trotz der Vorgaben in Art. 8 und 9 DA schränkt die Notwendigkeit eines Vertrages zwischen Dateninhaber und Dritten die Übertragungsmöglichkeiten der Nutzer erheblich ein. Die Inhaber haben ein geringes Interesse daran, Dritten Zugang zu den Daten zu gewähren.[34] Sie verlieren ihre Herrschaftsstellung über die Daten und die damit verbundenen exklusiven Nutzungsmöglichkeiten und den Wettbewerbsvorteil auf nachgelagerten Märkten. Hinzu kommt, dass das FRAND-Kriterium schwer anzuwenden und zu überprüfen ist.[35] Damit geht eine hohe Unsicherheit der zugangssuchenden Dritten einher. Dies zeigt schon die langanhaltende Diskussion dazu im Immaterialgüterrecht.[36] Damit sind Dateninhaber in einer Position, den Zugang Dritter zumindest zu verzögern, zu erschweren oder ganz zu vereiteln. Das schränkt die Übertragungsmöglichkeit der Nutzer erheblich ein, wenn diese auf die Mitwirkung der Dateninhaber angewiesen sind.[37]

III. Nutzerzentrierung und Transaktionskosten

29 Diese Konstruktion eines neuen Property Rights der Nutzer kann die Ziele des Data Acts nur eingeschränkt erreichen. Die Nutzerzentrierung führt zu einer Zersplitterung

31 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 7.
32 Grundlegend Wielsch, Zugangsregeln, 2008, S. 6 ff.
33 Zu technischen Schutzmaßnahmen Steege MMR 2024, 91.
34 Louven MMR 2024, 82 (84 f.); zu den Unsicherheiten Thomas/Wendehorst/Duller/Schwamberger, ELI Public Consultation on the Data Act, 2021, 20 ff.
35 Vgl. dazu Metzger/Schweitzer ZEuP 2023, 42 (66 ff.); Picht JECLAP 2023, 67 (74 f.); Metzger in Sattler/Zech, The Data Act: First Assessments, S. 67.
36 Vgl. zur beschränkten Übertragbarkeit Habic, IIC 2022, 1343 (1361 ff.).
37 Weitere Einschränkungen finden sich bspw. in. Art. 5 Abs. 3, 9-11 DA, Art. 6 Abs. 2 DA.

der Berechtigten und erhöht damit die Transaktionskosten, was zur sog. „tragedy of the anti-commons" führen kann. Ein eigenständiger Zugang wird außerdem lediglich den Nutzern und nicht auch Dritten ermöglicht.

1. Property Rights der Inhaber und Nutzer

30 Die deskriptive Analyse zeigt, dass dem faktischen Property Right der Dateninhaber ein rechtliches Property Right der Nutzer entgegengesetzt wird. Dieses basiert auf relativ wirkenden Regelungen im Verhältnis zwischen Inhaber und Nutzer. Der Data Act möchte kein neues absolutes Recht an Daten schaffen.[38] Allerdings ist das für die Property Rights Theory nur bedingt relevant, da der Ausschluss Dritter weiterhin über die faktische Herrschaftsstellung der Dateninhaber erfolgt, die rechtlich nur vom Nutzer durchbrochen werden kann.[39] Der Nutzer kann an der tatsächlichen Datenherrschaft des Dateninhabers partizipieren, die weiter bestehen bleibt.[40] Alle dem Nutzer nicht zugewiesenen Positionen und auch diese, die einfach nicht ausgeübt werden, verbleiben beim Dateninhaber, der auch an der Weitergabe der Daten durch den Nutzer wirtschaftlich beteiligt wird.[41]

31 Im Ergebnis zeigt sich damit ein gemischtes Property Right an Daten mit kombiniert rechtlicher und faktischer Ausschließlichkeit für Nutzer und Inhaber. Die Datenherrschaft wird durch den Data Act auf mehrere Personen aufgeteilt.[42]

2. Nutzerzentrierung und Anti-Commons

32 Die Nutzerzentrierung eröffnet zwar theoretisch die Möglichkeit des Handels mit Daten und damit eine effiziente Datenallokation, führt aber auch zu hohen Transaktionskosten, die dem entgegenstehen.[43]

33 Zunächst ist festzuhalten, dass die Inhaber weiterhin genügend Anreize haben dürften, in vernetzte Produkte zu investieren und Daten zu sammeln. Das setzt voraus, dass ihnen zumindest der Aufwand ersetzt wird, der dadurch entsteht, dass sie die Daten erheben. Während eine genaue empirische Bestimmung der Kosten hilfreich wäre, ist diese fast unmöglich, da sich die Kosten kaum für alle Sachverhalte einheitlich bestimmen lassen. Generell haben die Nutzer einen geringen bis keinen Aufwand, da die Daten bei der bestimmungsgemäßen Nutzung des Produkts generiert werden. Die Dateninhaber haben regelmäßig höhere Kosten. Sie müssen die Produkte so gestalten, dass diese Daten erheben können, und beispielsweise Sensoren integrieren und Software entwickeln. Es spricht vieles dafür, dass die Inhaber dennoch weiter ihre Kosten amortisieren können.[44] Ihnen verbleibt im Regelfall der Erstzugriff und die Nutzungsmöglichkeit auf Grundlage des Vertrages mit den Nutzern, in dem Sie sich die Rechte einräumen lassen.[45] Sie können diese weiterhin für die Weiterentwicklung der Produkte und für Aftermarket-Leistungen nutzen. Darüber hinaus stellt Art. 9 Abs. 2 lit. a) DA sicher, dass bei der Bestimmung eines angemessenen Preises für die Weitergabe der Daten an Dritte die Innovationsanreize berücksichtigt werden.

34 Daneben stellt sich die Frage, ob die Daten auch optimal verteilt und genutzt werden. Dabei zeigt sich ein fundamentales Problem des Regelungsansatzes. Der Data Act versucht den Datenhandel zu ermöglichen, indem die faktische Datenherrschaft der Inhaber über Ansprüche der Nutzer auf Zugang und Weitergabe der Daten aufgebrochen werden soll. Die Allokation der Daten über den Marktmechanismus kann allerdings nur dann funktionieren, wenn niedrige Transaktionskosten bestehen, da es ansonsten zu ineffizienten Ergebnissen kommen kann. Der Data Act führt durch die Regelung des Datenzugangs über die Nutzer in vielen Fällen aber zu höheren Transaktionskosten. Das resultiert daraus, dass zugangssuchende Dritte gem. Art. 4 Abs. 13, 13 und Art. 6 Abs. 1 DA jeden einzelnen Nutzer dazu bringen müssen, dass dieser die Datenweitergabe selbst vornimmt oder gegenüber dem Inhaber veranlasst. Der volle Wert der Daten lässt sich nicht durch einzelne Datensätze realisieren, sondern nur durch die Kombination aller oder zumindest eines Großteils der Datensätze. Die Zersplitterung der Verfügungsrechte am gesamten Datenbestand wird deswegen auch als tragedy of the anti-commons bezeichnet.[46] Diese führt zu hohen Transaktionskosten und verhindert economies of scope.[47] Hinzu kommen weitere Transaktionskosten, die daraus resultieren, dass die FRAND-Kriterien erst noch konkretisiert werden müssen. Das führt zu Unsicherheit, kann komplexe Verhandlungen nötig machen und verzögert den Erhalt der Daten.[48]

35 Im Ergebnis zeigt sich, dass der Data Act Property Rights zur Zielerreichung nur teilweise erfolgreich nutzen kann. Die Nutzerzentrierung kann zu einer „tragedy of the anti-commons" führen und Transaktionskosten erhöhen. Dies steht einer effizienten Datenallokation entgegen. Die dadurch gefährdeten gesamtgesellschaftlichen Vorteile sind erheblich.[49]

3. Fehlende Zugangsregeln zu Gunsten Dritter

36 Eine Analyse auf den vom Data Act ebenfalls angestrebten Zugang zu Daten zeigt, dass dieses Ziel nur teilweise er-

38 ErwGr 6.
39 So auch Wiebe GRUR 2023, 1569 (1577 f.).
40 Vgl. Specht-Riemenschneider MMR 2022, 809 (818).
41 Podszun/Offergeld WiVerw 2023, 103 (106).
42 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 14 ff.
43 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 18 f.; Podszun/Pfeifer GRUR 2022, 953 (960 f.); Funk CR 2023, 421.
44 Drexel et al., Max Planck Institute for Innovation and Competition Research Paper No. 22-05, 31 f., 33 f., Wiebe GRUR Int. 2017, 67.
45 Eckardt/Kerber in Sattler/Zech, The Data Act: First Assessments, S. 16 f.
46 Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 29 f.
47 Hierzu ausführlich Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 30; Datenintermediäre können dieses Problem abmildern, aber nicht beheben, da diese ebenfalls alle einzelnen Nutzer erreichen müssen, vgl. auch Hennemann/von Ditfurth NJW 2022, 1905.
48 Vgl. Kerber GRUR Int. 2023, 120 (125 f.).
49 Vgl. Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 42 f.

reicht werden kann. Property Rights stehen dem Zugang zunächst neutral gegenüber. Ein Property Right kann den Zugang zu einer Ressource verschließen. Je nach Zusammensetzung des Bündels von Rechten kann ein gesetzliches Property Right den Zugang aber auch erst ermöglichen, wenn es einem rein tatsächlichen Property Right gegenübertritt.[50] So verhält es sich hier zu Gunsten der Nutzer. Es trägt zur Erreichung der Ziele des Data Acts bei, dass den Nutzern, trotz Einschränkungen im Detail, sehr weitgehende Zugangsmöglichkeiten eingeräumt werden. Die starke Nutzerzentrierung des Data Acts bringt aber Zugangsprobleme für Dritte mit sich. Hier wirkt das Property Right der Nutzer zugangsfeindlich. Dritte können ausschließlich über die Nutzer Zugang zu den Daten erhalten. Ein Interessensausgleich außerhalb des Marktmechanismus zwischen Dritten und Nutzern ist gerade nicht möglich. Es fehlt eine Zugangsregel zu Gunsten Dritter, die einen Interessensausgleich abbilden und den Zugang notfalls auch erzwingen könnte. Die aktuelle Rechtslage kann insbesondere für die Forschung oder andere gemeinnützige Anwendungen ein erhebliches Hindernis darstellen.[51]

E. Integration der Erkenntnisse

37 Die Diagnose der Defizite auf Grundlage der Property Rights Theory hilft dabei, die Setzung neuer Regeln und die Anwendung der bestehenden Regeln zu informieren. Die Ergebnisse können bei der Schaffung sektorspezifischer Regulierung, bei der Auslegung der Bestimmungen des Data Acts und bei der Klauselkontrolle berücksichtigt werden.

I. Neue Regelungen

38 Am konsequentesten gelänge dies bei der Formulierung eines komplett neuen Regelwerks, das den Data Act ersetzt. Ein solcher Vorschlag wäre aber realitätsfern. Gleichzeitig bietet auch die aktuelle Rechtslage Möglichkeiten, neue Erkenntnisse zu integrieren. So lässt der Data Act bspw. Raum für sektorspezifische Regeln.[52] Diese Möglichkeit sollte beispielsweise genutzt werden, um das Zugangsproblem zu adressieren. So könnte eine spezielle Zugangsregel für gemeinnützige Forschung geschaffen werden, so wie sie in Art. 31 Nr. 2 DSA schon existiert.[53]

II. Auslegung des Data Acts

39 Die Erkenntnisse lassen sich aber auch direkt bei der Auslegung der bestehenden Regeln des Data Act nutzen. Dieser enthält – wie alle Regelwerke – eine Vielzahl unbestimmter Rechtsbegriffe. Nach Art. 9 Abs. 1 DA soll die Gegenleistung „angemessen" sein. Nach Art. 9 Abs 2 lit. b) DA müssen Investitionen nur „gegebenenfalls" berücksichtigt werden. Eine teleologische Auslegung dieser Begrifflichkeiten ermöglicht eine folgenorientierte Betrachtung, die die Ergebnisse einer ökonomischen Analyse einbeziehen kann. Das ist zumindest dann möglich, wenn die Ziele des Data Acts mit den Zielen übereinstimmen, die im Rahmen der Analyse berücksichtigt werden können. Dies ist nicht immer der Fall. Wohlfahrts- und Effizienzüberlegungen, die häufig im Vordergrund ökonomischer Analysen stehen, müssen nicht für alle Regelwerke entscheidend sein.[54] Im Fall des Data Acts gibt es indes erhebliche Überschneidungen. Wie dargestellt ist die ökonomische Effizienz zumindest ein wichtiges Ziel des Data Acts. Das bedeutet nicht, dass die Ergebnisse der ökonomischen Analyse Vorrang vor anderen Argumenten haben sollten. Sie sollten aber berücksichtigt und mit der Erreichung anderer Ziele abgewogen werden.

40 Da die Anreize zur Datensammlung auch unter dem Data Act ohnehin hoch sind und gleichzeitig hohe Transaktionskosten eine effiziente Allokation der Daten erschweren, sollte im Rahmen der Auslegung die Höhe der Gegenleistung nach Art. 9 Abs. 1 DA restriktiv bestimmt werden. Um dem Rechnung zu tragen, könnten beispielsweise Pauschalbeträge entwickelt werden. Forschungseinrichtungen könnten außerdem von dem Erfordernis einer Gegenleistung, komplett freigestellt werden. Durch den Wegfall einer Gegenleistung – auch wenn dies auf Kosten der Dateninhaber geht – können die Kosten für die zugangssuchenden Dritten gesenkt werden. Für kleine und mittlere Unternehmen können ähnliche Ausnahmen erwogen werden. Ebenfalls zur Senkung der Transaktionskosten kann die Europäische Kommission nach Art. 9 Abs. 5 DA tätig werden und Leitlinien erlassen, die diese Erkenntnisse integrieren und die Ermittlung der Gegenleistung erleichtern.

III. AGB-Kontrolle

41 Eine weitere Korrekturmöglichkeit eröffnen Generalklauseln. Hier ist ein Einfluss der Erkenntnisse ebenfalls im Rahmen einer teleologischen Auslegung möglich. Generalklauseln zeichnen sich auch dadurch aus, dass in diesen der Wortlaut in geringerem Maße einer teleologischen Auslegung entgegensteht.[55] Eine solche Generalklausel findet sich im Data Act in Art. 13 DA zur Kontrolle von Vertragsklauseln zwischen Unternehmen.[56] Im Verhältnis von Unternehmen zu Verbrauchern bleiben die Generalklauseln des AGB-Rechts anwendbar. Auf diesem Weg könnten beispielsweise Klauseln als missbräuchlich angesehen werden, wenn sie den Zugang der Dritten zu den Daten behindern.[57] Das können Klauseln sein, die Registrierungs-

50 Vgl. Duch-Brown/Martens/Mueller-Langer, JRC Digital Economy Working Paper 2017-01, 42, Zech in Sattler/Zech, The Data Act: First Assessments, S. 53.

51 Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, 2021, S. 119 ff.; Specht-Riemenschneider ZRP 2022, 137 (140); Specht-Riemenschneider MMR 2022, 809 (825 f.).

52 ErwGr 25, vgl. auch Staudenmayer EuZW 2022, 1037 (1043).

53 Zur Problematik im DGA: Lauber-Rönsberg/Becker RuZ 2023, 30.

54 Umfassend zu Rechten an Daten und normativen Begründungen Thomas/Wendehorst/Duller/Schwamberger, ELI Public Consultation on the Data Act, 2021, S. 10 ff.

55 Vgl. Rohner, Art. 102 AEUV und die Rolle der Ökonomie, 2023, S. 325 ff.

56 Umfassend Schwamberger MMR 2024, 96.

erfordernisse voraussetzen oder die Nutzung bestimmter kostenpflichtiger Software des Inhabers verlangen. Diese Erfordernisse würden erneut die ohnehin zu hohen Transaktionskosten erhöhen.

F. Fazit

42 Zu Beginn des Beitrags stand die Forschungsfrage: Kann der Data Act die Ziele der effizienten Datennutzung und des Datenzugangs erreichen? Im Ergebnis zeigt eine Analyse unter Zuhilfenahme der Property Rights Theory, dass die Ziele nur teilweise erreicht werden können. Der Data Act enthält Property Rights der Nutzer, die den weiter bestehenden faktischen Property Rights der Inhaber entgegengesetzt werden. Die faktischen Property Rights der Inhaber werden dadurch zumindest abgeschwächt. Gleichzeitig führt die Nutzerzentrierung zu hohen Transaktionskosten im Hinblick auf den Handel mit Daten und ist damit ein Hindernis für die effiziente Datenallokation. Dies ergibt sich aus den zersplitterten Verfügungsrechten an den Daten. Die Nutzerzentrierung kann ein Hindernis für den Zugang Dritter zu den Daten sein. Es fehlt an Zugangsregeln.

43 Die so ermittelten Defizite sollten Anlass für sektorspezifische Regeln sein. Sie können auch im Rahmen der Auslegung des Data Acts berücksichtigt werden. Da der Data Act auch das Ziel der ökonomischen Effizienz verfolgt, sind die Erkenntnisse der Property Rights Theory leicht zu integrieren. Methodisch kann dies über die Auslegung unbestimmter Rechtsbegriffe und Generalklauseln im Rahmen der Klauselkontrolle erfolgen.

57 Vgl. Wiebe CR 2023, 777 (783).

Moritz Köhler*

Das Verbot der automatisierten Einzelentscheidung und der hinreichende Einfluss des Menschen

Die KI-VO reguliert die Entwicklung und den Betrieb von KI-Systemen. Die Zulässigkeit der Verwendung KI-generierter Ergebnisse richtet sich dagegen im Wesentlichen nach den allgemeinen Gesetzen. Von besonderer Bedeutung ist vor dem Hintergrund wachsender technischer Möglichkeiten deshalb das Verbot der automatisierten Entscheidung im Einzelfall, wie es sich aus Art. 22 Abs. 1 DS-GVO ergibt. Seit jeher umstritten ist der erforderliche Grad menschlicher Einflussnahme auf eine algorithmisch generierte Entscheidung, um die Anwendbarkeit des Verbots auszuschließen. Der vorliegende Beitrag setzt sich mit dem aktuellen Meinungsstand unter besonderer Berücksichtigung der Rechtsprechung des EuGH zur SCHUFA auseinander und entwickelt auf dieser Basis ein Stufenmodell (I). Daran anknüpfend bespricht er das Verhältnis von Art. 22 Abs. 1 DS-GVO und den Vorgaben der KI-VO (II).

1 Die Verortung des Verbots der automatisierten Entscheidung im Einzelfall in Art. 22 Abs. 1 DS-GVO lässt vermuten, dass es in erster Linie den Schutz personenbezogener Daten bezweckt. Eine gewisse allgemeine Bedeutung für die Stellung der natürlichen Person in der Informationsgesellschaft lässt sich allerdings nicht leugnen.[1] Dies äußert sich unter anderem darin, dass der europäische Gesetzgeber nicht den einzelnen Verarbeitungsschritt, sondern die darauf beruhende Entscheidung als Anknüpfungspunkt der Vorschrift wählt.[2] Dementsprechend wird die grundrechtliche Verankerung von Art. 22 Abs. 1 DS-GVO überwiegend in Art. 1 Satz 1 GRCh gesehen.[3] In der Konsequenz statuiert Art. 22 Abs. 1 DS-GVO keinen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten im Rahmen einer automatisierten Entscheidungsfindung, sondern stellt für diesen Vorgang zusätzliche Anforderungen zum Schutz der Grundrechte, die von der Zulässigkeit der Datenverarbeitung selbst unabhängig sind.[4] Anders als die systematische Stellung nahelegt, handelt es sich zudem nicht um ein Recht der betroffenen Person, sondern um ein objektives Verbot.[5]

I. Menschliches Dazwischentreten

2 Das Verbot des Art. 22 Abs. 1 DS-GVO greift nach der Rechtsprechung des EuGH unter drei Voraussetzungen: Es

* Moritz Köhler ist wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln und Doktorand. Seine Promotion zur Zulässigkeit des Einsatzes algorithmischer Systeme in der Justiz wird von Rolf Schwartmann und Gregor Thüsing betreut.

1 Djeffal ZaöRV 2020, 847 (857).

2 BeckOK DatenschutzR/v. Lewinski, 49. Edition 1.8.2024, DS-GVO Art. 22 Rn. 3.

3 Paal/Hüger MMR 2024, 540.

4 v. Walter in Kaulartz/Braegelmann AI und Machine Learning-HdB, 2020, Kap. 8.4 Rn. 4; Kögel ZdiW 2022, 205 (207); Kumkar/Roth-Isigkeit JZ 2020, 277 (278).

5 EuGH Urt. 7.12.2023 – C-634/21 Rn. 52, NJW 2024, 413. Dazu in der Literatur bereits vor der Entscheidung des EuGH Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 22 Rn. 5; Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 22 Rn. 15.

muss eine „Entscheidung" vorliegen, die „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – [beruht]" und die „gegenüber [der betroffenen Person] rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt".[6] Menschliche Entscheidungen werden von Art. 22 Abs. 1 DS-GVO nicht erfasst. Es herrscht daher Einigkeit darüber, dass der Anwendungsbereich der Vorschrift bei hinreichender menschlicher Einflussnahme auf die Entscheidung nicht eröffnet ist.[7] Unklar ist allerdings, welcher Grad der Einflussnahme hinreichend in diesem Sinne ist. Verschärft wird die Diskussion durch die neue Rechtsprechung des EuGH, wonach auch entscheidungsvorbereitende Systeme dem Anwendungsbereich der Vorschrift unterfallen können.[8]

3 Die Diskussion um die erforderliche Beteiligung eines menschlichen Entscheiders knüpfte im bisherigen Diskurs üblicherweise am Tatbestandsmerkmal des Beruhens auf einer ausschließlich automatisierten Verarbeitung an (dazu 1.).[9] Es zeichnet sich ab, dass sie nach dem Urteil am neu eingeführten Begriff der Maßgeblichkeit fortgesetzt wird (dazu 2.).[10]

1. Stand der Diskussion vor dem Urteil des EuGH zur SCHUFA

4 Bereits vor dem Urteil des EuGH zur SCHUFA herrschte weitgehend Einigkeit darüber, dass eine rein formale Zwischenschaltung eines Menschen in den Entscheidungsprozess nicht genügt, um die Anwendung des Art. 22 Abs. 1 DS-GVO auszuschließen.[11] Wird eine menschliche Instanz installiert, die die automatisierten Entscheidungen lediglich alibimäßig abnickt, wird den Gefahren, vor denen Art. 22 Abs. 1 DS-GVO schützen soll, nicht ausreichend begegnet.[12] Der Mensch muss die Entscheidung stattdessen beeinflussen können.[13] Erforderlich sind daher zumindest eine eigene inhaltliche (Letzt-)Entscheidungskompetenz und ein eigener Beurteilungsspielraum.[14] Der hiernach zum Ausschluss des Verbots mindestens erforderliche Einfluss des Menschen lässt sich mit *Paal/Hüger* treffend als formelle Hoheit bezeichnen.[15]

5 In welcher Form darüber hinaus eine materielle Hoheit erforderlich ist, wurde vor dem Urteil des EuGH dagegen nicht einheitlich beurteilt. Eine materielle Hoheit verlangt nach den in diesem Beitrag gewählten Begrifflichkeiten eine inhaltliche Auseinandersetzung der menschlichen Instanz mit dem im Einzelfall ausgegebenen Ergebnis des algorithmischen Systems. In Bezug auf Art. 22 Abs. 1 DS-GVO wurde teilweise vertreten, dass ein menschliches Dazwischentreten im Sinne einer Plausibilitätskontrolle genügt.[16] Demnach sollte es für den Ausschluss von Art. 22 Abs. 1 DS-GVO ausreichen, wenn die menschliche Kontrollinstanz einzelne, nicht plausible Entscheidungen herausgreift und inhaltlich überprüft.[17] Lediglich rein stichprobenhafte Kontrollen seien unzureichend.[18]

6 Andere forderten eine umfassende inhaltliche Auseinandersetzung in jedem Einzelfall.[19] Wie eine solche konkret zu erfolgen hat, wurde dabei meist offengelassen. Regelmäßig wird nach dieser Ansicht allerdings erforderlich sein, dass der Mensch weitere Aspekte in die Entscheidung einbezieht.[20]

2. Stand der Diskussion nach dem Urteil des EuGH zur SCHUFA

7 In seinem Urteil zur SCHUFA hat der EuGH entschieden, dass die Ermittlung eines Wahrscheinlichkeitswerts eine verbotene Entscheidung im Sinne von Art. 22 Abs. 1 DS-GVO darstellt, wenn ein daran anknüpfendes Handeln mit rechtlicher Wirkung „maßgeblich" von diesem Wert geleitet wird.[21] Soweit dies bisher abzusehen ist, hat sich damit keine der beiden genannten Meinungen eindeutig durchsetzen können. Vielmehr setzt sich die Diskussion um den erforderlichen Grad menschlicher Beteiligung an der Entscheidung am Merkmal der Maßgeblichkeit fort. Dabei werden die Ausführungen des EuGH teilweise so verstanden, dass die automatisierte Entscheidungsvorbereitung nur maßgeblich für die Entscheidung ist, wenn der Mensch ihr Ergebnis nicht kippen kann.[22] Andere wollen auch unter Berücksichtigung der neuen Rechtsprechung des EuGH an das Erfordernis einer Plausibilitätskontrolle anknüpfen.[23] Schließlich wird der Begriff der Maßgeblichkeit herangezogen, um das Erfordernis einer umfassenden inhaltlichen Auseinandersetzung in jedem Einzelfall zu begründen.[24] Vor diesem Hintergrund ist hier zu klären, ob sich aus dem Verfahren vor dem EuGH neben der grundsätzlichen Anwendbarkeit von Art. 22 Abs. 1 DS-GVO auf automatisierte Entscheidungsvorbereitungen auch mit Blick auf die Qualität der erforderlichen menschlichen Einflussnahme neue Erkenntnisse ergeben.

---

6 EuGH 7.12.2023 – C-634/21 Rn. 43, NJW 2024, 413.
7 Schwartmann/Jaspers/Thüsing/Kugelmann/Atzert, 3. Aufl. 2024 DS-GVO Art. 22 Rn. 51, 105; Kühling/Buchner/Buchner, 4. Aufl. 2024, DS-GVO Art. 22 Rn. 15; Paal/Pauly/Martini DS-GVO Art. 22 Rn. 17b.
8 Vgl. EuGH 7.12.2023 – C-634/21 Rn. 45 f., NJW 2024, 413.
9 Schwartmann/Jaspers/Thüsing/Kugelmann/Atzert DS-GVO Art. 22 Rn. 105; Paal/Pauly/Martini DS-GVO Art. 22 Rn. 17-19c; BeckOK DatenschutzR/v. Lewinski DS-GVO Art. 22 Rn. 23-25.
10 Blasek ZD 2024, 258 (259 f.); Günter/Gerigk/Berger NZA 2024, 234 (235 f.); Rohrmoser, Stärkung des Faktors Mensch, LTO v. 13.12.2023, abrufbar unter https://www.lto.de/recht/meinung/m/EuGH-Schufa-Verfahren-Kommentar-Prozessvertreter-Mensch-gefahr-algorithmus; Thüsing, Das EuGH-Urteil wird zum Problem für KI, LTO v. 10.12.2023, abrufbar unter https://www.lto.de/recht/meinung/m/eugh-c63421-schufa-scoring-folgen-ki-automatisierte-verarbeitung-kreditauskunft.
11 Raji, Künstliche Intelligenz im öffentlichen Sektor, 2023, S. 207; Kögel ZdiW 2022, 205 (207).
12 Paal/Hüger MMR 2024, 540 (541).
13 Martini, Blackbox Algorithmus, 2019, S. 173.
14 Martini/Nink NVwZ-Extra 10 (2017), 1 (3); Kumkar/Roth-Isigikeit JZ 2020, 277 (279).
15 Paal/Hüger MMR 2024, 540 (542).
16 Kühling/Buchner/Buchner DS-GVO Art. 22 Rn. 15; BeckOK DatenschutzR/v. Lewinski DS-GVO Art. 22 Rn. 25.1.
17 Kühling/Buchner/Buchner DS-GVO Art. 22 Rn. 15.
18 Kühling/Buchner/Buchner DS-GVO Art. 22 Rn. 15.
19 Paal/Pauly/Martini DS-GVO Art. 22 Rn. 19; Kumkar/Roth-Isigikeit JZ 2020, 277 (279).
20 v. Walter in Kaulartz/Braegelmann AI und Machine Learning-HdB Kap. 8.4 Rn. 7.
21 EuGH 7.12.2023 - C-634/21 Rn. 48, NJW 2024, 413.
22 Rohrmoser Fn. 10; Blasek ZD 2024, 258 (259 f.).
23 Günter/Gerigk/Berger NZA 2024, 234 (236).
24 Paal/Hüger MMR 2024, 540 (541); Thüsing Fn. 10.

8 Für das Ausreichen einer formellen Hoheit wird angeführt, dass der EuGH im besprochenen Urteil die Maßgeblichkeit der Score-Werte für die Entscheidungsfindung mit dem Hinweis angenommen hat, dass ein unzureichender Wahrscheinlichkeitswert „in nahezu allen Fällen" dazu führt, dass die Bank die Gewährung des beantragten Kredits ablehnt. Da das VG Wiesbaden in seiner Vorlagefrage hervorgehoben hat, dass es um Fälle geht, in denen der Mensch nicht über den Score-Wert hinwegentscheiden kann, gelte dies auch für das Kriterium der Maßgeblichkeit: Art. 22 Abs. 1 DS-GVO sei demnach bereits ausgeschlossen, wenn ein Mensch die Möglichkeit hat, die Entscheidung der Maschine zu überstimmen.[25]

9 Dem wird entgegengehalten, dass der Begriff der Maßgeblichkeit schon etymologisch einen stärkeren Einfluss der menschlichen Entscheidungsinstanz verlangt als der vor dem Urteil des EuGH zentrale Begriff der Ausschließlichkeit.[26] Da aber bereits unter Anknüpfung an die Ausschließlichkeit regelmäßig zumindest eine Plausibilitätskontrolle verlangt wurde, müssenunmehr eine inhaltliche Auseinandersetzung im Einzelfall gefordert werden. Ein entsprechend weites Verständnis des Art. 22 Abs. 1 DS-GVO wird gestützt durch die Nutzung des Begriffs der Maßgeblichkeit in Abgrenzung zu den Schlussanträgen des Generalanwalts:[27] Dieser wollte noch von einer automatisierten Entscheidungsfindung im Sinne des Verbots ausgehen, wenn die Score-Werte die Entscheidung vorbestimmen.[28] Der EuGH hat diesen Begriff nicht übernommen, sondern auf den weiteren Begriff der Maßgeblichkeit zurückgegriffen, wie er sich aus der Vorlagefrage des VG Wiesbaden ergibt.[29]

10 Keine der genannten Ansichten vermag zu überzeugen. Der EuGH hat das Kriterium der Maßgeblichkeit nicht selbst eingeführt. Während dies für die Generalisierbarkeit der Rechtsprechung mit Blick auf die Anwendbarkeit von Art. 22 Abs. 1 DS-GVO im Rahmen von Entscheidungsvorbereitungen kein Hindernis darstellt, sollte die Übernahme aus der Vorlagefrage im Rahmen der weiteren Auslegung des Tatbestandsmerkmals selbst berücksichtigt werden. Aus den Ausführungen des EuGH lässt sich deshalb allenfalls ableiten, dass Maßgeblichkeit zumindest dann anzunehmen ist, wenn das Ergebnis der automatisierten Entscheidungsvorbereitung „in nahezu allen Fällen" übernommen wird. Ob unterhalb dieser Schwelle eine inhaltliche Auseinandersetzung im Einzelfall oder eine Plausibilitätskontrolle erforderlich ist, oder sogar die rein formelle Hoheit des Menschen genügt, lässt der EuGH in dem Urteil offen. Die weitere Konkretisierung des Merkmals der Maßgeblichkeit werden nationale Gerichte vornehmen müssen. Unter Verweis auf die dahinterstehende Tatsachenfrage hatte darauf bereits der Generalanwalt verwiesen.[30]

3. Eigener Ansatz: Entwicklung eines Stufenmodells

11 Während es sich bei der Beurteilung des Einflusses einer menschlichen Instanz auf die Entscheidungsfindung um eine Tatsachenfrage handelt, wäre eine Konkretisierung der rechtlichen Anforderungen an diesen menschlichen Einfluss durchaus wünschenswert gewesen. Nicht umsonst wird Art. 22 Abs. 1 DS-GVO für seine fehlende Klarheit in diesem Punkt kritisiert.[31] Im Folgenden soll deshalb und mit Blick auf die eingangs formulierte Forschungsfrage des erforderlichen Grads menschlicher Einflussnahme ein Vorschlag für eine praxisgerechte und angemessene Auslegung des Verbots der automatisierten Entscheidung erarbeitet werden.

12 Welcher Grad menschlicher Einflussnahme für den Ausschluss des Verbots in Art. 22 Abs. 1 DS-GVO im Einzelfall erforderlich ist, kann nicht pauschal beantwortet werden. Wie sich aus der Rechtsprechung des EuGH und einem wertenden Vergleich mit den Vorgaben der KI-VO ergibt, verlangt die Beantwortung dieser Frage vielmehr eine differenzierende Betrachtung.[32]

13 Fest steht dabei lediglich, dass die bloße Überwachung des Betriebs zur Sicherung einer formellen Hoheit des Menschen nicht ausreichen kann, um die Anwendung von Art. 22 Abs. 1 DS-GVO auszuschließen.[33] Zwar ließe sich einwenden, dass ErwG 71 Satz 1 DS-GVO in den angeführten Beispielen nur Fälle erwähnt, in denen eine Entscheidung „ohne jegliches menschliches Eingreifen" getroffen wird. Diese Fälle sind damit aber nach dem Willen des Gesetzgebers lediglich gesicherte Anwendungsfälle des Art. 22 Abs. 1 DS-GVO. Aus dem Einschub im Erwägungsgrund kann im Umkehrschluss nicht abgeleitet werden, dass Art. 22 Abs. 1 DS-GVO ausschließlich in diesen Fällen zur Anwendung kommen soll. Ebenso wenig lässt sich aus Art. 22 Abs. 3 DS-GVO folgern, dass bereits eine formelle Überwachung automatisierter Entscheidungen die Anwendung der Vorschrift ausschließt. Zwar wird darin festgelegt, dass eine betroffene Person im Falle der ausnahmsweisen Zulässigkeit einer automatisierten Entscheidung das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen hat. Damit ist allerdings keine Aussage zum erforderlichen Einfluss des Menschen getroffen. Aus der Vorschrift lässt sich lediglich ableiten, dass der menschliche Einfluss bei Ausübung dieses Rechts größer sein muss als im Rahmen der ursprünglichen Entscheidung. Dagegen sprechen historische Argumente für eine grundsätzlich erforderliche inhaltliche Mitverantwortung des Menschen:[34]

25 Rohrmoser Fn. 10; Blasek ZD 2024, 258 (259 f.).
26 Vgl. Thüsing Fn. 10.
27 Hense RDi 2024, 192 (195).
28 Generalanwalt beim EuGH (Pikamäe), Schlussantrag v. 16.3.2023 – C-634/21 Rn. 42, BeckRS 2023, 4643.
29 EuGH 7.12.2023 – C-634/21 Rn. 48, NJW 2024, 413.
30 Generalanwalt beim EuGH (Pikamäe), Schlussantrag v. 16.3.2023 – C-634/21 Rn. 45, BeckRS 2023, 4643.
31 Hense RDi 2024, 192 (195).
32 So bereits vor der KI-VO Steinbach, Regulierung algorithmenbasierter Entscheidungen, 2021, S. 120 ff.
33 Kätscher/Pesch KIR 2024, 46 (51); Art. 29 – Datenschutzgruppe, Leitlinien zu automatisierten Entscheidungen im Einzelfall, S. 22; aA DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 14, 18, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf.

§ 6a Abs. 1 Satz 2 BDSG aF konkretisierte das Kriterium der Ausschließlichkeit. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung sollte danach vorliegen, „wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat". Diese Wertung lässt sich auf Art. 22 Abs. 1 DS-GVO übertragen.[35] Außerdem lässt sich aufgrund psychologischer Erwägungen an der Wirksamkeit einer rein formellen Hoheit und damit an ihrer Vereinbarkeit mit dem *Telos* der Norm zweifeln: Insbesondere beim Einsatz algorithmischer Systeme zur Entscheidungsvorbereitung kommt der Automatisierungsbias zum Tragen.[36] Um dessen Risiken zu begrenzen, ist nach derzeitigem Erkenntnisstand die Zuweisung inhaltlicher Mitverantwortung erforderlich.[37] Daher ist zumindest eine irgendwie geartete inhaltliche Auseinandersetzung mit den automatisiert generierten Entscheidungsvorschlägen zu fordern, um die Anwendung von Art. 22 Abs. 1 DS-GVO auszuschließen.[38]

14 Dies zugrunde gelegt lässt sich die erforderliche menschliche Einflussnahme stufenweise bestimmen. Anknüpfungspunkt ist dabei abermals die Rechtsprechung des EuGH zur SCHUFA. Das Merkmal der Maßgeblichkeit, auf das darin zentral abgestellt wird, ermöglicht eine Differenzierung, die unter dem absolut wirkenden Merkmal der Ausschließlichkeit noch nicht ohne weiteres möglich war.[39] Grundlage der Differenzierung ist der Automatisierungsgrad des eingesetzten algorithmischen Systems: Je konkreter dessen Entscheidungsvorschlag ist, desto eher ist dessen Übernahme maßgeblich für die schlussendliche Entscheidung. So ist die Erstellung eines Score-Werts deutlich komplexer und weniger nachvollziehbar als die zusammenfassende Präsentation entscheidungserheblicher Parameter. Im zweitgenannten Fall ist die menschliche Entscheidungsinstanz schon aufgrund der technischen Konzeption zu einer inhaltlichen Auseinandersetzung gezwungen.

a) Erste Stufe: Unwesentlicher Einfluss der automatisierten Entscheidungsvorbereitung

15 Auf der ersten Stufe des hier vorgeschlagenen differenzierenden Modells steht daher der Einsatz algorithmischer Systeme, die einen lediglich unwesentlichen Einfluss auf die Entscheidungsfindung haben.[40] Sofern die automatisierte Entscheidungsvorbereitung bereits in einer Form organisiert ist, die eine inhaltliche Auseinandersetzung des menschlichen Entscheidungsträgers mit dem Einzelfall voraussetzt, ist keine weitere Dokumentation der Rolle des algorithmischen Systems im Entscheidungsprozess erforderlich. Dass der europäische Gesetzgeber den unwesentlichen Einsatz von KI-Systemen im Entscheidungsfindungsprozess gesondert behandeln will, ergibt sich bei wertender Betrachtung aus Art. 6 Abs. 3 KI-VO. Dessen Kriterien lassen sich auf die hier definierte Stufe übertragen, da sie ebenfalls jeweils eine materielle Hoheit des Menschen voraussetzen. Sie lassen sich im Kontext des Art. 22 Abs. 1 DS-GVO zudem auf einfache algorithmische Systeme übertragen. Anknüpfungspunkt von Art. 6 Abs. 3 KI-VO ist der Grad der Beeinflussung einer Entscheidung. Dieser Grad hängt nicht von den technischen Grundlagen des eingesetzten Systems, sondern allein von seinen Wirkungen ab. Parallel dazu differenziert Art. 22 Abs. 1 DS-GVO grundsätzlich nicht hinsichtlich technischer Hintergründe, sondern nimmt allein den Einfluss des algorithmischen Systems auf die Entscheidungsfindung in den Blick. So stellte *Martini* bereits 2019 fest: „Dass eine Computerentscheidung auf eine *menschliche* Programmierung zurückgeht […], macht die Entscheidung […] nicht zu einer menschlichen."[41] Sofern ein algorithmisches System in einem Entscheidungsprozess gem. den Vorgaben von Art. 6 Abs. 3 UAbs. 2 KI-VO eingesetzt wird, muss die menschliche Entscheidungsinstanz ihre materielle Hoheit deshalb im Einzelfall nicht weiter belegen. Die Dokumentation einer entsprechenden Organisation des Einsatzes muss allerdings erfolgen und den Anforderungen des Art. 5 Abs. 2 DS-GVO genügen.

b) Zweite Stufe: Wesentlicher Einfluss der automatisierten Entscheidungsvorbereitung

16 Beeinflusst der Vorschlag eines algorithmischen Systems die Entscheidung hingegen mehr als nur unwesentlich, wird eine weitergehende inhaltliche Auseinandersetzung des menschlichen Entscheidungsträgers erforderlich. Zwar darf ein algorithmisches System auch unter Geltung von Art. 22 Abs. 1 DS-GVO einen gewissen inhaltlichen Einfluss auf die Entscheidungsfindung haben. Ein wesentlicher Einfluss eines algorithmischen Systems auf den Entscheidungsprozess, in Abgrenzung zu Art. 6 Abs. 3 KI-VO etwa in Form konkreter Entscheidungsvorschläge oder Rankings, ist also nicht *per se* vom Verbot des Art. 22 Abs. 1 DS-GVO erfasst. In diesen Fällen muss aber sichergestellt werden, dass die Vorschläge oder das beste Ergebnis im Ranking nicht ungeprüft übernommen werden und der Einfluss des algorithmischen Systems auf den Entscheidungsprozess dadurch maßgeblich wird. Dazu ist ein zumindest geringfügiger inhaltlicher Einfluss des Menschen erforderlich.

Auf der zweiten Stufe steht daher der Einsatz algorithmischer Systeme, der die Entscheidung mehr als nur unerheblich beeinflusst. Dann ist nach dem hier vorgestellten Modell die erforderliche inhaltliche Mitverantwortung durch eine Plausibilitätskontrolle im Einzelfall gesichert.[42] Für eine solche ist mit *Heine* ein effektives Abweichen-Können

34 Ernst JZ 2017, 1026 (1029 f.).
35 Paal/Pauly/Martini DS-GVO Art. 22 Rn. 19a; Kühling/Buchner/Buchner DS-GVO Art. 22 Rn. 15.
36 Raji, Künstliche Intelligenz im öffentlichen Sektor, S. 207; dazu grundlegend Skitka/Mosier/Burdick International Journal of Human-Computer Studies 51 (1999), 991 (1001-1004).
37 Skitka/Mosier/Burdick International Journal of Human-Computer Studies 52 (2000), 701 (710 f.).
38 So iE auch HmbBfDI, Auswirkungen des Schufa-Urteils auf KI-Anwendungen – automatisierte Entscheidungen dürfen keine maßgebliche Rolle spielen, S. 2, abrufbar unter https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2023/2023-12-07-PM_EuGH_Urteil_Schufa_Auswirkungen_auf_KI.pdf.
39 Abstellend auf die persönlichen Beziehungen zwischen Verantwortlichem und betroffener Person Günter/Gerigk/Berger NZA 2024, 234 (236).
40 Ähnlich Kremer CR 2024, 50 (58).
41 Martini, Blackbox Algorithmus, S. 173.

zu fordern, das neben der Entscheidungsbefugnis auch das Vorliegen der erforderlichen Kenntnisse und Fähigkeiten des Entscheidungsträgers voraussetzt.[43]

Hinsichtlich des Umfangs der Plausibilitätsprüfung dürfte ein Abgleich der Datengrundlage[44] mit dem algorithmisch generierten Ergebnis anhand der Erfahrungssätze des kompetenten menschlichen Entscheidungsträgers genügen. Die Anforderungen an die Plausibilitätskontrolle können sich je nach Einzelfall unterscheiden und sind unter anderem abhängig von den Fähigkeiten und Limitierungen des eingesetzten algorithmischen Systems.[45] Eine umfassende inhaltliche Auseinandersetzung unter Einbeziehung neuer, außerhalb der automatisierten Verarbeitung liegender Aspekte ist hingegen nur bei negativem Ausgang der inhaltlichen Plausibilitätsprüfung erforderlich.[46] Bereits vor dem Urteil des EuGH zur SCHUFA wurde richtigerweise darauf hingewiesen, dass Art. 22 DS-GVO die Möglichkeit automatisierter Einzelentscheidungen grundsätzlich anerkennt, weshalb an die menschliche Einflussnahme keine unangemessen hohen Anforderungen gestellt werden dürfen.[47] Unter Berücksichtigung der erheblichen Weitung des Anwendungsbereichs der Vorschrift in Form der Einbeziehung von entscheidungsvorbereitenden Handlungen durch den EuGH gewinnt dieser Hinweis an Bedeutung. Zu beachten ist auch, dass der EuGH im Rahmen der Einführung der Maßgeblichkeit an die vom VG Wiesbaden geschilderte Praxis anknüpft, dass ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen dazu führt, dass die Bank die Gewährung des beantragten Kredits ablehnt. Wie oben dargelegt kann diese Äußerung zwar kaum als Definition der Maßgeblichkeit herhalten, sie legt aber nahe, dass an die erforderliche inhaltliche Mitverantwortung im Regelfall kein allzu strenger Maßstab angelegt werden darf.

17 Auf der zweiten Stufe steht daher der Einsatz algorithmischer Systeme, der die Entscheidung mehr als nur unerheblich beeinflusst. Dann ist nach dem hier vorgestellten Modell die erforderliche inhaltliche Mitverantwortung durch eine Plausibilitätskontrolle im Einzelfall gesichert.

c) Dritte Stufe: Wesentlicher Einfluss und hohes Schutzniveau des Art. 47 GRCh

18 Eine Plausibilitätskontrolle ist allerdings nicht mehr sachgerecht, wenn der Entscheidungsvorschlag von einem KI-System stammt und nach dem Ergebnis der Entscheidung ein schwerwiegender Grundrechtseingriff droht. Vor diesem Hintergrund erscheint eine weitere Differenzierung erforderlich, die ihre Berechtigung in der Rechtsprechung des EuGH zu Art. 7, 8 Abs. 1 GRCh findet:

19 Bereits im Jahr 2022 musste sich der EuGH mit der Frage auseinandersetzen, ob ein automatisierter Abgleich personenbezogener Daten mit bestimmten Datenbanken oder festgelegten Kriterien mit Art. 7, 8 Abs. 1 GRCh vereinbar ist.[48] In seinem Urteil zur PNR-Richtlinie[49] hat der EuGH auf die Gefahr fehlender praktischer Wirksamkeit einer individuellen Überprüfung der Ergebnisse „selbstlernender Systeme" hingewiesen.[50] Aufgrund der mangelnden Nachvollziehbarkeit von Technologien der künstlichen Intelligenz könne es sich demnach „als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat".[51] Zumindest, sofern aufgrund des Eingriffsgewichts das Recht auf einen wirksamen gerichtlichen Rechtsbehelf aus Art. 47 GRCh auf hohem Schutzniveau zu gewährleisten ist, genügt die individuelle Überprüfung eines KI-generierten Ergebnisses daher nicht.[52]

20 Dem ist zuzustimmen: Sofern zur Bestimmung von KI-Technologien im Wesentlichen auf deren Ableitungsfähigkeit abgestellt wird, was mit Blick auf Art. 3 Nr. 1 KI-VO naheliegt,[53] gehört es zum Wesen von KI-Systemen, dass die Gewichtung einzelner Parameter des Entscheidungsprozesses im Nachgang nicht umfassend nachvollzogen werden kann.[54] Das daraus resultierende Defizit der praktischen Wirksamkeit einer Überprüfung ist in vielen Anwendungsfällen aufgrund der geforderten Kenntnisse und Fähigkeiten der prüfenden menschlichen Instanz hinnehmbar. Sofern allerdings eine umfassende Kontrolle der Entscheidungsfindung durch ein Gericht gewährleistet sein muss, genügt eine Plausibilitätskontrolle nicht. Das Gericht muss vielmehr die Zusammensetzung und die Gewichtung der einzelnen Entscheidungsparameter nachvollziehen können. Solange dies beim Einsatz von KI-Systemen nicht sichergestellt werden kann, verbietet sich deren Einsatz zumindest, wenn das Recht auf einen wirksamen gerichtlichen Rechtsbehelf aus Art. 47 GRCh auf hohem Schutzniveau zu gewährleisten ist

21 Der EuGH verlangt in seiner neueren Rechtsprechung also eigene inhaltliche Erwägungen des Menschen, wenn der Einsatz eines KI-Systems mit einem hohen Schutzniveau des Art. 47 GRCh verbunden ist. Die dritte Stufe bildet deshalb der Einsatz von KI-Systemen mit wesentlichem Einfluss auf die Entscheidung, sofern das Recht auf einen wirksamen gerichtlichen Rechtsbehelf aus Art. 47 GRCh auf hohem Schutzniveau zu gewährleisten ist. In diesen Fällen wird eine inhaltliche Auseinandersetzung im Einzelfall erforderlich, die die Berücksichtigung weiterer, außerhalb des Entscheidungsvorschlags liegender Umstände verlangt.

---

42 AA Kätscher/Pesch KIR 2024, 46 (51), die allerdings nicht näher erläutern, was sie unter einer Plausibilitätskontrolle verstehen und im Folgenden für die demnach erforderliche „kritische inhaltliche Überprüfung" Kriterien aufstellen, die mit den hier vorgeschlagenen vergleichbar sind.
43 Heine, Der Vorbehalt menschlicher Entscheidungen, 1. Aufl. 2023, S. 263 ff.
44 Dazu Heine, Der Vorbehalt menschlicher Entscheidungen, S. 265 f.
45 So auch Kätscher/Pesch KIR 2024, 46 (51).
46 AA Heine NZA 2024, 1384 (1387); Höpfner/Daum ZfA, 467 (482).
47 BeckOK DatenschutzR/v. Lewinski DS-GVO Art. 22 Rn. 25.1.
48 EuGH 21.6.2022 – C-817/19, BeckRS 2022, 1384
49 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. 2016, L 119, 132.
50 EuGH 21.6.2022 – C-817/19 Rn. 195, BeckRS 2022, 13847.
51 EuGH 21.6.2022 – C-817/19 Rn. 195, BeckRS 2022, 13847.
52 EuGH 21.6.2022 – C-817/19 Rn. 195, BeckRS 2022, 13847.
53 Steen KIR 2024, 7 (8).
54 Heinze/Sorge/Specht-Riemenschneider KIR 2024, 11 (12 f.).

d) Das Stufenmodell in der Praxis

22 Zur Verdeutlichung der praktischen Auswirkungen des vorgestellten Stufenmodells seien im Folgenden einige Szenarien dargestellt und eingeordnet. Auf der ersten Stufe finden sich Anwendungsfälle, in denen das algorithmische System bereits aufgrund der Organisation seines Einsatzes oder seiner technische Konzeption lediglich unwesentlichen Einfluss auf die Entscheidungsfindung hat. Das ist etwa der Fall, wenn ein algorithmisches System eingehende Bewerbungen in vorgegebene Kategorien einordnet, sofern die Einordnung keinen Einfluss auf die Bewerberauswahl hat.[55] Der ersten Stufe unterfallen auch Einsatzszenarien, in denen das algorithmische System die Bewerberauswahl nachträglich auf eine Übereinstimmung mit dem bisherigen Auswahlmuster überprüft.[56] In der gerichtlichen Praxis sind dieser Stufe beispielsweise Fälle zuzuordnen, in denen ein algorithmisches System bestimmte Informationen aus einer Klageschrift extrahiert und strukturiert.[57] Auf die hinter dem algorithmischen System stehende Technologie kommt es auf der ersten Stufe des vorgeschlagenen Modells nicht an. Der Verantwortliche hat lediglich zu dokumentieren, dass der Einsatz des algorithmischen Systems so organisiert ist, dass die materielle Entscheidungshoheit beispielsweise schon aufgrund seiner technische Konzeption zwangsläufig beim Menschen liegt.

23 Der zweiten Stufe sind Anwendungsfälle zuzuordnen, in denen das algorithmische System mehr als nur unwesentlichen Einfluss auf die inhaltliche Entscheidung hat. Das ist etwa der Fall, wenn sich aus der Zuordnung eingehender Bewerbungen in Kategorien ein konkretes Ranking der Bewerber ergibt. Um den Anwendungsbereich von Art. 22 Abs. 1 DS-GVO unberührt zu lassen, ist das Ranking von einem Menschen mit hinreichenden Kenntnissen und Fähigkeiten durch einen Abgleich der Datengrundlage mit dem algorithmisch generierten Ergebnis auf Plausibilität zu prüfen.

24 Sofern das Recht auf einen wirksamen gerichtlichen Rechtsbehelf aus Art. 47 GRCh auf hohem Schutzniveau zu gewährleisten ist,[58] ist zudem die hinter dem algorithmischen System stehende Technologie zu berücksichtigen: So darf beispielsweise die Entscheidung über einen Vertragsschluss nicht wesentlich von einem KI-System beeinflusst werden, wenn es um lebenswichtige Güter oder Dienstleistungen geht.[59] Erforderlich ist eine inhaltliche Auseinandersetzung im Einzelfall durch Berücksichtigung weiterer Aspekte durch einen Menschen.

II. Verhältnis zur KI-VO

25 Basierend auf diesen Erkenntnissen stellt sich die Frage, in welchem Verhältnis das Verbot der automatisierten Einzelentscheidung in der hier vertretenen Auslegung zu den Vorgaben der KI-VO steht.

1. KI-VO als Rechtsgrundlage?

26 Dazu wird zunächst diskutiert, ob die KI-VO als Rechtsgrundlage i.S.v. Art. 22 Abs. 2 lit. b DS-GVO herangezogen werden kann.[60] Einer solchen Auslegung steht die allgemeine Konkurrenzregel in Art. 2 Abs. 7 Satz 2 KI-VO entgegen. Die Vorschrift besagt, dass die KI-VO die DS-GVO nicht berührt. Die unionsrechtliche Unberührtheitsklausel bedeutet aber nicht lediglich, dass im Kollisionsfall der in Bezug genommene Rechtsakt, hier die DS-GVO, Vorrang genießt. Unberührt bedeutet vielmehr, dass sich die beiden Rechtsakte völlig unabhängig voneinander gegenüberstehen.[61]

27 Von der Unberührtheitsklausel erfasst sind daher nicht nur Kollisionen der beiden Rechtsakte. Vielmehr folgt aus der Unberührtheit der DS-GVO auch, dass sie nicht ohne ausdrückliche Ausnahmeregelungen durch die Vorschriften der KI-VO ausgefüllt wird. Schon sprachlich deutet die Unberührtheitsklausel auf eine größtmögliche Autonomie der in Bezug genommenen DS-GVO hin.[62] Deutlich wird diese völlige Autonomie aber vor allem bei Betrachtung der Ausnahmen von der Unberührtheitsklausel: Diese soll nicht für Art. 10 Abs. 5 KI-VO sowie Art. 59 KI-VO gelten. Art. 10 Abs. 5 KI-VO ist aber laut ErwG 70 KI-VO eine Grundlage des Unionsrechts im Sinne von Art. 9 Abs. 2 lit. g DS-GVO. Würde die Unberührtheitsklausel der KI-VO nur im Kollisionsfall gelten und nicht auch die Ausfüllung von unionsrechtlichen Öffnungsklauseln in der DS-GVO betreffen, wäre die Ausnahme in Art. 2 Abs. 7 Satz 2 KI-VO jedenfalls in Bezug auf Art. 10 Abs. 5 KI-VO nicht erforderlich.[63]

28 Folglich füllen Vorgaben der KI-VO die Öffnungsklauseln der DS-GVO nur aus, sofern dies ausdrücklich vorgesehen ist. Da für die Öffnungsklausel in Art. 22 Abs. 2 lit. b DS-GVO keine entsprechende Regelung in der KI-VO existiert, können die Vorgaben der KI-VO keine Rechtsvorschrift i.S.v. Art. 22 Abs. 2 lit. b DS-GVO bilden.

2. Menschliche Aufsicht als hinreichendes Dazwischentreten?

29 Die KI-VO sieht ausdrücklich eine menschliche Aufsicht über Hochrisiko-KI-Systeme vor. Konkret sind Anbieter gem. Art. 14 Abs. 1 KI-VO i.V.m. Art. 16 lit. a KI-VO dazu verpflichtet, Hochrisiko-KI-Systeme so zu konzipieren und zu entwickeln, dass sie während der Dauer ihrer Verwendung von natürlichen Personen beaufsichtigt werden können. Komplementär müssen Betreiber gem. Art. 26 Abs. 2 KI-VO natürlichen Personen die menschliche Aufsicht übertragen. Art. 14 KI-VO enthält zwar lediglich Gestaltungsvorgaben für Hochrisiko-KI-Systeme.[64] Insbesondere Art. 14 Abs. 4 lit. a bis e KI-VO zeigen aber auf, welche konkreten Vor-

55 Vgl. Art. 6 Abs. 3 UAbs. 2 lit. a KI-VO, ErwG 53 S. 4 KI-VO.
56 Vgl. Art. 6 Abs. 3 UAbs. 2 lit. c KI-VO, ErwG 53 S. 11 KI-VO.
57 Vgl. Art. 6 Abs. 3 UAbs. 2 lit. a KI-VO, ErwG 53 S. 4 KI-VO.
58 EuGH 21.6.2022 – C-817/19 Rn. 195, BeckRS 2022, 13847.
59 Zur Anwendbarkeit von Art. 47 GRCh auf Streitigkeiten im Zusammenhang mit zivilrechtlichen Ansprüchen und Verpflichtungen vgl. Callies/Ruffert/Blanke GRCh Art. 47 Rn. 8.
60 Paal/Hüger MMR 2024, 540 (543 f.).
61 In diese Richtung auch Schild ZD 2024, 164 (165).
62 Vgl. Schmidt-Kessel MMR 2024, 122 (123).
63 Schwartmann/Jaspers/Thüsing/Kugelmann/Schwartmann/Keber/Köhler DS-GVO Anhang III Rn. 42.

kehrungen der menschlichen Aufsicht nach Vorstellung des europäischen Gesetzgebers vom Betreiber umzusetzen sind.

30 Die gesetzliche Verankerung der menschlichen Aufsicht in der KI-VO und deren Konkretisierung durch Art. 14 Abs. 4 lit. a bis c KI-VO stellen keine materielle Hoheit natürlicher Personen gegenüber Hochrisiko-KI-Systemen sicher.[65] Die darin vorgesehenen Maßnahmen verlangen lediglich ein ausreichendes Verständnis des KI-Systems und seiner Ausgaben.[66] Besondere Befugnisse der menschlichen Aufsicht oder ein Nachvollziehen der konkreten Einzelfallentscheidungen werden dagegen nicht verlangt.[67]

31 Gem. Art. 14 Abs. 4 lit. d KI-VO soll es der menschlichen Aufsicht möglich sein, in bestimmten Situationen zu beschließen, das Hochrisiko-KI-System nicht zu verwenden oder die Ausgabe des Hochrisiko-KI-Systems außer Acht zu lassen, außer Kraft zu setzen oder rückgängig zu machen. Außerdem soll sie gem. Art. 14 Abs. 4 lit. e KI-VO in den Betrieb des Hochrisiko-KI-Systems eingreifen oder den Systembetrieb mit einer „Stopptaste" unterbrechen können. Der Betreiber muss der natürlichen Person bei Übertragung der menschlichen Aufsicht laut ErwG 91 Satz 3 KI-VO entsprechende Befugnisse zugestehen. Der europäische Gesetzgeber legt hier folglich für den Einsatz von KI-Systemen fest, wie die formelle Hoheit der menschlichen Aufsicht über die KI-generierten Ergebnisse konkret auszugestalten ist.[68]

32 Eine materielle Hoheit ist demgegenüber nicht vorgesehen. Aus der technisch-organisatorisch sicherzustellenden Berechtigung, einzelne KI-generierte Ergebnisse zu überstimmen, lässt sich keine korrespondierende Pflicht zur Überprüfung aller KI-generierten Ergebnisse ableiten. Dies wird durch einen Umkehrschluss aus Art. 14 Abs. 5 UAbs. 1 KI-VO und Art. 26 Abs. 10 UAbs. 2 Satz 2 KI-VO deutlich: Demnach ist im speziellen Fall einer biometrischen Fernidentifizierung ausnahmsweise eine Überprüfung des KI-generierten Ergebnisses durch zwei natürliche Personen erforderlich.

33 Da der Ausschluss von Art. 22 Abs. 1 DS-GVO nach der hier vertretenen Ansicht die materielle Entscheidungshoheit eines Menschen voraussetzt, genügt die Einhaltung der Vorgaben von Art. 14 KI-VO dazu nicht.[69]

III. Thesenartige Zusammenfassung und Ausblick

34 Zusammenfassend lassen sich folgende Thesen festhalten:

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

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

2. Die KI-VO kann nicht als Rechtsgrundlage im Sinne von Art. 22 Abs. 2 lit. b DS-GVO herangezogen werden. Dem steht die Unberührtheitsklausel des Art. 2 Abs. 7 Satz 2 KI-VO entgegen, die nicht nur Kollisionen der beiden Rechtsakte erfasst, sondern ohne ausdrückliche Ausnahme auch Regelungen in der KI-VO entgegensteht, die die DS-GVO ausfüllen sollen.

3. Die nach der KI-VO erforderliche menschliche Aufsicht über Hochrisiko-KI-Systeme verlangt lediglich eine formelle Hoheit der menschlichen Instanz. Die Erfüllung der Vorgaben von Art. 14 Abs. 4 und Art. 26 Abs. 2 KI-VO genügt deshalb nicht, um die Anwendbarkeit von Art. 22 Abs. 1 DS-GVO auszuschließen.

35 Die KI-VO regelt abschließend, wie KI-Systeme zu entwickeln sind und wie ihr Einsatz zu organisieren ist. Wann KI-generierte Ergebnisse verwendet werden dürfen, bestimmt sich dagegen im Wesentlichen nach den allgemeinen Gesetzen. Die Bedeutung des Verbots der automatisierten Einzelentscheidung in Art. 22 Abs. 1 DS-GVO wird vor diesem Hintergrund deutlich zunehmen. In existenziellen Situationen, wie Art. 22 Abs. 1 DS-GVO sie in den Blick nimmt, genügt das Vertrauen in eine verantwortungsbewusste Entwicklung und einen organisierten Betrieb opaker Systeme nicht. Erforderlich ist vielmehr eine inhaltliche Mitwirkung des Menschen in jedem Einzelfall. Die erforderliche Abwägung zwischen praktischen und grundrechtlichen Belangen des Art. 22 Abs. 1 DS-GVO sollte deshalb künftig am Tatbestandsmerkmal der rechtlichen Wirkung oder Beeinträchtigung in ähnlicher Weise erfolgen. Wird dieses der Bedeutung der Vorschrift entsprechend eng ausgelegt, besteht für eine künstliche Begrenzung des Anwendungsbereichs im Rahmen der Bestimmung des hinreichenden menschlichen Einflusses auf die automatisierte Einzelentscheidung kein Bedürfnis mehr.

64 Horstmann ZD-Aktuell 2024, 01580.
65 AA wohl Paal/Hüger MMR 2024, 540 (542).
66 Dienes MMR 2024, 456 (459).
67 Dienes MMR 2024, 456 (461).
68 Paal/Hüger MMR 2024, 540 (542).
69 AA Golland EuZW 2024, 846 (853), der eine formelle Entscheidungshoheit ausreichen lässt.

Martin Kessen/Yvette Reif*

Einwilligungs- versus Vertragslösung bei der datenschutzrechtlichen Legitimation von „Service gegen Daten"-Geschäftsmodellen

Zugleich eine Einordnung von EuGH, Urt. v. 4.10.2024 – C-446/21 („Schrems III") in Verbindung mit EuGH, Urt. v. 4.7.2023 – C-252/21 sowie der EDSA-Stellungnahme 08/2024 zu „Consent or Pay"-Modellen

„Service gegen Daten"-Geschäftsmodelle, bei denen Nutzer mit ihren personenbezogenen Daten für einen im Übrigen kostenfreien Onlinedienst zahlen, sind aus Sicht vieler Anbieter unverzichtbar, um ihre Dienste wirtschaftlich rentabel betreiben zu können. Zwecks Refinanzierung ihrer Angebote sind die Anbieter darauf angewiesen, Einnahmen durch die Ausspielung an den Nutzerinteressen orientierter Onlinewerbung zu generieren. Die datenschutzrechtlichen Rahmenbedingungen solcher Geschäftsmodelle sind allerdings komplex und eng verwoben mit zivilrechtlichen Fragestellungen.

Mit der Vertrags- und der Einwilligungslösung stellt der Beitrag zwei Konstrukte vor, über die „Service gegen Daten"-Modelle realisiert werden können, und zeigt deren unterschiedliche Rechtsfolgen sowie Vor- und Nachteile auf. Im Zusammenhang mit der Vertragslösung werden dabei die hohen Anforderungen dargestellt, welche der EuGH an die Eröffnung des Anwendungsbereichs von Art. 6 Abs. 1 S. 1 lit. b DS-GVO als aus Anbietersicht günstige Rechtsgrundlage stellt. Der Beitrag berücksichtigt überdies die Stellungnahme 08/2024 des EDSA zu „Consent or Pay"-Modellen großer Plattformanbieter und geht der Frage nach, inwiefern das dort aufgestellte Erfordernis einer „dritten Variante" eine allgemeine Anforderung darstellen kann oder aber nur für große Plattformanbieter gilt.

I. Einleitung

1 Erneut hat Maximilian Schrems es bis vor den EuGH geschafft. Während die Verfahren „Schrems I"[1] und „Schrems II"[2] wichtige Fragen des Drittlandtransfers personenbezogener Daten klärten und die Praxis erschütterten, indem sie die jeweils bestehenden transatlantischen Abkommen mit den USA zum Transfer personenbezogener Daten in Drittländer zum Fall brachten, beim ersten Mal das „U.S.-EU Safe Harbor Framework" und beim zweiten Mal das „EU-U.S. Privacy Shield", ging es in der dritten Runde vor dem EuGH nicht um Fragen des internationalen Datentransfers, sondern um einen Streit zwischen Schrems und Meta Platforms Ireland (kurz „Meta") über die Zulässigkeit von Datenverarbeitungen im Zusammenhang mit der von Meta betriebenen Plattform Facebook.

2 Der Oberste Gerichtshof (Österreich), bei dem aktuell die Revision in der Rechtssache anhängig ist, setzte das Verfahren aus und rief den EuGH mit Blick auf insgesamt vier Rechtsfragen zur Vorabentscheidung an.

3 Schwerpunkt der vorliegenden Besprechung soll die erste Vorlagefrage nach der Abgrenzung der Erlaubnistatbestände in Art. 6 Abs. 1 S. 1 lit. a bzw. b DS-GVO sein. Diese erlangt praktische Relevanz für alle Anbieter von Onlinediensten, die ihr Angebot zumindest auch über die Anzeige verhaltensbasierter Werbung finanzieren. Aus wirtschaftlicher Perspektive ist es für diese erforderlich, die Nutzung ihres Angebots von der Gestattung verhaltensbasierter Werbung seitens der Nutzer abhängig zu machen. Auf rechtlicher Ebene stellt sich für entsprechende Anbieter die Frage, worüber sich ihre Bedürfnisse am besten abbilden lassen, über die Einholung einer Einwilligung nach Art. 7 DS-GVO oder ein Vertragskonstrukt, und welche konkreten Anforderungen im jeweiligen Fall zu stellen sind.

4 Zwar ist der EuGH auf diese Frage nicht mehr unmittelbar eingegangen, da er sie – in Übereinstimmung mit dem österr. OGH – bereits durch Urteil vom 4.7.2023[3] als beantwortet angesehen hat. Er hat allerdings in der Sachverhaltsschilderung „Consent or pay"-Modelle in den Blick genommen, indem er – ohne dass dies im vorliegenden Fall relevant wäre – darauf hingewiesen hat, dass Facebook seit November 2023 über ein solches Angebot verfügt. Daher werden im Rahmen der vorliegenden Betrachtung auch die Ausführungen des EDSA aus seiner Stellungnahme 08/2024 zu „Consent or Pay"-Modellen großer Onlineplattformen berücksichtigt.[4]

* Prof. Dr. Martin Kessen, LL.M. (University of Texas) ist Richter am BGH (III. Zivilsenat). RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn.

1 EuGH 6.10.2015 – C-362/14, BeckEuRS 2015, 487061.
2 EuGH 16.7.2020 – C-311/18, NJW 2020, 2613.
3 EuGH 4.7.2023 – C-252/2, BeckEuRS 2023, 762357.1.
4 EDSA, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (Stand: 17.4.2024).

II. Das Verfahren im Einzelnen[5]

5 Das Geschäftsmodell des sozialen Online-Netzwerks Facebook finanziert sich durch verhaltensbasierte Onlinewerbung, die sich insbes. am Konsumverhalten, den Interessen und der Lebenssituation der Nutzer ausrichtet. Zu diesem Zweck werden automatisiert detaillierte Profile der Nutzer des Netzwerks und der auf Ebene des Meta-Konzerns angebotenen Onlinedienste erstellt.

6 Bezüglich der personenbezogenen Datenverarbeitungen stützt sich Meta Platforms Ireland als Betreiber der sozialen Plattform auf den Nutzungsvertrag, den die Nutzer durch Betätigung der Schaltfläche „Registrieren" abschließen und mit dem sie den von Meta festgelegten allgemeinen Nutzungsbedingungen zustimmen. Letztere verweisen wiederum auf die von Meta festgelegten Richtlinien für die Verwendung von Daten und Cookies. Nach den Richtlinien erfasst Meta nutzer- und gerätebezogene Informationen über Aktivitäten der Nutzer innerhalb wie auch außerhalb des Netzwerks und ordnet sie den jeweiligen Facebook-Konten zu. „Off-Facebook-Daten" stammen aus dem Aufruf dritter Websites und Anwendungen, die über Programmierschnittstellen mit Facebook verbunden sind, sowie der Nutzung anderer zum Meta-Konzern gehörender Onlinedienste, insbes. Instagram und WhatsApp.

7 Schrems machte vor dem Landesgericht für Zivilrechtssachen Wien Verstöße gegen mehrere Bestimmungen der DS-GVO geltend. Aufgrund von Facebook Plug-ins auf den Websites politischer Parteien sowie auf Websites, die sich an ein homosexuelles Publikum richten, hatte Schrems zum einen Werbung für eine österreichische Politikerin und zum anderen regelmäßig Werbung erhalten, die an ein homosexuelles Publikum gerichtet war. Schrems hatte seine Homosexualität zwar öffentlich kommuniziert, seine sexuelle Orientierung aber im Rahmen seines Facebookprofils nicht angegeben.

8 Er vertrat die Ansicht, dass seine Zustimmung zu den Nutzungsbedingungen der Facebook-Plattform nicht den Voraussetzungen von Art. 6 Abs. 1 und Art. 7 DS-GVO genüge. Auch verarbeite Meta über ihn Daten i.S.v. Art. 9 DS-GVO ohne die insoweit erforderliche Einwilligung nach Art. 7 DS-GVO. Ferner habe er in die Verarbeitung der personenbezogenen Daten, die Meta von Dritten erhalten habe, nicht wirksam eingewilligt.

9 Meta sah die Datenverarbeitung nicht durch die Einwilligung von Herrn Schrems gerechtfertigt, sondern stützte sich hauptsächlich auf die Erforderlichkeit der Datenverarbeitung für die Erfüllung des mit Herrn Schrems bestehenden Vertrags i.S.v. von Art. 6 Abs. 1 S. 1 lit. b DS-GVO.[6]

10 Sowohl das Landesgericht Wien als auch die nachfolgende Berufungsinstanz, das Oberlandesgericht Wien, folgten der Rechtsauffassung von Meta. Der Oberste Gerichtshof (Österreich), bei dem aktuell die Revision von Schrems in der Rechtssache anhängig ist, entschied, wie bereits im Rahmen der Einleitung dargestellt, das Verfahren auszusetzen, um den EuGH u.a. mit Blick auf das Verhältnis von Art. 6 Abs. 1 S. 1 lit. b DS-GVO (Datenverarbeitung zur Erfüllung eines Vertrages bzw. zur Durchführung vorvertraglicher Maßnahmen) und Art. 6 Abs. 1 S. 1 lit. a i.V.m. Art. 7 DS-GVO (Einwilligung) um Vorabentscheidung zu ersuchen.[7] Weitere Vorlagefragen betrafen die Bedeutung des Grundsatzes der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) mit Blick auf Zwecke der zielgerichteten Werbung (Vorlagefrage 2), die Anwendbarkeit von Art. 9 Abs. 1 DS-GVO (Vorlagefrage 3) und die Auslegung von Art. 9 Abs. 2 lit. e DS-GVO, d.h. die Ausnahme vom grundsätzlichen Verarbeitungsverbot bzgl. besonderer Arten personenbezogener Daten mit Blick auf „offensichtlich öffentlich gemachte" Daten (Vorlagefrage 4).

11 Nach Hinweis des EuGH auf das – hier mitbesprochene – Urteil vom 4. Juli 2023 (C-252/21) zog der vorlegende Oberste Gerichtshof (Österreich) die erste und dritte Vorlagefrage zurück, weil er diese durch die zuletzt genannte Entscheidung bereits als beantwortet ansah. Maßgeblich mit Blick auf die hier relevanten „Service gegen Daten"-Geschäftsmodelle ist insofern die Aussage des Gerichts aus der Entscheidung vom 4. Juli 2023 (C-252/21), wonach Art. 6 Abs. 1 S. 1 lit. b DS-GVO dahingehend auszulegen ist, dass „die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als im Sinne dieser Vorschrift für die Erfüllung eines Vertrags, dessen Vertragsparteien die betroffenen Personen sind, erforderlich angesehen werden kann, wenn diese Verarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte".[8]

12 Konkret führt der EuGH hierzu u.a. aus, dass der Anwendungsbereich von Art. 6 Abs. 1 S. 1 lit. b DS-GVO nicht schon dadurch eröffnet wird, dass eine Verarbeitung im Vertrag erwähnt oder für dessen Erfüllung lediglich von Nutzen ist.[9] Insbesondere ist nach Auffassung des Gerichts die Personalisierung von Inhalten nicht erforderlich im Sinne der Vorschrift, um dem Nutzer die Dienste der Plattform offerieren zu können.[10] Die Personalisierung sei nicht objektiv unerlässlich, so der EuGH, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der Dienste ist.[11]

5 Vgl. hierzu EuGH 4.10.2024 – C-446/21 Rn. 12 bis 32.
6 EuGH 4.10.2024 – C-446/21 Rn. 27, BeckEuRS 2021, 7448.
7 EuGH 4.10.2024 – C-446/21 Rn. 34 , BeckEuRS 2021, 7448.
8 EuGH 4.7.2023 – C-252/21, 4. Leitsatz, BeckEuRS 2023, 762357.
9 EuGH 4.7.2023 – C-252/21 Rn. 99, BeckEuRS 2023, 762357.
10 EuGH 4.7.2023 – C-252/21 Rn. 102, BeckEuRS 2023, 762357.
11 EuGH 4.7.2023 – C-252/21 Rn. 102, BeckEuRS 2023, 762357.

13 Bzgl. der Vorlagefragen 2 und 4 traf der EuGH folgende Feststellungen:

- Der Grundsatz der Datenminimierung verbietet, dass „sämtliche personenbezogenen Daten, die ein Verantwortlicher wie der Betreiber einer Onlineplattform für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden".
- Der Umstand, dass sich eine Person bei einer öffentlichen Veranstaltung zu ihrer sexuellen Orientierung geäußert hat, berechtigt den Betreiber eines Netzwerkes wie Facebook nicht, „Daten über die sexuelle Orientierung dieser Person zu verarbeiten […], sie zu aggregieren und zu analysieren, um dieser Person personalisierte Werbung anzubieten".

14 Mit der ersten Aussage betont der EuGH die Bedeutung der in Art. 5 Abs. 1 DS-GVO geregelten „allgemeinen Strukturprinzipien"[12] und verdeutlicht, dass es sich hierbei nicht nur um bloße „Programmsätze" handelt, sondern um unmittelbar geltendes Recht.

III. EDSA-Position zum Facebook „Consent or Pay"-Modell

15 Zeitlich vor der EuGH-Entscheidung vom 4.10.2024 hat sich der EDSA im selben Jahr ausführlich mit dem „Consent or Pay"-Modell von Facebook auseinandergesetzt, nämlich im Rahmen einer Stellungnahme[13] auf Antrag der niederländischen, norwegischen und Hamburger Datenschutzbehörden, in der es um die Gültigkeit der Einwilligung zur Verarbeitung personenbezogener Daten zum Zwecke der verhaltensbezogenen Werbung im Rahmen von „Zustimmungs- oder Bezahlungsmodellen" ging, welche von großen Online-Plattformen eingesetzt werden.

16 In seiner Stellungnahme vertritt der EDSA die Auffassung, dass es für große Onlineplattformen in den meisten Fällen nicht möglich sein wird, die Anforderungen an die Einholung wirksamer datenschutzrechtlicher Einwilligungen zu erfüllen, sofern sie die Nutzer nur vor die Wahl stellen, entweder der Verarbeitung ihrer personenbezogenen Daten zu Zwecken der verhaltensbasierten Werbung zuzustimmen oder eine Gebühr zu entrichten.[14] Wenn sich der für die Verarbeitung Verantwortliche entscheide, eine Gebühr für den Zugang zu der „gleichwertigen Alternative"[15] zur Zustimmung zur verhaltensbasierten Werbung zu erheben, so sollte zudem erwogen werden, auch eine weitere kostenlose Variante ohne verhaltensbasierte Werbung anzubieten, z.B. mit Werbung, bei der weniger oder gar keine personenbezogenen Informationen verarbeitet werden, so der EDSA.[16]

17 Der Stellungnahme sollen Guidelines des EDSA zu „Consent or Pay"-Modellen nachfolgen, welche einen weiteren Anwendungsbereich als die Stellungnahme haben und sich auf alle Arten von Verantwortlichen und sämtliche Verarbeitungszwecke beziehen sollen. In Vorbereitung der Guidelines hat der EDSA am 18.11.2024 eine „Stakeholder-Anhörung" durchgeführt.[17]

IV. Analyse

1. Enge Interpretation des gesetzlichen Erlaubnistatbestandes nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO

18 Die dargestellte restriktive Interpretation von Art. 6 Abs. 1 S. 1 lit. b DS-GVO seitens des EuGH entspricht dem engen Verständnis, das auch der EDSA[18] und die herrschende Datenschutzliteratur[19] zugrunde legen. Um beurteilen zu können, in welchem Umfang eine Datenverarbeitung nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO erforderlich ist, muss nach deren Ansicht die vertragscharakteristische Leistung des Schuldverhältnisses bestimmt werden, d.h. das, was spezifisches Charakteristikum des vom Anbieter erbrachten Dienstes ist. Nur im Zusammenhang mit der vertragscharakteristischen Leistung erfolgende Verarbeitungen sind nach h.M. über Art. 6 Abs. 1 S. 1 lit. b DS-GVO gestattet.[20] Wollte man es demgegenüber für die Anwendung der Bestimmung ausreichen lassen, wenn sich ein Anbieter „bei Gelegenheit" des Vertragsschlusses Datenverarbeitungen gestatten lässt, welche mit den Beweggründen, warum die vertragliche Beziehung eingegangen wurde, nicht mehr in unmittelbarem Zusammenhang stehen, so hätten Anbieter mit entsprechender Verhandlungsmacht es in der Hand, durch Gestaltung der Vertragsbedingungen den Anwendungsbereich des gesetzlichen Erlaubnistatbestandes nahezu beliebig auszudehnen und auf diesem Weg die Grenzen zu umgehen, die sich aus dem Koppelungsverbot (Art. 7 Abs. 4 DS-GVO) ergeben.

12 Gola/Heckmann/Pötters, DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 4.

13 EDSA, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms (Stand: 17.4.2024); zur Möglichkeit solcher Stellungnahmen des EDSA nach Art. 64 Abs. 2 DS-GVO vgl. Rost K&R 2024, 698 (698).

14 EDSA, Opinion 08/2024, Executive Summary; zum Papier des EDSA ausführlich Rost K&R 2024, 698 (698 ff.).

15 Zum Konzept des gleichwertigen Alternativzugangs vgl. etwa Golland MMR 2018, 130 (134).

16 EDSA, Opinion 08/2024, Executive Summary.

17 https://www.edpb.europa.eu/news/news/2024/take-part-edpb-stakeholder-event-upcoming-guidelines-consent-or-pay_en.

18 EDSA, Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Vers. 2.0 (Stand: 8.10.2019), Rn. 26.

19 Vgl. etwa Kühling/Buchner/Buchner/Kühling, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 7 Rn. 49; Simitis/Hornung/Spiecker gen. Döhmann/Schantz, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 6 Abs. 1 Rn. 34 ff.; ähnlich BeckOK DatenschutzR/Albers/Veit, 49. Ed. 1.8.2024, DS-GVO Art. 6 Rn. 44.

20 Insoweit auch LG Frankfurt/Main 26.05.2023 - 2-24 O 156/21, GRUR-RS 2023, 18081.

2. Keine generelle Absage an die vertragliche Ausgestaltung von „Service gegen Daten"-Modellen!

19 Wichtig ist die Feststellung, dass weder mit der EuGH-Rechtsprechung noch mit der angesprochenen Stellungnahme des EDSA eine generelle Absage an eine vertragliche Ausgestaltung von „Service gegen Daten"-Modellen verbunden ist. Ganz im Gegenteil dürfte sich eine Vertragskonstruktion angesichts des Koppelungsverbots datenschutzrechtlich regelmäßig als einzig gangbarer Weg erweisen, um dem Nutzer eine Gestattung der wirtschaftlich relevanten verhaltensbasierten Onlinewerbung abzuringen.

20 Aus der Rechtsprechung des EuGH ergibt sich lediglich, dass im konkret zu beurteilenden Fall der Nutzungsbedingungen von Facebook die beklagte Meta nicht nachweisen konnte, dass „der Hauptgegenstand des Vertrages ohne die betreffende Verpflichtung nicht erfüllt werden könnte"[21]. Mit anderen Worten: Meta hatte es nicht geschafft, die geplante Verwendung der Nutzerdaten für die verfolgten kommerziellen Zwecke transparent in eine „do ut des"[22]-Austauschbeziehung im Hinblick auf die Nutzung des Netzwerks zu bringen.

21 Kern des EDSA-Papiers ist die Frage nach der Freiwilligkeit der Nutzereinwilligung. Der EDSA beschäftigt sich mit den datenschutzrechtlichen Rahmenbedingungen eines einwilligungsbasierten Geschäftsmodells.[23] Soweit die Erforderlichkeit der Verarbeitung zur Vertragserfüllung reicht, ist aber auch die Koppelung von Vertragserfüllung und datenschutzrechtlicher Einwilligung erlaubt.[24] Mit anderen Worten: Bei „echten" „Service gegen Daten"-Vertragsmodellen stellt sich die Frage nach der Freiwilligkeit der Einwilligung in dieser Form nicht.

22 Keine Lösung stellt es dar, statt auf einen Vertrag auf ein bloß tatsächliches Nutzungsverhältnis zu setzen in der Hoffnung, auf diese Weise könne ein Konflikt mit dem Koppelungsverbot vermieden werden, denn um das Konzept der Erforderlichkeit der Verarbeitung, die Zweckbindung personenbezogener Daten und die Freiwilligkeit der Einwilligung zu sichern, ist nach hier vertretener Ansicht das Verbot auch außerhalb des vertraglichen Kontexts beachtlich.[25] M.a.W.: Auch im Fall des rein faktischen Nutzungsverhältnisses dürfte die Datenschutzeinwilligung nicht verpflichtend sein.

3. Begründung echter Austauschmodelle

23 Die aus Anbietersicht wichtige „echte" vertragliche Gegenleistungsbeziehung kann nur entstehen, wenn aus (objektivierter) Nutzersicht das Angebot so zu verstehen ist, dass erstens der Anbieter sich zu seiner Leistung vertraglich verpflichten will und zweitens diese Verpflichtung eingegangen wird, damit der Nutzer seine Daten bereitstellt.[26] Dazu muss das Vertragsangebot diese Bedingungen transparent formulieren und die Annahme so gestaltet sein, dass der Verbraucher sich bewusst ist, hiermit eine auf diese Rechtsfolgen gerichtete Erklärung abzugeben.[27] Es genügt nicht, dass allein der Onlineanbieter die Bereitstellung der Daten als Gegenleistung des Nutzers betrachtet.

4. Erfordernis einer dritten Variante neben den Möglichkeiten der Zahlung von Geld bzw. der Einwilligung in Werbetracking?

24 In seiner Stellungnahme 08/2024 vertritt der EDSA zu „Consent or Pay"-Modellen wie bereits angesprochen die Auffassung, dass diese für große Plattformen nicht in der bekannten „binären Gestaltung"[28] zulässig sind, sondern stets ein „dritter Weg"[29] angeboten werden muss, welcher die Inanspruchnahme des Dienstes ermöglicht, ohne Geld zu zahlen oder in Werbetracking einzuwilligen („Free Alternative Without Behavioural Advertising").[30] Zum einen bezieht sich die EDSA-Stellungnahme aber, wie dargestellt,[31] nicht auf „Service gegen Daten"-Vertragslösungen, sondern auf bloße Einwilligungskonstrukte. Zum anderen bezieht sich das Papier des EDSA seinem Anwendungsbereich nach unmittelbar nur auf solche Einwilligungen, die von großen Plattformbetreibern eingeholt werden. Im Hinblick auf deren Marktposition und die Wichtigkeit der betroffenen Dienste bestehen insoweit erhöhte Anforderungen an den vom Anbieter zu führenden Nachweis der Freiwilligkeit der Einwilligung.[32] Zwar sollen nach dem EDSA Überlegungen aus der Stellungnahme auch herangezogen werden können, um die Wirksamkeit von Einwilligungen bei „Consent or Pay"-Modellen generell zu beurteilen[33] und zu Recht sieht der EDSA die Konditionalität als zentrales Element für die Beurteilung der Frage, ob im Fall eines „Consent or Pay"-Modells die Einwilligung freiwillig erteilt wurde.

25 Es entspricht aber dem Prinzip der Privatautonomie, dass jeder Anbieter grundsätzlich selbst entscheiden kann, wem er Dienstleistungen anbietet bzw. ob er hierfür ein Entgelt verlangt und in welcher Höhe. Nach hier vertretener Ansicht müssen daher im Ausgangspunkt auch solche Modelle zulässig sein, bei denen der Anbieter entweder Zahlung oder die Gestattung der Datenverarbeitung zu Zwecken der verhaltensbasierten Onlinewerbung verlangt, vorausge-

21 EuGH 4.7.2023 – C-252/21 Rn. 98, BeckEuRS 2023, 762357.
22 Ich gebe, damit du gibst.
23 EDSA, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, vgl. etwa Rn. 43.
24 Kühling/Buchner/Buchner/Kühling DS-GVO Art. 7 Rn. 49.
25 Vgl. bereits Kessen/Reif/Burkhardt RDV 2022, 64 (65); ebenso EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1 (4.5.2020), Rn. 25 ff.; BeckOK DatenschutzR/Stemmer, 49. Ed. 1.11.2023, DS-GVO Art. 7 Rn. 42; aA etwa Schulz, RDV 2020, 302 (306); Stroscher ZD-Aktuell 2021, 05337; Baumann/Alexiou ZD 2021, 349 (351).
26 Kessen/Reif/Burkhardt RDV 2022, 64 (67 f.).
27 Kessen/Reif/Burkhardt RDV 2022, 64 (67 f.).
28 Rost K&R 2024, 698 (698).
29 Rost K&R 2024, 698 (698).
30 EDSA, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Rn. 74; zur Bereitstellung einer kostenlosen Alternative ohne verhaltensbasierte Werbung vgl. Rost K&R 2024, 698 (702).
31 Vgl. vorstehend unter 2.
32 Rost K&R 2024, 698 (702 f.).
33 EDSA, Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms, Rn. 31.

setzt, das verlangte Entgelt ist der Höhe nach angemessen („Konzept des gleichwertigen Alternativzugangs“).[34] Denn der Betroffene erhält in diesen Fällen nur eine zusätzliche Option zur sonst einzigen Option der Bezahlung in monetärer Form.

26 Zwar ist nicht auszuschließen, dass es auch außerhalb der Konstellation großer Plattformen aus Anbieterperspektive sinnvoll sein kann, eine weitere Möglichkeit neben der Bezahlung bzw. der Gestattung verhaltensbasierter Werbung anzubieten, um im Rahmen der Accountability (Art. 5 Abs. 2 DS-GVO) den Nachweis einer wirksamen Einwilligung zu erleichtern. Entscheidend ist insofern allerdings stets der Einzelfall. Zumindest ein regelmäßiges Erfordernis für eine „dritte Variante“ ist nach hier vertretener Ansicht abzulehnen.

27 Ganz allgemein stellt sich schließlich die Frage, ob der EDSA mit dem Versuch der Festschreibung des Erfordernisses einer dritten Variante für große Plattformen nicht seine Befugnisse überschreitet. Diese Auffassung vertritt etwa Assion[35] und wirft dem EDSA vor, das Kriterium der Freiwilligkeit der Einwilligung in Richtung einer allgemeinen Inhaltskontrolle von Einwilligungen auszubauen.

V. Fazit

28 Im Ergebnis lassen sich für Onlineanbieter, welche die Nutzung ihrer Dienste nur erlauben möchten, wenn sie die Nutzerdaten zum Zwecke verhaltensbasierter Werbung verarbeiten dürfen, nachfolgende Rahmenbedingungen zusammenfassen:

Wegen des Koppelungsverbots bedarf es regelmäßig eines vertraglichen Konstruktes, um die Nutzung eines Dienstes von der Gestattung verhaltensbasierter Werbung abhängig machen zu können. Nicht ausreichend ist dabei eine bloß konditionale Verknüpfung der Gestattung,[36] wie sie jedoch in der Praxis heute noch der Regelfall zu sein scheint.[37] Es muss vielmehr ein echtes synallagmatisches Austauschverhältnis („do ut des“) entstehen, bei dem der Nutzer die Bereitstellung seiner Daten für Zwecke der verhaltensbasierten Werbung als Gegenleistung schuldet. Sofern Letzteres der Fall ist, darf eine ggf. erforderliche Einwilligung verpflichtend ausgestaltet sein.

29 Anlass, nicht allein auf Vertragsbasis zu arbeiten, sondern zudem eine Einwilligung einzuholen, kann insbes. sein, dass die Einwilligung aus anderen Rechtsgründen erforderlich ist, z.B. nach § 7 Abs. 2 Nr. 2 UWG, wenn E-Mail-Werbung versendet werden soll, oder datenschutzrechtlich, wenn allein ein Eingreifen von Art. 6 Abs. 1 S. 1 lit. b DS-GVO nicht ausreichend ist, um die Zulässigkeit der Datenverarbeitung zu begründen. Letzteres ist namentlich dann der Fall, wenn besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO verarbeitet werden sollen, z.B. Gesundheitsdaten. In diesen Fällen greift das Verarbeitungsverbot nach Art. 9 Abs. 1 DS-GVO, sofern nicht einer der Ausnahmetatbestände aus Art. 9 Abs. 2 DS-GVO einschlägig ist. Die Einholung einer ausdrücklichen Einwilligung der betroffenen Person ist der erste der in Art. 9 Abs. 2 DS-GVO genannten Ausnahmetatbestände vom Verarbeitungsverbot (lit. a).

34 Vgl. hierzu etwa Golland MMR 2018, 130 (134).
35 Assion NJW 2024, 2590 (2592).
36 Kessen/Reif/Burkhardt RDV 2022, 64 (66).
37 Hacker ZfPW 2019, 148 ff.; Kühling/Buchner/Buchner/Kühling DS-GVO Art. 7 Rn. 51.

Rechtsprechung

Kontrollverlust als Schaden beim Scraping sowie Tenorierung von Unterlassungsansprüchen im Datenschutz

DS-GVO Art. 82 Abs. 1

Leitsatz:

Immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO kann auch der bloße und kurzzeitige Verlust der Kontrolle über eigene personenbezogene Daten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung sein. Weder muss eine konkrete missbräuchliche Verwendung dieser Daten zum Nachteil des Betroffenen erfolgt sein noch bedarf es sonstiger zusätzlicher spürbarer negativer Folgen.

BGH, Urteil vom 18.11.2024 – VI ZR 10/24

I. Sachverhalt

1 Der Kläger macht Schadensersatz-, Feststellungs-, Unterlassungs- und Auskunftsansprüche wegen einer Verletzung der Datenschutz-Grundverordnung (DSGVO) durch die Beklagte geltend.

2 Die Beklagte, die ihren Sitz in Irland hat, betreibt das soziale Netzwerk Facebook, bei welchem der Kläger ein Nutzerkonto unterhält. Der Kläger hatte auf dem Netzwerk persönliche Daten eingestellt. Hierzu gehörte die für die Registrierung erforderliche und für alle Nutzer stets öffent-

lich einsehbare Angabe seines Namens, Geschlechts sowie der ihm zugewiesenen Nutzer-ID.

3 Neben den immer einsehbaren Pflichtangaben können die Nutzer in ihrem Profil weitere Daten zu ihrer Person angeben und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern ("Freunde", [auch] "Freunde von Freunden", "öffentlich") auf diese Daten zugreifen können. Die Beklagte stellt hierfür Privatsphäre-Einstellungen zur Verfügung, mit denen die Nutzer bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten. Über Funktion und Bedeutung der Privatsphäre-Einstellungen informierte die Beklagte ihre Nutzer im sog. Hilfebereich des Nutzerkontos. Der Kläger hatte in diesem Zusammenhang seine Arbeitsstätte öffentlich einsehbar angegeben, die Datenschutzeinstellung betreffend die Sichtbarkeit seiner Mobiltelefonnummer jedoch so gesetzt, dass diese nur für ihn sichtbar war. Bei den Suchbarkeitseinstellungen seines Profils, bei denen unter anderem festgelegt werden konnte, wer ihn anhand seiner Telefonnummer finden kann, hatte der Kläger es bei der Standardvoreinstellung "alle" belassen; diesen Kreis hätte er stattdessen auch auf "Freunde von Freunden" oder "Freunde" (ab Mai 2019 außerdem: "nur ich") begrenzen können.

4 War die Suchbarkeits-Einstellung eines Nutzers - wie beim Kläger - im Hinblick auf die Telefonnummer auf "alle" gestellt, erlaubte es die von der Beklagten implementierte sog. Kontakt-Import-Funktion bis September 2019 jedem Facebook-Nutzer, das Profil eines anderen Nutzers mit Hilfe der von diesem hinterlegten Telefonnummer zu finden. Hierzu konnten Nutzer Kontakte von Mobilgeräten auf Facebook hochladen, um mit Hilfe der Telefonnummern die jeweiligen Nutzer zu finden. Dies war auch dann möglich, wenn die Zielgruppenauswahl des jeweiligen Nutzers im Hinblick auf die Telefonnummer nicht auf "öffentlich", sondern etwa - wie hier - auf "nur ich" gestellt war.

5 Im Zeitraum von Januar 2018 bis September 2019 ordneten unbekannte Dritte durch die Eingabe randomisierter Ziffernfolgen über die Kontakt-Import- Funktion des Netzwerks Telefonnummern zu Nutzerkonten zu und griffen die zu diesen Nutzern vorhandenen Daten ab (sog. Scraping). Die auf diese Weise er- langten und nunmehr mit einer Telefonnummer verknüpften Daten von ca. 533 Millionen Nutzern wurden im April 2021 im Internet öffentlich verbreitet. Hiervon waren auch persönliche Daten des Klägers (Telefonnummer in Verknüpfung mit den Daten seines Nutzerkontos, d.h. Nutzer-ID, Vorname, Nachname, Ge- schlecht und Arbeitsstätte) betroffen. Nach dem Vortrag des Klägers informierte die Beklagte weder die zuständige Datenschutzbehörde noch ihn selbst über den Vorfall.

6 Der Kläger begehrt die Leistung von immateriellem Schadensersatz, weil die Beklagte in mehrfacher Hinsicht gegen die Datenschutz-Grundverordnung verstoßen und seine Daten nicht ausreichend geschützt habe. Er habe einen spürbaren Kontrollverlust über seine Daten erlitten, der zu einem massiven Anstieg von betrügerischen Kontaktversuchen geführt habe. Darüber hinaus begehrt er die Feststellung, dass die Beklagte verpflichtet ist, ihm in diesem Zusammenhang alle künftigen Schäden zu ersetzen, und macht Unterlassungs- und Auskunftsansprüche geltend. Mit Schreiben vom 23. August 2021 teilte die Beklagte dem Kläger mit, welche Daten sie über ihn gespeichert hat.

7 Das Landgericht hat der Klage teilweise stattgegeben und dem Kläger aus Art. 82 Abs. 1 DSGVO Schadensersatz in Höhe von 250 € sowie einen Teil der begehrten Rechtsverfolgungskosten zugesprochen. Im Übrigen hat es die Klage abgewiesen. Auf die vom Landgericht zugelassene Berufung der Beklagten hat das Oberlandesgericht die Entscheidung des Landgerichts unter Zurückweisung der Anschlussberufung des Klägers abgeändert und die Klage insgesamt abgewiesen. Mit seiner vom Oberlandesgericht zugelassenen Revision verfolgt der Kläger seine Ansprüche weiter.

II. Aus den Gründen

A.

8 Das Berufungsgericht hat zur Begründung seiner Entscheidung (GRUR- RS 2023, 37347) im Wesentlichen ausgeführt:

9 Der Antrag auf Feststellung einer Ersatzpflicht der Beklagten für zukünftige Schäden sei ebenso wie die Unterlassungsanträge bereits unzulässig. Hinsichtlich des Feststellungsantrags fehle es an dem notwendigen Feststellungsinteresse. Es bestehe mit Blick auf den Zeitablauf seit dem Scraping-Vorfall kein Grund, mit einem (weiteren) Schadenseintritt zu rechnen; der diesbezügliche Vortrag des Klägers sei unzureichend. Der Unterlassungsantrag zu Ziffer 3a, mit dem begehrt werde, dass die Beklagte es unterlasse, "personenbezogene Daten der Klägerseite … unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern", sei nicht hinreichend bestimmt. Hinsichtlich des Unterlassungsantrags zu Ziffer 3b, mit dem der Kläger begehre, dass die Beklagte es unterlasse, "die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf 'privat' noch durch Verwendung der Kontakt-Import-Funktion verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird", fehle es jedenfalls an dem erforderlichen Rechtsschutzbedürfnis. Denn der Kläger könne, soweit dies nicht ohnehin schon geschehen sei, seine Telefonnummer ohne Weiteres der Suchbarkeitsfunktion entziehen; auch bleibe es ihm unbenommen, seine Telefonnummer insgesamt aus dem bei der Beklagten gespeicherten Datensatz zu löschen.

10 Im Übrigen seien die geltend gemachten Ansprüche unbegründet. Ein Anspruch auf immateriellen Schadensersatz

gemäß Art. 82 DSGVO bestehe nicht. Zwar sei der Anwendungsbereich der Vorschrift eröffnet und die Beklagte auch Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Auch könne offenbleiben, ob ein Verstoß gegen die Datenschutz-Grundverordnung vorliege. Denn dem Kläger sei jedenfalls kein immaterieller Schaden entstanden.

11 Der Kläger habe einen immateriellen Schaden nicht substantiiert dargelegt. Hinsichtlich der immer öffentlichen Daten seien diese durch die Zustimmung zu den Nutzungsbedingungen der Beklagten mit Einverständnis des Klägers ohnehin öffentlich gewesen. Bezüglich der Telefonnummer habe der Kläger eine Bekanntgabe in der Öffentlichkeit zwar nicht gewollt. Er habe jedoch einen Kontrollverlust bereits nicht ausreichend dargelegt, weil er nicht dargetan habe, dass er zuvor die Kontrolle über seine Telefonnummer innegehabt habe. Die Darlegung sei erforderlich, weil es sich bei der Telefonnummer nicht um eine per se sensible Information handele, da deren Verwendung gerade dem Zweck der Kontaktaufnahme mit anderen Personen diene. Zudem stelle der Kontrollverlust als solcher keinen Schaden dar, es sei vielmehr ein Nachweis erforderlich, dass durch den Kontrollverlust ein immaterieller Schaden entstanden sei. Hierfür fehle substantiierter Vortrag. Die Behauptung von Angst, Sorge und Unwohlsein genüge nicht, der Kläger müsse vielmehr konkrete Indizien bzw. objektive Beweisanzeichen für das Vorliegen dieser Emotionen vortragen. Die verwendeten Textbausteine seien nicht ausreichend. Eine erneute Anhörung des Klägers sei nicht erforderlich, diese würde auf eine Ausforschung hinauslaufen. Auch der Vortrag zu immateriellen Schäden durch Spam-SMS und -Anrufe sowie zur aufgewendeten Zeit und Mühe genüge nicht, da ebenfalls nur Textbausteine verwendet worden seien.

[…]

B.

14 Diese Erwägungen halten der revisionsrechtlichen Überprüfung nicht in jeder Hinsicht stand. Zu Recht hat das Berufungsgericht allerdings angenommen, dass der Unterlassungsantrag zu Ziffer 3a unzulässig ist (III.) und die Klage hin- sichtlich des Auskunftsanspruchs unbegründet (V.). Hinsichtlich des Anspruchs auf Ersatz immateriellen Schadens (I.), des Feststellungsantrags (II.), des weiteren Unterlassungsantrags zu Ziff. 3b (IV.) und des Antrags auf Erstattung der vorgerichtlichen Rechtsanwaltskosten (VI.) hat die Revision des Klägers jedoch Erfolg.

I.

15 Mit der Begründung des Berufungsgerichts kann ein Anspruch auf Ersatz immateriellen Schadens aus Art. 82 Abs. 1 DSGVO nicht verneint werden.

16 1. Im Ergebnis zutreffend ist das Berufungsgericht davon ausgegangen, dass der Kläger mit seinem Antrag auf Zahlung eines immateriellen Schadensersatzes in Höhe von 1.000 € nicht mehrere selbständige, auf verschiedene Datenschutzverstöße gestützte prozessuale Ansprüche alternativ geltend macht, sondern vielmehr einen einheitlichen Anspruch auf Ersatz eines immateriellen Schadens, der sich aus mehreren Datenschutzverstößen der Beklagten ergeben soll. Soweit das Berufungsgericht allerdings den Antrag des Klägers auf Zahlung eines immateriellen Schadensersatzanspruches dahingehend ausgelegt hat, dass dieser einen Betrag von 500 € für den Scraping-Vorfall und einen weiteren Betrag von 500 € für eine unzureichende Auskunft der Beklagten geltend mache, begegnet diese Aufspaltung des einheitlichen Antrags Bedenken.

17 a) Der Streitgegenstand wird bestimmt durch das Rechtsschutzbegehren (Antrag), in dem sich die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt (Anspruchsgrund), aus dem der Kläger die begehrte Rechtsfolge herleitet (§ 253 Abs. 2 Nr. 2 ZPO). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören. Vom Streitgegenstand werden damit alle materiell-rechtlichen Ansprüche erfasst, die sich im Rahmen des gestellten Antrags aus dem zur Entscheidung unterbreiteten Lebenssachverhalt herleiten lassen (Senat, Urteil vom 14. März 2017 - VI ZR 605/15, NJOZ 2018, 1982 Rn. 17 mwN).

18 b) Danach bildet unter den Umständen des Streitfalles der geltend gemachte Anspruch auf Ersatz immateriellen Schadens in angemessener Höhe, mindestens aber von 1.000 €, den der Kläger auf den behaupteten Scraping-Vorfall und die damit in unmittelbarem Zusammenhang stehende behauptete fehlerhafte Umsetzung der Benachrichtigungs- und Auskunftspflichten durch die Beklagte stützt, einen einheitlichen Streitgegenstand. Von ihm werden sämtliche mit der inkriminierten Datenverarbeitung im Zusammenhang stehenden gerügten Verstöße gegen die Datenschutz-Grundverordnung umfasst. Denn bei natürlicher Betrachtung können die Verstöße gegen die Datenschutz-Grundverordnung nicht isoliert beurteilt werden, da sie sämtlich in einem einheitlichen Geschehen wurzeln, das hinsichtlich der damit verbundenen Folgen nicht in einzelne Datenschutzverstöße aufgespalten werden kann. Auch bildet der geltend gemachte Ersatzanspruch entgegen den in diese Richtung deutenden Ausführungen des Berufungsgerichts keinen teilbaren Streitgegenstand in dem Sinne, dass auf die verschiedenen vom Kläger behaupteten Datenschutzverstöße unterschiedliche Be- träge entfielen und diese einer gesonderten rechtlichen Beurteilung zugänglich wären. Nach der Rechtsprechung des Gerichtshofes der Europäischen Union (im Folgenden: Gerichtshof) kommt dem in Art. 82 Abs. 1 DSGVO niedergelegten Schadensersatzanspruch ausschließlich eine Ausgleichsfunktion zu. Er erfüllt keine Abschreckungs- oder gar Straffunktion, weshalb auch das Vorliegen mehrerer auf denselben Verarbeitungsvorgang bezogener Verstöße nicht zu einer Erhöhung des Schadensersatzes führt (vgl. EuGH, Urteil vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 59 f., 64 f. - juris). Diese Wertung würde unter- laufen, wenn unterschiedliche, aber sämtlich auf den Scraping-Vorfall bezogene Datenschutzverstöße in gesonderte Lebenssach-

verhalte aufgespalten würden und damit kumulativ geltend gemacht werden könnten.

19 2. Zutreffend ist das Berufungsgericht weiter davon ausgegangen, dass die Datenschutz-Grundverordnung räumlich (Art. 3 Abs. 1 DSGVO) und, da die bei der Beklagten gespeicherten Informationen des Klägers ohne Weiteres personenbezogene Daten des Klägers enthalten, auch sachlich (Art. 2 Abs. 1 DSGVO) anwendbar ist. Hinsichtlich der zeitlichen Anwendbarkeit ist nicht der Zeitpunkt der Registrierung eines Nutzerkontos im sozialen Netzwerk der Beklagten maßgeblich, sondern der Zeitpunkt des Scraping-Vorfalls. Dieser hat nach den Feststellungen des Berufungsgerichts jedenfalls in Bezug auf den Kläger nicht vor dem 25. Mai 2018 und damit dem Zeitpunkt stattgefunden, seit dem die Datenschutz-Grundverordnung gilt (Art. 99 Abs. 2 DSGVO).

20 3. Die internationale Zuständigkeit der deutschen Gerichte folgt aus Art. 82 Abs. 6 i.V.m. Art. 79 Abs. 2 Satz 2 DSGVO. Der Kläger als betroffene Person hat seinen gewöhnlichen Aufenthalt in Deutschland.

21 4. Nach der Rechtsprechung des Gerichtshofes erfordert ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DSGVO einen Verstoß gegen die Datenschutz-Grundverordnung, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (EuGH, Urteile vom 4. Oktober 2024 - C-507/23, juris Rn. 24 - Patērētāju tiesību aizsardzības centrs; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 34 - juris; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 58 - MediaMarktSaturn). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft die Person, die auf der Grundlage von Art. 82 Abs. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH, Urteile vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 35 - juris; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 60 f. - MediaMarktSaturn). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruches nach Art. 82 Abs. 1 DSGVO ein Verschulden des Verantwortlichen. Art. 82 DSGVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DSGVO dem Verantwortlichen (vgl. EuGH, Urteile vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 44 ff. - juris; vom 21. Dezember 2023 - C-667/21, EuZW 2024, 270 Rn. 94 - Krankenversicherung Nordrhein; vgl. ferner ErwG 146 Satz 2 DSGVO).

22 a) Der erforderliche Verstoß gegen die Datenschutz-Grundverordnung ist revisionsrechtlich zu unterstellen, nachdem das Berufungsgericht letztlich offengelassen hat, ob eine Verletzung insbesondere von Art. 5 Abs. 1 Buchst. b, Art. 25 Abs. 2, Art. 32 Abs. 1 DSGVO vorliegt, und deshalb die hierzu erforderlichen Feststellungen nicht getroffen hat (s. hierzu aber unten B.VIII.1).

23 aa) Dabei bedarf es im Streitfall keiner Entscheidung, ob ein Verstoß gegen die Datenschutz-Grundverordnung im Sinne des Art. 82 Abs. 1 DSGVO nicht nur die unrechtmäßige Verarbeitung von personenbezogenen Daten erfasst, wie es Art. 82 Abs. 2 Satz 1 und ErwG 146 Satz 1 DSGVO nahelegen (vgl. auch EuGH, Urteil vom 4. Mai 2023 - C-300/21, VersR 2023, 920 Rn. 36 - Österreichische Post: "Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO"), oder ob grundsätzlich auch bloße Verstöße gegen abstrakte Pflichten des Verantwortlichen außerhalb eines konkreten Verarbeitungsvorgangs haftungsbegründend sein können (zum Streitstand siehe Paal, ZfDR 2023, 325, 334 ff.; OLG Stuttgart, Urteil vom 22. November 2023 - 4 U 20/23, juris Rn. 381 ff.; offengelassen auch von OLG Oldenburg, Urteil vom 21. Mai 2024 - 13 U 100/23, juris Rn. 24; jeweils mwN). Denn angesichts des umfassenden Verarbeitungsbegriffs des Art. 4 Nr. 2 DSGVO (jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangs- reihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung) wäre auch bei einem engeren Verständnis des Art. 82 Abs. 1 DSGVO in Bezug auf den hier inmitten stehenden Scraping-Vorfall ohne Weiteres von einer Datenverarbeitung der Beklagten in Form der Speicherung, des Abfragens, der Offenlegung durch Übermittlung, der Bereitstellung und Verknüpfung auszugehen.

24 Entsprechend hat der Gerichtshof bereits entschieden, dass bei Verstößen gegen die Vorschriften der Art. 5 bis 11 DSGVO, mithin des zweiten Kapitels der Datenschutz-Grundverordnung, die Grundsätze für die Verarbeitung von Daten aufstellen, zugleich eine unrechtmäßige Datenverarbeitung vorliegt (vgl. EuGH, Urteil vom 4. Mai 2023 - C-60/22, ZD 2023, 606 Rn. 54-57 - Bundesrepublik Deutschland [Elektronisches Gerichtsfach]). Bedenken gegen die Anwendbarkeit des Art. 82 Abs. 1 DSGVO auf Verstöße gegen Art. 5 DSGVO bestehen daher nicht (vgl. auch bereits EuGH, Urteile vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 42 f. - MediaMarktSaturn; vom 14. Dezember 2023 - C-340/21, NJW 2024, 1091 Rn. 52 f. - Natsionalna agentsia za prihodite). Aber auch für Verstöße gegen Vorschriften aus dem vierten Kapitel der Datenschutz- Grundverordnung (Art. 24 bis 43 DSGVO) hat der Gerichtshof zu einzelnen Vorschriften bereits angenommen, dass ein Schadensersatzanspruch aus Art. 82 DSGVO möglich ist (vgl. zu einem Verstoß gegen Art. 32 DSGVO EuGH, Urteile vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 42 f. - MediaMarktSaturn; vom 14. Dezember 2023 - C-340/21, NJW 2024, 1091 Rn. 52 f. – Natsionalna agentsia za prihodite; für Verstöße gegen Art. 26 und 30 DSGVO Urteil vom 4. Mai 2023 - C-60/22, ZD 2023, 606 Rn. 66 f. - Bundesrepublik Deutschland [Elektronisches Gerichtsfach]).

25 bb) Es kommt in diesem Zusammenhang auch nicht darauf an, ob einer oder mehrere Verstöße gegen die Datenschutz-Grundverordnung festgestellt werden können, da der in Art. 82 Abs. 1 DSGVO vorgesehene Schadensersatz-

anspruch ausschließlich eine Ausgleichsfunktion, jedoch keine Abschreckungs- oder Straffunktion erfüllt und daher das Vorliegen mehrerer Verstöße nicht zu einer Erhöhung des Schadensersatzes führt (vgl. EuGH, Urteil vom 11. April 2024 -

C-741/21, NJW 2024, 1561 Rn. 59 f., 64 f. - juris; OLG Oldenburg, Urteil vom 21. Mai 2024 - 13 U 100/23, juris Rn. 24).

26 cc) Soweit der Kläger seinen Anspruch zusätzlich auf einen Verstoß gegen Benachrichtigungs- und Meldepflichten stützt, fehlt es mit dem Berufungsgericht jedenfalls an der Ursächlichkeit für den geltend gemachten Schaden.

27 b) Das Vorliegen eines immateriellen Schadens kann mit der Begründung des Berufungsgerichts nicht verneint werden.

28 aa) Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (st. Rspr., EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 31 - PS GbR; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 64 – MediaMarktSaturn; vom 4. Mai 2023 - C-300/21, VersR 2023, 920 Rn. 30 und 44 - Österreichische Post). Dabei soll nach ErwG 146 Satz 3 DSGVO 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, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 25 - PS GbR; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 34 - juris; vom 4. Mai 2023 - C-300/21, VersR 2023, 920 Rn. 42 - Österreichische Post).

29 Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DSGVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 26 - PS GbR; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 36 - juris; vom 4. Mai 2023 - C-300/21, VersR 2023, 920 Rn. 51 - Österreichische Post). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DSGVO verpflichtet ist, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die 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 (EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 27 - PS GbR; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 36 - juris).

30 Schließlich hat der Gerichtshof in seiner jüngeren Rechtsprechung unter Bezugnahme auf ErwG 85 DSGVO (vgl. ferner ErwG 75 DSGVO) klargestellt, dass schon der - selbst kurzzeitige - Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Be- griff des "immateriellen Schadens" den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (EuGH, Urteile vom 4. Oktober 2024 - C-200/23, juris Rn. 145, 156 i.V.m. 137- Agentsia po vpisvaniyata; vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 33 - PS GbR; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 42 - juris; vgl. zuvor bereits EuGH, Urteile vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 66 - MediaMarktSaturn; vom 14. Dezember 2023 - C-456/22, NZA 2024, 56 Rn. 17-23 - Gemeinde Ummendorf sowie - C-340/21, NJW 2024, 1091 Rn. 82 - Natsionalna agentsia za prihodite). Im ersten Satz des 85. Erwägungsgrundes der DSGVO heißt es, dass "[e]ine Verletzung des Schutzes personenbezogener Daten … - wenn nicht rechtzeitig und angemessen reagiert wird - einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen [kann], wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste … oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person". Aus dieser beispielhaften Aufzählung der "Schäden", die den betroffenen Personen entstehen können, geht nach der Rechtsprechung des Gerichtshofs hervor, dass der Unionsgesetzgeber unter den Begriff "Schaden" insbesondere auch den bloßen Verlust der Kontrolle ("the mere loss of control", "la simple perte de contrôle") über ihre eigenen Daten infolge eines Verstoßes gegen die Daten- schutz-Grundverordnung fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (EuGH, Urteile vom 4. Oktober 2024 - C-200/23, juris Rn. 145 - Agentsia po vpisvaniyata; vom 14. Dezember 2023 - C-340/21, NJW 2024, 1091 Rn. 82 - Natsionalna agentsia za prihodite).

31 Freilich muss auch insoweit die betroffene Person den Nachweis erbringen, dass sie einen solchen - d.h. in einem bloßen Kontrollverlust als solchem bestehenden - Schaden erlitten hat (vgl. EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 33 - PS GbR; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 36 und 42 - juris). Ist dieser Nachweis erbracht, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern.

32 Aber auch dann, wenn ein Kontrollverlust nicht nachgewiesen werden kann, reicht die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, aus, um einen Schadenser-

satzanspruch zu begründen (vgl. EuGH, Urteil vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 67 - MediaMarktSaturn; vom 14. Dezember 2023 - C-340/21, NJW 2024, 1091 Rn. 85 - Natsionalna agentsia za prihodite). Die Befürchtung samt ihrer negativen Folgen muss dabei ordnungsgemäß nachgewiesen sein (vgl. EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 36 - PS GbR; vom 14. Dezember 2023 - C-340/21, NJW 2024, 1091 Rn. 75-86 - Natsionalna agentsia za prihodite). 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, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 35 - PS GbR; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 68 - MediaMarktSaturn).

33 bb) Der Betroffene, der Ersatz des immateriellen Schadens verlangt, muss folglich geltend machen (und ggf. nachweisen), dass der Verstoß gegen die Datenschutz-Grundverordnung negative Folgen für ihn gehabt hat, die einen immateriellen Schaden darstellen.

34 Für eine ordnungsgemäße Darlegung muss das Gericht nach allgemeinen Grundsätzen anhand des Parteivortrags beurteilen können, ob die gesetzlichen Voraussetzungen der an eine Behauptung geknüpften Rechtsfolgen erfüllt sind. Ein Sachvortrag zur Begründung eines Anspruchs ist demnach bereits dann schlüssig und erheblich, wenn die Partei Tatsachen vorträgt, die in Verbindung mit einem Rechtssatz geeignet und erforderlich sind, das geltend gemachte Recht als in der Person der Partei entstanden erscheinen zu lassen. Die Angabe näherer Einzelheiten ist nicht erforderlich, soweit diese für die Rechtsfolgen nicht von Bedeutung sind. Das Gericht muss nur in die Lage versetzt werden, aufgrund des tatsächlichen Vorbringens der Partei zu entscheiden, ob die gesetzlichen Voraussetzungen für das Bestehen des geltend gemachten Rechts vorliegen. Sind diese Anforderungen erfüllt, ist es Sache des Tatrichters, in die Beweisaufnahme einzutreten und dabei gegebenenfalls die benannten Zeugen oder die zu vernehmende Partei nach weiteren Einzelheiten zu befragen oder einem Sachverständigen die beweiserheblichen Streitfragen zu unterbreiten (vgl. zur st. Rspr. - auch zur Geltung bei Massenverfahren wie etwa den Dieselfällen - nur Senat, Urteile vom 6. Februar 2024 - VI ZR 526/20, WM 2024, 761 Rn. 11; vom 13. Juli 2021 - VI ZR 128/20, VersR 2021, 1252 Rn. 20; vom 18. Mai 2021 - VI ZR 401/19, VersR 2021, 1046 Rn. 19; jeweils mwN).

35 cc) Nach diesen Grundsätzen durfte das Berufungsgericht den Vortrag des Klägers zu einem Schaden in Gestalt von Kontrollverlust nicht schon als per se unzureichend für die Annahme eines immateriellen Schadens im Sinne von Art. 82 Abs. 1 DSGVO ansehen. Soweit das Berufungsgericht darüber hinaus den Vortrag des Klägers zu einem weitergehenden Schaden in Gestalt von Angst, Sorge und Unwohlsein wegen Spam-SMS und -Anrufen, sowie in Gestalt von aufgewandter Zeit und Mühe in der Auseinandersetzung mit dem Scraping- Vorfall und dem Schutz vor künftigem Missbrauch für zu unsubstantiiert gehalten hat, hat es die Darlegungsanforderungen überspannt.

36 (1) Zwar ist dem Berufungsgericht zuzugestehen, dass es in Prozessen wie denen wegen des Scraping-Vorfalls bei der Beklagten nicht selten zu beobachten ist, dass "standardisierte", offenbar aus Textbausteinen zusammengesetzte Schriftsätze eingereicht werden, denen es teilweise am Bezug zum konkreten Fall und dem ihm zu Grunde liegenden spezifischen Sachverhalt fehlen mag. Für die Schlüssigkeit seiner Schadensersatzklage muss der Betroffene jedoch nur darlegen, dass und in welcher Weise gerade er von dem Scraping-Vor- fall betroffen war und welche Folgen dies für ihn hatte (vgl. zu einer vergleichbaren Situation in Anlegerschutzprozessen BGH, Urteil vom 6. Dezember 2012 - III ZR 66/12, VersR 2013, 359 Rn. 15, bei denen es jedoch zumindest individuelle Anlageberatungsgespräche gab, die zu schildern waren; vgl. ferner BGH, Beschluss vom 21. März 2022 - VIa ZB 4/21, NJW-RR 2022, 642 Rn. 13 zum Einzelfallbezug einer Berufungsbegründung). Hierbei ist mit der Revision zu berücksichtigen, dass bei einem einheitlichen Vorgang wie dem hier vorliegenden Scraping-Vorfall, bei dem vergleichbare Daten von Millionen Nutzern abgegriffen und ins Internet gestellt wurden, auch der Vortrag der Betroffenen zu den ihnen hieraus erwachsenden individuellen Folgen jedenfalls im Ausgangspunkt notwendig vergleichbare Züge trägt.

37 Das Risiko der Nichterweislichkeit - auch in Bezug auf das konkrete Ausmaß eines etwaigen Schadens - verbleibt freilich beim Anspruchsteller (vgl. EuGH, Urteil vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 35 - juris).

38 (2) Diesen Darlegungserfordernissen hat das Vorbringen des Klägers genüge getan.

39 (a) Der Scraping-Vorfall bei der Beklagten als solcher steht ebenso fest wie die anschließende Veröffentlichung der abgegriffenen Daten im Internet. Wie die Revision zu Recht rügt, hatte der Kläger bereits erstinstanzlich den Inhalt des von den Scrapern geleakten, auf ihn bezogenen Datensatzes in Form eines wörtlichen Zitats wiedergegeben und geltend gemacht, es handele sich um seine Telefonnummer, seine Nutzer-ID bei Facebook, seinen Vor- und Nachnamen, sein Geschlecht sowie seine Arbeitsstätte. Zum Kontrollverlust hat der Kläger angegeben, seine Telefonnummer stets bewusst und zielgerichtet weiterzugeben und diese nicht wahl- und grundlos der Öffentlichkeit, wie etwa im Internet, zugänglich zu machen.

40 Zu den weitergehenden Folgen hat der Kläger vorgetragen, wegen des Scraping-Vorfalls in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten verblieben zu sein. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Seit dem Vorfall erhalte er unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und Phishing-Attacken. Das habe dazu geführt, dass er nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre. Zur aufgewendeten Zeit und Mühe trug der Kläger vor, er habe sich

mit dem „Datenleak“ auseinandersetzen, den Sachverhalt er- mitteln, sich um eine Auskunft der Beklagten kümmern und selbst weitere Maß- nahmen ergreifen müssen.

41 (b) Dieses Vorbringen genügt sowohl hinsichtlich des eingetretenen Kontrollverlustes bezüglich seiner oben genannten Daten als auch hinsichtlich der sich hieraus entwickelnden besonderen Befürchtungen und Bemühungen den Anforderungen an einen hinreichend substantiierten Klagevortrag. Insbesondere war der Kläger nicht gehalten, im Einzelnen auszuführen, welchen anderen Personen er seine Daten - insbesondere seine Telefonnummer - offengelegt hat. Es genügt jedenfalls, wenn er wie hier angibt, dies zuvor bewusst und ausgewählt getan zu haben, d.h. die Daten nicht allgemein veröffentlicht zu haben.

42 Die Darlegungslast wird auch nicht dadurch erhöht, dass die Telefonnummer im Vergleich zu den in Art. 9 DSGVO genannten besonders sensiblen Daten weniger geheimhaltungsbedürftig ist. Dieser Umstand mag sich zwar auf die Höhe eines etwaigen Schadensersatzanspruches auswirken, beeinflusst die prozessuale Darlegungslast zum Anspruch dem Grunde nach hingegen nicht. Das Risiko, auch Dritte könnten seine Telefonnummer nicht datenschutzkonform verarbeiten, steht - solange sich dieses nicht unstreitig vor dem Eintritt des Scraping- Vorfalls verwirklicht hatte - der Darlegung eines Kontrollverlusts nicht entgegen. Insoweit unterscheidet sich der durch das Scraping und die dauerhafte Preisgabe der mit dem Namen des Klägers verknüpften Telefonnummer im Internet behauptete Kontrollverlust wesentlich von den Risiken, die mit einer bewussten und zielgerichteten Weitergabe der Telefonnummer an bestimmte Empfänger verbunden sind.

43 dd) Soweit das Berufungsgericht darüber hinaus in Bezug auf die "immer öffentlichen" personenbezogenen Daten des Klägers (Name, Geschlecht und Nutzer-ID) einen Schaden abgelehnt hat, weil sich der Kläger durch seine im Zuge der Registrierung auf der Plattform der Beklagten erklärte Zustimmung mit den dort geltenden Nutzungsbedingungen damit einverstanden erklärt habe, dass diese Daten in die Öffentlichkeit gelangen, hält auch diese Begründung einer revisionsrechtlichen Überprüfung nicht stand. Hinreichende Feststellungen zu den zum Registrierungszeitpunkt des Klägers geltenden Nutzungsbedingungen und deren konkreter Einbindung in das Registrierungsverfahren hat das Berufungsgericht nicht getroffen (vgl. dagegen etwa die Darlegungen in OLG Hamm, Urteil vom 15. August 2023 - 7 U 19/23, juris Rn. 112, 117 ff.; OLG Oldenburg, Urteil vom 21. Mai 2024 - 13 U 100/23, juris Rn. 30 ff.). Dies wäre jedoch erforderlich gewesen, um die Wirksamkeit einer etwaigen Einwilligung des Klägers nach Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO zu prüfen.

44 Dabei wäre insbesondere zu erörtern gewesen, ob sich die nach der Annahme des Berufungsgerichts im Rahmen der Registrierung erteilte Einwilligung des Klägers auf die konkrete Datenverarbeitung - hier: die Öffentlichkeit der Daten in Verbindung mit der Suchbarkeitsfunktion - bezieht (Art. 4 Nr. 11 DSGVO; vgl. EuGH, Urteil vom 1. Oktober 2019 - C-673/17, NJW 2019, 3433 Rn. 58, 60 - planet49), ob das dem Kläger im Zuge des Registrierungsverfahrens unterbreitete Ersuchen um Einwilligung transparent, d.h. in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache erfolgte (Art. 7 Abs. 2, ErwG 42 DSGVO), ob der Kläger seine Einwilligungserklärung auf dieser Grundlage in informierter Weise und unmissverständlich abgegeben hat (Art. 4 Nr. 11 DSGVO) und ob die Einwilligungserklärung letztlich freiwillig erfolgt ist (Art. 7 Abs. 4, ErwG 42, 43 DSGVO), wobei auch die beherrschende Stellung der Beklagten auf dem Markt für soziale Netzwerke zu berücksichtigen ist (vgl. EuGH, Urteil vom 4. Juli 2023 - C-252/21, NJW 2023, 2997 Rn. 140 ff. - Meta Platforms).

45 ee) Die Rechtsfehler sind auch entscheidungserheblich. Es kann nicht ausgeschlossen werden, dass das Berufungsgericht, hätte es den Schadensbegriff im Sinne der jüngeren Rechtsprechung des Gerichtshofes ausgelegt und die Anforderungen an die Substantiierung des klagebegründenden Vortrags nicht in unzulässiger Weise überspannt, zu dem Ergebnis gelangt wäre, dass der Kläger durch den Scraping-Vorfall einen immateriellen Schaden - ob nun allein in Gestalt des Kontrollverlustes als solchem oder darüber hinaus auch in Gestalt der geltend gemachten psychischen Beeinträchtigungen - erlitten hat.

II.

46 1. Auch die Abweisung des Feststellungsantrags als unzulässig beruht auf einem Rechtsfehler.

47 a) Der Kläger hat seinen Antrag im Berufungstermin dahingehend konkretisiert, dass er sich auf künftige materielle sowie auf künftige, derzeit noch nicht vorhersehbare immaterielle Schäden bezieht.

48 b) Im Ergebnis zutreffend hat das Berufungsgericht die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden zum Maßstab für die Annahme eines Feststellungsinteresses genommen; eine darüberhinausgehende hinreichende Schadenswahrscheinlichkeit ist nicht erforderlich. Die Möglichkeit künftiger Schäden reicht hier aus, weil es nicht um reine Vermögensschäden geht, sondern um Schäden, die aus der vom Kläger behaupteten Verletzung seines Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, mithin seines allgemeinen Persönlichkeitsrechts als einem sonstigen absolut geschützten Rechtsgut im Sinne von § 823 Abs. 1 BGB, resultieren (vgl. Senat, Urteile vom 5. Oktober 2021 - VI ZR 136/20, VersR 2022, 1184 Rn. 28; vom 29. Juni 2021 - VI ZR 10/18, ZUM 2022, 311 Rn. 30). Auch die primär als Anspruchsgrundlage herangezogene Vorschrift des Art. 82 DSGVO hat jedenfalls dann, wenn - wie hier - mit einem möglichen Verstoß gegen Art. 5 DSGVO auch eine unrechtmäßige Datenverarbeitung gerügt wird, eine Verletzung des Rechts auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh zum Inhalt (vgl. Art. 1 Abs. 2 DSGVO). Dabei kann die Möglichkeit ersatzpflichtiger künftiger Schäden ohne Weiteres zu bejahen sein, wenn ein deliktsrechtlich geschütztes absolutes Rechtsgut verletzt wurde und bereits ein Schaden eingetreten ist (Senat, Ur-

teil vom 30. Juli 2020 - VI ZR 397/19, NJW 2020, 2806 Rn. 29; vgl. eingehend Senat, Urteil vom 17. Oktober 2017 - VI ZR 423/16, BGHZ 216, 149 Rn. 49 mwN).

49 c) Nach diesen Grundsätzen ist die Möglichkeit des Eintritts künftiger Schäden hier ohne Weiteres zu bejahen. Der Kläger wurde durch den revisionsrechtlich zu unterstellenden Verstoß gegen die Datenschutz-Grundverordnung in seinem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG bzw. in seinem Recht auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh verletzt. Die Revision weist zutreffend darauf hin, dass bei der - mangels entgegenstehender Feststellungen nach dem Vortrag des Klägers revisionsrechtlich zugrunde zu legenden - fortdauernden Veröffentlichung der personenbezogenen Daten des Klägers (insbesondere seines Namens in Verbindung mit seiner Telefonnummer) das Risiko einer missbräuchlichen, ins- besondere betrügerischen Nutzung dieser Daten mit der Folge eines materiellen oder immateriellen Schadens fortbesteht. In Anbetracht des hier zu unterstellenden bereits eingetretenen und noch andauernden Kontrollverlusts über diese Daten ist eine künftige Schadensentwicklung auch nicht nur rein theoretischer Natur.

50 2. Auf Grundlage der bisherigen Feststellungen kann der Feststellungsanspruch auch in der Sache nicht verneint werden. Von seinem Rechtsstandpunkt aus folgerichtig hat sich das Berufungsgericht bislang nicht damit befasst, ob die weiteren Voraussetzungen des Anspruchs, sei es aus Art. 82 Abs. 1 DSGVO, sei es aus Vertrag, gegeben sind.

III.

51 Keinen Erfolg hat die Revision hingegen, soweit sie sich gegen die Zurückweisung des Unterlassungsantrags zu Ziffer 3a wendet. Das Berufungsgericht hat den Klageantrag zu Ziffer 3a zu Recht als unzulässig angesehen, da er nicht hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO ist.

52 1. Ein Klageantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Ur- teil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (Senat, Urteil vom 9. März 2021 - VI ZR 73/20, VersR 2021, 795 Rn. 15). Dies bedeutet bei einem Unterlassungsantrag insbesondere, dass dieser nicht derart undeutlich gefasst sein darf, dass die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (vgl. BGH, Urteile vom 28. Juli 2022 - I ZR 205/20, VersR 2022, 1389 Rn. 12; vom 2. Juni 2022 - I ZR 140/15, BGHZ 234, 56 Rn. 26).

53 Eine hinreichende Bestimmtheit ist bei einem Unterlassungsantrag für gewöhnlich gegeben, wenn eine Bezugnahme auf die konkrete Verletzungshandlung erfolgt oder die konkret angegriffene Verletzungsform antragsgegenständlich ist und der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchen Merkmalen des angegriffenen Verhaltens die Grundlage und der Anknüpfungspunkt für den Rechtsverstoß und damit das Unterlassungsgebot liegen soll (st. Rspr.; vgl. BGH, Urteil vom 2. Juni 2022 - I ZR 140/15, BGHZ 234, 56 Rn. 26 mwN; Senat, Urteile vom 9. März 2021 - VI ZR 73/20, VersR 2021, 795 Rn. 15; vom 15. Januar 2019 - VI ZR 506/17, AfP 2019, 40 Rn. 12 mwN). Die Verwendung auslegungsbedürftiger Begriffe im Klageantrag ist zulässig, wenn über ihren Sinngehalt zwischen den Parteien kein Streit besteht und objektive Maßstäbe zur Abgrenzung vorliegen, oder wenn der Kläger den auslegungsbedürftigen Begriff hinreichend konkret umschreibt und gegebenenfalls mit Beispielen unterlegt oder sein Begehren an der konkreten Verletzungshandlung ausrichtet (BGH, Urteile vom 2. Juni 2022 - I ZR 140/15, BGHZ 234, 56 Rn. 26; vom 9. September 2021 - I ZR 113/20, GRUR 2021, 1425 Rn. 12 mwN).

54 Demgegenüber sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen. Abweichendes kann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist, oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Die Wiedergabe des gesetzlichen Verbotstatbestands in der Antragsformulierung ist auch unschädlich, wenn sich das mit dem selbst nicht hinreichend klaren Antrag Begehrte im Tatsächlichen durch Auslegung unter Heranziehung des Sachvortrags des Klägers eindeutig ergibt und die betreffende tatsächliche Gestaltung zwischen den Parteien nicht infrage gestellt ist, sondern sich ihr Streit ausschließlich auf die rechtliche Qualifizierung der angegriffenen Verhaltensweise beschränkt. Eine auslegungs- bedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (st. Rspr.; vgl. nur BGH, Urteile vom 28. Juli 2022 - I ZR 205/20, VersR 2022, 1389 Rn. 12; vom 22. Juli 2021 - I ZR 194/20, GRUR 2021, 1534 Rn. 34 mwN).

55 2. An diesen Anforderungen gemessen ist der Antrag des Klägers zu Ziffer 3a, mit dem er begehrt, dass die Beklagte es unterlasse, personenbezogene Daten der Klägerseite unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern, nicht hinreichend bestimmt. Er lässt sich auch unter Heranziehung des

Klagevorbringens nicht in einer Weise auslegen, dass der Kläger ein hinreichend bestimmtes Unterlassen begehrt.

56 a) Insbesondere der Begriff des unbefugten Dritten, aber auch die an Art. 32 Abs. 1 DSGVO und damit an den bloßen Gesetzeswortlaut angelehnte Formulierung der "nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" sowie die Formulierung "Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme" sind unbestimmt. Dem steht nicht entgegen, dass die Beklagte in der Wahl der von ihr zu ergreifenden Maßnahmen eine Auswahl haben muss, solange diese geeignet sind, das konkrete Rechtsschutzziel zu erreichen (vgl. BGH, Beschluss vom 22. Februar 2024 - III ZR 63/23, juris Rn. 11; Urteil vom 5. Dezember 2023 - KZR 101/20, BGHZ 239, 116 Rn. 75; jeweils zu Unterlassungsansprüchen nach § 1004 BGB). Auch insoweit wäre es - auch mit Blick auf die Gewährung effektiven Rechtsschutzes (BGH, Urteil vom 26. Januar 2017 - I ZR 207/14, GRUR 2017, 422 Rn. 18) - dem Kläger zumutbar gewesen, die künftig zu unterlassende Verletzungshandlung weiter zu konkretisieren.

57 b) Der Kläger begehrt sinngemäß, dass die Beklagte keine Funktion anbietet, die es Dritten erlaubt, auf seine personenbezogenen Daten zuzugreifen, wenn die Beklagte nicht durch geeignete Sicherheitsmaßnahmen einem Miss- brauch dieser Funktion entgegenwirkt. Eine Eingrenzung der Verletzungshandlung findet allerdings nur insoweit statt, als auf die Kontakt-Import-Funktion Bezug genommen wird, welche der Kläger im Rahmen der Klageschrift als Einfallstor für das Datenscraping identifiziert hat. Der pauschale Hinweis auf eine Ausnutzung der Kontakt-Import-Funktion ist für eine Konkretisierung jedoch nicht hin- reichend. Er lässt nicht erkennen, durch welche konkrete Maßnahme die Be- klagte gegen die Datenschutz-Grundverordnung verstoßen hat, obwohl eine weiter gehende Konkretisierung - etwa durch Hinweis auf die Default-Einstellung der Suchbarkeitseinstellungen auf "alle", sofern dies das Klageziel sein sollte - möglich gewesen wäre. Auch der Begriff der "unbefugten Personen" hätte durch eine Darlegung der konkreten Verletzungshandlung näher definiert werden können.

58 c) Die Konkretisierung des Antrags ist auch nicht deswegen entbehrlich, weil sich eine solche aus dem Klagevorbringen ergäbe. Der Kläger hat zur Erläuterung seines Rechtsschutzziels lediglich angegeben, er verfolge ein Unterlassen, dass personenbezogene Daten ohne ausreichende Sicherheitsvorkehrungen verarbeitet werden. Eine Bezugnahme auf den Scraping-Vorfall als konkrete Verletzungsform enthält der Unterlassungsantrag nicht. Auch eine nähere Darlegung, welche konkrete Verletzungshandlung durch die Beklagte zu unterlassen sei, fehlt ebenso wie eine Erläuterung, in welchen Fällen von einer "Ausnutzung" der Kontakt-Import-Funktion bzw. von einer Nutzung durch "unbefugte Personen" auszugehen sei.

IV.

59 Mit Erfolg wendet sich die Revision aber gegen die Zurückweisung des Klageantrags zu Ziffer 3b.

60 1. Dieser Unterlassungsantrag ist entgegen der Ansicht des Berufungsgerichts zulässig.

61 a) Das Berufungsgericht ist der Ansicht, es könne offenbleiben, ob der Antrag auf Unterlassung einer Verarbeitung der Telefonnummer des Klägers auf Basis einer auf unübersichtlichen und unvollständigen Informationen beruhenden Einwilligung hinreichend bestimmt sei. Jedenfalls aber fehle es an einem Rechtsschutzbedürfnis, weil der Kläger die entsprechenden Einstellungen selbst ändern könne. Sein Vortrag, Dritte könnten diese Einstellungen umgehen, sei zu pauschal gehalten und betreffe zudem einen anderen Streitgegenstand. Schließlich könne der Kläger seine Telefonnummer im sozialen Netzwerk der Beklagten auch löschen, da die Nutzung des Netzwerks hiervon nicht abhänge. Die Telefonnummer sei nur für die erstmalige Registrierung bzw. die fakultative Zwei-Fak- tor-Authentifizierung bei der Anmeldung in seinem Nutzerkonto erforderlich.

62 b) Der Unterlassungsantrag ist trotz seiner weiten Formulierung bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Er lässt sich unter Heranziehung des Klagevorbringens dahingehend auslegen, dass der Kläger ein Unterlassen jeglicher Verarbeitung seiner Telefonnummer durch die Beklagte, die über die notwendige Verarbeitung für die Zwei-Faktor-Authentifizierung hinausgeht, begehrt.

63 Der Antrag, der als Prozesserklärung vom Revisionsgericht selbst auszulegen ist (vgl. Senat, Urteil vom 16. April 2024 - VI ZR 223/21, WM 2024, 991 Rn. 17 mwN), ist nicht so zu verstehen, dass der Kläger "die Unterlassung der Verarbeitung seiner Telefonnummer ohne eindeutige Informationen, dass diese auch bei der Einstellung 'privat' ausgelesen werden kann", begehrt (so aber OLG Stuttgart, Urteil vom 22. November 2023 - 4 U 20/23, juris Rn. 245, 247). Diese Information lag dem Kläger jedenfalls zum Zeitpunkt der Klageerhebung bereits vor, so dass ein entsprechendes Verständnis den Antrag sinnentleerte und der Auslegungsregel zuwiderliefe, nach der im Zweifel dasjenige gewollt ist, was nach den Maßstäben der Rechtsordnung vernünftig ist und der wohlverstandenen Interessenlage entspricht (vgl. hierzu BGH, Urteile vom 15. Mai 2024 - VIII ZR 293/23, MDR 2024, 924 Rn. 22; vom 14. Mai 2024 - XI ZR 51/23, juris Rn. 15; jeweils mwN). Vielmehr begehrt der Kläger, dass die Beklagte seine Telefonnummer nicht - wie zur Zeit des Scraping-Vorfalls - auf Basis einer von ihm erteilten Einwilligung weiterverarbeitet, da diese Einwilligung nach seinem Verständnis mangels Transparenz unwirksam ist, weil ihm das Ausmaß der Datenverarbeitung betreffend seine Telefonnummer bei Erteilung der Einwilligung nicht verständlich war. Der Unterlassungsantrag konkretisiert darüber hinaus - anders als der Unterlassungsantrag zu Ziffer 3a - die inkriminierte Verletzungshandlung, nämlich die behauptete unrechtmäßige Verarbeitung auf Grundlage einer unwirksamen Einwilligung. Aus welchen Gründen die Einwilligung unwirksam sein soll, ergibt sich aus der weiteren Formulierung des Antrags. Nach Ansicht des Klägers wurde diese "wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt […], namentlich ohne eindeutige Informationen dar- über, dass die Telefonnummer auch bei Einstellung auf 'privat' noch

durch Verwendung der Kontakt-Import-Funktion verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird".

64 Der so verstandene Unterlassungsantrag ist hinreichend bestimmt, da der Beklagten ohne weiteres deutlich wird, für welche Zwecke sie die Telefonnummer des Klägers noch verarbeiten darf und für welche der Kläger die Unterlassung der Datenverarbeitung begehrt.

[…]

92 2. Sollte das Berufungsgericht im wiedereröffneten Berufungsverfahren einen Anspruch aus Art. 82 Abs. 1 DSGVO dem Grunde nach bejahen, wird es bei der Ermittlung der dann festzustellenden Höhe des immateriellen Schadens zudem von Folgendem auszugehen haben:

93 a) Die Datenschutz-Grundverordnung enthält keine Bestimmung über die Bemessung des aus Art. 82 Abs. 1 DSGVO geschuldeten Schadensersatzes. Insbesondere können aufgrund des unterschiedlichen Zwecks der Vorschriften nicht die in Art. 83 DSGVO genannten Kriterien herangezogen werden (EuGH, Urteile vom 4. Oktober 2024 - C-507/23, juris Rn. 39 ff. - Patērētāju tiesību aizsardzības centrs; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 57, 62 - juris). Die Bemessung richtet sich vielmehr entsprechend dem Grundsatz der Verfahrensautonomie nach den innerstaatlichen Vorschriften über den Umfang der finanziellen Entschädigung (EuGH, Urteile vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 58 - juris; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 53 - MediaMarktSaturn; vom 21. Dezember 2023 - C-667/21, EuZW 2024, 270 Rn. 83 und 101 - Krankenversicherung Nordrhein; jeweils mwN). In Deutschland ist somit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden (BAG, NJW 2022, 2779 Rn. 14).

94 b) Die innerstaatliche Verfahrensautonomie bei der Ermittlung des nach Art. 82 DSGVO zu ersetzenden Schadens unterliegt freilich mehreren aus dem Unionsrecht folgenden Einschränkungen.

95 aa) Die Modalitäten der Schadensermittlung dürfen bei einem - wie im Streitfall - unter das Unionsrecht fallenden Sachverhalt nicht ungünstiger sein als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz). Auch dürfen sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz) (vgl. EuGH, Urteile vom 4. Oktober 2024 - C-507/23, juris Rn. 31 - Patērētāju tiesību aizsardzības centrs; vom 20. Juni 2024 - C-182/22 und C-189/22, NJW 2024, 2599 Rn. 32 - Scalable Capital; vom 4. Mai 2023 - C-300/21, NJW 2023, 1930 Rn. 53 - Österreichische Post).

96 bb) In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs, wie sie in ErwG 146 Satz 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld als "vollständig und wirksam" anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO dagegen nicht erfüllen (vgl. EuGH, Urteil vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 42 - PS GbR; vgl. auch EuGH, Urteile vom 4. Oktober 2024 - C-507/23, juris Rn. 43 f. - Patērētāju tiesību aizsardzības centrs; vom 20. Juni 2024 - C-182/22 und C-189/22, NJW 2024, 2599 Rn. 23 - Scalable Capital; vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 59 - juris; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 47 - MediaMarktSaturn). Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegen- über derselben Person begangen (EuGH, Urteil vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 60 und 64 f. - juris) und ob er vorsätzlich gehandelt hat (EuGH, Urteil vom 20. Juni 2024 - C-182/22 und C-189/22, NJW 2024, 2599 Rn. 29 f. - Scalable Capital).

97 Im Ergebnis soll die Höhe der Entschädigung zwar nicht hinter dem vollständigen Ausgleich des Schadens zurückbleiben, sie darf aber auch nicht in einer Höhe bemessen werden, die über den vollständigen Ersatz des Schadens hinausginge (vgl. EuGH, Urteile vom 11. April 2024 - C-741/21, NJW 2024, 1561 Rn. 60 - juris; vom 25. Januar 2024 - C-687/21, CR 2024, 160 Rn. 48 - MediaMarktSaturn). Ist der Schaden gering, ist daher auch ein Schadensersatz in nur geringer Höhe zuzusprechen (vgl. EuGH, Urteile vom 4. Oktober 2024 - C-507/23, juris Rn. 35 - Patērētāju tiesību aizsardzības centrs; vom 20. Juni 2024 - C-182/22 und C-189/22, NJW 2024, 2599 Rn. 45 f. - Scalable Capital). Dies gilt auch unter Berücksichtigung des Umstandes, dass der durch eine Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung (vgl. dazu EuGH, Urteile vom 4. Oktober 2024 - C-200/23, juris Rn. 151- Agentsia po vpisvaniyata; vom 20. Juni 2024 - C-182/22 und C-189/22, NJW 2024, 2599 Rn. 39 - Scalable Capital).

98 c) Daraus ergeben sich Vorgaben sowohl in Bezug auf die Untergrenze als auch auf die Obergrenze des nach Art. 82 Abs. 1 DSGVO zu gewährenden Schadensersatzes, die das Schätzungsermessen des Tatgerichts (§ 287 ZPO) rechtlich begrenzen.

99 aa) Ist nach den Feststellungen des Gerichts allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten gegeben, weil weitere Schäden nicht nachgewiesen sind, hat der Tatrichter bei der Schätzung des Schadens insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten (vgl. Art. 9 Abs. 1 DSGVO) und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Weiter hat er die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle etwa durch Entfernung einer

Veröffentlichung aus dem Internet (inkl. Archiven) oder Änderung des personenbezogenen Datums (z.B. Rufnummernwechsel; neue Kreditkartennummer) in den Blick zu nehmen. Als Anhalt für einen noch effektiven Ausgleich könnte in den Fällen, in denen die Wiedererlangung der Kontrolle mit verhältnis- mäßigem Aufwand möglich wäre, etwa der hypothetische Aufwand für die Wiedererlangung der Kontrolle (hier insbesondere eines Rufnummernwechsels) dienen.

100 bb) Äußerst zweifelhaft erscheint daher, ob hier eine Festsetzung in "gegebenenfalls nur einstelliger Höhe" mit dem Effektivitätsgrundsatz zu vereinbaren wäre (so aber obiter OLG Celle, Urteil vom 4. April 2024 - 5 U 31/23, juris Rn. 102). Dagegen hätte der Senat von Rechts wegen keine Bedenken, den not- wendigen Ausgleich für den eingetretenen Kontrollverlust als solchem in einem Fall wie dem streitgegenständlichen in einer Größenordnung von 100 € (so obiter OLG Hamm, GRUR-RS 2024, 16856 Rn. 40) zu bemessen.

101 cc) Macht der Betroffene psychische Beeinträchtigungen geltend, die über die mit dem eingetretenen Kontrollverlust für jedermann unmittelbar zusammenhängenden Unannehmlichkeiten hinausgehen, ist das Tatgericht gegebenenfalls gehalten, den Betroffenen anzuhören, um die notwendigen Feststellungen hierzu treffen zu können. Ausgehend davon wird es gegebenenfalls einen Betrag als Ausgleich festzusetzen haben, der über dem im Falle eines bloßen Kontrollverlustes zuzusprechenden Betrag liegt.

III. Anmerkung

1. Kontrollverlust als immaterieller Schaden

Die Erörterungen des BGH zum Kontrollverlust als immateriellem Schaden (Rn. 31 f.) stehen im Widerspruch zu der zuvor vom BGH selbst zusammengefassten Rechtsprechung des EuGH (Rn. 28 f.).

Der EuGH verlangt für einen Anspruch aus Art. 82 DSGVO den Eintritt eines Schadens, der über einen Verstoß gegen die Bestimmungen der DSGVO hinausgehen muss (EuGH 20.6.2024 – C-590/22, CR 2024, 460 Rn. 25). Zwar kann mit dem EuGH bereits der zeitlich begrenzte Verlust der Kontrolle über die eigenen personenbezogenen Daten durch deren öffentliche Zugänglichmachung auch ohne Hinzutreten „zusätzlicher spürbarer negativer Folgen" einen solchen immateriellen Schaden verursachen (EuGH 4.10.2024 - C-200/23, K&R 2025, 29 Rn. 156). Bedingung ist jedoch, dass die betroffene Person einen Schaden durch den Kontrollverlust nachweist (EuGH 20.6.2024 – C-590/22, CR 2024, 460 Rn. 27; EuGH 4.10.2024 - C-200/23, K&R 2025, 29 Rn. 156; ebenso EuG 8.1.2025 – T-354/22 zu Art. 65 VO 2018/1725, Rn. 54).

Statt nach den Vorgaben des EuGH zu subsumieren, ob a) ein Kontrollverlust vorliegt, und b) hieraus der betroffenen Person ein Schaden entstanden ist, stellt der BGH lapidar fest, dass die Feststellung des Kontrollverlusts hinreichend ist, weil „dieser selbst den immateriellen Schaden dar[stellt]" (Rn. 31). Diese Ausführungen bestätigt der BGH sodann, wenn er vom „Vortrag des Klägers zu einem Schaden in Gestalt von Kontrollverlust" spricht (Rn. 35). Wenn aber wie im vom BGH zu entscheidenden Sachverhalt der Verstoß gegen die DSGVO – unbefugter Zugang zu personenbezogenen Daten durch Dritte mittels Scraping nebst anschließender Verbreitung der Daten im Internet (Rn. 5) – zugleich den Kontrollverlust bewirkt und dieser Kontrollverlust wiederum der entstandene Schaden ist, setzt der BGH damit den Verstoß gegen die Bestimmungen der DSGVO doch dem Eintritt eines Schadens gleich. Dies hat der EuGH jedoch – wie vom BGH selbst dargestellt – ausdrücklich abgelehnt (anders und zutreffend bei der Wegnahme eines USB-Sticks BAG 17.10.2024 – 8 AZR 215/23 Rn. 10 ff.). Ebenso wie der BGH argumentiert bedauerlicherweise zuletzt das EuG, was den mit einer rechtswidrigen Drittlandübermittlung aus seiner Sicht einhergehenden Kontrollverlust mit einem Schadensersatz in Höhe von 400,00 EUR belegt (EuG 8.1.2025 – T-354/22, BeckRS 2025, 12 zu Art. 65 VO 2018/1725, Rn. 194 ff.). Das Urteil des EuG ist allerdings noch nicht rechtskräftig.

Aufgrund der Gleichsetzung von Kontrollverlust und Schaden mussten sich BGH und EuG auch mit der bedeutsamen Frage nicht mehr befassen, ob ein Kontrollverlust beim Scraping in einem sozialen Netzwerk überhaupt noch eintreten und in der Folge zu einem immateriellen Schaden führen kann, wenn zuvor die betroffene Person durch die Teilnahme am sozialen Netzwerk einen Kontrollverlust initial selbst und bewusst bereits bewirkt und sich dieser durch das Scraping allenfalls in einem im Einzelfall festzustellenden Umfang intensiviert hat.

2. Schadensbegriff

Der BGH befasst sich ausführlich mit den Anforderungen an die Darlegungslast bei immateriellen Schäden (Rn. 34) und legt dar, was alles – aus Sicht des BGH ausreichende (Rn. 41) – mögliche nachteilige Folgen und damit immaterielle Schäden der betroffenen Person sein könnten. Neben einem „Zustand großen Unwohlseins" sowie „großer Sorge über möglichen Missbrauch der […] Daten" stellt der BGH dabei auch auf die „Zeit und Mühe" ab, die der Kläger für die Auseinandersetzung mit dem „Datenleck", die Ermittlung des Sachverhalts und das Ergreifen weiterer Maßnahmen aufgewendet habe (Rn. 35, 40).

Das überrascht, denn aufgewendete Zeit und Mühe für konkrete Handlungen sind quantitativ ermittelbar und ein materieller Schaden, kein immaterieller Schaden. Um materielle Schäden geht es aber ausweislich der Einführung des BGH in die Rechtsfrage (Rn. 27) gar nicht. Auch wenn § 287 Abs. 1 ZPO der geschädigten Person bereits die Darlegung erleichtert, ob ein Schaden entstanden ist (BGH 30.07.2024 – VI ZR 122/23, NJW-RR 2024, 1350, Rn. 12), dürfte ein Vortrag zu Art und Umfang der aufgewendeten Zeit und Mühe zur

Substantiierung unverzichtbar sein, um überhaupt eine Beweisaufnahme und Tatsachenfeststellungen durch das erkennende Gericht zu ermöglichen. Dabei wäre dann auch zu erörtern, ob die behauptete „Zeit und Mühe" angemessen oder unverhältnismäßig waren, weil etwa einem Übereifer der betroffenen Person geschuldet. Auf all dies verzichtet der BGH, indem er diese materiellen Aufwände dem Kontrollverlust und den „sich hieraus entwickelnden besonderen Befürchtungen und Bemühungen" zuordnet. Damit übersteigert der BGH den von ihm mit dem immateriellen Schaden gleichgesetzten Kontrollverlust weiter und verselbständigt diesen zu einem (vermeintlichen → oben Ziff. 1) Gesamtschadensbild.

3. Unterlassungsanträge

Von besonderem Praxisinteresse sind die Ausführungen des BGH zur Bestimmtheit von Unterlassungsanträgen (B.III. und B.IV.). Ein Vorabentscheidungsersuchen des BGH (BGH 26.9.2023 – VI ZR 97/22, ZD 2024, 90, beim EuGH anhängig unter C-655/23) zur Frage, ob betroffene Personen Unterlassungsansprüche geltend machen können, wurde vom EuGH bislang nicht entschieden. Auf den ersten Blick überrascht es daher, dass der BGH das Verfahren in Bezug auf die geltend gemachten Unterlassungsansprüche nicht ausgesetzt hat. Er begründet dies damit, dass mangels entsprechender Feststellungen des Berufungsgerichts die Entscheidungserheblichkeit nicht beurteilt werden könne (Rn. 83). Nicht überzeugen kann jedoch seine nicht weiter begründete Mutmaßung, dass unabhängig von einer möglichen Sperrwirkung der DSGVO insbesondere ein Unterlassungsanspruch aus dem Nutzungsvertrag selbst in Betracht käme (Rn. 83). Sollte der EuGH eine Sperrwirkung der DSGVO bejahen, wäre auch eine vertragliche Herleitung von Unterlassungsansprüchen betroffener Personen kaum rechtlich haltbar. Denn die Argumente für eine Sperrwirkung dürften sowohl Unterlassungsansprüche nach §§ 1004 Abs. 1 Satz 2 iVm 823 BGB erfassen als auch solche aus §§ 280 Abs. 1, 241 Abs. 2 BGB (zu den Argumenten ausführlich Koetsier/Kremer CR 2023, 359).

Sollte die DSGVO keine Sperrwirkung entfalten, besteht für Verantwortliche ein erhebliches Risiko, mit pauschalen und inhaltlich überschießenden Unterlassungsansprüchen von einer im Zweifel kaum überschaubaren Anzahl an Einzelpersonen konfrontiert zu werden. Erst recht, wenn Verantwortliche personenbezogene Daten im Zusammenhang mit neuen Technologien und innovativen Geschäftsmodellen verarbeiten. Daher sind die Ausführungen des BGH zur Frage der notwendigen Bestimmtheit von Unterlassungsanträgen (Rn. 52 ff.) von erheblicher Bedeutung. Zentral ist dabei seine Feststellung, dass Ungenauigkeiten nicht zu Lasten des Beklagten gehen dürfen und es nicht dem Vollstreckungsgericht überlassen bleiben darf, was dem Beklagten verboten ist (Rn. 52). Unterlassungsanträge sind für den BGH dann hinreichend bestimmt, wenn sie sich auf die konkrete Verletzungshandlung beziehen, die konkret angegriffene Verletzungsform enthalten und zumindest unter Heranziehung des Klagevortrags erkennbar ist, in welchen Merkmalen des angegriffenen Verhaltens die behauptete Rechtsverletzung liegen soll (Rn. 53). Dagegen erachtet er bloße Wiederholungen des Gesetzeswortlauts für nicht ausreichend (Rn. 54). Folgerichtig hält er auslegungsbedürftige Begriffe in Unterlassungsanträgen wie den „unbefugten Dritten" oder eine dem Gesetzeswortlaut vergleichbare Formulierung wie der „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" für zu unbestimmt und verlangt vom Kläger zumutbare Anstrengungen, die künftig zu unterlassende Verletzungshandlung weiter zu konkretisieren (Rn. 56). Dass Gerichte nach diesen Maßstäben Unterlassungsanträge genau und kritisch prüfen müssen, zeigt sich am zweiten – vom BGH für zulässig erachteten – Unterlassungsantrag. Ein Antrag, die Telefonnummer nicht ohne eine „wirksamen Einwilligung" auszulesen, wäre nicht nur zu unbestimmt gewesen, sondern auch insofern unzulässig, als eine Verarbeitung der Telefonnummer auch ohne Einwilligung zur Zwei-Faktor-Authentifizierung erforderlich sein kann. Bestimmtheit erlangt der Unterlassungsantrag nur, weil er die vermeintliche Verletzungshandlung (Verarbeitung aufgrund einer unwirksamen Einwilligung) konkretisiert und auch die Gründe, aus denen die Einwilligung unwirksam sein soll, konkret benennt (Rn. 63).

4. Risiko von Massenverfahren

Die niedrigen Darlegungs- und Beweispflichten, die der BGH betroffenen Personen für den Nachweis immaterieller Schäden auferlegt, seine irrtümliche Gleichsetzung von Pflichtverletzung und Schaden (→ oben Ziff. 1) sowie seine Annahme, dass nicht nur Verstöße gegen Pflichten aus Kapitel 2, sondern auch aus Kapitel 4 der DSGVO grundsätzlich einen immateriellen Schadensersatzanspruch begründen können (Rn. 24), befeuert das Risiko von Massenverfahren, die eine bereits heute an der Belastungsgrenze operierende Justiz endgültig überlasten könnten. Die einzelne Klage mag bei einem Schadensersatz von 100 EUR für Anwälte finanziell unattraktiv sein. Der BGH lässt es für einen schlüssigen Sachvortrag aber bereits genügen, dass die vorgetragenen Tatsachen geeignet und erforderlich sind, einen Schadensersatzanspruch zu begründen. Individuelle Einzelheiten hält er für nicht erforderlich und betont, dass bei einem viele Personen betreffenden Ereignis auch die daraus erwachsenden individuellen Folgen grundsätzlich vergleichbar seien. (Rn. 34 ff.) Dies ermöglicht hochstandardisierte Klageerhebungen, was bei einer entsprechenden Verfahrensanzahl auch bei niedrigen Streitwerten für hierauf spezialisierte Anwaltskanzleien und Legal Tech Provider ein lohnendes Geschäftsmodell sein kann.

Nicht entschieden hat der BGH, ob immaterielle Schadensersatzansprüche übertragbar sind. Offen bleibt damit, ob zusätzlich zur Möglichkeit von Verbänden, nach Art. 80 DSGVO bzw. nach dem VDuG Ansprüche geltend zu machen, Dritte – wie etwa Kanzleien – gegen

Übernahme des Prozessrisikos Schadensersatzansprüche im Wege der gewillkürten Prozessstandschaft eine Vielzahl von Ansprüchen in einer Klage bündeln können (dies für zulässig erachtend OLG Hamm 24.07.2024 – 11 U 69/23, GRUR-RS 2024, 24099, Rz. 66 ff.). Sollte der EuGH dies künftig für zulässig erachten, dürfte der BGH mit seinem Urteil den Weg bereitet haben, dass Verantwortliche selbst bei im Ergebnis kaum erheblichen Datenschutzverstößen auch auf diese Weise mit uU existenzbedrohenden Ersatzansprüchen konfrontiert werden können.

Sascha Kremer/Philip Laue
Sascha Kremer ist Fachanwalt für Informationstechnologie-Recht, externer Datenschutzbeauftragter und Datenschutzauditor; Dr. Philip Laue ist Syndikusrechtsanwalt und Datenschutzbeauftragter.

Zur Datenverarbeitung aufgrund berechtigter Interessen: Wirtschaftliches Interesse rechtfertigt Datenverarbeitung nur bei absoluter Notwendigkeit

DS-GVO Art. 1, 4, 5, 6, 13

Leitsatz:

Art. 6 Abs. 1 Unterabs. 1 Buchst. f der Verordnung (EU) 2016/679 […] ist dahin auszulegen, dass eine Verarbeitung personenbezogener Daten, die darin besteht, personenbezogene Daten der Mitglieder eines Sportverbands in Verfolgung des wirtschaftlichen Interesses des Verantwortlichen gegen Entgelt offenzulegen, nur dann als im Sinne dieser Vorschrift zur Wahrung der berechtigten Interessen dieses Verantwortlichen erforderlich angesehen werden kann, wenn die Verarbeitung zur Verwirklichung des in Rede stehenden berechtigten Interesses absolut notwendig ist und sofern in Anbetracht aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten dieser Mitglieder gegenüber dem berechtigten Interesse nicht überwiegen. Diese Vorschrift verlangt zwar nicht, dass ein solches Interesse gesetzlich bestimmt wird, sie erfordert jedoch, dass das geltend gemachte berechtigte Interesse rechtmäßig ist.

EuGH, Urteil vom 4.10.2024 – C-621/22

I. Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 6 Abs. 1 Unterabs. 1 Buchst. f der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1, berichtigt in ABl. 2018, L 127, S. 2, im Folgenden: DSGVO).

Es ergeht im Rahmen eines Rechtsstreits zwischen dem Koninklijke Nederlandse Lawn Tennisbond (Königlicher Niederländischer Rasentennisverband, im Folgenden: KNLTB) und der Autoriteit Persoonsgegevens (Datenschutzbehörde, Niederlande, im Folgenden: AP) wegen der Entscheidung dieser Behörde, aufgrund eines Verstoßes gegen die Vorschriften der DSGVO gegen den KNLTB eine Geldbuße zu verhängen.

Aus der Vorlageentscheidung geht hervor, dass der KNLTB ein in Form eines Vereins gegründeter Sportverband ist. Die Mitglieder dieses Sportverbands sind die ihm angeschlossenen Tennisvereine sowie deren Mitglieder. Tritt eine Person einem dem KNLTB angeschlossenen Tennisverein bei, wird sie automatisch auch Mitglied des KNLTB. Der KNLTB arbeitet mit Sponsoren zusammen, mit dem erklärten Ziel, die Verbreitung und Sichtbarkeit des Tennissports sowie den Bestand seiner Mitglieder zu steigern.

Im Jahr 2018 legte der KNLTB gegenüber zweien seiner Sponsoren, der SportshopsDirect BV (im Folgenden: TennisDirect), einer Gesellschaft, die Sportartikel vertreibt, und der Nederlandse Loterij Organisatie BV (im Folgenden: NLO), dem größten Anbieter von Glücks- und Kasinospielen in den Niederlanden, personenbezogene Daten seiner Mitglieder offen. Für die Bereitstellung der betreffenden personenbezogenen Daten erhielt der KNLTB von seinen Sponsoren ein Entgelt.

Insbesondere stellte der KNLTB TennisDirect am 11. Juni 2018 die Namen, Anschriften und Wohnorte seiner Mitglieder für den postalischen Versand eines Werbebriefs bereit. Zu diesem Zweck übermittelte TennisDirect diese Daten wiederum dem Postdienstleister PostNL zum Drucken dieses Werbebriefs.

Außerdem legte der KNLTB gegenüber der NLO am 29. Juni 2018 neben den Namen, Anschriften und Wohnorten seiner Mitglieder deren Geburtsdaten, Festnetznummern, Mobiltelefonnummern und E-Mail-Adressen sowie die Namen der Tennisclubs offen, denen diese Mitglieder angehörten. Zweck dieser Bereitstellung war eine Telefonwerbemaßnahme, in deren Rahmen die NLO diese Daten an die von ihr beauftragten Callcenter übermittelte.

Auf Beschwerden einiger Mitglieder des KNLTB hin stellte die AP fest, dass der KNLTB gegen Art. 6 Abs. 1 Unterabs. 1 Buchst. a und f in Verbindung mit Art. 5 Abs. 1 Buchst. a DSGVO verstoßen habe, weil er die personenbezogenen Daten seiner Mitglieder ohne deren Einwilligung und ohne rechtmäßige Grundlage offengelegt habe. Die AP verhängte daher mit Entscheidung vom 20. Dezember 2019 gegen den KNLTB eine Geldbuße in Höhe von 525 000 Euro.

Der KNLTB erhob gegen diese Entscheidung Klage bei dem vorlegenden Gericht, der Rechtbank Amsterdam (Bezirksgericht Amsterdam, Niederlande).

Zwar ist zwischen den Parteien des Ausgangsverfahrens unstreitig, dass der KNLTB nicht die Einwilligung seiner Einzelmitglieder zur Bereitstellung ihrer personenbezogenen Daten an die oben genannten Sponsoren erhalten hatte und dass Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO nicht als Grundlage für die betreffende Verarbeitung herangezogen werden kann. Laut dem KNLTB beruhte die Bereitstellung dieser Daten jedoch auf einem berechtigten Interesse im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO. Dieses Interesse bestehe zum einen darin, eine enge Verbindung zwischen diesem Verband und seinen Mitgliedern herzustellen, und zum anderen darin, diesen einen Mehrwert für die Mitgliedschaft in Form von Preisnachlässen und Angeboten bei Partnern bieten zu können, die es diesen Mitgliedern ermöglichten, Tennis zu einem günstigen und erschwinglichen Preis zu betreiben.

Die AP ist der Ansicht, dass nur zum Gesetz gehörende, gesetzliche und in einem Gesetz festgelegte Interessen berechtigte Interessen im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO seien. Es müsse sich um Interessen handeln, die vom Unionsgesetzgeber oder vom nationalen Gesetzgeber als schutzwürdig angesehen würden und unter Rückgriff auf ein „positives Kriterium" zu beurteilen seien. Im vorliegenden Fall handele es sich nicht um solche Interessen.

Der KNLTB ist anderer Ansicht und argumentiert, dass sich ein berechtigtes Interesse nicht zwangsläufig aus einem Grundrecht oder einem Rechtsgrundsatz ergeben müsse, sondern dass jedes Interesse ein berechtigtes Interesse darstellen könne, außer wenn es gesetzeswidrig sei, so dass ein solches Interesse unter Rückgriff auf ein „negatives Kriterium" zu beurteilen sei.

Im Verfahren vor dem vorlegenden Gericht wurde von den Parteien die Bedeutung des Begriffs „berechtigtes Interesse" in Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO sowie insbesondere die Frage erörtert, ob ein rein wirtschaftliches Interesse, das darin bestehe, personenbezogene Daten der Mitglieder eines Tennisverbands ohne deren Einwilligung zum Zweck der Direktwerbung an Sponsoren zu verkaufen, als berechtigtes Interesse angesehen werden könne.

Da die Rechtbank Amsterdam (Bezirksgericht Amsterdam) Zweifel hinsichtlich der Auslegung des Begriffs „berechtigte Interessen" im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO hat, hat sie beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Wie hat das vorlegende Gericht den Begriff „berechtigtes Interesse" im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO auszulegen?
2. Ist dieser Begriff so auszulegen, wie die Beklagte ihn auslegt? Erfasst er ausschließlich zum Gesetz gehörende, gesetzliche und in einem Gesetz festgelegte Interessen?
3. Oder kann jedes Interesse ein berechtigtes Interesse sein, sofern es dem Gesetz nicht zuwiderläuft? Konkreter: Sind ein rein kommerzielles Interesse und das vorliegende Interesse, nämlich die Bereitstellung personenbezogener Daten gegen Entgelt ohne Zustimmung der betroffenen Person, unter bestimmten Umständen als ein berechtigtes Interesse einzustufen? Falls ja: Welche Umstände bestimmen, ob ein rein kommerzielles Interesse ein berechtigtes Interesse ist?

II. Gründe

23 Nach ständiger Rechtsprechung ist es im Rahmen des durch Art. 267 AEUV eingeführten Verfahrens der Zusammenarbeit zwischen den nationalen Gerichten und dem Gerichtshof Aufgabe des Gerichtshofs, dem nationalen Gericht eine für die Entscheidung des bei diesem anhängigen Rechtsstreits sachdienliche Antwort zu geben. Hierzu hat er die ihm vorgelegten Fragen gegebenenfalls umzuformulieren (Urteil vom 20. Juni 2024, Greislzel, C-35/23, EU:C:2024:532, Rn. 39 und die dort angeführte Rechtsprechung).

24 Im vorliegenden Fall betreffen die Vorlagefragen die Möglichkeit, auf der Grundlage von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO zu rechtfertigen, dass ein Sportverband personenbezogene Daten seiner Mitglieder gegen Entgelt gegenüber Sponsoren dieses Verbands für Werbemaßnahmen offenlegt.

25 Daraus folgt, dass das vorlegende Gericht mit seinen Vorlagefragen, die zusammen zu beantworten sind, im Wesentlichen wissen möchte, ob Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO dahin auszulegen ist, dass eine Verarbeitung personenbezogener Daten, die darin besteht, personenbezogene Daten der Mitglieder eines Sportverbands in Verfolgung des wirtschaftlichen Interesses des Verantwortlichen gegen Entgelt offenzulegen, als im Sinne dieser Vorschrift zur Wahrung der berechtigten Interessen dieses Verantwortlichen oder eines Dritten erforderlich angesehen werden kann und ob diese Vorschrift verlangt, dass ein solches Interesse gesetzlich bestimmt wird.

26 Vorab ist darauf hinzuweisen, dass das Ziel der DSGVO, wie sich aus ihrem Art. 1 sowie ihren Erwägungsgründen 1 und 10 ergibt, u. a. darin besteht, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres in Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union und in Art. 16 Abs. 1 AEUV verankerten Rechts auf Privatleben – bei der Verarbeitung personenbezogener Daten zu gewährleisten (Urteil vom 7. März 2024, IAB Europe, C-604/22, EU:C:2024:214, Rn. 53 und die dort angeführte Rechtsprechung).

27 Gemäß diesem Ziel muss jede Verarbeitung personenbezogener Daten insbesondere mit den in Art. 5 dieser Verordnung aufgestellten Grundsätzen für die Verarbeitung solcher Daten im Einklang stehen und die in Art. 6 der Verordnung aufgezählten Rechtmäßigkeitsvoraussetzungen erfüllen (vgl. in diesem Sinne Urteile vom 6. Oktober 2020, La Quadrature du Net u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 208, sowie vom 11. Juli 2024, Meta Platforms Ireland [Verbandsklage], C-757/22, EU:C:2024:598, Rn. 49).

28 Insoweit ist hervorzuheben, dass personenbezogene Daten nach Art. 5 Abs. 1 Buchst. a DSGVO auf rechtmäßige Weise, nach Treu und Glauben sowie in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen.

29 Insbesondere enthält, wie der Gerichtshof entschieden hat, Art. 6 Abs. 1 Unterabs. 1 DSGVO eine erschöpfende und abschließende Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann. Daher muss eine Verarbeitung unter einen der in dieser Bestimmung vorgesehenen Fälle subsumierbar sein, um als rechtmäßig angesehen werden zu können (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 90).

30 Nach Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung dazu für einen oder mehrere bestimmte Zwecke gegeben hat. Liegt keine solche Einwilligung vor oder wurde die Einwilligung nicht freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich im Sinne von Art. 4 Nr. 11 DSGVO erteilt, ist eine solche Verarbeitung gleichwohl gerechtfertigt, wenn sie eine der in Art. 6 Abs. 1 Unterabs. 1 Buchst. b bis f genannten Voraussetzungen in Bezug auf die Erforderlichkeit erfüllt.

31 In diesem Zusammenhang sind die in Art. 6 Abs. 1 Unterabs. 1 Buchst. b bis f DSGVO vorgesehenen Rechtfertigungsgründe eng auszulegen, da sie dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 93 und die dort angeführte Rechtsprechung).

32 Außerdem braucht nach der Rechtsprechung des Gerichtshofs, wenn festgestellt werden kann, dass eine Verarbeitung personenbezogener Daten aus einem der in Art. 6 Abs. 1 Unterabs. 1 Buchst. b bis f DSGVO vorgesehenen Gründe erforderlich ist, nicht geprüft zu werden, ob diese Verarbeitung auch unter einen anderen dieser Gründe fällt (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 94 und die dort angeführte Rechtsprechung).

33 Der Gerichtshof hat zudem entschieden, dass nach Art. 5 DSGVO der Verantwortliche die Beweislast dafür trägt, dass die Daten u. a. für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Ferner obliegt es nach Art. 13 Abs. 1 Buchst. c dieser Verordnung, wenn personenbezogene Daten bei der betroffenen Person erhoben werden, dem Verantwortlichen, diese Person über die Zwecke, für die diese Daten verarbeitet werden sollen, sowie über die Rechtsgrundlage dieser Verarbeitung zu informieren (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 95).

34 Im vorliegenden Fall geht aus den dem Gerichtshof vorliegenden Akten hervor, dass die Mitglieder des KNLTB nicht im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. a DSGVO eingewilligt haben, dass der KNLTB sie betreffende personenbezogene Daten gegen Entgelt gegenüber Dritten, namentlich TennisDirect und der NLO, offenlegt.

35 Unter diesen Umständen ist, um dem vorlegenden Gericht eine sachdienliche Antwort zu geben, zu prüfen, ob Art. 6 Abs. 1 Unterabs. 1 Buchst. f dieser Verordnung, auf den sich das Vorabentscheidungsersuchen speziell bezieht, herangezogen werden kann, um die Offenlegung solcher Daten gegenüber Dritten zu rechtfertigen.

36 Insoweit ist darauf hinzuweisen, dass nach Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO eine Verarbeitung personenbezogener Daten rechtmäßig ist, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz dieser personenbezogenen Daten erfordern, überwiegen.

37 Wie der Gerichtshof bereits entschieden hat, ist die Verarbeitung personenbezogener Daten nach dieser Bestimmung unter drei kumulativen Voraussetzungen rechtmäßig: Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein, und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 106 und die dort angeführte Rechtsprechung).

38 Was erstens die Voraussetzung der Wahrnehmung eines „berechtigten Interesses" betrifft, kann in Ermangelung einer Definition dieses Begriffs durch die DSGVO, wie der Gerichtshof bereits entschieden hat, ein breites Spektrum von Interessen grundsätzlich als berechtigt gelten (vgl. in diesem Sinne Urteil vom 7. Dezember 2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 76).

39 Wie sich auch aus dem 47. Erwägungsgrund der DSGVO ergibt, der den Begriff „berechtigtes Interesse" betrifft, hat der Unionsgesetzgeber nicht verlangt, dass das Interesse eines Verantwortlichen gesetzlich geregelt sein muss, damit die von diesem Verantwortlichen vorgenommene Verarbeitung personenbezogener Daten rechtmäßig im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f dieser Verordnung ist. Dies gilt umso mehr, als dieser Erwägungsgrund die Zwecke der Direktwerbung im Allgemeinen als Beispiel für

berechtigte Interessen anführt, die von einem Verantwortlichen wahrgenommen werden können.

40 Allerdings verlangt der Begriff „berechtigtes Interesse“ im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO, auch wenn er nicht auf gesetzlich verankerte und bestimmte Interessen beschränkt ist, dass das geltend gemachte berechtigte Interesse rechtmäßig ist.

41 Außerdem obliegt es nach Art. 13 Abs. 1 Buchst. d DSGVO dem Verantwortlichen, einer betroffenen Person zu dem Zeitpunkt, zu dem personenbezogene Daten bei ihr erhoben werden, die verfolgten berechtigten Interessen mitzuteilen, wenn diese Verarbeitung auf Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO beruht (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 107).

42 Was zweitens die Voraussetzung der Erforderlichkeit der Verarbeitung personenbezogener Daten zur Verwirklichung des wahrgenommenen berechtigten Interesses angeht, so verlangt diese vom vorlegenden Gericht, zu prüfen, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Art. 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen (Urteil vom 7. Dezember 2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 77 sowie die dort angeführte Rechtsprechung).

43 In diesem Zusammenhang ist auch darauf hinzuweisen, dass die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem Grundsatz der „Datenminimierung“ zu prüfen ist, der in Art. 5 Abs. 1 Buchst. c DSGVO verankert ist und verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sind (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 109 und die dort angeführte Rechtsprechung).

44 Was schließlich drittens die Voraussetzung betrifft, dass die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen, so hat der Gerichtshof bereits entschieden, dass diese Voraussetzung eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen gebietet, die grundsätzlich von den konkreten Umständen des Einzelfalls abhängt, und dass es daher Sache des vorlegenden Gerichts ist, diese Abwägung unter Berücksichtigung dieser spezifischen Umstände vorzunehmen (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 110 und die dort angeführte Rechtsprechung).

45 Außerdem können, wie sich aus dem 47. Erwägungsgrund der DSGVO ergibt, die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen insbesondere dann überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer solchen Verarbeitung rechnet (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 112).

46 Letztlich ist es Sache des vorlegenden Gerichts, zu beurteilen, ob im Hinblick auf die Verarbeitung personenbezogener Daten, um die es im Ausgangsverfahren geht, die drei in Rn. 37 des vorliegenden Urteils genannten Voraussetzungen erfüllt sind; der Gerichtshof kann dem nationalen Gericht auf dessen Vorabentscheidungsersuchen hin jedoch sachdienliche Hinweise für diese Prüfung geben (Urteile vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 96, und vom 7. Dezember 2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 81 sowie die dort angeführte Rechtsprechung).

47 Im vorliegenden Fall verweist das vorlegende Gericht erstens zur Voraussetzung der Wahrnehmung eines berechtigten Interesses durch den Verantwortlichen oder einen Dritten im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO auf das wirtschaftliche Interesse des Verantwortlichen, d. h. eines Sportverbands wie des KNLTB, personenbezogene Daten seiner Mitglieder gegen Entgelt für Werbe- und Marketingzwecke, insbesondere den Versand von Werbebotschaften und Angeboten an seine Mitglieder durch Dritte, gegenüber diesen Dritten, nämlich im vorliegenden Fall einem Unternehmen, das Sportartikel vertreibt, sowie einem Anbieter von Glücks- und Kasinospielen in den Niederlanden, offenzulegen.

48 Insoweit hat der Gerichtshof nicht ausgeschlossen, dass ein wirtschaftliches Interesse des Verantwortlichen, das in der Bewerbung und dem Verkauf von Werbeflächen für Marketingzwecke besteht, als ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO angesehen werden kann (vgl. entsprechend Urteil vom 13. Mai 2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 73).

49 Unter diesen Umständen könnte ein wirtschaftliches Interesse des Verantwortlichen wie das oben in Rn. 47 genannte ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO darstellen, sofern es nicht gesetzeswidrig ist. Es ist jedoch Sache des vorlegenden Gerichts, das Vorliegen eines solchen Interesses im Einzelfall unter Berücksichtigung des anwendbaren Rechtsrahmens und aller Umstände der Rechtssache zu beurteilen.

50 Sollte ein solches Interesse als berechtigt angesehen werden, müsste der Verantwortliche zudem allen anderen ihm obliegenden Pflichten aus der DSGVO nachkommen, damit die Wahrnehmung dieses Interesses eine Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO rechtfertigen kann.

51 Was zweitens die Voraussetzung der Erforderlichkeit dieser Verarbeitung zur Verwirklichung des betreffenden Interes-

ses angeht und insbesondere das Vorliegen von Mitteln, die ebenso geeignet sind und weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen, ist festzustellen, dass es einem Sportverband wie dem KNLTB, der personenbezogene Daten seiner Mitglieder gegen Entgelt gegenüber Dritten offenlegen möchte, insbesondere möglich wäre, seine Mitglieder im Voraus zu informieren und sie zu fragen, ob sie möchten, dass ihre Daten für Werbe- oder Marketingzwecke an Dritte weitergegeben werden.

52 Diese Lösung würde es den betroffenen Mitgliedern ermöglichen, im Einklang mit dem oben in Rn. 43 genannten Grundsatz der Datenminimierung die Kontrolle über die Offenlegung ihrer personenbezogenen Daten zu behalten und so die Offenlegung dieser Daten auf das zu beschränken, was für die Zwecke, für die diese Daten übermittelt und verarbeitet werden, tatsächlich notwendig und erheblich ist (vgl. entsprechend Urteil vom 12. September 2024, HTB Neunte Immobilien Portfolio und Ökorenta Neue Energien Ökostabil IV, C-17/22 und C-18/22, EU:C:2024:738, Rn. 60).

53 Ein Verfahren wie das in der vorstehenden Randnummer beschriebene könnte einen geringeren Eingriff in das Recht auf Schutz der Vertraulichkeit der personenbezogenen Daten der betroffenen Person beinhalten und es gleichzeitig dem Verantwortlichen ermöglichen, das von ihm geltend gemachte berechtigte Interesse ebenso wirksam wahrzunehmen; dies zu prüfen ist jedoch Sache des vorlegenden Gerichts (vgl. entsprechend Urteil vom 12. September 2024, HTB Neunte Immobilien Portfolio und Ökorenta Neue Energien Ökostabil IV, C-17/22 und C-18/22, EU:C:2024:738, Rn. 61).

54 Drittens muss das vorlegende Gericht bei der Abwägung der Interessen, die es im Hinblick auf die besonderen Umstände des Ausgangsverfahrens vorzunehmen hat, insbesondere die vernünftigen Erwartungen der betroffenen Person sowie den Umfang der in Rede stehenden Verarbeitung und deren Auswirkungen auf diese Person berücksichtigen (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 116).

55 Bei der entsprechenden Abwägung hat das vorlegende Gericht zu prüfen, ob das in Art. 8 Abs. 1 der Charta und in Art. 16 Abs. 1 AEUV verankerte Recht der Mitglieder von Tennisvereinen auf Privatsphäre hinsichtlich der Verarbeitung ihrer personenbezogenen Daten Vorrang vor dem wirtschaftlichen Interesse eines nationalen Tennisverbands hat. Hierbei ist, wie sich aus dem 47. Erwägungsgrund der DSGVO ergibt, der Frage besondere Bedeutung beizumessen, ob diese Mitglieder zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten zum Zweck des Beitritts zu einem Tennisverein vernünftigerweise absehen konnten, dass diese Daten gegen Entgelt für Werbe- und Marketingzwecke gegenüber Dritten, im vorliegenden Fall Sponsoren des KNLTB, offengelegt werden.

56 Außerdem wird das vorlegende Gericht den Umstand zu berücksichtigen haben, dass die betreffenden Daten u. a. an einen Anbieter von Glücks- und Kasinospielen wie die NLO übermittelt werden, dessen Werbe- und Marketingmaßnahmen, auch wenn sie rechtmäßig sind, in einem Kontext stattfinden, der entgegen dem 47. Erwägungsgrund der DSGVO nicht durch eine maßgebliche und angemessene Beziehung zwischen den betroffenen Personen und dem Verantwortlichen gekennzeichnet zu sein scheint. Außerdem könnte sich die Verarbeitung solcher Daten unter bestimmten Umständen nachteilig auf die Mitglieder der betreffenden Tennisvereine auswirken, da sie sie der Gefahr der Entwicklung einer Spielsucht aussetzen könnten.

57 Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 6 Abs. 1 Unterabs. 1 Buchst. f DSGVO dahin auszulegen ist, dass eine Verarbeitung personenbezogener Daten, die darin besteht, personenbezogene Daten der Mitglieder eines Sportverbands in Verfolgung des wirtschaftlichen Interesses des Verantwortlichen gegen Entgelt offenzulegen, nur dann als im Sinne dieser Vorschrift zur Wahrung der berechtigten Interessen dieses Verantwortlichen erforderlich angesehen werden kann, wenn die Verarbeitung zur Verwirklichung des in Rede stehenden berechtigten Interesses absolut notwendig ist und sofern in Anbetracht aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten dieser Mitglieder gegenüber dem berechtigten Interesse nicht überwiegen. Diese Vorschrift verlangt zwar nicht, dass ein solches Interesse gesetzlich bestimmt wird, sie erfordert jedoch, dass das geltend gemachte berechtigte Interesse rechtmäßig ist.

III. Anmerkung

Der EuGH verweist in ständiger Rechtsprechung auf den dreistufigen Prüfaufbau der Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Der Verantwortliche muss vor Beginn der Datenverarbeitung nachweisen können, dass er erstens ein berechtigtes Interesse an der Datenverarbeitung hat, zweitens die Datenverarbeitung zur Verwirklichung dieses berechtigten Interesses erforderlich ist und drittens die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen. Die dritte Voraussetzung ist im Rahmen einer Abwägung des Einzelfalls zu prüfen.

Im Ausgangsverfahren hat die niederländische Datenschutzaufsichtsbehörde eine restriktive Auslegung des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO vertreten. Sie war der Ansicht, dass nur solche Interessen als berechtigt gelten, die ausdrücklich nach einer Vorschrift des Unionsrechts oder des nationalen Rechts als schutzwürdig anerkannt sind.

Diese Auffassung überrascht, da sie von den Leitlinien der europäischen Datenschutzaufsichtsbehörden abweicht. Bereits die Artikel-29-Datenschutzgruppe hat in der Stellungnahme 06/2014 zum Begriff des berechtigten Interesses klargestellt, dass der für die Verarbeitung Verantwortliche oder ein Dritter Interessen jeder Art verfolgen kann, solange diese nicht rechtswidrig sind. An diesem Verständnis hält auch der Europäische Da-

tenschutzausschuss (EDSA) in seiner unmittelbar nach der EuGH-Entscheidung veröffentlichten Leitlinie zum berechtigten Interesse fest (Leitlinie 01/2024, angenommen am 8.10.2024).

Der EuGH geht in der vorliegenden Entscheidung nicht darauf ein, ob die Übermittlung der Mitgliederdaten durch den Sportverband an Sponsoren eine Form des Direktmarketings darstellt. Der Begriff „Direktmarketing" wird zwar in Erwägungsgrund 47 genannt, jedoch in der DSGVO nicht definiert.

Nach Auffassung der deutschen Aufsichtsbehörden umfasst der Begriff des Direktmarketings die unmittelbare Ansprache einer Zielperson, beispielsweise postalisch, per E-Mail, Telefon oder SMS (DSK, Orientierungshilfe Werbung, Februar 2022). Hiervon ausgehend liegt im Ausgangsverfahren kein Fall einer Direktwerbung vor, da die Werbemaßnahme nicht durch den Sportverband als Verantwortlichen durchgeführt wird, sondern durch Dritte, d.h. den Sponsoren, denen die Daten der Vereinsmitglieder übermittelt wurden. Gleichwohl erkennt der EuGH darin ein wirtschaftliches Interesse des Sportverbandes, da dieser für die Datenübermittlung zur Werbezwecken der Sponsoren ein Entgelt erhält.

Der EuGH führt unter Verweis auf die Entscheidungen zu Meta (EuGH 4.7.2023 - C-252/21) und SCHUFA (EuGH 7.12.2023 - C-634/21) aus, dass das Interesse eines Verantwortlichen gesetzlich nicht geregelt sein muss, damit die Verarbeitung rechtmäßig im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO ist. Demnach ist auch das wirtschaftliche Interesse an der Weitergabe personenbezogener Daten gegen eine Vergütung ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Die Datenverarbeitung zum Zwecke des Adresshandels oder anderer Formen der Verarbeitung personenbezogener Daten durch Datenbroker für Werbezwecke kann daher ebenfalls ein berechtigtes Interesse darstellen.

Auf der zweiten Stufe betont der EuGH das enge Verständnis der Erforderlichkeit. Eine Datenverarbeitung ist nur erforderlich, wenn das berechtigte Interesse nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen. Die Voraussetzung der Erforderlichkeit konkretisiert den Grundsatz der „Datenminimierung" gem. Art. 5 Abs. 1 lit. c DSGVO. Das vorlegende Gericht hat im Einzelfall zu prüfen, ob weniger einschneidende Maßnahmen als die Offenlegung der Mitgliederdaten in Betracht kommen. Einen großen Entscheidungsspielraum hat das Ausganggericht dabei nicht, denn der EuGH deutete an, dass es wohl möglich wäre, die Mitglieder zu fragen, ob sie die Weitergabe ihrer Daten für Werbezwecke „möchten". Der EuGH verwendet bewusst nicht den Begriff „einwilligen", weil dies angesichts der Gleichrangigkeit der Rechtsgrundlagen nach Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO systemwidrig wäre und auch die Datenverarbeitung aufgrund einer Einwilligung dem Gebot der Datenminimierung unterliegt. Der EuGH kann daher nur so verstanden werden, dass er als milderes Mittel ein „Einverständnis light" fordert, d.h. eine Zustimmung der betroffenen Person, die nicht die strengen Anforderungen an eine vorherige, informierte und freiwillige Einwilligung nach Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 7 DSGVO erfüllt. So verstanden dürfte die Datenverarbeitung auf Grundlage eines berechtigen Interessen regelmäßig ausscheiden, wenn die betroffene Person die Datenverarbeitung auf Nachfrage ablehnt.

Schließlich befasst sich der EuGH mit der dritten Voraussetzung für eine Datenverarbeitung auf Grundlage berechtigter Interessen ein - der Abwägung im engeren Sinne. Wie bereits in der Entscheidung im Verfahren Meta (EuGH 4.7.2023 - C-252/21) ausgeführt, misst der EuGH den vernünftigen Erwartungen der betroffenen Personen an die Datenverarbeitung besonderes Gewicht bei.

Für die Abwägung bedeutet dies, dass die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen regelmäßig überwiegen, wenn die betroffene Person nicht mit der Datenverarbeitung rechnet. Dies ist beispielsweise der Fall, wenn die Verarbeitung überraschend oder unüblich ist und nicht den typischen Geschäftspraktiken entspricht.

Darüber hinaus weist der EuGH darauf hin, dass im Rahmen der dritten Stufe auch die Beziehung zwischen der betroffenen Person und dem Verantwortlichen berücksichtigt werden muss. Eine enge und vertrauensvolle Beziehung könnte dabei zugunsten des Verantwortlichen sprechen, während eine lose Beziehung die Rechte der betroffenen Person stärker ins Gewicht fallen lässt.

Zudem hat der Verantwortliche negative Folgen oder Gefahren, die sich aus der Datenverarbeitung ergeben können, in die Abwägung einzubeziehen – selbst dann, wenn diese nicht unmittelbar von ihm selbst verursacht werden, sondern durch Dritte, beispielsweise durch Sponsoren oder Datenempfänger. Diese Verpflichtung verdeutlicht die Pflicht des Verantwortlichen, auch indirekte Risiken und Folgen der Datenverarbeitung für die betroffenen Personen in den Blick zu nehmen.

Weitere Kriterien für die Abwägung auf der dritten Stufe sind in der Leitlinie des EDSA zu finden. Diese Leitlinie gehört zur Pflichtlektüre, weil sie auch Hinweise enthält, wie die Interessenabwägung zu dokumentieren ist, damit Verantwortliche ihrer Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO nachkommen können.

Kristin Benedikt
Kristin Benedikt ist Richterin am Verwaltungsgericht Regensburg.

Grenzen der vollständigen Aufzeichnung der Onlineaktivitäten für Werbezwecke („Schrems III“)

DS-GVO Art. 5, 6, 7, 9

Leitsätze:

1. Art. 5 Abs. 1 Buchst. c der Verordnung (EU) 2016/679 [...] ist dahin auszulegen, dass der darin festgelegte Grundsatz der „Datenminimierung“ dem entgegensteht, dass sämtliche personenbezogenen Daten, die ein Verantwortlicher wie der Betreiber einer Onlineplattform für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden.

2. Art. 9 Abs. 2 Buchst. e der Verordnung 2016/679 ist dahin auszulegen, dass der Umstand, dass sich eine Person bei einer öffentlich zugänglichen Podiumsdiskussion zu ihrer sexuellen Orientierung geäußert hat, dem Betreiber einer Onlineplattform für ein soziales Netzwerk nicht gestattet, andere Daten über die sexuelle Orientierung dieser Person zu verarbeiten, die er gegebenenfalls außerhalb dieser Plattform von Anwendungen und Websites dritter Partner im Hinblick darauf erhalten hat, sie zu aggregieren und zu analysieren, um dieser Person personalisierte Werbung anzubieten.

EuGH, Urteil vom 4.10.2024 – C-446/21

I. Sachverhalt

Dem Urteil liegt ein Rechtsstreit zwischen Schrems und Meta Platforms Ireland (Meta) über die Zulässigkeit von personalisierter Werbung auf der Plattform Facebook zugrunde. Um die auf der Plattform veröffentliche Werbung zu personalisieren, erstellt Meta detaillierte Nutzerprofile. Diesen Profilen liegen nicht nur Informationen zugrunde, die auf dem Netzwerk selbst gesammelt wurden, sondern auch Daten von externen Webseiten und anderen Meta-Diensten wie Instagram und WhatsApp.

Schrems klagte vor dem Landgericht Wien, da er Facebook-Werbung zu politischen Themen und für Webseiten erhielt, die sich an ein homosexuellen Publikum richteten, obwohl er weder seine politische Einstellung noch seine sexuelle Orientierung im Profil angegeben hatte. Facebook hatte die Daten an anderer Stelle erhoben und daraufhin seinem Nutzerprofil zugrunde gelegt. Er trug vor, in seinen Rechten verletzt zu sein, da die Analyse seines Nutzungsverhaltens auf externen Webseiten einer Einwilligung bedürfe. Dies gelte insb., wenn besondere Kategorien personenbezogener Daten, wie die Sexualität und politische Orientierung, betroffen seien. Eine Einwilligung habe er nicht wirksam erteilt. Seine Zustimmung zu den Nutzungsbedingungen entspreche nicht den Anforderungen an eine Einwilligung im Sinne der DS-GVO.

Meta verteidigte sich mit der Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung und wollte die Datenverarbeitung auf Art. 6 Abs. 1 lit. b DS-GVO stützen. Art. 9 DS-GVO fordere keine Einwilligung, da Schrems seine sexuelle Orientierung öffentlich auf einer Podiumsdiskussion bekannt gemacht habe (Art. 9 Abs. 2 lit. e DS-GVO). Der Oberste Gerichtshof Österreichs legte die Sache dem EuGH vor, um Klarheit über das Verhältnis zwischen Vertragserfüllung und Einwilligung, über das Gebot der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO und die Auslegung von Art. 9 DS-GVO im Kontext personalisierter Werbung zu bekommen. Da einige der Vorlagefragen bereits durch das Urteil vom 4. Juli 2023 (C-252/21) geklärt worden waren, zog das Gericht die Vorlagefragen eins und drei nach einem Hinweis des EuGH zurück. Im Zentrum des Urteils steht daher nicht die Frage nach der richtigen Rechtsgrundlage für Datenverarbeitungen zu Werbezwecken, sondern nach den Anforderungen an das „Wie“ der Datenverarbeitung zu Werbezwecken.

II. Aus den Gründen

Zur zweiten Frage:

52 [Es] ist zur zeitlichen Begrenzung einer Verarbeitung personenbezogener Daten wie der Verarbeitung, um die es im Ausgangsverfahren geht, darauf hinzuweisen, dass der Gerichtshof bereits entschieden hat, dass der Verantwortliche unter Berücksichtigung des Grundsatzes der Datenminimierung verpflichtet ist, den Zeitraum der Erhebung der betreffenden personenbezogenen Daten auf das im Hinblick auf den Zweck der beabsichtigten Verarbeitung absolut Notwendige zu beschränken.

[…]

54 Des Weiteren ist darauf hinzuweisen, dass gemäß Art. 5 Abs. 1 Buchst. e DSGVO die personenbezogenen Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

55 Somit ist diesem Artikel eindeutig zu entnehmen, dass der in ihm verankerte Grundsatz der „Speicherbegrenzung“ verlangt, dass der Verantwortliche in der Lage ist, gemäß dem Grundsatz der Rechenschaftspflicht, auf den in Rn. 51 des vorliegenden Urteils hingewiesen worden ist, nachzuweisen, dass die personenbezogenen Daten nur so lange gespeichert werden, wie es für die Erreichung der Zwecke, für die sie erhoben oder weiterverarbeitet wurden, erforderlich ist (vgl. in diesem Sinne Urteil vom 20. Oktober 2022, Digi, C-77/21, EU:C:2022:805, Rn. 53).

56 Daraus ergibt sich, wie der Gerichtshof bereits entschieden hat, dass selbst eine ursprünglich zulässige Verarbeitung von Daten im Lauf der Zeit gegen die DSGVO verstoßen kann, wenn diese Daten für die Erreichung der Zwecke, für die sie erhoben oder später verarbeitet wurden, nicht mehr erforderlich sind, und dass diese Daten gelöscht werden müssen, wenn diese Zwecke erreicht sind (vgl. in diesem Sinne Urteil vom 20. Oktober 2022, Digi, C-77/21,

EU:C:2022:805, Rn. 54 und die dort angeführte Rechtsprechung).

57 Daher ist es, wie der Generalanwalt in Nr. 22 seiner Schlussanträge im Wesentlichen ausgeführt hat, Sache des nationalen Gerichts, unter Berücksichtigung aller maßgeblichen Umstände und unter Anwendung des Grundsatzes der Verhältnismäßigkeit, auf den in Art. 5 Abs. 1 Buchst. c DSGVO hingewiesen wird, zu beurteilen, ob die Dauer der Speicherung der personenbezogenen Daten durch den Verantwortlichen im Hinblick auf das Ziel, die Schaltung personalisierter Werbung zu ermöglichen, angemessen gerechtfertigt ist.

58 Jedenfalls ist eine zeitlich unbegrenzte Speicherung personenbezogener Daten der Nutzer einer Plattform für ein soziales Netzwerk zu Zwecken der zielgerichteten Werbung als unverhältnismäßiger Eingriff in die Rechte, die die DSGVO diesen Nutzern garantiert, anzusehen.

59 Was […] den Umstand betrifft, dass die im Ausgangsverfahren fraglichen personenbezogenen Daten ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung erhoben, aggregiert, analysiert und verarbeitet werden, hat der Gerichtshof bereits entschieden, dass der Verantwortliche in Anbetracht des in Art. 5 Abs. 1 Buchst. c DSGVO festgelegten Grundsatzes der Datenminimierung nicht allgemein und unterschiedslos personenbezogene Daten erheben darf und er von der Erhebung von Daten absehen muss, die für die Zwecke der Verarbeitung nicht unbedingt notwendig sind (Urteil vom 24. Februar 2022, Valsts ieņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C-175/20, EU:C:2022:124, Rn. 74).

60 Ferner muss der Verantwortliche gemäß Art. 25 Abs. 2 DSGVO geeignete Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Nach dieser Bestimmung gilt diese Verpflichtung u. a. für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung und ihre Zugänglichkeit.

61 Vorliegend geht aus der Vorlageentscheidung hervor, dass Meta Platforms Ireland die personenbezogenen Daten der Nutzer von Facebook, darunter Herrn Schrems, über deren Tätigkeiten sowohl innerhalb als auch außerhalb dieses sozialen Netzwerks, darunter u. a. Daten über den Abruf der Onlineplattform sowie von Websites und Anwendungen Dritter, erhebt und auch das Navigationsverhalten der Nutzer auf diesen Seiten mittels Social Plug-ins und Pixels, die auf den betreffenden Websites eingefügt werden, verfolgt.

62 Wie der Gerichtshof bereits entschieden hat, ist eine solche Verarbeitung besonders umfassend, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta Platforms Ireland aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 118).

63 Unter diesen Umständen stellt die im Ausgangsverfahren in Rede stehende Datenverarbeitung einen schweren Eingriff in die Grundrechte der betroffenen Personen dar, insbesondere in ihre durch die Art. 7 und 8 der Charta der Grundrechte der Europäischen Union gewährleisteten Rechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der vorbehaltlich der vom vorlegenden Gericht vorzunehmenden Überprüfungen im Hinblick auf das Ziel, die Schaltung gezielter Werbung zu ermöglichen, nicht angemessen gerechtfertigt erscheint.

64 Jedenfalls erscheint die unterschiedslose Verwendung sämtlicher personenbezogener Daten, die von einer Plattform für ein soziales Netzwerk zu Werbezwecken gespeichert werden, unabhängig vom Sensibilitätsgrad dieser Daten nicht als ein verhältnismäßiger Eingriff in die Rechte, die den Nutzern dieser Plattform durch die DSGVO garantiert werden.

65 Nach alledem ist auf die zweite Frage zu antworten, dass Art. 5 Abs. 1 Buchst. c DSGVO dahin auszulegen ist, dass der darin festgelegte Grundsatz der „Datenminimierung" dem entgegensteht, dass sämtliche personenbezogenen Daten, die ein Verantwortlicher wie der Betreiber einer Onlineplattform für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden.

Zur vierten Frage:

70 Zur Beantwortung dieser Frage ist als Erstes darauf hinzuweisen, dass nach dem 51. Erwägungsgrund der DSGVO personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, einen besonderen Schutz verdienen, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können. Ferner wird in diesem Erwägungsgrund ausgeführt, dass derartige personenbezogene Daten nicht verarbeitet werden sollten, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig.

71 In diesem Zusammenhang stellt Art. 9 Abs. 1 DSGVO den Grundsatz auf, dass die Verarbeitung der in dieser Vorschrift genannten besonderen Kategorien personenbezogener Daten untersagt ist. Dabei handelt es sich u. a. um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen oder religiöse Überzeugungen hervorgehen, sowie um Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

72 Für die Zwecke der Anwendung von Art. 9 Abs. 1 DSGVO ist im Fall einer Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks zu prüfen, ob aus diesen Daten Informationen hervorgehen können, die unter eine der in dieser Bestimmung genann-

ten Kategorien fallen, unabhängig davon, ob diese Informationen einen Nutzer dieses Netzwerks oder eine andere natürliche Person betreffen. Ist dies der Fall, ist eine solche Verarbeitung personenbezogener Daten vorbehaltlich der in Art. 9 Abs. 2 DSGVO vorgesehenen Ausnahmen untersagt.

73 Wie der Gerichtshof bereits entschieden hat, gilt dieses in Art. 9 Abs. 1 DSGVO vorgesehene grundsätzliche Verbot unabhängig davon, ob die aus der fraglichen Verarbeitung hervorgegangene Information richtig ist oder nicht und ob der Verantwortliche mit dem Ziel handelt, Informationen zu erhalten, die unter eine der in dieser Bestimmung genannten besonderen Kategorien fallen. In Anbetracht der erheblichen Risiken für die Grundfreiheiten und Grundrechte der betroffenen Personen, die sich aus jeder Verarbeitung personenbezogener Daten ergeben, die unter eine der in Art. 9 Abs. 1 DSGVO genannten Kategorien fallen, zielt diese Vorschrift nämlich darauf ab, solche Datenverarbeitungen unabhängig von ihrem erklärten Zweck zu verbieten (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 69 und 70).

74 Zwar ist nach Art. 9 Abs. 1 DSGVO die Verarbeitung von Daten u. a. zur sexuellen Orientierung grundsätzlich untersagt, Art. 9 Abs. 2 DSGVO sieht allerdings in seinen Buchst. a bis j zehn Ausnahmen vor, die voneinander unabhängig sind und daher autonom zu beurteilen sind. Folglich ist ein Verantwortlicher durch die Tatsache, dass die Voraussetzungen für die Anwendung einer der in Art. 9 Abs. 2 aufgeführten Ausnahmen nicht erfüllt sind, nicht daran gehindert, sich auf eine andere in dieser Bestimmung genannte Ausnahme zu berufen (Urteil vom 21. Dezember 2023, Krankenversicherung Nordrhein, C-667/21, EU:C:2023:1022, Rn. 47).

75 Insbesondere zur Ausnahme des Art. 9 Abs. 2 Buchst. e DSGVO ist darauf hinzuweisen, dass nach dieser Bestimmung das in Art. 9 Abs. 1 DSGVO aufgestellte grundsätzliche Verbot jeder Verarbeitung besonderer Kategorien personenbezogener Daten nicht gilt, wenn sich die Verarbeitung auf personenbezogene Daten bezieht, die „die betroffene Person offensichtlich öffentlich gemacht hat".

76 Da Art. 9 Abs. 2 Buchst. e DSGVO eine Ausnahme vom Grundsatz des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten vorsieht, ist er eng auszulegen (vgl. in diesem Sinne Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 76 und die dort angeführte Rechtsprechung).

77 Folglich ist für die Zwecke der Anwendung der in Art. 9 Abs. 2 Buchst. e DSGVO vorgesehenen Ausnahme zu prüfen, ob die betroffene Person die Absicht hatte, die fraglichen personenbezogenen Daten ausdrücklich und durch eine eindeutige bestätigende Handlung der breiten Öffentlichkeit zugänglich zu machen (Urteil vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 77).

78 Vorliegend geht aus der Vorlageentscheidung hervor, dass die am 12. Februar 2019 in Wien veranstaltete Podiumsdiskussion, in deren Rahmen Herr Schrems sich zu seiner sexuellen Orientierung äußerte, der Öffentlichkeit, die innerhalb der Grenzen der verfügbaren Plätze Eintrittskarten zur Teilnahme erhalten konnte, zugänglich war, und dass die Podiumsdiskussion per Streaming übertragen wurde. Zudem soll eine Aufzeichnung der Podiumsdiskussion später als Podcast sowie auf dem Youtube-Kanal der Kommission veröffentlicht worden sein.

79 Unter diesen Umständen und vorbehaltlich der vom nationalen Gericht vorzunehmenden Überprüfungen ist nicht auszuschließen, dass die betreffende Äußerung, auch wenn sie Teil eines umfassenderen Redebeitrags war und nur zu dem Zweck erfolgte, die Verarbeitung personenbezogener Daten durch Facebook zu kritisieren, eine Handlung darstellt, mit der der Betroffene in voller Kenntnis der Sachlage seine sexuelle Orientierung im Sinne von Art. 9 Abs. 2 Buchst. e der DSGVO offensichtlich öffentlich gemacht hat.

80 Als Zweites führt zwar der Umstand, dass die betroffene Person Daten zu ihrer sexuellen Orientierung offensichtlich öffentlich gemacht hat, dazu, dass diese Daten abweichend von dem Verbot gemäß Art. 9 Abs. 1 DSGVO und im Einklang mit den Anforderungen, die sich aus den anderen Bestimmungen der DSGVO ergeben, verarbeitet werden können (vgl. in diesem Sinne Urteil vom 24. September 2019, GC u. a. [Auslistung sensibler Daten], C-136/17, EU:C:2019:773, Rn. 64). Entgegen dem Vorbringen von Meta Platforms Ireland berechtigt dieser Umstand allein jedoch nicht, andere personenbezogene Daten zu verarbeiten, die sich auf die sexuelle Orientierung dieser Person beziehen.

81 So liefe es zum einen dem eng auszulegenden Art. 9 Abs. 2 Buchst. e DSGVO zuwider, wenn sämtliche Daten über die sexuelle Orientierung einer Person bereits deswegen dem Schutz des Art. 9 Abs. 1 DSGVO entzogen wären, weil die betroffene Person personenbezogene Daten, die sich auf ihre sexuelle Orientierung beziehen, offensichtlich öffentlich gemacht hat.

82 Zum anderen lässt die Tatsache, dass eine Person Daten über ihre sexuelle Orientierung offensichtlich öffentlich gemacht hat, nicht die Feststellung zu, dass sie ihre Zustimmung im Sinne von Art. 9 Abs. 2 Buchst. a DSGVO dazu erteilt hat, dass der Betreiber einer Onlineplattform für ein soziales Netzwerk andere Daten über ihre sexuelle Orientierung verarbeitet.

83 Nach alledem ist auf die vierte Frage zu antworten, dass Art. 9 Abs. 2 Buchst. e DSGVO dahin auszulegen ist, dass der Umstand, dass sich eine Person bei einer öffentlich zugänglichen Podiumsdiskussion zu ihrer sexuellen Orientierung geäußert hat, dem Betreiber einer Onlineplattform für ein soziales Netzwerk nicht gestattet, andere Daten über die sexuelle Orientierung dieser Person zu verarbeiten, die er gegebenenfalls außerhalb dieser Plattform von Anwendungen und Websites dritter Partner im Hinblick

darauf erhalten hat, sie zu aggregieren und zu analysieren, um dieser Person personalisierte Werbung anzubieten.

III. Anmerkung

Der EuGH hat in der vorliegenden Entscheidung die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung im Kontext personalisierter Werbung mit Blick auf den Grundsatz der Datenminimierung und auf die Verarbeitung besonderer Kategorien personenbezogener Daten konkretisiert und so den Handlungsspielraum für Anbieter von Onlinediensten, die sich über verhaltensbasierte Werbung finanzieren, eingeschränkt.

Grundlegend klargestellt hat er, dass der Grundsatz der Datenminimierung den Anbietern von Onlinediensten verbietet, sämtliche personenbezogenen Daten, die durch den betroffenen Dienst selbst und außerhalb des Dienstes erworben werden, zeitlich unbegrenzt und ohne Unterscheidung nach Zweckbestimmung zu verarbeiten. Stattdessen muss je nach Art des Datums und Zweckbestimmung differenziert werden. Anderenfalls, so der EuGH, könnte das Tracking bei den Betroffenen das Gefühl auslösen, kontinuierlich überwacht zu werden.

Damit hat der EuGH die umfassende Sammlung von Daten durch große Konzerne mittels Social Plugins, d.h. auch außerhalb der eigenen Plattform, zwar nicht verboten, aber er hat ihr immerhin Grenzen gesetzt. Eine vollständige und grenzenlose Aufzeichnung der Onlineaktivität zu Werbezwecken ist damit nicht (mehr) datenschutzkonform.

Noch strengere Kriterien legte der EuGH im Kontext der Verarbeitung sensibler Daten an. In einem vorangegangenen Rechtsstreit (EuGH Urt. v. 04.07.2023 – C-252/21) hatte er bereits klargestellt, dass Angaben auf Onlineprofilen über sensible Daten wie der sexuellen Orientierung grundsätzlich kein bewusstes „Öffentlichmachen" darstellen. Eine Ausnahme gilt nur dann, wenn die individuellen Einstellungen explizit die Entscheidung der Person zum Ausdruck bringen, die Informationen der Öffentlichkeit zugänglich machen zu wollen. Angaben in einem nicht öffentlichen Profil können die Ausnahme des Art. 9 Abs. 2 lit. e DS-GVO damit nicht begründen. Daher sind Onlinedienste auch dann nicht dazu berechtigt, sensible Daten ohne Einwilligung zu verarbeiten, wenn die entsprechende Information im Profil angegeben wurde.

Zwar deutete der EuGH dies für die Aussagen in einer analogen Podiumsdiskussion tendenziell anders und schloss ein bewusstes „Öffentlichmachen" hier nicht aus, er schränkte jedoch gleichzeitig die sich hieraus ergebenden Rechte der Betreiber deutlich ein. Selbst dann, wenn die Äußerung als „öffentlich" im Sinne des Art. 9 Abs. 2 lit. e DS-GVO anzusehen wäre, berechtigte dies die Plattform nicht, die selbe Information auch an anderer, nicht öffentlicher Stelle zu sammeln, so der EuGH. Die öffentliche Bekanntgabe hebe den Schutz des spezifischen Datums durch Art. 9 DS-GVO nicht in Gänze auf. Die Sammlung von inhaltsgleichen Daten an anderen Stellen bliebe dennoch verboten.

Damit bleibt es für Online-Dienste auch dann unzulässig, nicht öffentliche Daten im Sinne des Art. 9 DS-GVO ohne explizite Einwilligung der Nutzer zu sammeln, wenn die Information der Öffentlichkeit an anderer Stelle bekannt geworden ist. Eine Umgehung des besonderen Schutzes des Art. 9 DS-GVO mithilfe eines Verweises auf eine an anderer Stelle getätigte, öffentliche Aussage der betroffenen Person scheidet aus. Basierend auf Daten im Sinne des Art. 9 DS-GVO dürfte personalisierte Werbung damit in Zukunft rechtswidrig sein bzw. bleiben, insofern die betroffene Person nicht ausdrücklich einwilligt.

Lucia Burkhardt

Brüssel Inside

Rolf Schwartmann/Kai Zenner/Moritz Köhler

Leitlinien der Kommission zu verbotenen KI-Praktiken

Am 4. Februar hat die Kommission Leitlinien zu den gem. Art. 5 KI-VO verbotenen KI-Praktiken veröffentlicht. Das ursprünglich erklärte Ziel, die Leitlinien noch vor Geltungsbeginn der Verbotsvorschrift am 2. Februar herauszugeben, wurde damit knapp verpasst. Dennoch liefern die Leitlinien eine wichtige erste Orientierung für Rechtsanwender.

Das Verbot der in Art. 5 Abs. 1 KI-VO genannten KI-Praktiken ist umfassend. Verboten sind das Inverkehrbringen, die Inbetriebnahme und die Verwendung der genannten

KI-Systeme. Auch wenn Bußgelder erst ab dem 2. August verhängt werden dürfen, sollten die Adressaten der KI-VO schon jetzt verbotene KI-Praktiken in ihrem Verantwortungsbereich identifizieren und Alternativen finden.

In den Leitlinien stellt die Kommission einen Überblick zu den einzelnen Tatbeständen des Art. 5 Abs. 1 KI-VO und zu den Ausnahmen der Abs. 2 bis 7 zur Verfügung. Zu jeder beschriebenen Praktik nennen die Leitlinien die gesetzgeberische Erwägung hinter dem Verbot und gehen auf die einzelnen Tatbestandsmerkmale ein. Konkretisiert werden die Voraussetzungen der einzelnen Verbote durch Beispiele. Außerdem werden die verbotenen Praktiken von ähnlichen Praktiken abgegrenzt, die dem Verbot von Art. 5 Abs. 1 KI-VO nicht unterfallen. Von Relevanz für den Rechtsanwender ist darüber hinaus das Verhältnis der einzelnen Verbote zu den übrigen Vorschriften der KI-VO, insbesondere zu den Anforderungen an Hochrisiko-KI-Systeme und den Vorgaben für KI-Systeme mit allgemeinem Verwendungszweck, sowie zum sonstigen Recht der Union.

Zur Erarbeitung der Leitlinien ist die Kommission gem. Art. 96 Abs. 1 lit. d KI-VO verpflichtet. Die formelle Annahme stand bei Redaktionsschluss noch aus. Auch nach der Annahme entfalten die Leitlinien keine rechtliche Bindung. Sie sollten aber bei der Prüfung der Vereinbarkeit einer KI-Praktik mit Art. 5 KI-VO berücksichtigt werden.

Rolf Schwartmann, Kai Zenner und Moritz Köhler werden sich in der nächsten Ausgabe der EuDIR, die am 11. April erscheint, mit dem Gesetzgebungsprozess der verbotenen KI-Praktiken beschäftigen und das Ergebnis in Form von Art. 5 Abs. 1 KI-VO politisch einordnen.

Michael Hattermann

Europas digitale Herausforderung: Zeit für einen mutigen Neustart

Die Zukunftsfähigkeit Europas hängt entscheidend davon ab, Schlüsseltechnologien wie Künstliche Intelligenz, Quantencomputing und zukunftssichere Netztechnologien voranzutreiben. In Europa gibt es viele gute Ideen und Ansätze, doch der globale Wettbewerb und die Skalierung auf internationaler Ebene stellen große Herausforderungen dar. 2024 setzte die EU ihre Wettbewerbsfähigkeit auf den Prüfstand – mit ernüchternden Ergebnissen. In den Berichten des ehemaligen EZB-Chefs Mario Draghi und des ehemaligen italienischen Ministerpräsidenten Enrico Letta werden Europas Schwächen im Wettbewerb deutlich benannt: Die Wettbewerbsintensität innerhalb der Union hat abgenommen, die EU-Wirtschaft droht im globalen Vergleich, insbesondere gegenüber den USA und China, zurückzufallen. Gleichzeitig verschärfen sich geopolitische Spannungen und geoökonomische Rivalitäten, während Europa mit einer rasanten technologischen Entwicklung, einer sich wandelnden internationalen Wirtschaftsordnung und einer zunehmenden Abhängigkeit von globalen Supergiganten konfrontiert ist – und nach überzeugenden Antworten sucht. Die Berichte sind damit nicht nur eine Analyse der Schwächen, sondern auch ein Appell, die drängendsten Probleme entschlossen und gemeinsam anzugehen sowie herauszufinden, wie Europa trotz der globalen Herausforderungen zukunftsfähig bleiben kann.

I. Stärkung digitaler Infrastruktur

Besonders die digitalen Defizite des Kontinents sind tief in der schleppenden digitalen Transformation verwurzelt. Der Ausbau im Wettbewerb von Glasfasernetzen und 5G-Infrastrukturen ist unverzichtbar, um die Wettbewerbsfähigkeit Europas langfristig zu sichern. Leistungsstarke Netze sind die Grundlage für Innovationen und eine zukunftsorientierte Wirtschaft. Doch die politischen Empfehlungen Draghis und Lettas, den Markt auf wenige große „europäische Champions“ zu konzentrieren, stoßen auf erhebliche Kritik. Eine solche Bevorzugung weniger Anbieter widerspricht dem Grundgedanken eines dynamischen Binnenmarktes, gefährdet den Wettbewerb und die Innovationskraft im Telekommunikationssektor. Statt den Netzausbau zu beschleunigen, könnte dies den Fortschritt sogar ausbremsen.

Ein Blick auf die Realität zeigt, dass Europa bei Netzqualität und Abdeckung im internationalen Vergleich gut abschneidet, während die Preise für Telekommunikationsdienste deutlich niedriger sind als in den USA. Diese Erfolge sind das Ergebnis eines dynamischen und wettbewerbsfähigen Marktes, der durch regulatorische Stabilität ermöglicht wurde. Maßnahmen zur Deregulierung könnten diese Wettbewerbsvorteile gefährden und den Fortschritt hemmen. Gleichzeitig wird deutlich, wie wichtig die Förderung innovativer Netzarchitekturen ist. Im Mobilfunk bietet der gezielte Ausbau zukunftsfähiger Technologien wie z.B. Open-RAN die Chance, Europas Herstellerunabhängigkeit zu stärken und die digitale Souveränität zu sichern. Offene Standards und die Trennung von Hard- und Software verringern Abhängigkeiten von kritischen Ausrüstern und fördern Innovationen in der gesamten Branche.

II. Souveräne Nutzung von Daten

Eine leistungsfähige und zukunftssichere digitale Infrastruktur ist nicht nur die Grundlage für Innovationen, sondern auch für eine sichere und souveräne Nutzung von Daten. Insbesondere hier muss die EU mutiger agieren. Daten sind das Rückgrat der digitalen Transformation und die Basis für innovative Geschäftsmodelle sowie technologische Fortschritte. Dennoch bleibt noch immer ein Großteil der verfügbaren Daten ungenutzt. Die Gründe dafür sind fehlende Zugänglichkeit und Interoperabilität oder häufig einfach datenschutzrechtliche Bedenken. Das klassische europäische Datendilemma wird in der Praxis sichtbar – Europa tut sich schwer mit pragmatischen Lösungen. Der Fokus auf Sicherheit und Datenschutz steht oft im Konflikt mit einfacher Nutzbarkeit.

Um dieses Potenzial auszuschöpfen, hat die EU-Kommission mit ihrer Datenstrategie den Stein ins Rollen gebracht. „Die Europäische Datenstrategie soll die EU an die Spitze einer datengesteuerten Gesellschaft bringen", heißt es in der entsprechenden Pressemitteilung. Mit dem Data Governance Act (DGA) und dem Data Act (DA) sind die Grundpfeiler der Datenstrategie mittlerweile in Kraft getreten. Die beiden Rechtsakten sollen die Grundlage eines europäischen Binnenmarkts für Daten bilden, damit deren Potenzial als Innovationstreiber endlich voll genutzt werden kann. Der Konflikt des entstehenden Datenwirtschaftsrechts mit dem bestehenden Datenschutzrecht liegt auf der Hand. Er ist nicht unlösbar, doch Kritiker bemängeln zurecht, dass der europäische Gesetzgeber nicht mutig vorangeht und das Verhältnis zwischen den beiden Teilrechtsgebieten eindeutig regelt. Die derzeitige Rechtsunsicherheit geht letztlich zulasten des Wettbewerbs.

III. Datenbasierte Geschäftsmodelle

Ein konkretes Beispiel, das diese Herausforderungen verdeutlicht, ist die Einführung der EU-ID Wallet. Sie soll als sichere und vertrauenswürdige Lösung etabliert werden, steht jedoch im Wettbewerb mit bereits etablierten Wallets großer US-Plattformen. Ein zentrales Hindernis ist die derzeitige Voraussetzung einer Identifizierung per Personalausweis für die Nutzung. Doch die geringe Häufigkeit von Behördenkontakten bietet den Bürgern wenig Anreiz, sich zu registrieren.

Für eine breite Akzeptanz muss die Wallet jedoch von Anfang an auch mit alltäglichen Anwendungen wie E-Mail, sozialen Netzwerken oder Streaming-Diensten kompatibel sein – und das ohne eine zwingende Vorab-Freischaltung per Personalausweis. Nur so kann die EU-Wallet fit für die tägliche Massenanwendung werden. Zwar scheint man mittlerweile – vor allem durch Druck aus der Wirtschaft und von einzelnen nationalen Behörden – erkannt zu haben, dass pragmatische Übergangslösungen notwendig sind. Doch dieser Ansatz muss auch verbindlich durchgesetzt werden. Ein weiterer wichtiger Punkt betrifft gleiche Wettbewerbsbedingungen innerhalb der EU. Es darf keine Unterschiede bei der Umsetzung von Regelungen geben, z.B. in unterschiedlichen Zertifizierungsanforderungen oder -verfahren zwischen Mitgliedstaaten, die eine Zertifizierung in bestimmten Ländern attraktiver macht. Ein einheitlicher Ansatz ist entscheidend, um die wirtschaftliche Wettbewerbsfähigkeit Europas zu gewährleisten. Die Chance, europäische Innovation wirksam voranzutreiben, darf nicht durch zögerliches Handeln verspielt oder im Regulierungsprozess ausgebremst werden. Nur mit entschlossenem und nutzerorientiertem Handeln kann Europa im globalen Wettbewerb den Anschluss halten und seine Position langfristig sichern.

Auch bei anderen datenbasierten Geschäftsmodellen zeigt sich, dass Europa immer wieder vor der Frage steht, wie die Nutzung von Daten und Verbraucherschutz in Einklang gebracht werden können, ohne Innovationen zu behindern. Viele innovative Geschäftsmodelle nutzen personalisierte Werbung zur Finanzierung kostenloser digitaler Dienste und ermöglichen so deren breite Verfügbarkeit. Dennoch wird dieses Modell oft kritisiert, als käme es einem „Verkauf" von Datenschutzrechten gleich. Dabei schafft es echte Wahlfreiheit und wurde mehrfach von nationalen Datenschutzbehörden sowie der europäischen Rechtsprechung als zulässig bestätigt. Das so genannte Pay-or-Consent-Modell gibt Nutzern die Möglichkeit, entweder für einen Dienst zu bezahlen oder ihre Daten für personalisierte Werbung bereitzustellen. Es kombiniert wirtschaftliche Tragfähigkeit mit dem Recht auf Selbstbestimmung und hat sich als anerkanntes Konzept für eine faire und nachhaltige Datenökonomie etabliert. Während Pay-or-Consent Innovationen und Wahlfreiheit fördert, stehen aber insbesondere europäische Anbieter vor erheblichen Herausforderungen. Anders als große Plattformen, die ihre Marktposition durch umfassende Ökosysteme und diversifizierte Geschäftsmodelle absichern, sind kleinere europäische Anbieter stärker auf werbe- oder nutzerfinanzierte Modelle angewiesen. Im Wettbewerb mit globalen Gatekeepern fehlt es ihnen jedoch an vergleichbaren Ressourcen, Synergieeffekten und Möglichkeiten einer Querfinanzierung, was die bestehenden strukturellen Ungleichgewichte verstärkt und den Wettbewerb zusätzlich erschwert.

IV. Fazit

Europa darf sich nicht ausruhen, sondern muss aktiv nach Lösungen suchen, die Innovationen und faire Wettbewerbsbedingungen gleichermaßen fördern. Wir sollten dabei nicht alles eins zu eins kopieren, sondern eigene Akzente und Schwerpunkte setzen, um unseren Führungsanspruch zu untermauern. Europa hat das Potenzial, die Ressourcen, die Expertise und die Werte, um eine prägende Rolle in der digitalen Welt einzunehmen. Doch um diese Position zu sichern, müssen wir mutiger und vor allem pragmatischer handeln. Andernfalls laufen wir Gefahr, unsere Innovationskraft zu verschenken und lediglich den globalen Entwicklungen zuzusehen oder hinterherzurennen.

Vollzugspraxis

Ganesh Srinivasan

Navigating the legal landscape for GPAI – a bottom-up view

Redaktionelle Vorbemerkung: *Der nachfolgende Beitrag stammt von Ganesh Srinivasan, General Manager für Informationssicherheit bei Icertis, einem amerikanischen Anbieter von Vertragsmanagementsoftware. Er wird hier in der englischen Originalfassung veröffentlicht. Der Beitrag behandelt die verschiendenen Akteure und ihre Verantwortlichkeiten entlang der Wertschöngskette von KI-Systemen mit allgemeinem Verwendungszweck (engl: general purpose AI, kurz: GPAI) aus einer technischen sowie wirtschaftlichen Perspektive. Die rechtlichen Pflichten der Akteure nach der KI-VO werden in diesem Heft ab Seite 3 von Rolf Schwartmann und Kai Zenner beleuchtet. Die nachfolgend als Model Provider bezeichneten Akteure sind in der Terminologie der KI-VO Anbieter eines GPAI-Modells. Die hier als AI-ML Engineers bezeichneten Akteure werden im Beitrag von Schwartmann/Zenner in Anlehnung an die Terminologie der KI-VO als Fine-Tuner eines GPAI-Modells bezeichnet. Unter den hier sogenannten AI App Developers versteht die KI-VO die Anbieter von KI-Systemen.*

I. Introduction

GPAI has taken the world by storm, not just with its remarkable ability to generate human-like responses, but also by challenging our understanding of ethics, integrity, and accuracy in AI. The question of who should be held accountable for these aspects remains complex. When existing laws and regulations were drafted, there was little foresight into how this technology would evolve. Consequently, the current requirements set forth are too broad, making it harder for those involved in the lifecycle to better understand their own spheres of influence and control.

With this in mind, let's explore how the legal framework can adapt to better address the nuances of this ecosystem, focusing on a bottom-up approach that considers the roles of key players involved.

II. Identities that matter

There are 3 key actors in this landscape today.

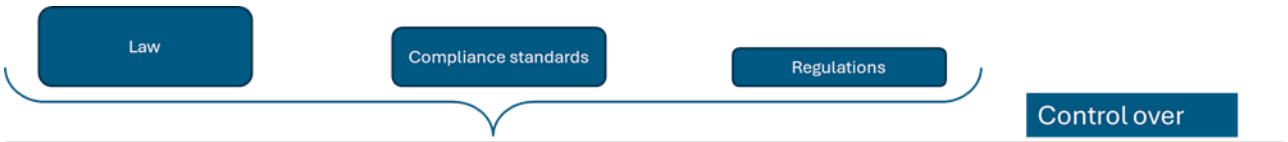
- **Model Providers**: Develop and design advanced AI models and algorithms to drive innovation and maintain competitive advantage.
- **AI-ML Engineers**: Fine-tune and customize AI models for specific use cases, ensuring they are scalable, efficient, and aligned with business needs.
- **AI App Developers**: Create user-friendly applications that integrate AI models, enhancing customer experience and driving revenue growth through innovative solutions.
- An abstraction of their key roles and responsibilities is captured below.

Role	Responsibilities	Skills Required	Context, legal framework drivers
Model Providers	Develop and design AI models and algorithms	Deep understanding of machine learning	Innovate and create cutting-edge AI solutions to maintain competitive advantage
	Conduct research to advance AI capabilities	Proficiency in programming (Python, R)	Ensure models align with business strategy and market needs
	Optimize models for performance and accuracy	Knowledge of data science and statistics	Publish models to drive industry standards and thought leadership
	Publish and share models for use by others	Research and analytical skills	Address ethical considerations to build trust and compliance
	Ensure ethical considerations in model development	Familiarity with AI frameworks (TensorFlow, PyTorch)	Contribute to intellectual property and patent portfolio

AI-ML Engineers	Fine-tune and customize AI models for specific use cases	Strong programming skills	Adapt AI models to meet specific business requirements and customer needs
	Integrate models into larger systems and workflows	Experience with model training and tuning	Ensure models are scalable and efficient to support business growth
	Optimize models for deployment and scalability	Knowledge of cloud platforms (AWS, Azure)	Maintain model performance to ensure consistent business operations
	Monitor and maintain model performance in production	Understanding of software engineering	Collaborate with cross-functional teams to align AI solutions with business goals
	Collaborate with data scientists and domain experts	Problem-solving and debugging skills	Drive innovation by implementing the latest AI advancements
AI App Developers	Develop applications that utilize AI models for real-world use cases	Proficiency in application development	Create user-friendly applications that enhance customer experience and engagement
	Design user interfaces and user experiences for AI-powered applications	Knowledge of front-end and back-end development	Ensure seamless integration of AI to provide value-added services and products
	Ensure seamless integration of AI models into applications	Familiarity with APIs and SDKs	Test and validate application functionality to meet business quality standards
	Test and validate application functionality and performance	Experience with mobile and web development	Gather user feedback to continuously improve and align with market demands
	Gather user feedback and iterate on application features	UX/UI design skills	Drive revenue growth through innovative AI applications and solutions

III. Key drivers

As we pivot to examine the legal responsibilities of each role, it becomes evident that the burden of compliance, regulatory, and legal scrutiny gradually shifts from model providers to AI app developers. While it is not solely the responsibility of any single actor, the onus primarily falls on them to ensure that the final product delivered to the public adheres to all necessary legal and regulatory standards. Before we can get to the more traditional shared responsibility matrix, we need to look at the perspectives that drives priorities across these actors, and the consequent control over the outcome (Infrastructure, Data, Applications) in this context.



Role	Law Perspective	Compliance Standards Perspective	Regulations Perspective	Infra	Data	Apps
Model providers	Focus on adhering to fundamental legal principles such as data privacy, intellectual property rights, and ethical AI development.	Ensure transparency in model development, document data sources, and implement bias detection and mitigation strategies.	Control over the selection and use of data to define the base model, ensuring compliance with data protection regulations like GDPR.	HIGH	HIGH	LOW
AIML engineers	Customize models in accordance with industry-specific legal requirements, ensuring data security and ethical use.	Implement robust data security measures, monitor model performance, and maintain compliance during deployment.	Fine-tune models using targeted industry/domain-specific data, ensuring compliance with sector-specific regulations and data security standards.	MEDIUM	MEDIUM	MEDIUM
AI App developers	Integrate AI models while ensuring end-user data protection and compliance with overarching legal standards.	Design applications with user consent and transparency features, conduct regular security assessments, and provide clear user guidelines.	Ensure application layer compliance with regulations like GDPR and CCPA, perform security audits, and continuously improve adherence based on user feedback.	LOW	LOW	HIGH

To further detail, the following table outlines the specific legal responsibilities, compliance focus, and regulatory considerations for each role within the AI development ecosystem.

Role	Legal Responsibilities	Compliance Focus	Regulatory Considerations
Model Providers	Ensure ethical AI development practices	Data privacy and protection	Adhere to GDPR and other data protection regulations
	Document and disclose model training data sources	Transparency in model development	Maintain records of data sources and consent for data usage
	Implement bias detection and mitigation strategies	Bias and fairness	Conduct regular audits for bias and fairness in models
	Provide clear documentation and usage guidelines	Accountability	Ensure models are explainable and interpretable
	Address intellectual property rights and licensing	Intellectual property	Comply with IP laws and manage licensing agreements
AI-ML Engineers	Customize models in compliance with industry-specific regulations	Sector-specific compliance	Ensure models meet sector-specific regulatory requirements (e.g., healthcare, finance)
	Implement robust data security measures	Data security	Adhere to data security standards and protocols (e.g., encryption, access controls)
	Monitor and document model performance and updates	Performance monitoring	Maintain logs and documentation for model updates and performance
	Ensure models are scalable and maintain compliance during deployment	Scalability and compliance	Conduct compliance checks during model deployment and scaling
	Collaborate with legal teams to ensure ongoing regulatory adherence	Cross-functional collaboration	Work with legal and compliance teams to stay updated on regulatory changes

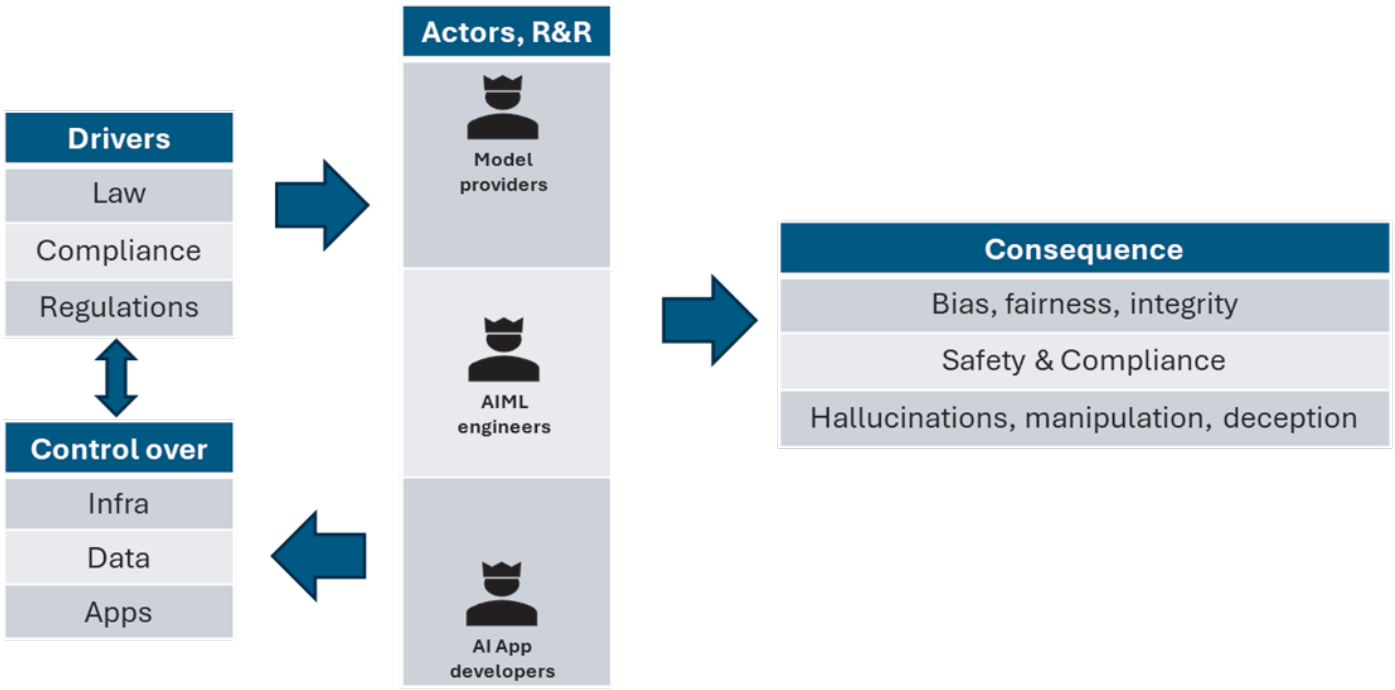
AI App Developers	Integrate AI models in compliance with end-user data protection laws	End-user data protection	Ensure applications comply with GDPR, CCPA, and other end-user data protection regulations
	Design applications with user consent and transparency features	User consent and transparency	Implement features for user consent, data access, and data deletion
	Conduct regular security assessments and vulnerability testing	Security and vulnerability management	Perform regular security audits and vulnerability assessments
	Ensure applications provide clear user guidelines and disclosures	User guidelines and disclosures	Provide clear terms of service, privacy policies, and user guidelines
	Gather and act on user feedback to address compliance issues	Continuous compliance improvement	Use user feedback to identify and address potential compliance issues

IV. Consequence

Following along the same distribution of roles, if we are to now evaluate a finished product against a standard set of criteria (not exhaustive by any means) here is a starting point.

Evaluation Area	**Model Provider Impact**	**AI-ML Engineer Impact**	**AI App Developer Impact**
Bias and Fairness	High: Responsible for initial bias detection and mitigation.	Medium: Fine-tunes models to reduce bias in specific contexts.	Low: Ensures app-level fairness and user transparency.
Safety and Harmful Content	Medium: Ensures base model does not generate harmful content.	Medium: Customizes models to avoid harmful outputs.	High: Implements safeguards to prevent harmful content dissemination.
Privacy and Confidentiality	High: Ensures data used for training is compliant with privacy laws.	Medium: Maintains data security during model customization.	High: Ensures end-user data protection and compliance with privacy regulations.
Misinformation and Accuracy	Medium: Ensures base model accuracy.	High: Fine-tunes models to improve accuracy in specific domains.	High: Ensures app does not spread misinformation.
Ethical and Moral Boundaries	High: Develops models adhering to ethical guidelines.	Medium: Customizes models to align with ethical standards.	High: Ensures app usage aligns with ethical guidelines.
Legal and Compliance	High: Ensures base model complies with legal standards.	High: Customizes models to meet industry-specific legal requirements.	High: Ensures app complies with all relevant legal standards.
Sensitive and Disturbing Topics	Medium: Filters out sensitive content during model training.	Medium: Customizes models to avoid sensitive topics.	High: Implements app-level filters to prevent exposure to sensitive content.
Profanity and Inappropriate Language	Medium: Ensures base model does not generate inappropriate language.	Medium: Customizes models to filter out profanity.	High: Implements app-level filters to prevent inappropriate language.
Hallucinations and Fabrications	Medium: Ensures base model accuracy.	High: Fine-tunes models to reduce hallucinations.	High: Ensures app does not disseminate fabricated information.
Manipulation and Deception	Medium: Ensures base model does not enable manipulation.	High: Customizes models to prevent deceptive outputs.	High: Implements app-level safeguards to prevent manipulation and deception.

V. Summary



GPAI presents us with a new set of actors that have respective roles and responsibilities through the lifecycle of building the models, fine-tuning for specific industries, eventual applications that is made available to the end-user. The drivers for each of these actors vary based on the extent of control they wield on the underlying infrastructure, data and applications that are built on top, eventually. The outcome (consequence) further cascades from the above responsibilities to what can be logically attributed to the respective actors in this ecosystem.

For example, Article 10 in the EU AI act talks about : *AI systems must be trained, validated, and tested using data sets that are relevant, representative, free of errors, and complete.* Based on the above discussion, this would apply largely to the first 2 actors than the third one.

Finally, there is also the end-user who could potentially cause malice through their sublimal queries to exploit the way these systems are designed to operate. While the controls discussed through this document have primarily focused on enterprises designing AI systems, it's important to acknowledge that resilience to malice from end-users is another critical aspect.

Tobias Keber/Clarissa Henning

Datenpolitische Highlights vom Schreibtisch des Landesdatenschutzbeauftragten Baden-Württemberg

Das Jahr 2024 stand mit all seinen Themen aus Sicht der Aufsicht stark unter dem Einfluss der am 01.08.2024 in Kraft getretenen EU-Verordnung zur Künstlichen Intelligenz (KI-VO). Die Diskussionen rund um die Zuständigkeiten bzgl. der Aufsicht über die Einhaltung der KI-VO machten offenbar, welche Sicht die politische Landschaft auf den Datenschutz hat. Auch wenn die Datenschutzbehörden aufgrund der bei KI-Systemen zumeist verarbeiteten personenbezogenen und -beziehbaren Daten von Grunde auf in der Aufsichtszuständigkeit sind und damit auch sektorspezifische Zuständigkeiten nach KI-VO als Marktüberwachung naheliegend wären[1], war und ist der politische Diskurs davon geprägt, nicht die „gleichen Fehler

1 Vergleiche hierzu auch die Positionierung der DSK, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), 2024, abruf-

wie bei der DS-GVO“ machen zu wollen. Insoweit wird ein verzerrtes Bild der Überregulierung gezeichnet, die Innovation behindere. Entsprechend scheint der politische Wille zu sein, die Datenschutzaufsicht nicht auch noch KI-spezifisch berufen zu sehen. Die begleitenden Debatten zeigen, dass der Datenschutz derzeit politisch eine kaum belastbare Lobby hat – selbst bei den traditionell bürger- und freiheitsrechtspropagierenden Parteien. Trotz oder wegen der weltpolitischen Herausforderungen scheinen die Antagonismen konsensfähig: Sicherheit durch Kontrolle, Innovation auf Kosten der informationellen Selbstbestimmung. Gemeinsam ist beiden ein Mehr an uneingeschränkter Datenverarbeitung.

I. Narrative im Realitätscheck

Als plakatives Beispiel für Überzeichnung zeigte sich 2024, trotz insgesamt konstruktiver Zusammenarbeit mit Ministerien und kommunalen Spitzenverbänden, ein Zungenschlag, der stellenweise im Kontext „Entbürokratisierung“ gegenüber dem Datenschutz zu vernehmen war. So fanden sich Vorschläge zur Entbürokratisierung bei Ehrenämtern und Vereinen, die sich gegen eine „Übererfüllung der DS-GVO“ aussprachen, bspw. durch die Abschaffung der Pflicht zur Bestellung eines Datenschutzbeauftragten für ehrenamtlich geführte Vereine ebenso wie die Abschaffung von Bußgeldern bei Erstverstößen. Mit Blick auf die Bußgeldrealität in Baden-Württemberg kann konstatiert werden, dass hierzulande noch nie seit Inkrafttreten der DS-GVO ein Bußgeld gegen einen ehrenamtlich geführten Verein verhängt wurde. Darüber hinaus liest man die Forderung, der Datenschutz müsse vom „Verhinderungs- zum Ermöglichungsinstrument“ entwickelt werden.[2]

Die Polemik verfängt bisweilen, bedient sie doch ein inzwischen tradiertes Narrativ: Der Datenschutz wird gefällig als Sündenbock für komplexe Probleme stilisiert, weil die zu Grunde liegende Herausforderung systemisch, multifaktoriell und damit zu vielschichtig ist, um sie schnell und einfach und öffentlich leicht vermittelbar lösen zu können. Datenschutz ist Bürokratie? Das kann man bejahen, wenn „Bürokratie“ im ursprünglichen Wortsinn gemeint ist und damit einen Zustand der Verlässlichkeit, Gleichbehandlung, Ordnung und Rechtssicherheit beschreibt. Es geht um Vertrauen in staatliche Strukturen.

Im Austausch mit Vertretungen der Ministerien (genauer der Entlastungsallianz Baden-Württemberg[3]) und der kommunalen Spitzenverbände Baden-Württemberg ebenso wie mit Vertreterinnen und Vertretern direkt aus kommunalen Stellen zeigte sich, dass der Datenschutz als hohes Gut für einen freiheitlich geprägten Staat eingeschätzt wird, den es zu bewahren gilt.[4] Im schlechten Fall aber sorgen Unwissenheit, mangelnde personelle, fachliche und zeitliche Ressourcen bei den verantwortlichen Stellen dafür, dass Datenschutz als Hemmnis und Belastung in den Behörden wahrgenommen wird. Hier schließt sich also im Konkreten der Kreis, dass die Sensibilisierung für die Bedeutung des Datenschutzes als Ausdruck der informationellen Selbstbestimmung weiterhin durch Veranstaltungen und populärwissenschaftliche Publikationen über die Datenschutz-Fach-Community hinaus betrieben werden muss, um – schlicht und ergreifend – Imagepflege zu betreiben. Hierbei sind auch die Aufsichtsbehörden in der Pflicht, Datenschutzrecht trotz mancher Widrigkeiten selbstbewusst und lösungsorientiert zu verteidigen.

II. TikTok: Meinungsbildung und der Datenschutz

Diese Notwendigkeit zeigt sich auch schon seit vielen Jahren beim Thema des Social Media-Einsatzes zur behördlichen Kommunikation mit Bürgerinnen und Bürgern, die in 2024 durch die zunehmende Nutzung von TikTok durch staatliche Stellen erneut Fahrt aufnahm – spätestens seit dem Start des TikTok-Auftritts des Bundeskanzlers[5]. Nicht nur Ministerien, auch Fraktionen wählen vermehrt den in der Kritik stehenden Dienst TikTok des chinesischen Konzerns Bytedance, um eine junge Zielgruppe mit behördlichen und politischen Informationen zu attrahieren. Bei Polizeibehörden scheint der Dienst bisweilen zum Inventar der Nachwuchsgewinnung zu gehören.
Hier veranschaulicht sich ein Dilemma, mit dem der Datenschutz in ähnlicher Weise immer wieder im Kampf der abzuwägenden Rechtsgüter zu kämpfen hat. In Zeiten von Desinformation, Manipulation und Polemik ist der Bedarf groß, ein Gegengewicht zu setzen – genau dort, wo diese Kommunikation stattfindet. Dennoch stellt sich die Frage, wie weit öffentliche Stellen ihre rechtsstaatlich begründete Vorbildfunktion zu diesem Zweck suspendieren dürfen. Aus datenschutzrechtlicher Sicht ist bei der Nutzung von TikTok nämlich zu bezweifeln, ob die Verarbeitung personenbezogener Daten den Anforderungen der in Art. 5 und Art. 25 DS-GVO geregelten Vorgaben gerecht wird, ob sie auf einer gültigen Rechtsgrundlage nach Art. 6 DS-GVO beruht und ob die spezifischen Anforderungen des Art. 8 DS-GVO an die Datenverarbeitung von Minderjährigen sowie Art. 13 und 14 DS-GVO an die transparente Informati-

bar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf.

2 Gemeindetag Baden-Württemberg, Digitales Rathaus - Gemeinsam zur zukunftsfähigen Verwaltung, 2024, abrufbar unter: https://www.gemeindetag-bw.de/system/files/downloads_buch/Positionspapier-Verwaltungsdigitalisierung_final.pdf, S. 6.

3 Mehr zur Entlastungsallianz und ihrer Agenda abrufbar unter: https://stm.baden-wuerttemberg.de/de/themen/verwaltungsmodernisierung-und-buerokratieabbau/entlastungsallianz-fuer-baden-wuerttemberg.

4 Dies deckt sich auch mit einer repräsentativen Studie zu Künstlicher Intelligenz und Kompetenz aus dem Jahr 2023, gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend. Obgleich sich nur eine Minderheit der Befragten beim Thema Datenschutz als (eher) kompetent erlebt, hat diese Fähigkeit für die meisten (92 Prozent) eine (große) Bedeutung. 97 Prozent der Befragten messen dem Schutz der eigenen Online-Daten eine (große) Bedeutung zu. Hier wird Handlungsbedarf bei Tech-Branche, Bildung und Politik gesehen, da Datenschutz als hochrelevantes Thema für ein souveränes Leben in der digital vernetzten Welt eingeschätzt wird. Vgl. Cousseran/Lauber/Herrmann/Brüggen, Kompass: Künstliche Intelligenz und Kompetenz, 2023, abrufbar unter: https://zenodo.org/records/10058588, S. 32, 54.

5 Zur datenschutzrechtlichen und -ethischen Einordnung siehe Keber/Henning, Olaf Scholz und die auf TikTok herrschenden Datenschutzpraktiken, 2024, abrufbar unter: https://netzpolitik.org/2024/wahlkampf-olaf-scholz-und-die-auf-tiktok-herrschenden-datenschutzpraktiken/.

on der betroffenen Personen abgebildet werden.[6] Ähnlich wie bereits bei Twitter und Facebook sucht der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) auch bei der Nutzung von TikTok den Austausch und gibt Hilfestellungen[7], ohne dabei die zahlreichen datenschutzrechtlichen Probleme bei der Nutzung dieses Dienstes unbeachtet zu lassen. Womöglich kann der Ausgang der noch anhängigen Verfahren zum Betrieb von Facebook Fanpages durch Regierungsstellen[8] eine (erste) Weichenstellung auch für den Einsatz von TikTok leisten. Abzuwarten bleibt auch, welchen Einfluss die voraussichtlich im Herbst 2025 zu erwartende Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung haben wird, die sich massiv auf die Rechtmäßigkeit der Nutzung von Diensten wie TikTok im politischen Kontext auswirken könnte.

III. Licht im Dunkel: Deceptive Design Patterns

Konkrete Erfolge der Datenschutzbehörden in der europäischen Zusammenarbeit konnten beim Thema Social Media, genauer: Deceptive Design Patterns, bereits 2023 erreicht werden, deren positive Auswirkungen sich in 2024 zeigten. Deceptive Design Patterns (auch: Dark Patterns) tragen maßgeblich dazu bei, die Nutzerinnen und Nutzer durch Gestaltungsprinzipien des User-Interface zu einem bestimmten Nutzungsverhalten zu bewegen, unter Vortäuschung, sie könnten ihre Account-Einstellung völlig frei wählen. Ziel ist hierbei, User dazu zu verleiten, möglichst viele personenbezogene Daten von sich zur Verfügung zu stellen. Auch das Auffinden von Datenschutzhinweisen oder datenschutzfreundlichen Account-Einstellungen bis hin zur Account-Löschung wird durch Deceptive Design Patterns so erschwert, dass Nutzende den Vorgang abbrechen. Hierunter fallen auch die allseits bekannten Cookie-Banner, die zumeist so gestaltet sind, dass unerwünschtem Tracking trotzdem zugestimmt wird.

Aufgrund derartiger Praktiken, die die informationelle Selbstbestimmung durch Manipulation einschränken, verhängte die irische Datenschutzaufsicht im September 2023 gegen das Unternehmen TikTok Technology Limited (TikTok) ein Bußgeld in Höhe von 345 Millionen Euro. Grundlage für die Sanktion war die Verletzung der Rechte Minderjähriger – was damit ein Fingerzeig auch im Kontext staatlicher Kommunikation ist, um eine junge Zielgruppe zu erreichen. Im Zuge des begleitenden Streitbeilegungsverfahrens vor dem Europäischen Datenschutzausschuss (EDSA) konnte der LfDI BW gemeinsam mit Berlin bewirken, dass die irische Aufsicht den Umgang mit Deceptive Design Patterns auch unter dem Gesichtspunkt von Fairness und Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) in ihrer Unterlassungsanordnung berücksichtigt, um damit im Besonderen auch die jungen User vor Manipulation zu schützen.[9] In der Folge dieses Verfahrens konnten entsprechende Änderungen der Nutzer-Oberfläche bei Social Media-Anbietern in 2024 erwartet werden. Zudem erschienen flankierend FAQs zum Umgang mit Deceptive Design Patterns.[10]

IV. Meta-Thema: Künstliche Intelligenz (KI) und Datenschutz

Zurück zum eingangs erwähnten Einfluss der KI auf die datenschutzrechtliche Arbeit der Aufsichten, von denen auch mehrere gemeinsame Positionen der Datenschutzkonferenz (DSK) im Jahr 2024 Zeugnis sind.

In der Orientierungshilfe „Künstliche Intelligenz und Datenschutz" vom 6. Mai 2024 adressierte die DSK die Auswahl, Implementierung und Nutzung von KI-Anwendungen, gab Empfehlungen zu Zweckbestimmung, Transparenzpflichten und Betroffenenrechten und zeigte – auch anhand von Beispielen – wichtige Kriterien entlang der Vorgaben der Datenschutz-Grundverordnung auf.[11] Bereits am 3. Mai hatte die DSK hinsichtlich der nationalen Zuständigkeit für bestimmte Bereiche der Aufsicht über die KI-VO darauf hingewiesen, dass die sektorspezifische Zuständigkeit der Datenschutzbehörden als Marktüberwachungsbehörden unionsrechtlich partiell bereits vorgegeben und auch der Sache nach zielführend wäre, um Synergien zu ermöglichen und Doppelstrukturen zu vermeiden.[12]

Auch auf der Strategieklausur vom 30. August bis 1. September 2024 war KI ein zentrales Thema. Die DSK betonte die parallele Geltung von KI-Verordnung und DS-GVO und hob ferner hervor, dass ein kohärentes europäisches Daten-, Digital- und KI-Recht einer sorgfältigen Analyse und Diskussion über passgenau spezifische datenschutz-

6 Vgl. hierzu auch den 40. Tätigkeitsbericht des LfDI BW, in Kürze abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/.

7 Siehe bspw. die Checkliste des LfDI BW zum Einsatz von TikTok, 2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/datenschutz-oeffentliche-stellen-tik-tok/.

8 Untersagung des Betriebs einer Fanpage der Bundesregierung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 2023, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf?__blob=publicationFile&v=1; Untersagung der Nutzung einer Fanpage der Sächsischen Staatskanzlei durch die Sächsische Datenschutz- und Transparenzbeauftragte, 2023, abrufbar unter: https://www.datenschutz.sachsen.de/download/20230707_Bescheid_Untersagung_Facebook_SK.

9 Vgl. hierzu LfDI BW, Datenschutz durch Technikgestaltung statt Irreführen durch Design, 2023, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/datenschutz-durch-technikgestaltung-statt-irrefuehren-durch-design/

10 LfDI BW, FAQ zu Deceptive Design Patterns, 2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/faq-zu-Deceptive-Design-Patterns/. Die FAQs in deutscher Sprache stellen eine Zusammenfassung der „Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them" dar, abrufbar unter: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

11 DSK, Orientierungshilfe für datenschutzkonformen Einsatz von KI, 2024, abrufbar unter: https://www.datenschutzticker.de/2024/05/dsk-orientierungshilfe-fuer-datenschutzkonformen-einsatz-von-ki/

12 DSK, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

rechtliche Anforderungen bedarf, die beim Ringen um die KI-Verordnung ausgeblendet wurden.[13]

Auf der 108. DSK-Konferenz am 14./15. November 2024 wurde ein neuer Arbeitskreis Künstliche Intelligenz eingerichtet, dem es künftig obliegen wird, die Entwicklung der KI-Technologie und ihrer Regulierung zu beobachten, Handlungsempfehlungen zu geben und die innovationsfreundliche und risikospezifische Aufsichtspraxis zu fördern.[14]

V. Orientierungshilfen für Verantwortliche vor Ort - Diskussionspapier und ONKIDA

Am 17. Oktober 2024 hat die Dienststelle des LfDI BW ein Update des im November 2023 erschienen Diskussionspapiers „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ vorgelegt.[15] Das Papier soll verantwortlichen Stellen in Baden-Württemberg dabei helfen, sich mit den Rechtsgrundlagen auseinanderzusetzen, die das Datenschutzrecht für den Einsatz von Systemen der Künstlichen Intelligenz[16] vorsieht. Im Zuge der Überarbeitung des Diskussionspapiers (Version 2.0) wurden Rückmeldungen von Praktiker_innen[17] sowie von Bürger_innen abgebildet, die sich an der Diskussion beteiligt haben. Einen besonderen Schwerpunkt bildete die Überarbeitung der Ausführungen zur Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DS-GVO (berechtigtes Interesse) sowie die Betrachtung einzelner Nutzungsszenarien, etwa im schulischen Bereich.

Auf nationaler und europäischer Ebene haben sich zwischenzeitlich bereits verschiedene Datenschutzaufsichtsbehörden intensiv mit den datenschutzrechtlichen Implikationen beim Einsatz von Künstlicher Intelligenz auseinandergesetzt. Neben dem EDSA haben auch der European Data Protection Supervisor (EDPS) und auf nationaler Ebene verschiedene Datenschutzbehörden der Mitgliedsstaaten umfassende Hilfestellungen in Form von Leitlinien und Checklisten bereitgestellt. Diese bieten Verantwortlichen eine wertvolle Unterstützung im Umgang mit datenverarbeitenden KI-Systemen. Sie sind ein wichtiger Schritt, um sicherstellen zu können, dass die Entwicklung und Anwendung von KI-Technologien im Einklang mit den hohen Datenschutzstandards in Europa erfolgt und die Rechte von Betroffenen hinreichend gewahrt bleiben. Der LfDI BW hat mit dem Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA)[18] eine umfassende Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschutzrechts in aufsichtsrechtlichen Orientierungshilfen zu Künstlicher Intelligenz erstellt, um einen schnellen Zugang zu ermöglichen.

VI. KI und Datenschutz konkret - EDSA Opinion AI Models

Am 18.12.2024 hat der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme zur Verwendung personenbezogener Daten für die Entwicklung und Einführung von KI-Modellen angenommen.[19] Erörtert wird, wann und wie KI-Modelle als anonym angesehen werden können, ob und wie ein berechtigtes Interesse als Rechtsgrundlage für die Entwicklung oder Nutzung von KI-Modellen geltend gemacht werden kann sowie was passiert, wenn ein KI-Modell unter Verwendung unrechtmäßig verarbeiteter personenbezogener Daten entwickelt wurde.

VII. Kohärentes Daten- und Digitalrecht – Lost in Interplays

Angesichts der Fülle legislativer Neuerungen im europäischen Digital- und Datenrecht wünscht sich der Rechtsanwender gewiss deutlich mehr Kohärenz, als dies gegenwärtig der Fall ist, auch wenn der Idealfall in Gestalt einer systematischen Kodifikation der Materie derzeit unrealistisch sein dürfte. Ausgehend von der Erkenntnis, dass KI-VO und DS-GVO künftig parallel anwendbar sein werden, stellen sich zur Wechselwirkung der beiden Regelwerke viele Fragen („interplay issues“). Das gilt namentlich für diejenigen Sachverhalte, die in der gemeinsamen Schnittmenge der Verordnungen angesiedelt sind, also sowohl KI-Systeme/Modelle im Anwendungsbereich der KI-VO betreffen, als auch die Verarbeitung personenbezogener Daten im Anwendungsbereich der DS-GVO zum Gegenstand haben. Künftig näher erörterungsbedürftig ist in diesem Kontext u.a. beispielsweise die Frage, wie weit die Befugnis zur Datenverarbeitung i.S.d. Art. 10 Abs. 5 KI-VO reicht, wie das Gebot menschlicher Aufsicht (Art. 14 KI-VO) und Artikel 22 DS-GVO zusammenwirken, welche Synergien es ggfls. zwischen nach DS-GVO gebotener Datenschutzfolgenabschätzung und Grundrechtsfolgenabschätzung nach KI-VO gibt und ob es Unterschiede in den Transparenzanforderungen zwischen den beiden Regelungskreisen gibt.

VIII. Forschung und Gesundheitsdaten

In der Entscheidungspraxis der DSK spielten 2024 auch die Forschung und Gesundheitsdaten eine gewichtige Rol-

13 DSK, Pressemitteilung Strategieklausur der Datenschutzkonferenz in Speyer:
Nutzung von KI zentrales Thema, 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/pm/2024-09-02_Klausurtagung_KI.pdf

14 Weitere Informationen unter: https://www.datenschutz.rlp.de/themen/arbeitskreis-ki

15 LfDI BW, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, 2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/

16 Das Datenschutzrecht definiert den Begriff der Künstlichen Intelligenz nicht. Unter dem in Wissenschaft und Praxis umstrittenen Begriff verstehen wir in diesem Papier – im Sinne einer denkbar weiten Arbeitsdefinition – alle Systeme des maschinellen Lernens. Vgl. dazu auch Art. 3 Nr. 1 KI-VO.

17 Eine ausführliche Auseinandersetzung mit dem Diskussionspapier erfolgte bspw. durch die Kanzlei Scheja und Partner Rechtsanwälte mbB, Stellungnahme zum Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von
Künstlicher Intelligenz, V. 1.0, 2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/09/Beitrag_Diskussionspapier_Scheja_und_Partner.pdf

18 LfDI BW, Orientierungshilfen-Navigator KI & Datenschutz,2024, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/onkida/

19 EDSA, Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI, 2024, abrufbar unter: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de

le. Dass es sich bei Gesundheitsdaten um besonders sensible Daten mit entsprechend hohem Schutzbedarf handelt, was technisch und organisatorisch über den gesamten Lebenszyklus der Verarbeitung abgebildet werden muss, unterstrich die DSK in ihrer Entschließung vom 15. Mai 2024 zum besseren Schutz von Patientendaten bei Schließung von Krankenhäusern.[20]

Den Zugang zu Informationen in der Patientenakte im Lichte des Rechts der Betroffenen auf Kopie personenbezogener Daten aus Art. 15 Abs. 3 DS-GVO betraf die Entschließung[21] der DSK vom 11. September 2024.[22] Die DSK stellte klar, dass nach der Rechtsprechung des EuGH[23] das Recht auf kostenlose Erstkopie der Patientenakte durch eine nationale Regelung nicht, wie das durch § 630g Abs. 2 S. 2 BGB und z.T. auch durch Berufsordnungen der Heilberufskammern erfolgt ist, eingeschränkt werden kann.

Breiten Raum in der Befassung der DSK im letzten Jahr nahm der Umgang mit Gesundheitsdaten im besonderen Verarbeitungskontext der Forschung ein. Die bereits 2022 in der „Petersberger Erklärung" der Datenschutzkonferenz[24] niedergelegten Grundsätze zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung[25] wurden durch ein Positionspapier zum Begriff des „wissenschaftlichen Forschungszwecks"[26] sowie einen Beschluss zu genetischen Daten[27] weiter konkretisiert.

Im Beschluss vom 11. September 2024[28] setzte sich die DSK intensiv mit dem Begriff des wissenschaftlichen Forschungszwecks auseinander, der in der Datenschutzgrundverordnung an verschiedener Stelle geregelt ist[29] und für Datenverarbeitungen unter Ägide des Forschungsprivilegs Vorgaben enthält, die der ebenfalls grundrechtlich geschützten Forschungsfreiheit und dem damit verbundenen Beitrag für das Gemeinwohl in einem europäischen Raum der Forschung Rechnung tragen.[30] Damit die privilegierenden Vorschriften der DS-GVO für die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung zur Anwendung kommen können, ist nach der DSK erforderlich, dass:

[1] mittels einer methodisch und systematische Vorgehensweise und mit dem [2] Ziel eines Erkenntnisgewinns [3] nachprüfbare[31] Ergebnisse gewonnen werden. Wissenschaftliche Forschung erfordert weiter [4] Unabhängigkeit und Selbstständigkeit sowie ein [5] Gemeinwohlinteresse dergestalt, dass wissenschaftliche Forschung dem Gemeinwohl zugutekommen muss und nicht ausschließlich kommerziellen oder sonstigen Einzelinteressen dienen darf.

IX. Sonderproblem genetische Daten

In ihrem Beschluss vom 15. Mai 2024 setzte sich die DSK in einem Positionspapier mit den Anforderungen an die Sekundärnutzung von genetischen Daten[32] zu Forschungszwecken auseinander.[33] Die DSK unterstrich, dass die Nutzung genetischer Daten einerseits die Grundlage für eine personalisierte, auf die individuelle Patientin oder den individuellen Patienten angepasste Präzisionsmedizin ist und Forschung in diesem Bereich den biomedizinischen Fortschritt wesentlich und die medizinische Versorgung

20 DSK, Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern, 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf

21 Entscheidungsformate der Datenschutzkonferenz sind nach ihrer Geschäftsordnung u.a. Entschließungen (öffentliche Stellungnahmen zu datenschutzpolitischen Fragen) und Beschlüsse (Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen).

22 DSK, Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung
nicht eingeschränkt werden!, 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf

23 EuGH 26.10.2023 – C-307/22, ZD 2024, 22 .

24 DSK, Petersberger Erklärung, 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

25 Zentrale Punkte der Erklärung, die darauf abzielt, der Bedeutung wissenschaftlicher Forschung mit Gesundheitsdaten ebenso Rechnung zu tragen, wie den Schutz besonders sensibler personenbezogener Daten zu gewährleisten sind unter anderem die Forderung nach Transparenz und Nachvollziehbarkeit der Datenverarbeitungsprozesse für die betroffenen Personen. Empfohlen wird die möglichst aktive Einbindung der betroffenen Personen, auch wenn die Datenverarbeitung auf gesetzlicher Grundlage erfolgt. Damit korrespondiert ein Vorschlag zur Implementierung digitaler Managementsysteme für verbesserte Informations-, Kontroll- und Mitwirkungsmöglichkeiten. Gefordert werden weiter einheitliche, länderübergreifende Regelungen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken sowie eine lückenlose Überwachung und Durchsetzung datenschutzrechtlicher Regelungen durch unabhängige Datenschutz-Aufsichtsbehörden. Besonders betont schließlich wird die Notwendigkeit eines Forschungsgeheimnisses zum Schutz personenbezogener medizinischer Forschungsdaten. Schlüsselgrundsatz des Papiers ist schließlich die Aussage: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen (bspw. Verschlüsselung, Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung), desto umfangreicher und spezifischer können die Daten genutzt werden („Petersberger Maxime").

26 DSK, DS-GVO privilegiert wissenschaftliche Forschung
Positionspapier zum Begriff „wissenschaftliche Forschungszwecke", 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf.

27 DSK, Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken, 2024, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf.

28 DSK, DS-GVO privilegiert wissenschaftliche Forschung
Positionspapier zum Begriff „wissenschaftliche Forschungszwecke", 2024, Dokument abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf.

29 Art. 5 Abs. 1 Buchst. b DS-GVO (Zweckbindung), Art. 9 Abs. 2 Buchst. j DS-GVO (Öffnungsklausel für die Verarbeitung besonderer Kategorien personenbezogener Daten), Art. 14 Abs. 5 Buchst. b DS-GVO (Einschränkung der Informationspflichten), Art. 17 Abs. 3 Buchst. d DS-GVO (Einschränkung des Rechts auf Löschung), Art. 21 Abs. 6 DS-GVO (Widerspruchsrecht) und Art. 89 DS-GVO (besondere Garantien und Ausnahmen).

30 Art. 13 GRCh; Artikel 179 Absatz 1 AEUV; ErwG 159 DSGVO.

31 Die Durchführung und die Ergebnisse des Forschungsvorhabens müssen nach wissenschaftlichen Standards dokumentiert werden und dürfen nicht von vornherein von Geheimhaltungsabsicht getragen sein.

32 „Genetische Daten" sind nach Artikel 4 Nummer 13 der Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

33 DSK, Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken, 2024, https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

wesentlich verbessern kann. Andererseits hob die DSK die besonders hohen Risiken hervor, die mit der Verarbeitung genetischer Daten einhergehen. Das folgt einmal aus dem besonderen prädiktiven Potenzial der Daten, weil Erkenntnisse über gesundheitliche Prädispositionen, Gesundheitsrisiken und vererbliche Erkrankungen ableitbar sind. Weiter betreffen diese Erkenntnisse nicht nur die betroffene Person selbst, sondern können sich auch auf leibliche Familienangehörige erstrecken. Das Diskriminierungs- und Stigmatisierungsrisiko bei Kenntnis dieser Daten, z. B. durch Versicherungen und Arbeitgeber, ist daher enorm.

Vor diesem Hintergrund fordert die DSK u.a., dass ein spezieller gesetzlicher Rahmen für diesen Verarbeitungskontext geschaffen wird, die Verarbeitung genetischer Daten zu Forschungszwecken grundsätzlich nur mit Einwilligung[34] der betroffenen Personen erfolgt und zusätzliche (technisch organisatorische) Schutzmaßnahmen sowie spezifische Garantien (Mitwirkungs- und Kontrollmöglichkeiten für die betroffenen Personen) implementiert werden.

In Ansehung des zwischenzeitlich ausverhandelten EHDS[35] befindet sich der Gesetzgeber in einem herausfordernden Gestaltungskorridor.[36]

X. Fazit

Rückblickend ist für das vergangene Datenschutzjahr eine politische Großwetterlage zur Kenntnis zu nehmen, in dem der Datenschutz seine Daseinsberechtigung und Anschlussfähigkeit mehr denn je zu beweisen hat – und dass informationelle Selbstbestimmung und Innovation keine Gegenspieler sind, sondern Ausdruck unseres gesellschafts- und damit auch rechtspolitischen Selbstverständnisses. Im Zentrum des technischen Fortschritts muss der Mensch stehen. Gesichert wird dies durch eine wertebasierte Regulierung von Künstlicher Intelligenz ebenso wie durch einen grundrechtssensiblen Umgang mit personenbezogenen Daten. Für Normadressaten und Aufsichtsbehörden gleichermaßen herausfordernd ist, den bis dato wenig kohärenten Kanon des Digital- und Datenrechts für Europas digitale Dekade zu durchdringen.

34 Ggfls. auch im Wege des Broad Consent im Sinne des Erwägungsgrunds 33 DS-GVO.

35 Zur Genese Hofmann jurisPR-ITR 18/2024 Anm. 2.

36 Im Trilog zum EHDS waren die Regelungen zur Sekundärnutzung bis zuletzt umstritten. Das Ergebnis enthält jetzt einen Kompromiss. Demnach steht natürlichen Personen ein Widerspruchsrecht hinsichtlich der Sekundärnutzung ihrer Daten zu (Art. 71 EHDS-E). Die Mitgliedstaaten können im Rahmen einer Öffnungsklausel indes strengere Maßnahmen und Garantien zum Schutz von besonders sensiblen Datenkategorien einführen, wie etwa das Erfordernis eines Opt-ins hinsichtlich der Sekundärdatennutzung von Daten besonders sensibler Kategorien (Art. 51 Abs. 4, Art. 51 Abs. 1 lit. f EHDS-E). Den Mitgliedstaaten steht ferner offen, das Widerspruchsrecht für die Sekundärdatennutzung zum Zweck der öffentlichen Gesundheit, Politikgestaltung, Statistik oder Forschung von besonderem öffentlichem Interesse außer Kraft zu setzen (Art. 71 Abs. 4 EHDS-E). Diese Ausnahmen sind jedoch nur in grundrechtswahrender und verhältnismäßiger Weise zulässig und erfordern zudem spezifische und geeignete zusätzliche Maßnahmen zum Schutz der Grundrechte und personenbezogener Daten der betroffenen natürlichen Personen (Art. 71 Abs. 4 UA 2 EHDS-E).

Andreas Jaspers*

Mut zum Datenschutz – KI mit Verantwortung: Vorträge und Diskussion am datenpolitischen Vormittag der DAFTA 2024

Am 14. und 15. November 2024 richteten die Gesellschaft für Datenschutz und Datensicherheit (GDD) und Datakontext im Kölner Maternushaus die 48. Datenschutzfachtagung (DAFTA) aus. Auch in diesem Jahr standen die rechtlichen Herausforderungen des KI-Einsatzes im Fokus der Vorträge und Diskussionen. Der nachfolgende Beitrag fasst zentrale und besonders praxisrelevante Aussagen des datenpolitischen Vormittags zusammen.

Künstliche Intelligenz (KI) beschäftigt nach wie vor Unternehmen und Behörden sowie ihre Datenschutzbeauftragten. Während die erste Welle der Begeisterung über die Fähigkeiten moderner KI-Systeme langsam abklingt, geht es nun darum, die Technologie verantwortungsbewusst in Unternehmensabläufe zu integrieren. Das Datenschutzrecht wird dabei oftmals als hemmender Faktor der Einführung KI-basierter Prozesse bezeichnet. Welche Potenziale die Technologie tatsächlich birgt und welche Vorgaben dem Datenschutzrecht bei einer angemessenen Auslegung zu entnehmen sind, war Thema der 48. DAFTA, die am 14. und 15 November 2024 unter der Schirmherrschaft der GDD im Kölner Maternushaus stattfand.

Den traditionellen datenpolitischen Vormittag zu Beginn der DAFTA eröffnete Prof. Dr. Rolf Schwartmann, Vorstandsvorsitzender der GDD, mit einem Vortrag zu KI-Kompetenz. Diese müssen Unternehmen, die KI entwickeln oder einsetzen, ihren Mitarbeitern gem. Art. 4 KI-VO bis zum

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

2. Februar 2025 vermitteln. Schwartmann betonte, dass KI-Kompetenz nicht nur die Risiken, sondern auch die Möglichkeiten des KI-Einsatzes aufzeigen soll. Welche technischen Möglichkeiten der KI-Einsatz eröffnet, war sodann Gegenstand einer Untersuchung von Prof. Dr. Katharina Zweig, Data Scientist der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau und Mitglied der Enquete-Kommission Künstliche Intelligenz des Deutschen Bundestags. Sie beschäftigte sich in ihrem Vortrag mit der Frage, ob es sich bei KI-Chatbots wie ChatGPT um plappernde Papageien oder doch um nachdenkende Superhumen handelt. Mit vielen anschaulichen Beispielen erklärte sie, wie die Maschinen Entscheidungen treffen und Texte generieren. Sie kam zu dem Ergebnis, dass KI-Systeme noch weit entfernt sind von den übermenschlichen Fähigkeiten, die ihnen insbesondere von ihren Entwicklern bisweilen angedichtet werden. Die Maschine sei nicht in der Lage die emotionalen Assoziationen abzubilden, die ein Begriff typischerweise in einem Menschen auslöst. Das sei aber eine wichtige Voraussetzung für die Annahme, dass die KI nachdenken kann. Allerdings sei der Kontext der Bedeutung des Begriffs semantisch in die Datenstruktur der KI eingebettet. Zweig bezeichnete ChatGPT deshalb abschließend als „plappernden Papagei mit Nachdenken light".

Anknüpfend an die Darstellung der technischen Möglichkeiten des KI-Einsatzes beschäftigte sich die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Louisa Specht-Riemenschneider, mit der Frage, ob sich KI und Datenschutz in einem Spannungsfeld befinden. Wegen der zeitgleich stattfindenden Datenschutzkonferenz war Specht-Riemenschneider per Videobotschaft zugeschaltet. Sie stellte die wichtigsten Rechtsakte des Daten- und KI-Rechts, namentlich die DS-GVO, die KI-VO sowie den Data Governance Act vor. Specht-Riemenschneider bedauerte, dass ihre Behörde kaum aufsichtsrechtliche Kompetenzen im Rahmen der KI-VO bekommen werde. Sie betonte aber, dass sie sich dafür einsetzen werde, innovative KI-Lösungen unter Einhaltung der DS-GVO zu ermöglichen. Dazu wolle sie auf eine klare Definition der Zusammenarbeit zwischen BfDI und Bundesnetzagentur hinwirken.

Im Anschluss an die Videobotschaft der BfDI räumte Kristin Benedikt, Richterin am Verwaltungsgericht Regensburg und Mitglied des Vorstands der GDD, mit einigen Mythen zu datenschutzrechtlichen Herausforderungen beim Einsatz von KI auf. Sie betonte, dass KI nicht geeignet sei, Prozesse zu digitalisieren. Vielmehr seien Maßnahmen zur Digitalisierung Grundvoraussetzung der Einführung KI-basierter Prozesse. Am Beispiel der BayernKI, die Behördenmitarbeitern im Freistaat zur Verfügung gestellt wird, beschäftigte sie sich mit den datenschutzrechtlichen Vorgaben, die beim KI-Einsatz zu beachten sind. KI müsse im Rahmen einer datenschutzkonformen Implementierung als Mittel und nicht als Zweck der Verarbeitung begriffen werden. Der Zweck der Verarbeitung richte sich nach dem Use Case und bestimme über die Möglichkeiten eines rechtskonformen Einsatzes. Wichtig sei, dass Unternehmen den KI-Einsatz regeln. Den Arbeitgeber treffe die Verantwortung, Use Cases zu bestimmen, Rechte und Pflichten in Unternehmensrichtlinien festzulegen und den Mitarbeitern die erforderliche KI-Kompetenz zu vermitteln.

Im Anschluss an die Vorträge diskutierten die Referenten gemeinsam mit Gabriela Krader, Konzerndatenschutzbeauftragte bei der Deutsche Post DHL Group, David Pfau, externer Datenschutzbeauftragter des Bundesverbands Digitale Wirtschaft, und Andreas Jaspers, Geschäftsführer der GDD, unter der Moderation von Schwartmann über die Herausforderungen und Möglichkeiten der Implementierung KI-gestützter Prozesse in unterschiedlichen Branchen. Die Diskussionsteilnehmer waren sich einig, dass ein verantwortungsvoller Einsatz Künstlicher Intelligenz nur in Kenntnis der Risiken und Potenziale stattfinden kann. Sie forderten Unternehmen deshalb dazu auf, Verantwortung zu übernehmen und den KI-Einsatz zu regeln. Als Negativbeispiel wurde eine Umfrage der Bitkom zum um sich greifenden Einsatz sogenannter Schatten-KI angeführt.[1] Demnach werden in jedem dritten Unternehmen private KI-Zugänge benutzt und regelmäßig geduldet. Benedikt betonte, dass der Arbeitgeber auch in dieser Konstellation für die Einhaltung rechtlicher Vorgaben verantwortlich sei. Am Ende der Diskussion und damit auch des datenpolitischen Vormittags stand die Erkenntnis, dass Unternehmen die Verantwortung für den Einsatz Künstlicher Intelligenz übernehmen müssen, wenn sie dessen Potenziale nutzen wollen.

Wie immer schlossen sich an den datenpolitischen Vormittag zahlreiche Vorträge und Diskussionen in insgesamt neun Foren an. Am Abend des ersten DAFTA-Tages verlieh außerdem der wissenschaftliche Beirat der GDD unter Vorsitz von Prof. Dr. Tobias Keber den GDD-Wissenschaftspreis als Würdigung für herausragende wissenschaftliche Arbeiten an Dr. Sarah Rachut für ihre Dissertation zur Grundrechtsverwirklichung in digitalen Kontexten sowie an Dr.-Ing. Hossein Yalame für seine IT-Dissertation "Advancing MPC: From Real-World Applications to LUT-Based Protocols". Den Förderpreis erhielt Agnes Lipp für ihre Masterarbeit "Informationsrecht betroffener Personen zu technischen und organisatorischen Maßnahmen (TOMs)". Der GDD-Datenschutzpreis für besondere Verdienste um die Entwicklung und Akzeptanz von Datenschutz und Datensicherheit in Deutschland und Europa ging an Prof. Dr. Katharina Zweig.

Nach einem Schlusswort von Prof. Dr. Rainer W. Gerling ging die 48. DAFTA am Freitagnachmittag zu Ende. Die Teilnehmer durften sich über zahlreiche praxisrelevante Hinweise und Informationen freuen, verließen die Tagung aber auch mit einigen Aufgaben, die es umzusetzen gilt. Besonders dringlich ist nun die Regelung des KI-Einsatzes in den Unternehmen und die Vermittlung von KI-Kompetenz bis zum 2. Februar 2025.

1 Bitkom, Wenn das Unternehmen keine KI verwendet, bringen die Beschäftigten sie mit, 4.11.2024, https://www.bitkom.org/Presse/Presseinformation/Wenn-Unternehmen-keine-KI-verwendet-bringen-Beschaeftigte-sie-mit.

Rezension

Rolf Schwartmann/Moritz Köhler, Textbuch Deutsches Recht: Datenrecht. Datenschutz, Datenwirtschaft, Digitalwirtschaft und KI., C. F. Müller, 2025, 1085 Seiten, ISBN 978-3-8114-6453-7

Bei dem zu besprechenden Werk handelt es sich um ein Textbuch, sprich um eine Gesetzessammlung. Rezensionen solcher Werkgattungen sind selten – zu Unrecht, denn trotz der rasant voranschreitenden Digitalisierung mit ihren Möglichkeiten des ubiquitären und jederzeitigen Abrufs von Normtexten im Internet kommt ihnen nach wie vor eine wichtige Rolle für das rechtswissenschaftliche und rechtspraktische Arbeiten zu.

Es ist deshalb angezeigt, zunächst eine Lanze für die Textbuch-Reihe des C. F. Müller-Verlags im Allgemeinen zu brechen. Seit Jahrzehnten erweist sie sich als wertvolle Begleiterin von Studierenden, Dozierenden und Praktikern. Dies liegt nicht nur an ihrem sehr handlichen Format. Es liegt auch an dem Umstand, dass sie in sehr sachkundiger Art und Weise die wichtigsten Rechtstexte zu einem Themenkreis – aus den Forschungs- und Lehrbereichen des Rezensenten seien insoweit das Medienrecht, das Staats- und Verwaltungsrecht sowie das Völker- und Europarecht hervorgehoben – komprimiert zusammenstellt und regelmäßig aktualisiert. Trotz der skizzierten Möglichkeiten des World Wide Web sind diese Textbücher ein wertvolles Arbeitsmittel des Juristen geblieben. Denn noch immer vermag die virtuelle Darstellung von Rechtstexten auf einem wie auch immer gearteten „Screen" mit der Handlichkeit, Übersichtlichkeit und Schnelligkeit, die eine Textsammlung bei der Erschließung des wichtigsten Werkzeugs des Juristen – dem Gesetz – bietet, nicht zu konkurrieren. Hierzu tragen insbesondere das alphabetische Schnellregister und die Ordnungsnummern der C. F. Müller-Textbücher bei. Allein ihr Preis – für das aktuelle Datenrecht schlagen 35,00 € zu Buche – mag den ein oder anderen Nutzer, vor allem studentischer Provenienz, schmerzen.

Um die vorstehend skizzierten Funktionen zu erfüllen, bedarf es versierter Herausgeber, die Rechtstexte zu bestimmten Themengebieten sachkundig zusammenstellen und präsentieren. *Rolf Schwartmann* – einer der Mitherausgeber des hier zu besprechenden Textbuchs – leistet diese verdienstvolle Aufgabe schon seit Jahren durch die Herausgabe diverser Gesetzessammlungen mit einem Schwerpunkt im Internet- und Datenschutzrecht. Für das nun vorgelegte Textbuch zum Datenrecht haben sich die Herausgeber von der zutreffenden Erwägung leiten lassen, dass auf europäischer und nationaler Ebene jüngst zahlreiche und teils neue Rechtsakte zum Umgang mit Daten und datenverarbeitenden Technologien ergangen sind. Die Herausgeber fassen diese Entwicklung unter dem Oberbegriff „Datenrecht" zusammen, was in einer kurzen sowie instruktiven Einführung näher erläutert wird. Als Unterkategorien, die zugleich der Systematisierung des Textbuchs dienen, identifizieren sie das klassische Datenschutzrecht (DS-GVO etc.), das Datenwirtschaftsrecht (DA, DGA etc.), das Digitalrecht (DSA, DMA, DDG etc.) und das KI-Recht (KI-VO). Das Kuratieren der insoweit relevanten Haupt-, Begleit- und Umsetzungsgesetze, die zudem durch sachgebietsrelevante Auszüge übergeordneter Rechtsvorschriften (AEUV, GRCh, GG, Landesverfassungen etc.) oder sonstiger allgemeiner Kodifikationen (BGB, GWB, UrhG, UWG) ergänzt werden, erweist sich als gelungen und lässt *prima facie* nichts Wesentliches zum Thema Datenrecht vermissen. Im Übrigen können den Herausgebern eventuell identifizierte Lücken über die im Vorwort abgedruckten E-Mail-Adressen mitgeteilt werden. Zur Erhöhung der Lesbarkeit und Zugänglichkeit der Rechtstexte haben *Schwartmann* und *Köhler* die Erwägungsgründe zu den unionalen Rechtsakten dankenswerterweise nachgestellt und diese für den Nutzer durch Fußnotenhinweise an den Überschriften der Normtexte erschlossen. Auf den Abdruck von Richtlinien scheinen die Herausgeber hingegen bewusst verzichtet zu haben, was mit Blick auf den Umstand, dass diese bereits durch die abgedruckten nationalen Umsetzungsakte (z.B. DDG für die E-Commerce-Richtlinie) abgebildet werden, nachvollziehbar erscheint und den Umfang des Werks auf ein sinnvolles Maß begrenzt.

Dies leitet zu einer Besonderheit der Textsammlung über: Mit Blick auf die adressierte Notwendigkeit einer Begrenzung haben sich die Herausgeber darauf beschränkt, Rechtsakte mit der aus ihrer Sicht größten Relevanz für Studium und Praxis in das Textbuch aufzunehmen. Andere sachgebietsrelevante Gesetze unter Einschluss von Richtlinien, auf die diese Charakterisierung nach ihrer Auffassung nicht zutrifft, werden deshalb nur digital über eine Link-Sammlung auf der Webseite der Kölner Forschungsstelle für Medienrecht zugänglich gemacht. Diese an sich nachvollziehbare Ausgliederung thematisch eher nachgeordneter oder sektorspezifischer Gesetzestexte in den virtuellen Raum durchbricht allerdings den oben beschriebenen Vorzug körperlich greifbarer Gesetzessammlungen. Ob die Nutzer dieses digitale Angebot annehmen werden oder sich den gesuchten Rechtstext selbst über eine Suchmaschine erschließen, bleibt abzuwarten. Durch die Erwähnung der digital verfügbaren Vorschriften im Inhaltsverzeichnis des Textbuchs erfährt der Nutzer jedenfalls, welche sonstigen Rechtsakte zum Themenkreis „Datenrecht" für ihn von Interesse sein könnten.

Gewiss, das von den Herausgebern kuratierte Textbuch weist Überschneidungen zu anderen Textbüchern des C. F. Müller-Verlags – wie etwa zum Medienrecht oder zu dem von *Schwartmann* selbst mit herausgegebenen Internet- und Datenschutzrecht – auf. Die Fülle an Rechtsakten, die in den letzten Jahren auf europäischer und nationaler Ebene zum Thema Datenschutz und Datennutzung ergangen ist, erlaubt es mittlerweile allerdings nicht mehr, alle insoweit relevanten Gesetze und Normen kompakt „zwischen zwei Buchdeckel zu pressen". Trotz der angesprochenen Überschneidungen weisen die erwähnten Sachbereiche unterschiedliche Schwerpunkte auf, was es rechtfertigt, für sie je eigene Gesetzessammlungen herauszugeben. Mit einem Textbuch zu dem noch jungen sowie gesellschaftlich

und wirtschaftlich immens wichtigen Datenrecht haben *Schwartmann* und *Köhler* ohne Zweifel einen „guten Riecher" bewiesen. Jeder, der sich im Studium, in der Wissenschaft oder in der Praxis mit diesem Sachgebiet befasst, dürfte deshalb großen Gefallen an der Nutzung dieser Gesetzessammlung finden.

Prof. Dr. Ralf Müller-Terpitz
Inhaber des Lehrstuhls für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien an der Universität Mannheim

Lina Marie Schauer, Reputation auf Online-Plattformen, Nomos-Verlag, 2024, 384 Seiten, ISBN 978-3-7560-1720-1

Die zunehmend in das digitale Umfeld verlagerte Kommunikation birgt nicht nur Gefahren der Desinformation und Hassrede für Verbraucher. Auch für die Reputation von Unternehmen sind neue Risiken entstanden. Online-Bewertungen und Äußerungen auf sozialen Netzwerken sind nicht selten weltweit einsehbar und werden von einer Vielzahl potentieller Kunden gelesen. Sie haben – ungleich mehr als mündliche Äußerungen im Freundes- und Bekanntenkreis – das Potential, den Ruf eines Unternehmens zu schädigen. Obwohl ihr Wahrheitsgehalt ggfs. schwer überprüfbar ist, sind Online-Bewertungen eine zentrale Informationsquelle für Verbraucher geworden. Zum Schutz vor diffamierenden Bewertungen werden vorrangig zivil- und lauterkeitsrechtliche Unterlassungs- und Beseitigungsansprüche bemüht. Einigen spezifischen Risiken im digitalen Umfeld hat sich der Unionsgesetzgeber jüngst in Novellen des europäischen Lauterkeitsrechts – z.B. hinsichtlich des Influencer-Marketings – als auch durch Verabschiedung des Digital Services Acts angenommen. Dennoch mangelt es an einer systematischen Aufarbeitung des rechtlichen Schutzes der Reputation im digitalen Umfeld. So können auch Online-Plattformen z.B. durch ihre Darbietung der Nutzerbewertungen Einfluss auf den unternehmerischen Ruf nehmen. Die Dissertation von *Lina Marie Schauer* nimmt sich daher einem Thema mit wachsender praktischer Bedeutung an.

Die Arbeit beginnt mit einer Grundlegung (S. 25–95). Darin nähert sich die Verfasserin dem Begriff der Reputation aus interdisziplinärer Perspektive und legt für den weiteren Gang der Untersuchung eine weite Arbeitsdefinition fest, wonach der Reputationsbegriff mit dem des Rufs bzw. des Ansehens gleichgesetzt wird (S. 64 f.). Zugleich wird mit dem Fokus auf Bewertungsplattformen eine sinnvolle Eingrenzung des Untersuchungsgegenstands vorgenommen (S. 68–79). Neben Internetseiten wie „*Yelp*" oder „*Tripadvisor*" zählt die Verfasserin dazu auch integrierte Reputationssysteme, die u.a. auf Plattformen wie „*eBay*" und „*Amazon*" vorzufinden sind (S. 70 f.). Dieser Zuschnitt überzeugt, werden die dort genutzten Bewertungssysteme doch durch dieselben Merkmale geprägt. Insbesondere sind die dargebotenen Meinungen für eine breite Öffentlichkeit zugänglich, während die Bewertenden bisweilen in der Anonymität verbleiben.

Der zweite und umfassendste Teil der Arbeit widmet sich dem Reputationsschutz de lege lata (S. 97–333). Die Verfasserin untersucht, wie die unternehmerische Reputation nach geltendem Recht Schutz erfährt. Besonders positiv sticht der Aufbau der Arbeit hervor. Es wird danach differenziert, welcher Akteur – Reputationsträger selbst (S. 97–163), Rezensent (S. 164–217) oder Plattformbetreiber (S. 218–333) – auf das unternehmerische Reputationsbild Einfluss zu nehmen sucht. Strategien von Unternehmen, ihre Online-Reputation zu verbessern, sind vielfältig. Die Verfasserin stellt verschiedene Methoden dar, die von dem Erwerb gefälschter Bewertungen und Likes über subtilere Wege wie der Aufbereitung von Drittbewertungen und der Aufforderung zur Bewertungsabgabe reichen. Jede diese Strategien wird einer rechtlichen Bewertung unterzogen. Die Verfasserin kommt zu überzeugenden Ergebnissen. Insbesondere vertritt sie, dass die Beauftragung von gefälschten Bewertungen gegen die „schwarze Liste" des UWG verstößt (S. 120 f.). Möglicherweise hätte eine deutlichere Schwerpunktsetzung den Zugang zu diesem Teil der Arbeit etwas erleichtert. An einigen wenigen Stellen wirkt die Abhandlung der lauterkeitsrechtlichen Verbote lehrbuchartig, etwa wenn das weite Tatbestandsmerkmal der geschäftlichen Handlung oder offensichtlich nicht verwirklichte Tatbestände subsumiert werden. Der übersichtlichen Gestaltung tut dies insgesamt jedoch keinen Abbruch.

Anschließend widmet sich die Arbeit Reputationsrisiken aus der Sphäre der Rezensenten, die insbesondere aus abträglichen und unwahren Bewertungen rühren können. Innerhalb des allgemeinen Beseitigungs- und Unterlassungsanspruchs aus § 1004 BGB konkretisiert die Verfasserin die einzelfallbezogene Abwägung zwischen Persönlichkeitsschutz und Meinungsfreiheit. Sie kann hierbei auf eine breite Judikatur zurückgreifen, die nicht nur, aber auch Bewertungen auf Online-Portalen umfasst. Die Verfasserin macht sich um eine Konkretisierung der vorhandenen Rechtsprechung zu „*Leitlinien*" verdient, mit welcher sie die in die Abwägung einzustellenden Erwägungen für Online-Bewertungen konkretisiert (S. 177–182). Die Ausführungen zur Beeinflussung des Reputationsbildes durch den Plattformbetreiber legen zunächst einen Schwerpunkt auf die für die Vermittlung von rechtswidrigen Drittinhalten vorhandenen Haftungsprivilegierungen im Digital Services Act. Die Grundsätze der Störerhaftung werden für den Kontext von Online-Bewertungen konkretisiert. Mit Blick auf die Reputationsbeeinflussung durch die plattforminduzierte Darstellung einer Gesamtbewertung erarbeitet die Verfasserin vor allem lauterkeitsrechtliche Grenzen und sieht in § 5a UWG die Pflicht des Diensteanbieters zur Information über die Berechnungsmethode des Gesamtergebnisses (S. 303–312). Der zweite Teil der Arbeit kumuliert in dem überzeugenden Gesamtergebnis, wonach „*bereits ein starkes Regelungsgeflecht zum Schutz des Rufes auf Online-Plattformen*" vorhanden ist (S. 342).

Im dritten Teil wendet sich die Verfasserin Regelungsvorschlägen zu (S. 335–353). Vorgeschlagen wird insbesondere eine Novellierung der UGP-Richtlinie vor. Die Arbeit spricht sich für die Aufnahme einer klarstellenden Informationspflicht hinsichtlich der Kriterien und der Gewichtung einzelner Bewertungen aus, welche durch den Platt-

formbetreiber zu Gesamtbewertungen kumuliert werden. Der zutreffend thematisierte Einwand, dass weitere Informationspflichten zu einem *information overload* beitragen könnten, wird etwas schnell abgetan (S. 350 f.). Verhaltensökonomische Erkenntnisse legen nahe, dass gerade im digitalen Umfeld eine Reizüberflutung vorherrscht, die allenfalls eine partielle Aufnahme der dargebotenen Informationen durch Verbraucher zulässt. Insoweit ist der Verfasserin aber zuzugestehen, dass selbst der (Unions-)Gesetzgeber Informationspflichten auch und gerade auf Plattformen als das Mittel der Wahl ansieht, um Informiertheit auf Seiten der Verbraucher herzustellen. Zumindest legen neuere Rechtsakte (z.B. der Digital Services Act) einen stärken Fokus auf die Art und Weise der Informationsdarbietung. Der von der Verfasserin unterbreitete Regelungsvorschlag fügt sich damit nahtlos in vorhandene Regulierungsansätze ein.

Die Arbeit liefert eine umfassende Untersuchung zum Schutz der Online-Reputation. Die Verfasserin führt den Leser gekonnt durch ein Dickicht an Regelungsmaterien, ohne vom Weg abzukommen. Hinzu kommen anschauliche Beispiele zur Erläuterung der gelegentlich komplexen technischen Sachverhalte. Bei künftigen Regulierungsbestrebungen zum Schutz des unternehmerischen Rufs auf Plattformen ist der Gesetzgeber gehalten, die dargebotenen Ansätze eingehend zu würdigen.

Prof. Dr. Sarah Legner
Inhaberin des Lehrstuhls für Bürgerliches Recht, Wettbewerbs- und Immaterialgüterrecht, Europäisches Privatrecht an der EBS Universität für Wirtschaft und Recht in Oestrich-Winkel

Amélie Heldt/Sarah Legner (Hrsg.), Digitale-Dienste Gesetz, Nomos Verlag, 2025, 364 Seiten, ISBN 978-3-7560-1533-7

Noch rechtzeitig vor Zusammenbruch der derzeitigen Regierungskoalition hat der 20. Deutsche Bundestag am 06.05.2024 das DDG beschlossen. Bereits am 14.5.2024 ist es nach Art. 37 Abs. 1 Gesetz vom 06.05.2024 (BGBl. I Nr. 149) in Kraft getreten. Noch nicht einmal ein halbes Jahr später liegt der hier anzuzeigende Kommentar zu ihm vor – und zwar nicht etwa ein klassischer Referenten-Kommentar, sondern ein nahezu reiner Wissenschaftler-Kommentar. Kann das gut gehen? Zumal, wenn man bedenkt, dass, soweit ersichtlich, kein einziger der Kommentatoren am Gesetzgebungsverfahren als Sachverständiger oder in anderer Eigenschaft beteiligt war.

Es kann und das gleich aus mehreren Gründen. Nicht zuletzt deswegen aber, weil das Gesetz lediglich der Anpassung des nationalen Rechtsregimes an den schon seit 16.11.2022 in Kraft befindlichen DSA dient. Zwar bedarf dieser als EU-Verordnung nach Art. 288 Abs. 2 AEUV keiner Umsetzung in das nationale Recht der Mitgliedstaaten, er setzt in ihnen aber Aufsichts-, bzw. Governance-Strukturen voraus (vgl. Art. 49 ff. DSA). Und genau diese werden durch das DDG geschaffen. Sie stehen denn auch, neben anderem, im Mittelpunkt des Gesetzes (5. Teil: §§ 12–33 DDG) und der Kommentierung. Im Mittelpunkt des Gesetzes steht damit mit anderen Worten aber auch die Bundesnetzagentur (BNA), eine mit nahezu 3.000 Mitarbeitern gerade im digitalen Bereich immer mächtiger werdende Behörde. Sie ist nach § 12 Abs. 1 DDG nicht nur „zuständige Stelle" im Sinne von Art. 49 Abs. 1 DSA, sie ist nach § 14 DDG als „Teilorgan" der BNA (§ 14 Rn. 13) auch „Koordinierungsstelle für digitale Dienste" und in dieser Eigenschaft nach § 20 Abs. 1 S. 2 DDG zugleich auch noch „zentrale Beschwerdestelle". Dass der Leiter der Koordinierungsstelle nach § 16 Abs. 2 S. 1 DDG darüber hinaus zugleich deutscher Vertreter im „Europäischen Gremium für digitale Dienste" ist und damit an entscheidender Stelle sitzt, mag zwar in der Tat systemkonform und „lediglich klarstellend" sein (§ 16 Rn. 11). Zusammen mit seinen umfangreichen, nicht nur polizeiähnlichen, sondern regelrecht polizeilichen Befugnissen (§§ 24 ff. DDG) verschafft ihm dies alles aber eine derartige Machtposition, dass auch der Gesetzgeber daran nicht vorbeigehen konnte. Zahlreiche der Einhegung der Stellung des Leiters der Koordinierungsstelle dienende Vorsichtsmaßnahmen zeugen davon: Unabhängigkeit (§ 15 DDG), Beamtenstatus (§ 16 Abs. 3 DDG), Qualifikationserfordernisse (§ 16 Abs. 4 DDG), Ernennungsmodus (§ 16 Abs. 5 DDG), Inkompatibilitätsregelung (§ 16 Abs. 6 DDG), Rechenschaftspflicht (§ 17 DDG), Attachierung eines pluralistisch zusammengesetzten Beirats (§ 21 DDG). Ob und wie alle diese gut gemeinten Vorkehrungen in der Praxis wirken, bleibt abzuwarten. Wegen des mit der Machtfülle der Koordinierungsstelle verbundenen, nicht von der Hand zu weisenden Missbrauchspotentials hätten ihre Stellung und Befugnisse unter rechtsstaatlichen oder zumindest rechtspolitischen Gesichtspunkten durchaus hinterfragt werden können (zu anderen im Verlauf des Gesetzgebungsverfahrens erörterten Alternativen vgl. § 14 Rn. 6 ff.). Anpassungsbedingt, bzw. Vorschriften des TMG (zB in § 8 DDG) modifizierend, sind auch die im 1. bis 4. Teil geregelten Allgemeinen Vorschriften (§§ 1–4 DDG), die Informationspflichten (§§ 5 und 6 DDG) und Haftungsprivilegierungen der Diensteanbieter (§§ 7 und 8 DDG) und die Vorschriften für Anbieter von audiovisuellen Mediendiensten und für Anbieter von Videosharing-Plattformen (§§ 9–11 DDG).

Kein Zweifel, auch der vorliegende Kommentar beweist, dass das europäische und deutsche Informations-, Daten- und Digitalrecht bei Nomos in guten Händen ist. Angesichts der schieren Quantität, Schnelllebigkeit und Änderungshäufigkeit dieser Rechtsmaterie, aber auch ihrem hohen Komplexitäts- und Schwierigkeitsgrad eine nicht hoch genug einzuschätzende Leistung, die der Rechtsanwender mehr als zu schätzen wissen wird. Angesichts dessen mag man dem Verlag und den dort ganz konkret Verantwortlichen einen langen Atem wünschen, mit diesem aller Voraussicht nach auch in Zukunft nicht nachlassenden Regulierungs-Tempo – wegen des weitgehenden Stillstandes der Gesetzgebung derzeit ungewiss aber etwa das Schicksal des DGG, BT-Drucks. 20/13090 v. 30.9.2024 – Schritt halten zu können.

Ministerialrat a.D. Dr. Michael Fuchs, M.A., Magister rer. publ., Berlin

Zum Gedenken an Prof. Dr. Prof. h.c. Jürgen Taeger

Mit großer Bestürzung haben wir vom plötzlichen Tod von Jürgen Taeger erfahren. Wir verlieren mit ihm einen herausragenden Wissenschaftler, einen geschätzten Herausgeber und Autor und vor allem einen liebenswerten Menschen.

Jürgen Taeger hat mit seiner außerordentlichen Sachkenntnis und seinen analytischen Fähigkeiten wertvolle wissenschaftliche Beiträge vor allem zum Daten- und Informationsrecht geleistet. In den letzten Jahren widmete er sich verstärkt auch produktrechtlichen Fragestellungen und war Mitherausgeber eines Großkommentars zum Produkthaftungs- und Produktsicherheitsrecht sowie Mitbegründer der Zeitschrift für Product Compliance (ZfPC). Auch seine Tätigkeit als Mitglied des Wissenschaftlichen Beirates der Gesellschaft für Datenschutz und Datensicherheit (GDD) war von unschätzbarem Wert. Besonders am Herzen lag ihm die Förderung des wissenschaftlichen Nachwuchses. Mit der Herbstakademie der DSRI hat er dem juristischen Diskurs ein eindrucksvolles und weithin anerkanntes Forum geschaffen.

Neben seiner fachlichen Brillanz war Jürgen Taeger ein Mensch von großer Bodenständigkeit und Herzlichkeit. Mit seiner offenen Art und seinem liebenswerten, trockenen Humor hat er alle, die mit ihm zusammenarbeiten durften, für sich gewonnen. Sein ansteckender Arbeitseifer, sein unermüdlicher Ideenreichtum und die vielen bereichernden Gespräche und Diskussionen mit ihm werden uns sehr fehlen.

Jürgen Taeger wurde 70 Jahre alt. Sein Tod hinterlässt eine Lücke, die nur schwer zu schließen ist. Unsere Gedanken sind in dieser schweren Zeit bei seiner Familie und seinen Angehörigen. Wir danken ihm von Herzen für seine herausragenden Leistungen und seine inspirierende Persönlichkeit. Wir werden ihm ein ehrendes Andenken bewahren.

Verlag, Schriftleitung, Herausgeber und Herausgeberbeirat der EuDIR

Von Governance bis Data Protection

Alles, was Jurist:innen über KI wissen müssen

»Das Werk bietet eine umfassende Analyse der rechtlichen Rahmenbedingungen und Compliance-Anforderungen für den Einsatz von KI. Es handelt sich um einen ***praxisorientierten Leitfaden*** *für Anwaltschaft und Unternehmen, Justiz und Verwaltung sowie für alle, die sich für ›KI und Recht‹ interessieren.«*

Jetzt lieferbar!

KI-Recht international
Compliance Field Guide
Von RA Prof. Dr. Lothar Determann und Prof. Dr. Boris P. Paal, M. Jur. (Oxford)
2025, 205 S., brosch., 49,– €
ISBN 978-3-7560-0989-3
E-Book 978-3-7489-4648-9

Die Autoren präsentieren in ihrem verständlichen und praxisnahen Handbuch konkrete Ansätze zur Einhaltung der internationalen gesetzlichen Rahmenbedingungen. Ziel ist es, die Chancen im Umgang mit KI zu nutzen und gleichzeitig die Risiken zu minimieren. Praktische Empfehlungen helfen, Unternehmensprogramme zur Einhaltung von KI-Richtlinien aufzubauen und aufrechtzuerhalten. Das Werk leitet zudem sicher durch die komplizierten rechtlichen Anforderungen und unterstützt dabei, zukunftssicher (auch) eigene Expertise zur Identifizierung sowie Lösung von neuen Fragestellungen aufzubauen.

Digital verfügbar im Modul NomosOnline PREMIUM bei Beck-Online
Inkl. jährlicher Aktualisierung

Bestellen Sie im Buchhandel oder versandkostenfrei unter nomos-shop.de
Kundenservice +49 7221 2104-222 | service@nomos.de
Alle Preise inkl. Mehrwertsteuer

Nomos

C.F. Müller

Datenschutz- und KI-Recht
auf höchstem Niveau!

DS-GVO/BDSG
Herausgegeben von Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Prof. Dr. Gregor Thüsing und Prof. Dr. Dieter Kugelmann.
3. Auflage 2024, 2.200 Seiten, € 200,– ISBN 978-3-8114-5656-3

Top-Themen in der 3. Auflage des HK DS-GVO/BDSG sind:

- ✓ die Anforderungen an die Praxis durch das **Hinweisgeberschutzgesetz** und die Änderungen im **Nachweisgesetz** mit neuen Transparenzpflichten etwa beim Kündigungsverfahren,
- ✓ die **aktuelle Rechtsprechung** der nationalen Gerichte und des EuGH u.a. zum Beschäftigtendatenschutz, Scoring-System der SCHUFA, zur personalisierten Online-Werbung (TC-String) sowie zu Meta;
- ✓ verschärfte **Sanktionen durch die Datenschutzbehörden**;
- ✓ das **Verhältnis der DS-GVO zu DGA/DA und KI-VO**; tabellarische Übersichten zum Verhältnis der DS-GVO zu den neuen Digitalrechtsakten der EU machen die komplexe Materie transparent.

Wichtiger Hinweis für die Praxis: Die geplanten Änderungen des BDSG zur besseren Durchsetzung des Datenschutzrechts und Rechtssicherheit beim Scoring werden in der Kommentierung bereits berücksichtigt.

Ein besonderes Plus ist die Kommentierung der DS-GVO mit thematisch integrierter Kommentierung des BDSG.

KI-VO
Herausgegeben von Prof. Dr. Rolf Schwartmann, Prof. Dr. Tobias O. Keber und Dipl.-Jur. Kai Zenner M.Sc.
2. Auflage 2024, 360 Seiten, € 85,– ISBN 978-3-8114-6454-4
In englischer Sprache:
AI Act, 322 Seiten, € 85,– ISBN 978-3-8114-6411-7

Der Praxisleitfaden zum Einsatz Künstlicher Intelligenz ermöglicht dem Rechtsanwender **eine verlässliche Orientierung beim Einsatz der neuen Technik**. Neben den Grundlagen in der KI-Verordnung selbst werden praxisrelevante Bereiche in den Anhängen über Hochrisiko-KI-Systeme eingeordnet.

Aufgezeigt werden zudem die in der unternehmerischen Praxis auftretenden **Abgrenzungsfragen zum übrigen Digital- und Datenrecht der EU**, vor allem der DS-GVO. Besonders relevant wird dies etwa bei den **Transparenzvorschriften**, beim **technischen Datenschutz** sowie bei der **Risikofolgenabschätzung**. Schließlich behandelt das Werk praxisrelevante Haftungsfragen, das Verhältnis zum Urheberrecht und stellt die Durchsetzung durch das Aufsichtsregime dar.

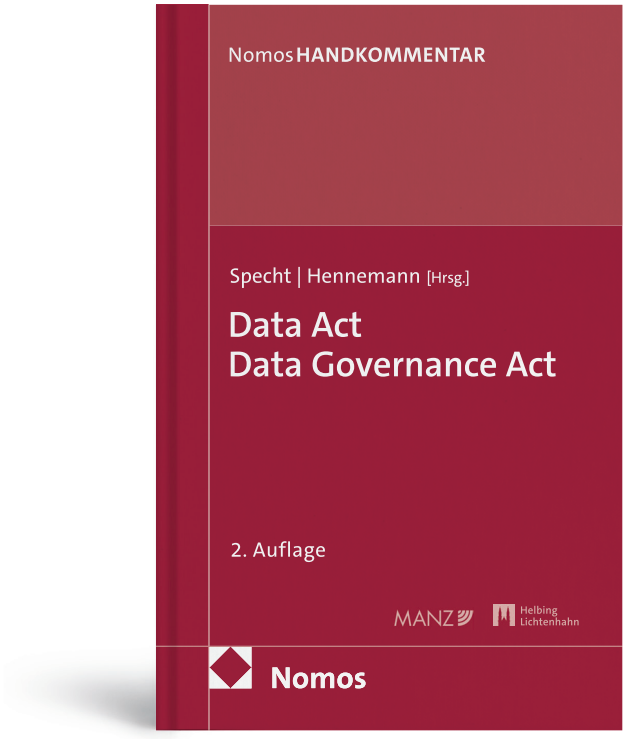
Der Herausgeberkreis und das Autorenteam bestehen aus Angehörigen aus der Aufsichts- und Unternehmenspraxis und von Verbänden, aus der Richter- und Anwaltschaft, aus dem Europäischen Parlament sowie aus praxisnah arbeitenden Wissenschaftlern. Es sind neben juristischen Mitwirkenden insbesondere auch mit KI befasste **Techniker** und **Informatiker** eingebunden.

Schwartmann/Köhler
Datenrecht
Datenschutz, Datenwirtschaft, Digitalwirtschaft und KI
2025, 1.107 Seiten, € 35,–
ISBN 978-3-8114-6453-7

Versandkostenfrei bestellen bei **otto-schmidt.de**
C.F. Müller GmbH, Waldhofer Str. 100, 69123 Heidelberg
Bestell-Tel. 06221/1859-599, kundenservice@cfmueller.de

»Uneingeschränkte Empfehlung«

RA Dr. David Bomhard, ZGI 4/2023, zur Vorauflage



Data Act, Data Governance Act: DA, DGA

Handkommentar

Herausgegeben von Prof. Dr. Louisa Specht
und Prof. Dr. Moritz Hennemann, M.Jur.

2. Auflage 2025, 1.460 S., geb., 179,– €
ISBN 978-3-7560-1516-0

Der Data Act (DA) und der Data Governance Act (DGA) regeln zentrale Bausteine der Datengenerierung, der Datennutzung sowie des Datentransfers – und prägen damit das neue europäische Datenrecht. Dabei hat der DA insbesondere Datenverträge sowie den fairen Zugang zu Daten für Unternehmen, die öffentliche Hand und Verbraucher:innen im Blick. Der DGA ergänzt das bestehende Regulierungsumfeld, vor allem das Datenschutz- und Open Data-Recht, zugunsten einer sicheren gemeinsamen Nutzung von Daten in einer vertrauenswürdigen Zugangs- und Nutzungsumgebung.

Aus einem Guss

Die Neuauflage des „Specht/Hennemann" bietet eine wissenschaftlich fundierte und praxisnahe Vollkommentierung der beiden eng miteinander verknüpften Rechtsakte. Die gemeinsame Kommentierung in einem Band ermöglicht eine umfassende und zusammenhängende Darstellung der rechtlichen Vorgaben. Die Autor:innen arbeiten Überschneidungen, Wechselwirkungen und Abgrenzungen zwischen den beiden Regelwerken präzise heraus und tragen dadurch zu einem besseren Verständnis der jungen unionalen Datenregulierung bei.

Weitere Vorzüge des Werkes

Der Handkommentar besticht durch seine systematische Erläuterungstiefe bei gleichzeitigem Praxisbezug. Die mit Satzziffern abgedruckten Erwägungsgründe erleichtern das Verständnis der komplexen Regelungsstruktur der Rechtsakte. In einer umfassenden Einleitung legen die Autor:innen übergreifende Themen wie die zugrundeliegenden datenpolitischen Weichenstellungen, aktuelle rechtspolitische Entwicklungen auf nationaler, supranationaler und internationaler Ebene und einen Blick ins EU-Ausland sowie eine Gesamtbewertung und -kritik der Verordnungen dar.

Inhaltliche Schwerpunkte

- Datenzugang
- Datenverträge
- Cloud-Anwendungen
- Open Data
- Datenvermittlungsdienste
- Datenaltruismus
- Rahmenbedingungen zur Rechtsdurchsetzung
- Verhältnis zu anderen Rechtsakten, insbesondere zur DS-GVO

Nomos