HZ217004 · ISSN 0178-8930 · www.rdv-online.com
41. Jahrgang **Februar 1/2025**
G 20 141

RDV
Recht der Datenverarbeitung

Zeitschrift für Datenschutz und Digitalisierung

AUFSÄTZE

KURZBEITRÄGE

RECHTSPRECHUNG

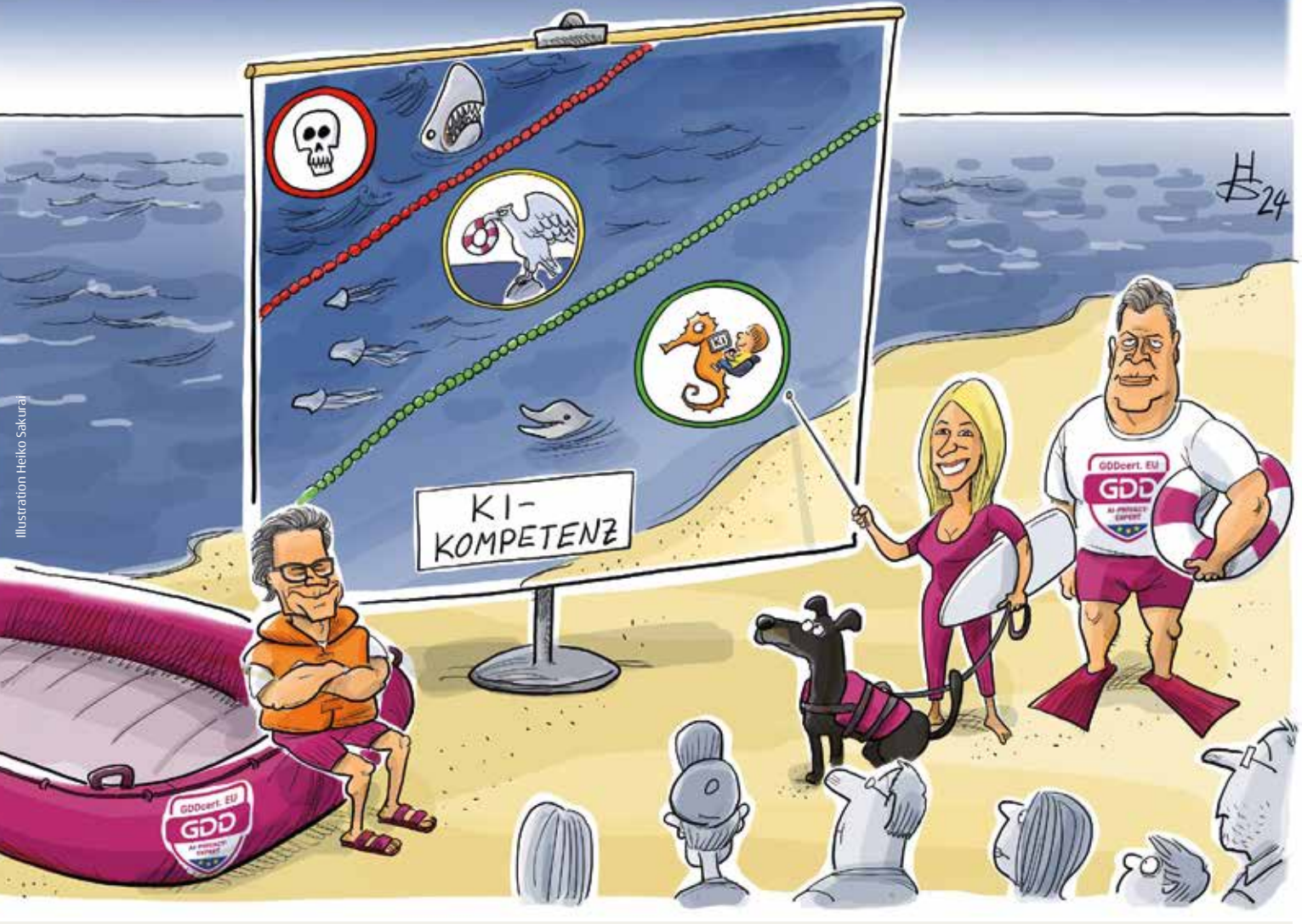


Illustration Heiko Sakurai

Mit KI-Kompetenz sicher zu neuen Ufern

Künstliche Intelligenz bietet Chancen und Risiken – besonders im Datenschutz. Die KI-Verordnung fordert: Nur gut geschulte Schwimmer dürfen hinaus ins offene Meer. Für die ersten Meter genügt das Seepferdchen, doch für tiefergehende Unternehmungen braucht es Rettungsschwimmer.

Merkblatt »KI-Kompetenz«

Das Merkblatt hilft Ihnen, KI-Kompetenzen bei Ihren Beschäftigten gemäß Art. 4 KI-VO aufzubauen. Ermöglichen Sie allen Mitarbeitenden, ihr „Seepferdchen" im Umgang mit KI zu erwerben und setzen Sie die KI-Verordnung fristgerecht bis Februar 2025 um.

GDDcert. EU
GDD
AI-PRIVACY-EXPERT

Ausbildung »AI-Privacy-Expert GDDcert. EU«

Die zertifizierte Ausbildung bereitet Sie optimal auf die anstehenden Herausforderungen vor. Werden Sie „Rettungsschwimmer" und erwerben Sie umfassende Kenntnisse über KI und Datenschutz.

Jetzt KI-Kompetenz aufbauen: www.datakontext.com/ki-kompetenz

GDD

DATAKONTEXT

Redaktion
Lucia Burkhardt | Moritz Köhler | Eva-Maria Pottkämper (Verantwortlich für den Rechtsprechungsteil)

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

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 185,–
Einzelheft	€ 32,–

MwSt. im Preis enthalten, jeweils zzgl. Versandkosten

Vertrieb/Produktsicherheit
Dieter Schulz | Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com
www.datakontext.com produktsicherheitsverordnung

Abo-Service
Telefon: +49 89 2183-7110
Telefax: +49 89 2183-32
aboservice@hjr-verlag.de

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag/Hersteller
DATAKONTEXT GmbH
Augustinusstr. 11A | 50226 Frechen-Königsdorf
Telefon: +49 2234 98949-0
Telefax: +49 2234 98949-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich
HRB 337678

Satz
alka mediengestaltung gmbh
Rücksgasse 3 | 53332 Bornheim

Druck
Grafisches Centrum Cuno GmbH & Co. KG
Gewerbering West 27 | 39240 Calbe (Saale)

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf (verantwortlich)
Telefon: +49 2234 98949-60
wolfgang.scharf@datakontext.com
www.datakontext.com

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

Hinweis
Weil in der RDV bereits bestehende und veröffentlichte Texte integriert sind, wird teilweise, auch zur besseren Lesbarkeit, nur die männliche Sprachform verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Beilagenhinweis:
Sachregister 2024

EDITORIAL

RDV
Recht der Datenverarbeitung

Prof. Dr. Prof. h.c. Jürgen Taeger

* 5. Juni 1954 † 18. Januar 2025

Am 18. Januar 2025 ist Jürgen Taeger im Alter von 70 Jahren verstorben. Sein Tod, der für viele unerwartet kam, lässt uns innehalten in einer Zeit, die einen Menschen wie ihn bitter nötig hat. Unsere Gedanken sind bei seiner Familie, die den Verlust eines geliebten und großherzigen Menschen verschmerzen muss. Zugleich wollen wir an dieser Stelle die Bedeutung unseres langjährigen und äußerst geschätzten Weggefährten würdigen, dessen klugen Rat und dessen große und besondere Expertise uns sehr fehlen wird.

Sein breit gefächertes und wirkmächtiges Schaffen bleibt in zahlreichen wissenschaftlichen Veröffentlichungen sowie Studien- und Fachveranstaltungen erhalten. Die von ihm begründeten Werke müssen nun in seinem Sinne fortgeschrieben werden. Sie sind von seiner interdisziplinären Sicht auf die Dinge gekennzeichnet. Er hatte die Gabe, auf beeindruckende Weise Recht und Technik innovativ zusammendenken. Dies geschah schon in einer Zeit, in der das Daten- und Technikrecht unter seinem Einfluss erst entstand.

Der ehemalige Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Wirtschaftsrecht an der Carl von Ossietzky Universität Oldenburg war zunächst Mitherausgeber und später Mitglied des Praxisbeirates dieser Zeitschrift. Der GDD war Jürgen Taeger seit 2007 als Mitglied des Wissenschaftlichen Beirates verbunden. Das Gremium hat die Aufgabe, die GDD zu beraten und zu unterstützen. Auf dessen Vorschlag hin verleiht unsere Gesellschaft jährlich den Wissenschaftspreis für hervorragende wissenschaftliche Arbeiten im Bereich des Datenschutzes und der Datensicherheit. Es war stets ausgesprochen bereichernd, im Wissenschaftlichen Beirat der GDD mit Jürgen Taeger zusammenzuarbeiten. Ihm oblag die Evaluation juristischer Arbeiten, im Wesentlichen Dissertationen. Es war den Mitgliedern des Gremiums eine Freude, sich mit ihm bei der Auswahl der auszuzeichnenden Arbeiten auszutauschen. Seine Argumentation war fair und engagiert und seine Voten überzeugten mit ihrer glasklaren und präzisen Argumentation. Sein Rat war unschätzbar wertvoll.

Jürgen Taeger hat den wissenschaftlichen Nachwuchs insgesamt geprägt. Dessen Förderung (und Forderung) war ihm ein zentrales Anliegen. Dem wissenschaftlichen Diskurs hat mit der Herbstakademie der DSRI einen eindrucksvollen und breit anerkannten Rahmen gegeben.

Das Wirken und Schaffen von Jürgen Taeger wird seine Lebzeit überdauern und wir werden seiner dankbar und ehrend gedenken.

Peter Gola, Andreas Jaspers, Rolf Schwartmann, Gregor Thüsing
Für die RDV und die GDD

Tobias Keber
Für den Wissenschaftlichen Beirat der GDD

Termine	Thema	Ort	Kontakt
26. – 27.03.2025	Ausbildung zum/zur Datenschutzkoordinator/in	Online	GDD e.V./DATAKONTEXT
01. – 02.04.2025	Ausbildung zum/zur Datenschutzauditor/in GDDcert. EU	Berlin	GDD e.V./DATAKONTEXT
02.04.2025	Prüfung zum/zur Datenschutzkoordinator/in	Online	GDD e.V./DATAKONTEXT
08. – 09.04.2025	Datenschutz-Management nach der DS-GVO - Teil 3	Köln	GDD e.V./DATAKONTEXT
08.04.2025	OKK – Update Datenschutz	Online	GDD e.V./DATAKONTEXT
08. – 10.04.2025	Fortbildung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
10.04.2025	Prüfung zum KI-Datenschutz-Experten (AI-Privacy-Expert) GDDcert. EU	Online	GDD e.V./DATAKONTEXT
11.04.2025	Kollege ChatGPT	Online	GDD e.V./DATAKONTEXT
29.04.2025	Prüfung zum/zur Datenschutzauditor/in GDDcert. EU	Online	GDD e.V./DATAKONTEXT
29.04.2025	Datenschutz International	Online	GDD e.V./DATAKONTEXT
30.04.2025	Compliance-Tests und Schwachstellenscannen	Online	GDD e.V./DATAKONTEXT
13.05.2025	Datenschutz-Folgenabschätzung	Online	GDD e.V./DATAKONTEXT
13.05.2025	ISO 27001 und Datenschutz	Köln	GDD e.V./DATAKONTEXT
14.05.2025	Repetitorium zum GDDcert. - Vorbereitung auf die GDDcert. EU-Prüfung	Köln	GDD e.V./DATAKONTEXT
14.05.2025	IT-Sicherheitsmanagement aus Sicht des Datenschutzbeauftragten	Online	GDD e.V./DATAKONTEXT
15.05.2025	Repetitorium zum GDDcert. - Vorbereitung auf die GDDcert. EU-Prüfung	Online	GDD e.V./DATAKONTEXT
15.05.2025	Strategischer Umgang mit Bußgeldbescheiden und Verbandssanktionengesetz	Online	GDD e.V./DATAKONTEXT
20. – 21.05.2025	Ausbildung zum/zur Datenschutzkoordinator/in	Mannheim	GDD e.V./DATAKONTEXT
20.05.2025	OKK: Kennzahlen und KPIs als Mittel zur Überwachung des Datenschutzes	Online	GDD e.V./DATAKONTEXT
22.05.2025	Einführung in die ISO 27701	Online	GDD e.V./DATAKONTEXT
27.05.2025	Datenschutz im Internet	Online	GDD e.V./DATAKONTEXT
03.06.2025	Datenschutz Management light	Online	GDD e.V./DATAKONTEXT
26. – 27.06.2025	12. Hamburger Datenschutztage	Hamburg	GDD e.V./DATAKONTEXT

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

AUFSÄTZE

Prof. Dr. Rolf Schwartmann

Datenrecht 2025 – Fünf Thesen für einen Neuanfang

„Mehr als die Vergangenheit interessiert mich die Zukunft, denn in ihr gedenke ich zu leben". Getreu dieser Weisheit von Albert Einstein sollte man die Vergangenheit des Daten- und Digitalrechts 2024 hinter sich lassen, um sich einer besseren Zukunft zuzuwenden. Das sind fünf Thesen für eine Bestandsaufnahme des Jahres 2024 und einen Neuanfang.*

I. Die Datenwirtschaft braucht Koordination und ein Digitalministerium

Das Datenrecht hat sich seit 2016 mit dem Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO)[1] bis Ende 2024 zu einem europäisch harmonisierten Datenschutz- und Datenwirtschaftsrecht entwickelt. War die DS-GVO zunächst die einzige Geige im Konzert der Datenrechtsakte, so muss sie sich heute in das Orchester der hinzugekommenen Datenakte mit unterschiedlichen und teilweise gegenläufigen Ausrichtungen einfügen. Zentral sind der Daten-Governance--Rechtsakt (DGA),[2] die Datenverordnung (DA),[3] das Gesetz über digitale Märkte (DMA),[4] das Gesetz über digitale Dienste (DSA)[5] und die Verordnung über Künstliche Intelligenz (KI-VO).[6] All diesen Rechtsakten geht es nicht um Datenschutz. Sie regeln die Strukturen des Datenaustauschs (DGA), das Datenteilen zu wirtschaftlichen Zwecken für Nutzer und Unternehmen (DA), die Sicherung des Wettbewerbs im EU-Binnenmarkt gegenüber den internationalen „Tech-Giganten" (DMA) und den Schutz der Meinungsfreiheit und der Bekämpfung von „Hasskriminalität" auf Plattformen wie Sozialen Netzwerken (DSA). Es kommen weitere Rechtsakte und ganze Pakete hinzu, über Digitale Identitäten (eIDAS),[7] den Bereich Platform-to-Business (P2B),[8] Fluggastdaten (API)[9] und die Digitalisierung des Finanzmarktes (DORA),[10] um nur einige zu nennen. Damit das Zusammenspiel harmonisch klingt, muss es orchestriert werden. Daran sind neben der EU auch die Mitgliedstaaten beteiligt.

Der Digitalausschuss des Deutschen Bundestages hat im Juni 2024 Sachverständige unter der Überschrift „Innovative Datenpolitik: Potenziale und Herausforderungen" angehört.[11] Ihr Ergebnis kann man mit einem Wort zusammenfassen: „Herkulesaufgabe". Benennt man von den vielen Problemen nur das spezifisch deutsche, so lautet das Lösungswort: „Koordination". Sie ist der Knackpunkt der Datenpolitik und ihr Fehlen ist ein enormer Missstand. Bürger und Wirtschaftsunternehmen haben es mit einer Vielzahl von Behörden zu tun. Diese sind teilweise überfordert und überlastet. Das Recht ist faktisch kaum vollziehbar. Allein die Durchführung der DS-GVO obliegt in Bund und Ländern 18 Behörden. Es gibt ein Bundesdatenschutzgesetz und 16 Landesdatenschutzgesetze. Jede Aufsichtsbehörde ist völlig unabhängig und dennoch muss die DS-GVO einheitlich ausgelegt werden. Die Konferenz der Datenschutzbeauftragten arbeitet an der Einheitlichkeit ihrer Entscheidungen, kann aber die Hindernisse aus eigener Kraft nicht überwinden. Der Bundesgesetzgeber könnte versuchen, den Datenschutz über die Wirtschaft bei der Bundesbeauftragten anzusiedeln. Das geht nicht ohne die Länder und würde eine „Superbehörde" beim Bund für den Datenschutz erzeugen. Zu einer solchen entwickelt sich aber gerade jenseits des Datenschutzes die Bundesnetzagentur, die den DSA beaufsichtigt und wohl auch die Aufsicht über die Durchführung der KI-VO durchführen soll. Da

* Der Beitrag basiert auf einem Text, der in der F.A.Z. v. 30.12.2024, S. 18 veröffentlicht wurde. Alle Internetquellen wurden zuletzt am 02.01.2024 abgerufen.

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

2 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30.05.2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Verordnung).

3 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).

4 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.09.2022 über wettbewerbsfähige und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Digital Markets Act).

5 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Digital Services Act).

6 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung verschiedener Verordnungen und Richtlinien (Verordnung über Künstliche Intelligenz).

7 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23.07.2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

8 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.06.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten.

9 Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27.04.2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

10 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die digitale operationelle Resilienz des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

11 Vgl. Schwartmann, Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestags zum Thema Innovative Datenpolitik: Potenziale und Herausforderungen, abrufbar unter: https://www.bundestag.de/resource/blob/1010058/15b3c22909f8abd112260e5eaa1cfdc1/Stellungnahme-Schwartmann.pdf.

aber KI-Modelle und -Systeme nicht ohne personenbezogene Daten auskommen, sehen sich die 18 Datenschutzbehörden als sachnäher an und reklamieren die Marktüberwachung nach der KI-VO für sich.[12] Wenn auch die Aufsicht über die Durchführung des DA der Bundesnetzagentur zufiele, läge faktisch die Koordination des Vollzuges des Datenrechts mit Ausnahme der DS-GVO bei einer Behörde. Diese Koordinationsaufgabe ist zentral.

Die neue Bundesregierung muss sie angehen und kann sie schlecht einer Behörde überlassen. Vielleicht wäre das kürzlich ins Gespräch gebrachte Datengesetzbuch ein Anlass, die diversen Rechtsakte in Deutschland zu konsolidieren und zu systematisieren.[13] Ob man die nationalen Begleitrechtsakte zum EU-Datenrecht sinnvoll in einem Gesetz bündeln kann, wird zu prüfen sein. Möglicherweise entscheidet man sich wie beim Umweltgesetzbuch für einen anderen Weg.[14] Eine Vereinheitlichung und Systematisierung des Digital- und Datenrechts in Deutschland ist aber elementar und sie kann nicht dezentral und ressortübergreifend gelingen. Deshalb ist es Zeit für ein „echtes" Digitalministerium. Dieses müsste als Querschnittsministerium schnell mit eigenen Haushaltsmitteln ausgestattet werden und für die Digitalpolitik der Bundesregierung zuständig sein. So könnte es eine effektive und effiziente Digitalisierung vorantreiben. Wichtige erste Projekte wären die Systematisierung des Datenrechts, das Vorantreiben der Verwaltungsdigitalisierung, und die digitalpolitische Koordination innerhalb der Bundesregierung und den Bundesbehörden sowie zwischen Bund, Ländern und EU.

II. Der Datenschutz braucht Augenmaß

Die DS-GVO bleibt auch im neuen Datenrecht der Ausgangspunkt des menschenzentrierten Datenumgangs in der EU. Man muss sie aber entsprechend ihrer Ratio und mit Augenmaß anwenden. Die Ziele der DS-GVO beschreiben ein Spannungsverhältnis. Die DS-GVO verpflichtet einerseits zum Schutz personenbezogener Daten. Zum anderen schützt sie den freien Verkehr solcher Daten.[15] Die Datenschutzaufsichtsbehörden verpflichtet das Gesetz explizit dazu, beide Pflichten umzusetzen.[16] Sie verlieren das zweite und gleichrangige Ziel zu oft aus den Augen. Die Rechtsprechung bestärkt diesen Trend. So hat der Bundesgerichtshof (BGH) in seiner sogenannten „Scraping-Entscheidung" aus dem November 2024 die entsprechende Rechtsprechung des EuGH von 2023 in das deutsche Recht übertragen.[17] Es geht darum, ob ein bloß kurzer Verlust über die Kontrolle personenbezogener Daten einen Schaden im Sinne der DS-GVO darstellt. Der EuGH sieht in jedem noch so belanglosen Kontrollverlust einen potenziellen Schaden.[18] Verlangt der Betroffene deshalb Schadenersatz, muss er allerdings nachweisen, dass er eine missbräuchliche Verwendung seiner Daten befürchtet, die aufgrund des Kontrollverlustes möglich erscheint.[19] Diesen Unterschied ebnet der BGH ein, indem er den Kontrollverlust und die Befürchtung einer missbräuchlichen Verwendung gleichsetzt.[20] Das geht über das Urteil des EuGH hinaus und provoziert massenhaft Rechtsstreitigkeiten, was bei richtiger Umsetzung der EuGH-Entscheidung vermeidbar gewesen wäre. Die Folgen dieser Entscheidung sind weitreichend. Schließlich entsteht Kontrollverlust nicht nur bei Datenlecks infolge schlechter Voreinstellungen zum Nutzerdatenschutz wie bei Facebook im Fall des BGH. Auch jede Eingabe personenbezogener Daten in ein autonom datenverarbeitendes KI-System wie ChatGPT kann einen Kontrollverlust und damit nach der BGH-Rechtsprechung einen Schaden darstellen. Denn über die Datenverarbeitung in autonomen Systemen ist jede Kontrolle technisch ausgeschlossen. Vor dem EuGH ist allerdings bereits ein neues Verfahren zum Kontrollverlust als Schaden anhängig, das eine Nachschärfung durch den BGH veranlassen könnte.[21]

Auch Datenschutzaufsichtsbehörden standen 2024 in der Kritik; etwa der Europäische Datenschutzausschuss (EDSA) bei der Bewertung des Modells „Pay-or-Consent". Dieses Zahlen mit Daten entspricht nach der Rechtsprechung des EuGH grundsätzlich dem Prinzip unternehmerischer Privatautonomie: Niemand kann gezwungen werden, seine Dienstleistungen oder Waren kostenlos anzubieten. Wenn Anbieter entweder Zahlung oder die Gestattung der Datenverarbeitung zu Zwecken der verhaltensbasierten Onlinewerbung verlangen, erhält der Betroffene eine zusätzliche Option zur sonst einzigen Möglichkeit der Bezahlung in monetärer Form. Das ist nach der sog. „Meta-Entscheidung" des EuGH aus dem Jahr 2023 rechtmäßig, solange das verlangte Entgelt der Höhe nach angemessen ist.[22] Beim EuGH ging es darum, ob die von Facebook durchgeführten kommerziellen Verarbeitungen von Nutzerdaten im Zusammenhang mit dem Nutzungsvertrag von Facebook gestattet sind. Anstatt diese Entscheidung zu vollziehen, machte der EDSA einen eigenen Vorschlag.[23] Die Vertragslösung des EuGH wurde ignoriert. Stattdessen schwenkte die Behörde auf die Einwilligung zur Datenverarbeitung um. Diese sei nicht freiwillig. Der EDSA muss als Verwaltungsverbund der europäischen Datenschutzbehörden mit entscheidungsleitender Wirkung gegenüber den unabhängigen Behörden in den Mitgliedstaaten im Rahmen der Rechtsprechung des EuGH für einen einheitlichen Vollzug der DS-GVO sorgen. Ein eigener behördlicher Vorschlag primär vor dem Hintergrund, dass über das Merkmal der Freiwilligkeit der Einwilligung Einfluss auf gesellschaftspolitische Entwicklungen genommen wird, ist im gewaltenteilenden System übergriffig. Hilfreich erscheint hingegen die im Dezember veröffentlichte Stellungnahme

12 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO). Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 03.05.2024, abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf.

13 Hennemann, Ein Datengesetzbuch für alles v. 12.12.2024, abrufbar unter: https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ein-datengesetzbuch-fuer-alles.

14 Deutsche Welle, Pressebericht v. 01.02.2009, abrufbar unter https://www.dw.com/de/gabriel-umweltgesetzbuch-gescheitert/a-3994088?.

15 Schwartmann/Jacquemain in HK DS-GVO/BDSG, Art. 1 Abs. 3 Rn. 14.

16 Kugelmann in HK DS-GVO/BDSG, Art. 51 Abs. 1 Rn. 19 ff.

17 BGH, Urt. v. 18.11.2024 – VI ZR 10/24 Rn. 30 ff.

18 EuGH, Urt. v. 14.12.2023 – C-456/22 Rn. 22.

19 EuGH, Urt. v. 25.01.2024 – C-687/21 Rn. 67 f.

20 BGH, Urt. v. 18.11.2024 – VI ZR 10/24 Rn. 30 f.

21 RS C-526/24 auf Grundlage eines Vorabentscheidungsersuchens des AG Arnsberg vom 31.07.2024.

22 EuGH, Urt. v. 04.07.2023 – C-252/21.

23 EDSA, Stellungnahme 08/2024 zur „Wirksamkeit von Einwilligungen im Kontext von „Consent or Pay"-Modellen großer Online- Plattformen", abrufbar unter https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_de.pdf.

des EDSA, die Klarheit bei der praxisrelevanten Frage schafft, ob personenbezogene Daten während des Trainings eines KI-Sprachmodells anonymisiert werden oder ob sie nach Abschluss des Trainings in den Parametern des Modells fortleben.[24] Der Datenschutz lebt von einer maßvollen Auslegung der DS-GVO. Man muss auf kluge Behörden- und Gerichtsentscheidungen zu dessen Umsetzung bauen. Die deutschen Datenschutzaufsichtsbehörden leisten dazu das ihnen Mögliche. Auch die im Dezember 2024 veröffentliche Agenda der BfDI hilft, weil sie Positionen erkennbar macht, auf die man sich einstellen kann.[25] An den erreichten Zielen kann man die Behörde künftig messen.

III. Künstliche Intelligenz braucht Kompetenz

Generative KI im Sinne der am 1. August 2024 in Kraft getretenen KI-VO hat das Potenzial, die europäische Wirtschaft zu revolutionieren. Europa ist auf Fortschritt und einen verlässlichen Rahmen für Innovation angewiesen. Fortschrittsoptimismus ist selbst dann alternativlos, wenn die Technik sich dahin entwickelt, dass man sich vor ihr in Acht nehmen muss. Das ist bei generativer KI der Fall, denn es geht um autonome und deshalb unbeherrschbare Technik. Das Werkzeug kann sich ohne menschliches Zutun verändern. Jenseits der Grenzen der KI-VO herrscht Freiheit zum Einsatz von KI, soweit nicht das von der KI-VO unberührte und unabhängig davon geltende sonstige Recht – etwa das Verfassungsrecht, das Datenschutz- oder Urheberrecht, das Arbeitsrecht, das Bildungsrecht etc. – Grenzen setzt. Die KI-VO muss beweisen, ob sie sich zum Goldstandard der verantwortungsvollen Ermöglichung eines Fortschritts entwickelt, der die Menschenrechte und die demokratischen und rechtsstaatlichen Errungenschaften Europas stärkt. Sie will vertrauenswürdige KI ohne schädliche Auswirkungen in der Union fördern und entsprechende Innovationen unterstützen. Offen bleiben etwa Fragen danach, wo die Grenzen des autonom agierenden KI-Arztes verlaufen und wie weit der Rat des Kollegen Chatbot gehen darf, wenn es um Personalentscheidungen im Betrieb oder um die Benotung von Schülern geht und ob Bots am Ende gar Tipps für faire Gerichtsurteile geben dürfen. Die ersten Pflichten der KI-VO gelten ab Februar 2025.[26] Konkret muss dann jeder, insbesondere jedes Unternehmen und jede Behörde, bei der eigenverantwortlichen Verwendung, sprich beim Betrieb eines KI-Systems, der nicht ausschließlich zu privaten Zwecken erfolgt, KI-Kompetenz vermitteln.[27] Die neue Bundesregierung muss zügig Recht zur Durchführung der KI-VO schaffen und dabei verantwortungsvoll auf dem schmalen Grat zwischen KI-Euphorie und Überregulierung balancieren. Es wäre schlimm, wenn Deutschland auf den rasenden Zug der KI nicht aufspränge, aber es wäre noch schlimmer, wenn wir auf dem Zug dessen Bremse nicht fänden.

IV. Die Demokratie braucht Schutz

Die Demokratie in Europa ist erheblichen Gefahren ausgesetzt. In Rumänien annullierte das Verfassungsgericht Anfang Dezember 2024 die Präsidentschaftswahl, weil nach Informationen des Geheimdienstes tausende zuvor inaktive TikTok-Konten im Zuge eines „aggressiven hybriden russischen Angriffs" Propaganda für einen rechtsextremen Kandidaten gemacht hatten.[28] Dass die Annullierung der Wahl ihrerseits den Anforderungen des hiesigen Wahlprüfungsrechts entsprechen würde, kann man bezweifeln. Trotzdem ist das Problem der Demokratiegefährdung mit den Mitteln der Digitalisierung virulent. Es wurde in Deutschland 2024 mit Blick auf die Gefahren durch KI thematisiert. Open AI, der Entwickler von ChatGPT teilte schon im Frühjahr mit, fünf Desinformations-Kampagnen staatlich unterstützter Akteure gestoppt zu haben.[29] Die Bevölkerung ist also Fälschungen von Fotos, Videos und Tonaufnahmen per KI ausgeliefert. Sie sind oft satirisch gemeint und werden teilweise auch entsprechend gekennzeichnet. Es gibt aber auch ein gefälschtes Video von Kanzler Scholz, dessen „Urheber" sich unter Berufung auf die Kunstfreiheit einer Kenntlichmachung als Fälschung verwahrte.[30] Das Landgericht Berlin II untersagte es wegen einer Verletzung des Namensrechts des Noch-Kanzlers.[31]

Es gab 2024 auch Stimmen, etwa der Friedrich-Naumann-Stiftung, die Beispiele für den Einsatz von KI zur Stärkung der Demokratie benannte, etwa durch die Stärkung der Barrierefreiheit mittels eines Avatars für Gebärdensprache.[32] Darauf, dass KI die demokratische Willensbildung des Volkes beeinträchtigen kann, wies AlgorithmWatch hin. Die Organisation hatte mit Blick auf die Wahlen zum EU-Parlament im Juni 2024 den Output von Sprachmodellen untersucht. Sie bemängelte, dass Anbieter von KI-Bildgeneratoren es offenbar nicht verhindern konnten, dass ihre Systeme Bilder von realen EU-Parlamentskandidaten hervorbringen und so den Wettbewerb verzerren.[33] Der Onlinemedienexperte Felix Beilharz berichtete zum Thema Demokratie und KI bei LinkedIn über einen selbst durchgeführten Versuch.[34] Er hat die wichtigsten Sprachbots um ChatGPT & Co. mit den 38 Fragen des Wahl-O-Mats gefüttert. Die Antworten sollten jeweils mit "Stimme zu", "Neutral" oder "stimme nicht zu", basierend auf dem Verständnis der politischen und gesellschaftlichen Welt des Bots gegeben werden. Das Ergebnis: Gesamtsieger waren Die Grünen. CDU/CSU und FDP lagen durchgehend (fast) ganz hinten. Ganz hinten liegt bei allen Chatbots die AfD. Wer auf KI-Positionen vertraut und diese als Wahlempfehlung

24 EDSA, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, abrufbar unter https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

25 BfDI, Datenschutzpolitische Agenda für die 21. Wahlperiode des Deutschen Bundestages vom 17.12.2024, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Datenschutzpolitische-Agenda/Datenschutzpolitische-Agenda-21-WP.pdf?__blob=publicationFile&v=6.

26 Art. 113 UAbs. 3 lit. a) KI-VO.

27 Schwartmann/Köhler in Schwartmann/Keber/Zenner, KI-VO, 2. Teil 1. Kap. Rn. 55 ff.

28 The Constitutional Court of Romania, Pressemitteilung des rumänischen Verfassungsgerichts v. 06.12.2024, abrufbar unter https://www.ccr.ro/en/press-release-6-dec/.

29 Reuters, Pressebericht v. 30.05.2024, abrufbar unter https://www.reuters.com/technology/cybersecurity/openai-has-stopped-five-attempts-misuse-its-ai-deceptive-activity-2024-05-30/?utm_.

30 ZDF heute, Pressebericht v. 27.11.2023, abrufbar unter https://www.zdf.de/nachrichten/politik/aktion-gefaengnis-afd-verbot-100.html?utm.

31 LG Berlin II Beschl. v. 13.02.2024 – 15 O 579/23.

32 Friedrich-Naumann-Stiftung, Gutachten v. 27.05.2024, abrufbar unter: https://www.freiheit.org/de/demokratie-und-ki-wie-technologischer-fortschritt-unsere-demokratie-staerken-kann?utm.

33 AlgorithmWatch, Bericht zur Beeinträchtigung der demokratischen Willensbildung durch KI vom 29.05.2024, abrufbar unter https://algorithmwatch.org/de/openai-bricht-eigene-regeln-generatoren-produzieren-tauschende-ki-bilder-zur-eu-wahl/?utm.

34 Vgl. https://felixbeilharz.de/europawahl-analyse-ki/?utm.

übernimmt, hat der autonomen Technik auf Basis von Verzerrungen, die ausländische Datenpools hervorbringen, seinen Anteil an der Staatswillensbildung übertragen.

2024 gab es auch eine kontroverse Debatte darüber, ob es vom Auftrag zur Öffentlichkeitsarbeit der Regierung umfasst ist, dass die Aktentasche des Bundeskanzlers bei TikTok eine Karriere als „Politikinfluencer" machen darf.[35] Das ist nicht nur deshalb interessant, weil die BfDI ein Verfahren vor dem Verwaltungsgericht Köln gegen die Bundesregierung führt, das ihr Amtsvorgänger angestoßen hat.[36] Es geht um das Verbot der Facebook-Fanpage des Bundespresseamts. Rechtlich streitet man im Kern insbesondere darüber, ob das Bundespresseamt eine Rechtsgrundlage nach der DS-GVO für die im Zuge des Betriebs der Fanpage erforderliche Übermittlung personenbezogener Daten an Meta benennen kann.[37] Die Regierung klagt gegen das Verbot ihrer Facebook-Fanpage als zentrale Kommunikationsplattform. Die BfDI erwartet von der nächsten Bundesregierung zumindest im selben Umfang Kommunikation auf datenschutzfreundlichen Diensten wie Mastodon, wie auf den werbefinanzierten Diensten von Meta & Co. Das klingt nicht nach einem Facebook-Verbot. Vielleicht nimmt sie es ja zurück und die Klage erledigt sich.

Facebook ist unstreitig ein Dienst aus den USA. Das zentrale Medium der Jugend ist aber TikTok, und dieser Dienst stammt aus China. Hier wird befürchtet, dass Peking nicht nur Einfluss auf die angezeigten Inhalte nimmt, sondern dass chinesische Behörden zudem auf die Daten des Bundeskanzlers zugreifen. Wie löst man so ein Problem? In den USA sollte TikTok ab dem 19. Januar verboten werden, wenn der chinesische Eigentümer sein USA-Geschäft nicht bis dahin verkauft hätte. Einen Tag später wurde Donald Trump Präsident. Ihm hat der Dienst Erfolge bei jungen Wählern beschert. Deshalb hat er sich bereits vor seiner Ernennung am 20. Januar gegen das Verbot stark gemacht und den Obersten Gerichtshof um die Aussetzung des Verbotsgesetzes gebeten.[38] Eine derartige Intervention ist aus der Perspektive der Demokratie und der Gewaltenteilung äußerst bedenklich. Die Regierung in Albanien will TikTok ab 2025 für ein Jahr sperren, um die Jugend zu schützen.[39] Damit dürfte sie bei jungen Menschen kaum punkten. 2025 finden in Albanien Parlamentswahlen statt. Die Opposition wirft der Regierung wegen des TikTok-Verbots Demokratiegefährdung und Machtmissbrauch vor.

In Brüssel hat die Kommission der EU im Dezember ein Verfahren gegen TikTok eingeleitet, um unter anderem zu prüfen, ob russische Einflussnahme auf der Plattform zu einer Verzerrung der Wahlergebnisse in Rumänien führte.[40] In Deutschland hat die Bundesnetzagentur 2024 ihre Aufgabe als Digital Services Coordinator (DSC) aufgenommen. Er überwacht die Einhaltung der Vorgaben des DSA. Die Lösung der Probleme scheint zu voraussetzungsvoll für unseren aktuellen rechtlichen Ansatz. Am Ende gilt das Böckenförde-Diktum: „Der freiheitliche, säkularisierte Staat lebt von Voraussetzungen, die er selbst nicht garantieren kann".[41]

Zudem passt vieles nicht zusammen. Die Bildungspolitik etwa diskutiert auf der einen Seite Handy- und Social-Media-Verbote an Schulen.[42] Zugleich führt sie ohne erkennbare Grundrechtefolgenabschätzung autonome KI-Systeme in Schulen und Hochschulen ein. Dabei ist die Verwendung generativer KI potenziell hochriskant und sie verlangt weit mehr Kompetenz von Lehrern und Schülern als ein Soziales Netzwerk. Die Lernkurve ist gigantisch, auch wenn man sie gar nicht erkennt.

V. Die Freiheit braucht Daten für die Sicherheit

Auch die Sicherheit durch Daten war 2024 im Fokus. Im Oktober scheiterte im Bundesrat das sogenannte Sicherheitspaket der Ampelkoalition in wesentlichen Teilen.[43] Die Länderkammer monierte zu viel und nicht zu wenig Datenschutz. Nun muss sich die neue Bundesregierung mit dem Ausgleich der Bürgerrechte auf Schutz der Privatsphäre auf der einen Seite und der Sicherheit der Menschen zur Wahrung ihrer Freiheit auf der anderen Seite befassen. Es geht beim Thema „Daten für die Sicherheit zum Schutz der Freiheit" konkret um eine Datenspeicherung auf Vorrat zur Bekämpfung schwerer Verbrechen in engen Grenzen. Der EuGH lässt das zu.[44] Das Bundesverfassungsgericht (BVerfG) hat sich im Oktober 2024 in der sogenannten BKAG II-Entscheidung mit einem Detail, nämlich der vorsorgenden Speicherung der von Sicherheitsbehörden erhobenen Daten befasst.[45] Diese ist nun an noch strengere Voraussetzungen geknüpft als nach der BKAG I-Entscheidung aus dem Jahr 2016.[46]

Zugleich wird der politische Wille immer deutlicher, vorhandene Datenpotenziale für mehr Sicherheit zu nutzen. So hat sich die Bundesregierung Ende 2024 für eine Neuauflage der Vorratsdatenspeicherung ausgesprochen und hält am sogenannten Sicherheitspaket fest.[47] Die Diskrepanz zwischen politischem Willen und Rechtsprechung des BVerfG scheint also zu wachsen. Möglicherweise könnte der Graben überwunden und das Verlangen nach immer umfassenderen Überwachungstechnologien verringert werden, wenn die strenge Linie bei der einfachen Weiterverarbeitung personenbezogener Daten gelockert und vorhandene Daten-

35 Bundeskanzler, Pressemitteilung v. 08.05.2024, abrufbar unter https://www.bundeskanzler.de/bk-de/aktuelles/-teambundeskanzler-auf-tiktok-2269038?utm.

36 BfDI, Dürfen Bundesbehörden Facebook-Fanpages betreiben?, abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/FacebookFanpages.html#:~:text=Bis%20heute%20ist%20ein%20datenschutzkonformer,Informationsfreiheit%20(%20BfDI%20)%20nicht%20m%C3%B6glich.

37 Https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telemedien/Facebook-Fanpages.html

38 Deutschlandfunk, Pressebericht v. 29.12.2024, abrufbar unter https://www.deutschlandfunk.de/trump-bittet-obersten-gerichtshof-um-aussetzung-von-auflage-gegen-tiktok-100.html.

39 Tagesschau, Pressebericht v. 21.12.2024, abrufbar unter https://www.tagesschau.de/ausland/europa/albanien-tiktok-verbot-100.html.

40 Tagesschau, Pressebericht v. 17.12.2024, abrufbar unter https://www.tagesschau.de/ausland/europa/eu-verfahren-tiktok-102.html.

41 Böckenförde, Die Entstehung des Staates als Vorgang der Säkularisation, abrufbar unter https://homepage.univie.ac.at/henning.schluss/seminare/035-Paed-und-Rel/boecken/Boeckenfoerde.PDF.

42 News4teachers, Pressebericht vom 13.12.2024, abrufbar unter https://www.news4teachers.de/2024/12/kultusminister-beraten-ueber-generelles-handy-verbot-an-schulen-gew-haelt-dagegen-wer-soll-das-kontrollieren/?utm.

43 LTO, Pressebericht v. 18.10.2024, abrufbar unter https://www.lto.de/recht/nachrichten/n/bundestag-verabschiedet-sicherheitspaket-der-ampel-koalition?utm.

44 EuGH, Urt. v. 30.04.2024 – C-470/21.

45 BVerfG, Urt. v. 01.10.2024 – 1 BvR 1160/19.

46 BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09.

47 Heise online, Pressebericht v. 30.12.2024, abrufbar unter https://www.heise.de/news/Nach-Magdeburg-Bundesregierung-will-Vorratsdatenspeicherung-10222129.html.

bestände dadurch der effizienten Nutzung durch die Sicherheitsbehörden zugänglich gemacht würden. Ein Staat, der nicht alle rechtskonformen Möglichkeiten der Digitalisierung ausschöpft, damit seine Bürger frei und sicher leben, handelt verantwortungslos. Wenn die neue Bundesregierung das nächste Gesetz über „Daten für die Sicherheit" erlässt, wird es vermutlich wieder in Karlsruhe landen. Dort muss eine grundsätzliche Lösung zur Befriedung des für Bürger und Staat fundamentalen Spannungsfeldes von Freiheit und Sicherheit gefunden werden. Das gilt insbesondere vor dem Hintergrund, dass Anwendungen autonomer KI im Sinne der KI-VO etwa für staatliche und polizeiliche Zwecke in Karlsruhe erst noch verfassungsrechtlich eingeordnet werden müssen.

VI. Fazit: Die Digitalpolitik braucht einen neuen Anfang

Es liegen viele große Steine auf dem Weg der künftigen Bundesregierung. Nun kann sie daraus frei nach Goethe etwas Schönes bauen. Einen kleinen Wunsch kann sie vielleicht gleich zu Beginn der Amtszeit erfüllen. Wer einen neuen Personalausweis bekommt, der kann dessen Online-Ausweisfunktion erst nutzen, wenn er diese freigeschaltet hat. Das ist vielen zu kompliziert. Vielleicht kann man das ändern und der Ausweis wird schon freigeschaltet ausgeliefert. Digitalisierung und Entbürokratisierung bekämen dann einen kleinen Schub. Das wäre kein Game-Changer, aber ein guter Vorsatz für ein gesundes und erfolgreiches 2025 als erstem Jahr einer neuen digitalen Dekade mit Daten für Freiheit, Sicherheit und Wohlstand.

Prof. Dr. Rolf Schwartmann
ist Leiter der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln und Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

Dr. Oliver Daum

DS-GVO und immaterieller Schadenersatz in der Praxis

Deutsche Gerichte und der Europäische Gerichtshof ("EuGH") haben in den vergangenen Monaten verschiedene Entscheidungen zum immateriellen Schadenersatz gesprochen. Anlass für die Verfahren gaben Unklarheiten zu den Voraussetzungen und Rechtsfolgen des Art. 82 DS-GVO, in dem der Anspruch auf Schadenersatz normiert ist. In den Entscheidungen wurden verschiedene Aspekte adressiert, die erhebliche Auswirkungen auf die Praxis haben.

So ging der EuGH auf Tatbestandseite u.a. auf die Frage ein, ob von einem Verstoß gegen die DS-GVO ohne Weiteres auf einen ersatzfähigen Schaden geschlossen werden könnte. Diesen Standpunkt vertrat beispielsweise noch das Bundesarbeitsgericht im Jahr 2021.[1] Andererseits ist im Hinblick auf die Rechtsfolgenseite zunächst festzuhalten, dass ein Verstoß gegen den Datenschutz in der Regel zu emotionalen oder psychischen Belastungen beim Betroffenen führt und nur in den seltenen Fällen zu finanziellen Verlusten. Deshalb begründen Datenschutzverstöße in der Praxis häufig einen immateriellen Schadenersatz,[2] der – anders als materielle Schäden – nicht bezifferbar ist. Für Anspruchsteller und -gegner bedeutet das wiederum, dass eine erhöhte Sorgfalt bei der Bearbeitung der Schadensberechnung auf Rechtsfolgenseite anzuwenden ist. Daher wurden die einschlägigen Ausführungen des EuGH und die der deutschen Gerichte speziell zur Schadenshöhe von Datenschutzrechtlern auch mit Spannung erwartet.

Vor diesem Hintergrund wird die Rechtsprechung des EuGH mit dem Fokus auf den immateriellen Schadenersatz gemäß DS-GVO seit dem Urteil in der Rechtssache "Österreichische Post" vom 4. Mai 2023 nachgezeichnet. Erfasst werden auch die Urteile der Verfahren "Ummendorf" und "NAP" (jeweils vom 14.12.2023), das Verfahren "MDK Nordrhein" (21.12.2023), "MediaMarkt-Saturn" (25.01.2024), "Juris" (11.04.2024) sowie die Verfahren "Dt. Steuerkanzlei" und "Scalable Capital" (jeweils vom 20.6.2024) sowie "Bulg. Handelsregister" (04.10.2024). Es werden die Tatbestandsvoraussetzungen des immateriellen Schadenersatzes gem. Art. 82 DS-GVO nach dem EuGH dargestellt und erläutert. Zudem werden die entwickelten Leitlinien des Gerichtshofes zur Bestimmung der Schadenshöhe herausgearbeitet.

Ergänzt werden die Ausführungen zur Rechtsprechung des EuGH durch einschlägige aktuelle Entscheidungen deutscher Gerichte. Hervorzuheben ist in diesem Zusammenhang das sog. Facebook-Scraping-Urteil des BGH vom 18. November 2024, das im Rahmen der neuen Leitentscheidungsverfahren gem. § 552b ZPO ergangen ist. Darüber hinaus gibt der Beitrag einen kennzeichnenden Querschnitt vorrangig der oberlandesgerichtlichen Judikatur, die zum immateriellen Schadenersatz und dabei insbesondere zu Scraping-Fällen ergangen ist. Wie aufgezeigt wird, argumentiert der EuGH Betroffenen-freundlich dahingehend,[3] dass dem immateriellen Schadenersatz ein weites Anwendungsfeld gegeben ist. Diese weite Rechtsprechung des europäischen Gerichtshofs hat aufseiten vieler deutscher Oberlandesgerichte, die über die praktischen Folgen der EuGH-Rechtsprechung zu entscheiden hatten, zu der – mutmaßlichen – Sorge geführt, damit potenziellen Masseverfahren Vorschub zu leisten. Es hat daher den Anschein, dass die Gerichte versucht waren, die Auswirkungen der Judikatur des EuGH auf den deutschen Anwendungsbereich abzufedern. Diesem restriktiven Praxisansatz setzte der BGH zumindest punktuell einen vorläufigen Schlusspunkt, indem er u.a. feststellte, dass der bloße Kontrollverlust für sich genommen einen ersatzfähigen Schaden gem. Art. 82 DS-GVO darstellen kann.[4]

Der Beitrag richtet sich primär an praktizierende Richter und Anwälte sowie an weitere Praktiker im Bereich des immateriellen Schadenersatzes gem. Art. 82 DS-GVO. Es werden im Rahmen der Erläuterungen der Tatbestandsmerkmale relevante Praxishinweise gegeben, in denen die jeweilige Darlegungs- und Beweislast thematisiert wird.

I. Tatbestandsvoraussetzungen nach dem EuGH

In dem Urteil "Österreichische Post" stellte der EuGH zunächst klar, dass der bloße Verstoß gegen die DS-GVO nicht ausreicht, um einen Schadenersatzanspruch gem. Art. 82 Abs. 1 DS-GVO zu begründen.[5] Vielmehr bedarf es u.a. zusätzlich eines eingetretenen Schadens, womit sich der Gerichtshof zum o. g. Urteil des Bundesarbeitsgerichts von 2021 positionierte. Der EuGH stützte sich dabei auf den Wortlaut des Art. 82 Abs. 1 DS-GVO, der zwischen dem Verstoß und dem Schaden unterscheidet.[6] Bestätigung findet diese Schlussfolgerung in ErwG 146 S. 1 DS-GVO, worin ebenfalls zwischen einer (rechtswidrigen) Datenverarbeitung und einem daraus entstandenen Schaden unterschieden wird.[7]

Hieraus folgt, dass zum Ersatz des immateriellen Schadens gem. Art. 82 DS-GVO drei Voraussetzungen erfüllt sein müssen. Die Voraussetzungen sind: 1.) ein Verstoß gegen die DS-GVO, 2.) ein eingetretener Schaden und 3.) ein Kausalzusammenhang zwischen Schaden und Verstoß.[8] Alle drei Voraussetzungen müssen kumulativ vorliegen.

In dem Urteil "Ummendorf" bestätigte der EuGH die Trias der Tatbestandsvoraussetzungen und ergänzte diese um ein Verschuldenselement. Nach Ansicht des Gerichtshofs wird das Verschulden vermutet, wobei der Verantwortliche die Möglichkeit hat, nachzuweisen, "dass die Handlung, die den Schaden

1 BAG, Beschl. v. 26.08.2021, Az: 8 AZR 253/20 (A), BeckRS 2021, 29622, Rn. 33.
2 Paal/Aliprandi, ZD 2021, 242; Singraven/Bissels, ArbRAktuell 2024, 242.
3 Schmidt, ZD 2024, 318.
4 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24.
5 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 42.
6 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 33.
7 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 37.
8 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 32.

verursacht hat, ihm nicht zurechenbar ist".[9] Im Kern begründet der EuGH das vermutete Verschulden mit einer kombinierten Analyse des Schadenersatzanspruchs gem. Art. 82 Abs. 1 und 2 DS-GVO und der Regelung des Art. 82 Abs. 3 DS-GVO.[10]

Damit ergeben sich für den Ersatz des immateriellen Schadens gem. Art. 82 DS-GVO die folgenden vier Tatbestandsvoraussetzungen: 1.) Verstoß gegen die DS-GVO, 2.) vermutetes Verschulden, 3.) Schaden und 4.) Kausalzusammenhang zwischen Schaden und Verstoß. Diese Voraussetzungen werden in diesem Beitrag daher auch nachfolgend herausgestellt und erläutert.

II. "Negative Folgen" als Tatbestandsvoraussetzung?

Ungeachtet der zuvor skizzierten Rechtsprechung des EuGH zu den vier Voraussetzungen des Art. 82 DS-GVO zeigte sich die kurzzeitige Tendenz, die "negativen Folgen" als weitere eigenständige Tatbestandsvoraussetzung vorzusehen. Ein Ausgangspunkt hierfür war ein Urteil des OLG München vom 24. April 2024, mit dem ein Verantwortlichen-freundlicher Weg gewählt wurde. In dem Urteil setzte das OLG München zur Begründung eines immateriellen Schadenersatzes nach einem Scraping-Vorfall die negative Folge als weiteres Tatbestandsmerkmal wie folgt voraus: "Dreistufigkeit der Prüfung (Verstoß gegen DS-GVO -> negative Folge, z.B. Kontrollverlust -> Schaden)".[11] Damit forderte das OLG München im Ergebnis aber mehr als der EuGH.

Dass der EuGH die negativen Folgen nicht als ausdrückliches Tatbestandsmerkmal genannt hatte, als er die Voraussetzungen des immateriellen Schadenersatzes aufzählte, sprach bereits gegen die Ansicht des OLG München. Vielmehr hat der EuGH die negativen Folgen ausdrücklich als Schaden erfasst.[12] Im Verfahren "Bulg. Handelsregister" vom 4. Oktober 2024 hat der EuGH überdies klargestellt, dass Betroffene keine negativen Folgen nachzuweisen hätten, um einen Schaden gem. Art. 82 DS-GVO zu begründen.[13] Dieser Ansicht schloss sich dann auch der BGH im Scraping-Urteil an.[14]

Damit ist festzuhalten, dass die Ansicht des OLG München, und die einiger kommentierender Praktiker, die negativen Folgen als eigenständige Tatbestandsvoraussetzung neben dem Verstoß und dem Schaden zu verstehen, abzulehnen ist. In den folgenden Ausführungen werden die negativen Folgen daher nicht als eigenes Tatbestandsmerkmal behandelt.

III. Die Voraussetzungen des immateriellen Schadenersatzes

Nachfolgend werden die einzelnen Voraussetzungen des immateriellen Schadenersatzes gem. Art. 82 DS-GVO thematisiert. Dazu wird das jeweilige Tatbestandsmerkmal inhaltlich bestimmt und anschließend mit einem Praxishinweis versehen.

1. Verstoß gegen die DS-GVO

Die erste Voraussetzung des immateriellen Schadenersatzes bildet der Verstoß gegen die DS-GVO gem. Art. 82 Abs. 1 DS-GVO. In den gegenständlichen Urteilen hatte sich der EuGH hierzu wie folgt geäußert:

a) Inhalt "Verstoß gegen die DS-GVO"

In dem Urteil "Dt. Steuerberaterkanzlei" hatte sich der EuGH u.a. mit der Frage zu befassen, ob ein Verstoß nur gegen die DS-GVO den immateriellen Schadenersatz auslösen kann oder ob auch ein Verstoß gegen andere Normen in Frage kommt. Nach dem Wortlaut des Art. 82 Abs. 1 DS-GVO wird ein "Verstoß gegen diese Verordnung" vorausgesetzt.

Zur Beantwortung nimmt der EuGH Bezug auf den ErwG 146 S. 5 DS-GVO. Demnach können auch Verstöße gegen "nach Maßgabe der vorliegenden Verordnung erlassene delegierte Rechtsakte und Durchführungsrechtsakte und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung" einen immateriellen Schadenersatz begründen.[15] Die genannten Anforderungen erfüllen jedoch diejenigen Normen nicht, die zwar auf den Datenschutz gerichtet sind, aber nicht bezwecken, die DS-GVO zu präzisieren. Dies dürfte z.B. bei Datenschutznormen einschlägig sein, die vor dem Inkrafttreten der DS-GVO erlassen wurden. In der Praxis sollten also die Normen, gegen die verstoßen worden sein soll, und die keine Regelung der DS-GVO sind, auf Ihre Tauglichkeit bzw. Präzisierung der DS-GVO hin überprüft werden.

Im Verfahren "NAP" hatte der Gerichtshof konkret zu klären, ob eine unbefugte Offenlegung oder die Verschaffung eines unbefugten Zugangs zu personenbezogenen Daten durch Dritte ausreicht, um anzunehmen, dass die technischen und organisatorischen Maßnahmen ("TOM") gem. Art. 24 und Art. 32 DS-GVO nicht geeignet waren. In der Konsequenz hätte dies einen Verstoß gegen die DS-GVO begründet. Den Hintergrund des Verfahrens bildete ein erfolgreicher Hackerangriff gegen die IT-Infrastruktur der bulgarischen Agentur für Einnahmen (= NAP), woraufhin personenbezogene Daten im Internet veröffentlicht wurden.

Der EuGH führte hierzu aus, dass der Verantwortliche gem. Art. 24 und Art. 32 DS-GVO jede Verletzung des Schutzes personenbezogener Daten "so weit wie möglich verhindern" soll.[16] Ob die ergriffenen TOM ungeeignet waren, und damit ein Verstoß gegen die DS-GVO vorliegt, ist eine Frage des Einzelfalls. Ein erfolgreicher Cyberangriff macht die ergriffenen TOM nicht per se ungeeignet. Daher kann mit dem EuGH nicht geschlussfolgert werden, dass allein die unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch Dritte ausreicht, um einen Verstoß gegen die DS-GVO zu begründen.[17]

Zum gleichen Ergebnis gelangte der Gerichtshof im Urteil "MediaMarktSaturn". Der EuGH hatte die Vorlagefrage zu beantworten, ob die vom Verantwortlichen ergriffenen TOM ungeeignet waren, weil ein Mitarbeiter des Verantwortlichen irrtümlich ein Dokument mit personenbezogenen Daten an einen unbefugten Dritten herausgegeben hatte. Der EuGH ver-

9 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 103; Gola/Piltz, in: Gola/Heckmann, DS-GVO/BDSG – Kommentar, 3. Aufl. 2022, Art. 82, Rn. 24.

10 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 93 f; siehe auch EuGH, Urt. v. 04.10.2024, Az: C-200/23, Rn. 161.

11 OLG München, Urt. v. 24.04.2024, Az: 34 U 2306/23 e, GRUR-RS 2024, 8563, Rn. 24.

12 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 50; EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 82; EuGH, Urt. v. 20.06.2024, Az: C-590/22, Rn. 36.

13 EuGH, Urt. v. 04.10.2024, Az: C-200/23, Rn. 148, 156.

14 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24, Rn. 30, 33.

15 EuGH, Urt. v. 20.06.2024, Az: C-590/22, Rn. 47.

16 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 30.

17 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 39; a.A. OLG Karlsruhe, Urt. v. 07.11.2023, Az: 19 U 23/23, ZD 2024, 406, Rn. 31.

neinte diese pauschale Schlussfolgerung mit der Begründung, dass ein nationales Gericht nicht nur den Umstand der irrtümlichen Herausgabe der personenbezogenen Daten heranziehen hat, sondern sämtliche Beweise, um die Geeignetheit der TOM gem. Art. 24 und Art. 32 DS-GVO zu überprüfen.[18]

b) Praxishinweise

Hinsichtlich der Darlegungs- und Beweislast für das Vorliegen des Verstoßes gegen den Datenschutz hat der EuGH festgelegt, dass "die Ausgestaltung von Klageverfahren, die den Schutz der dem Einzelnen aus Art. 82 DS-GVO erwachsenden Rechte gewährleisten sollen, und insbesondere die Regeln für die Beweismittel" Aufgabe der innerstaatlichen Rechtsordnung ist.[19] Nach den allgemeinen zivilprozessualen Grundsätzen der deutschen Rechtsordnung liegt die Darlegungs- und Beweislast beim Anspruchsteller, der seine den Anspruch begründenden Tatsachen darlegen und ggf. beweisen muss.[20]

Allerdings wird in Anbetracht der Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO des Verantwortlichen diskutiert, ob in Hinblick auf den Verstoß ausnahmsweise der Verantwortliche die Beweislast trägt.[21] Diese Auffassung vertrat jedenfalls das OLG Hamm in einem Urt. v. 15.08.2023. Nach Auffassung des OLG Hamm tritt gem. Art. 5 Abs. 2 DS-GVO eine Beweislastumkehr ein, wonach der Verantwortliche für das Nichtvorliegen eines Verstoßes gegen den Datenschutz beweisbelastet ist.[22] Eine belastbare Begründung liefert das OLG Hamm hingegen nicht.

Die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO hat den Zweck, den Art. 58 Abs. 1 lit. a) DS-GVO zu flankieren. Nach dieser Regelung können die Aufsichtsbehörden den Verantwortlichen auffordern, bestimmte Informationen bereitzustellen. Nach herrschender Meinung handelt es sich bei der Rechenschaftspflicht aber nicht um eine Beweislastregelung der DS-GVO,[23] sondern um eine Regelung eines öffentlich-rechtlichen Verhältnisses zur Aufsichtsbehörde. Die Ansicht des OLG Hamm ist daher abzulehnen.

2. Verschulden

Im Urteil "Österreichische Post" hatte der EuGH das Verschuldenselement nicht als ausdrückliches Tatbestandsmerkmal des immateriellen Schadenersatzes identifiziert. In der deutschen Literatur hat das zwischenzeitlich zu der Ansicht geführt, dass ein Verschulden beim immateriellen Schadenersatz nicht zu fordern sei.[24] Im Urteil "MDK Nordrhein" stellte der EuGH jedoch klar, dass das – vermutete – Verschulden eine weitere Tatbestandsvoraussetzung des immateriellen Schadenersatzes gem. Art. 82 DS-GVO ist.[25]

a) Inhalt "Verschulden"

Vor Verkündung des Urteils in der Rechtssache "MDK Nordrhein" war in der deutschen Rechtsordnung umstritten, ob es sich bei Art. 82 DS-GVO um eine Verschuldenshaftung oder um eine verschuldensunabhängige Gefährdungshaftung handelt.[26] Mit dem MDK-Nordrhein-Urteil des EuGH ist nunmehr entschieden worden, dass es sich beim immateriellen Schadenersatz um eine Verschuldenshaftung handelt. Hinsichtlich der Ersatzpflicht des Verantwortlichen bzw. des Auftragsverarbeiters ist daher zu fordern, dass der Verstoß gegen den Datenschutz entweder vorsätzlich oder fahrlässig begangen wurde.[27]

b) Praxishinweise

Der zivilprozessuale Grundsatz, dass der Anspruchsteller für die anspruchsbegründenden Umstände die Darlegungs- und Beweislast trägt, gilt nicht beim Verschulden des Art. 82 DS-GVO: In dem Urteil "MDK Nordrhein" hatte der Gerichtshof nicht nur das Verschulden des immateriellen Schadenersatzes herausgestellt. Zugleich erklärte er, dass das Verschulden aufseiten des Verantwortlichen bzw. Auftragsverarbeiters zu vermuten ist.[28] Bestätigt hat dies der EuGH im späteren Verfahren "Bulg. Handelsregister".[29] Für die Praxis folgt daraus, dass der Anspruchsteller lediglich das vermutete Verschulden im Sachvortrag darlegen muss. Aber anschließend wäre er nicht beweisbelastet.

3. Immaterieller Schaden

Im Zentrum der gegenständlichen Urteile des EuGH stand indes der Begriff des immateriellen Schadens, der nachfolgend analysiert wird. Die Erläuterungen zu Inhalt und Anwendung in der Praxis werden zudem ergänzt durch einschlägige Urteile aus der deutschen Rechtsprechung.

a) Inhalt "Immaterieller Schaden"

Den Ausgangspunkt der folgenden Ausführungen bildet der Befund, dass der Begriff "immaterieller Schaden" in Art. 82 Abs. 1 DS-GVO nur genannt wird. Eine Definition wird nicht gegeben. Letzteres gilt auch für den ErwG 146 DS-GVO, der speziell den Schadenersatzanspruch gem. Art. 82 Abs. 1 betrifft.[30]

aa) Keine Erheblichkeitsschwelle/Bagatellgrenze

Jedenfalls hat sich der Gerichtshof zu der Frage geäußert, ob der immaterielle Schadenersatz von den nationalen Gerichten erfordert, festzustellen, dass der Schaden einen bestimmten Grad an Erheblichkeit erreicht hat. Konkret ging es im Verfahren "Österreichische Post" um vorübergehende gefühlsmäßige Beeinträchtigungen wie Ärgernis, Vertrauensverlust und ein Gefühl der Bloßstellung[31] und im Verfahren "Ummendorf" um den kurzfristigen Verlust des Betroffenen über die Hoheit seiner personenbezogenen Daten (Kontrollverlust).[32] Der EuGH stellte zusammenfassend fest, dass Art. 82 DS-GVO einer nationalen Regelung entgegensteht, sofern diese für den Ersatz eines immateriellen Schadens eine Erheblichkeitsschwelle

18 EuGH, Urt. v. 25.01.2024, Az: C-687/21, Rn. 45.

19 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 60.

20 Quaas, in: Wolff/Brink, Datenschutzrecht – Kommentar, 2. Aufl. 2022, Art. 82, Rn. 51.

21 Thüsing/Zou, ZD 2024, 4.

22 OLG Hamm, Urt. v. 15.08.2023, Az: 7 U 19/23, GRUR 2023, 1791, Rn. 74 ff.

23 Thüsing/Zou, ZD 2024, 5; i.E. auch OLG Stuttgart, Urt. v. 31.03.2021, Az: 9 U 34/21, Rn. 41; Quaas in: Wolff/Brink, Datenschutzrecht – Kommentar, 2. Aufl. 2022, Art. 82, Rn. 51a.

24 Nemitz, in: Ehmann/Selmayr, DS-GVO – Kommentar, 3. Aufl. 2024, Art. 82, Rn. 23.

25 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 93 f.

26 Vgl. OLG Koblenz, Urt. v. 18.05.2022, Az: 5 U 2141/21, BeckRS 2022, 11126, Rn. 54 ff.; Golland/Kriegesmann, MMR 2023, 734.

27 Gola/Piltz, in: Gola/Heckmann, DS-GVO/BDSG – Kommentar, 3. Aufl. 2022, Art. 82, Rn. 24.

28 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 103.

29 EuGH, Urt. v. 04.10.2024, Az: C-200/23, Rn. 161.

30 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 81.

31 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 12.

32 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 11.

vorsieht[33] bzw. das Überschreiten einer Bagatellgrenze.[34] Zur Begründung führte der Gerichtshof den Wortlaut des Art. 82 DS-GVO sowie den ErwG 146 DS-GVO an, woraus sich jeweils keine Erheblichkeitsschwelle/Bagatellgrenze ergibt.[35] Zudem könnte es aufgrund der Vielzahl und Verschiedenartigkeit der nationalen Gerichte der Mitgliedstaaten zu unvereinbaren Urteilen in der Höhe des Schadens kommen. Dies stünde aber dem Grundsatz der unionsweiten gleichmäßigen und einheitlichen Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten der Betroffenen entgegen.[36]

bb) Befürchtung als Schaden

Bemerkenswert waren die Ausführungen des EuGH zum immateriellen Schadenersatz im Verfahren "NAP", dem bekanntlich ein erfolgreicher Hackerangriff zugrunde lag. Der Gerichtshof hatte die Frage zu beantworten, ob allein die Befürchtung des Anspruchstellers, seine personenbezogenen Daten könnten nach einem Datenschutzverstoß durch Dritte missbräuchlich verwendet werden, einen immateriellen Schaden darstellen kann. Der EuGH bejahte diese Frage.[37] Er argumentierte, dass der Begriff des Schadens weit auszulegen ist und dass ein Ausschluss von Fällen der Befürchtung, dass die personenbezogenen Daten zukünftig missbraucht werden könnten, dieser weiten Auslegung nicht entspricht.[38] Zudem ergibt sich aus ErwG 85 S. 1 DS-GVO, dass insbesondere der bloße Verlust der Kontrolle über die eigenen Daten als Schaden nach der DS-GVO erfasst wurde, selbst wenn keine konkrete missbräuchliche Verwendung der Daten erfolgen sollte.[39]

Diese weite Auslegung des immateriellen Schadensbegriff erfuhr im Verfahren "MediaMarktSaturn" eine Konkretisierung. Wenngleich die Befürchtung einer missbräuchlichen Verwendung der personenbezogenen Daten einen Schaden darstellen kann, reicht ein "rein hypothetisches Risiko der missbräuchlichen Verwendung" nicht aus. Die bloße Möglichkeit also, ohne dass Dritte tatsächlich Kenntnis von den personenbezogenen Daten nehmen, stellt keinen Schaden dar.[40] Das ist z.B. gegeben, wenn ein Mitarbeiter eines Verantwortlichen irrtümlich Vertragsunterlagen eines Kunden an einen anderen Kunden herausgibt und diese Unterlagen nach ca. 30 Minuten zurückgelangen, ohne dass der andere Kunde – nachweislich – Kenntnis von den personenbezogenen Daten nahm.

Zusammenfassend bedeutet das, dass die Befürchtung, es könnte aufgrund eines vorangegangenen Hackerangriffs zu einer missbräuchlichen Verwendung der personenbezogenen Daten durch Dritte kommen, einen Schaden gem. Art. 82 DS-GVO darstellen kann. Ist jedoch ausgeschlossen, dass Dritte Kenntnis von den personenbezogenen Daten genommen haben, liegt nach dem EuGH kein Schaden vor.

cc) Kontrollverlust als Schaden

Von praktischer Bedeutung sind auch die Ausführungen des EuGH und der deutschen Judikatur zum Kontrollverlust als Schaden. In diesem Zusammenhang ist zunächst festzustellen, dass auch der Begriff des Kontrollverlustes nicht definiert ist. Eine Definition ergibt sich weder aus der DS-GVO, den ErwGn oder der Rechtsprechung des EuGH.

Ungeachtet dessen hat der EuGH den Verlust der Kontrolle über die eigenen personenbezogenen Daten als immateriellen Schaden gem. Art. 82 DS-GVO bewertet. Er stellte klar, dass selbst ein kurzzeitiger[41] Kontrollverlust einen Schaden darstellen kann, möge der Kontrollverlust noch "so geringfügig" sein.[42] In diesem Zusammenhang drängt sich unweigerlich die Frage auf, ob die verspätete Erteilung der Auskunft gem. Art. 15 DS-GVO zu einem Kontrollverlust beim Anspruchsteller führt und damit zu einem Schaden. Das Bundesarbeitsgericht hat diese Frage in einem Urt. v. 20.06.2024 jedenfalls verneint.[43]

Insgesamt ist zu beobachten, dass sich die deutschen Gerichte mit der Einordnung des Kontrollverlustes als Schaden – trotz der klaren Rechtsprechung des EuGH – schwertut. Ein Teil der Gerichte scheint diese Schlussfolgerung ohnehin abzulehnen.[44] Ein anderer Teil erkennt den Kontrollverlust zwar als Schaden grundsätzlich an, verneint jedoch im Anschluss dessen Vorliegen aus tatsächlichen Gründen.[45] Diese Uneinheitlichkeit dürfte nunmehr jedoch ein Ende gefunden haben, da der BGH im Scraping-Fall festgestellt hat, dass der Kontrollverlust auch in Deutschland ein Schaden gem. Art. 82 DS-GVO sein kann.[46]

b) Praxishinweise

Genauso wie bei den anderen Tatbestandsmerkmalen – mit Ausnahme des Verschuldens – trägt der Anspruchsteller beim Schaden die Darlegungs- und Beweislast.[47] Dabei ist zu berücksichtigen, dass es für Anspruchsteller (gerade nach den Entscheidungen der deutschen Gerichte) grundsätzlich eine besondere Herausforderung darstellen kann, das Vorliegen eines immateriellen Schadenersatzes darzulegen und zu beweisen.[48]

Der EuGH hat in dieser Hinsicht festgehalten, dass der Anspruchsteller den Nachweis darüber zu erbringen hat, dass ein immaterieller Schaden eingetreten ist.[49] Nur weil es keine Erheblichkeitsschwelle oder Bagatellgrenze gibt, folgt daraus nicht, dass kein Nachweis des Schadens erforderlich wäre. Immerhin führt ein Verstoß gegen die DS-GVO nicht zwangsläufig zu einem Schadenersatz.

aa) Darlegungs- und Beweislast nach dem EuGH

Bei der Darlegungs- und Beweislast bezüglich des Schadens in Form der Befürchtung der missbräuchlichen Verwendung hat der EuGH eine gesonderte Anforderung aufgestellt. Demnach haben die nationalen Gerichte zu prüfen, ob die Befürchtung der missbräuchlichen Verwendung auch "begründet"

33 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 51.

34 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 23.

35 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 45.

36 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 48.

37 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 86; siehe auch BAG, Urt. v. 20.06.2024, Az: 8 AZR 124/23, Rn. 15.

38 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 81.

39 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 82.

40 EuGH, Urt. v. 25.01.2024, Az: C-687/21, Rn. 68; Schneider, CR-online.de Blog 2024, CRBLOG0007609 (6. Gebot); a. A. Wolf, CR 2023, 515, Rn. 22.

41 EuGH, Urt. v. 11.04.2024, Az: C-741-/21, Rn. 42.

42 EuGH, Urt. v. 25.01.2024, Az: C-687/21, Rn. 66.

43 BAG, Urt. v. 20.06.2024, Az: 8 AZR 91/22, NZA 2024, 1496, Rn. 18.

44 OLG Köln, Urt. v. 07.12.2023, Az: 15 U 99/23, ZD 2024, 463, Rn. 36-38; OLG Stuttgart, Urt. v. 22.11.2023, Az: 4 U 20/23, ZD 2024, 60, 1. LS; OLG Hamm, Urt. v. 15.08.2023, Az: 7 U 19/23, GRUR 2023, 1799, Rn. 135, 144; OLG Karlsruhe, Urt. v. 07.11.2023, Az: 19 U 23/23, ZD 2024, 406: "Beunruhigung nach Cyberangriff kein immaterieller Schaden".

45 LAG Rheinland-Pfalz, Urt. v. 08.02.2024, Az: 5 Sa 154/23, BeckRS 2024, 4219, Rn. 25; OLG Bamberg, Urt. v. 11.06.2024, Az: 10 U 58/23 e.

46 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24, Rn. 30, 33.

47 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 84; OLG Bamberg, OLG Bamberg, Urt. v. 11.06.2024, Az: 10 U 58/23 e, 4. LS.

48 Schneider, CR-online.de Blog 2024, CRBLOG0007609.

49 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 50; EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 21; EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 84.

ist. Wie genau die begründete Befürchtung festzustellen ist, erläuterte der EuGH nicht. Lediglich zu den Prüfungskriterien äußerte er sich dahingehend, dass sich die begründete Befürchtung der missbräuchlichen Verwendung der personenbezogenen Daten durch Dritte aus den gegebenen Umständen und hinsichtlich der betroffenen Person ergeben muss.[50] Zudem ergänzte der EuGH im Verfahren "Dt. Steuerkanzlei", dass der Anspruchsteller nicht nachzuweisen habe, dass im Anschluss eines Verstoßes gegen den Datenschutz auch tatsächlich eine Weitergabe an Dritte erfolgte. Nachzuweisen habe der Anspruchsteller die begründete Befürchtung mitsamt bzw. inklusive ihrer negativen Folgen.[51]

bb) Darlegungs- und Beweislast nach der deutschen Rechtsprechung

Nach einem Urteil des OLG Hamm, das in einem Scraping-Fall entschieden hat, ist der Anspruchsteller bezüglich der Darlegungs- und Beweislast des immateriellen Schadens grundsätzlich gehalten, Umstände darzulegen, in denen sich seine erlebten Empfindungen widerspiegeln und dass nach der Lebenserfahrung der Datenschutzverstoß mit seinen Folgen Einfluss auf das subjektive Empfinden hatte. Unzureichend ist ein nicht näher konkretisierter Vortrag – ohne konkret-individuelle Ausführungen des Anspruchstellers – zu den Gefühlen eines Kontrollverlustes, eines Beobachtetwerdens und einer Hilflosigkeit. Denn mit solch einem Sachvortrag würden nicht genügend Beweisanzeichen objektiver Art vorgetragen, in denen sich solche Gefühle konkret widerspiegeln.[52]

Die zuvor genannten Anforderungen des OLG Hamm übernahm das OLG Dresden in einem Urt. v. 23.01.2024 konkret zur Darlegungs- und Beweislast der begründeten Befürchtung als Schaden. Diese Befürchtung muss vom Anspruchsteller gem. § 286 ZPO "hinreichend konkret dargelegt und glaubhaft gemacht" werden, da es sich um innere Tatsachen handelt, die dem Beweis nur eingeschränkt zugänglich sind und auf sie nur mittelbar von äußeren Tatsachen geschlossen werden kann.[53] Zur begründeten Befürchtung wäre u.a. zum Umgang des Anspruchstellers mit seinen Daten vor dem Datenschutzverstoß vorzutragen (z.B. Weitergabe an Dritte) sowie zur Frage, ob eine Veröffentlichung Auswirkungen auf die Lebensführung hatte und welche Konsequenzen der Anspruchsteller aus den Verstoß gezogen hat (z.B. Wechsel der Telefonnummer).

Schließlich reicht nach dem OLG Stuttgart der Vortrag des Anspruchstellers "eine mit dem Verlust der Daten seelisch belastende Ungewissheit über das Schicksal der Daten" sei eingetreten, nicht aus, um die begründete Befürchtung eines Missbrauchs der Daten darzulegen. Allerdings hat das OLG Stuttgart nicht erläutert, wie die begründete Befürchtung eines immateriellen Schadenersatzes darzulegen und zu beweisen ist.[54] Diese Frage blieb offen.

Das BAG hat zur Darlegung und ggf. zum Beweis der begründeten Befürchtung ausgeführt, dass das bloße Berufen auf die Gefühlslage nicht ausreichend ist. Da negative Gefühle objektiv nicht beweisbar sind, bedarf es der tatrichterlichen Beurteilung der "Gesamtsituation und letztlich auch [der] Glaubwürdigkeit der Klagepartei auf der Grundlage eines substanziierten Sachvortrages."[55] Sind diese Voraussetzungen erfüllt, mindert sich das Beweismaß in Bezug auf die Entstehung und der Höhe des Schadens gem. § 287 Abs. 1 ZPO.

Als Zwischenergebnis ist damit festzuhalten, dass die deutschen Gerichte hohe Anforderungen an die Darlegungs- und Beweislast zur begründeten Befürchtung als Schaden stellen. Diese Anforderungen dürfte den Verantwortlichen zupasskommen, die somit die Durchsetzung von Schadenersatzforderungen der Anspruchsteller erschweren können.

Gleichwohl hat der BGH im Scraping-Fall – im Rahmen des Kontrollverlustes – darauf hingewiesen, dass keine "überspannten" Anforderungen an die Darlegungslast beim Anspruchsteller gestellt werden dürfen.[56] Anders als z.B. das OLG Dresden in seinem o. g. Urt. v. 23.01. 2024 hält der BGH den Sachvortrag des Anspruchstellers, die personenbezogenen Daten in der Vergangenheit nur gezielt und ausgewählt weitergegeben zu haben, für ausreichend, um einen Kontrollverlust substanziiert begründen zu können. Zudem ist u.a. der Vortrag des Anspruchstellers, er befinde sich infolge eines Datenschutzverstoßes – hier: Hackerangriff auf Facebook-Accounts – in einem Zustand großen Unwohlseins und in Sorge um den Missbrauch seiner personenbezogenen Daten durch Dritte, substanziiert, um einen Schaden darzulegen.[57] Für Anspruchsteller wiederum bedeuten diese Ausführungen des BGH eine Vereinfachung der Durchsetzung von Schadenersatzansprüchen.

4. Kausalzusammenhang

Eine weitere Voraussetzung für den immateriellen Schadenersatz gem. Art. 82 DS-GVO auf Tatbestandseite ist die Kausalität zwischen Schaden und Verstoß gegen den Datenschutz. Erstattet werden nur solche immateriellen Schäden, die kausal durch einen Datenschutzverstoß verursacht wurden.

a) Inhalt "Kausalzusammenhang"

Dass die Kausalität zwischen Schaden und Datenschutzverstoß eine weitere kumulative Voraussetzung des immateriellen Schadenersatzes gem. Art. 82 DS-GVO bildet, hatte der EuGH erstmalig im Verfahren "Österreichische Post" festgestellt[58] und in den folgenden Entscheidungen weiterhin zugrunde gelegt. Den EuGH-Urteilen lassen sich aber keine Hinweise darauf entnehmen, wie die Kausalität ausgestaltet ist.

Auch in der deutschen Rechtsprechung sind entsprechende Ausführungen selten. Dennoch hat das OLG Hamm in seinem Urt. v. 15.08.2023 die Äquivalenztheorie (conditio-sine-qua-non-Formel) zur Begründung der Kausalität angewendet.[59] Demgegenüber hatte das LG München I im Rahmen des Art. 82 Abs. 1 DS-GVO festgestellt, dass "es bei Einhaltung der als adäquat geltenden Sicherheitsmaßstäbe nicht zu dem konkreten Datenvorfall gekommen wäre."[60] Damit hat sich das Landgericht München I für die Anwendung der Adäquanztheorie entschieden – freilich ohne weitere Begründung.

Dass Kausalitätstheorien zu unterschiedlichen Ergebnissen führen können, und daher praxisrelevant sind, zeigt das folgen-

50 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 85.

51 EuGH, Urt. v. 20.06.2024, Az: C-590/22, Rn. 35 f.

52 OLG Hamm, Urt. v. 15.08.2023, Az: 7 U 19/23, GRUR 2023, 1800, Rn. 151.

53 OLG Dresden, Urt. v. 23.01.2024, Az: 4 U 1313/23; OLG Bamberg, Urt. v. 11.06.2024, Az: 10 U 58/23 e, 4. LS.

54 OLG Stuttgart, Hinweisbeschluss v. 02.02.2024, Az: 2 U 63/22, ZD 2024 399, Rn. 18.

55 BAG, Urt. v. 20.06.2024, Az: 8 AZR 124/23, Rn. 16.

56 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24, Rn. 35, 45.

57 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24, Rn. 39 f.

58 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 32.

59 OLG Hamm, Urt. v. 15.08.2023, Az: 7 U 19/23, GRUR 2023, 1802, Rn. 176.

60 LG München I, Urt. v. 09.12.2021, Az: 31 O 16606/20, ZD 2022, 243, Rn. 36.

de Beispiel: Ein Mitarbeiter eines Verantwortlichen vergisst, ein Sicherheitsupdate zu installieren. Anschließend kommt es zu einem Cyberangriff, in dessen Zuge personenbezogene Daten im Darknet veröffentlicht werden. Nach der Äquivalenztheorie wäre das Unterlassen der Installation des Sicherheitsupdates kausal für die Veröffentlichung im Darknet, da das Unterlassen nicht hinweggedacht werden könnte, ohne dass es zur Veröffentlichung gekommen wäre. Gemäß der Adäquanztheorie ist – zusammengefasst – zu prüfen, ob das Sicherheitsupdate die Veröffentlichung nach der allgemeinen Lebenserfahrung und den Umständen des Einzelfalls verhindert hätte. Wäre dies nicht der Fall, wie es bei gezielten Hackerangriffen oftmals der Fall ist, wäre keine Kausalität gegeben.

Das Beispiel verdeutlicht, dass die Bestimmung der anwendbaren Kausalitätstheorie in der Praxis von erheblicher Relevanz sein kann.

Aus der deutschen Kommentarliteratur ergibt sich, dass die Kausalität des Art. 82 DS-GVO unter Anwendung der Adäquanztheorie zu begründen ist.[61] Demnach hat der Verantwortliche nur solche Schäden zu ersetzten, mit deren Eintritt nach der allgemeinen Lebenserfahrung vernünftigerweise zu rechnen war. Eine völlig außergewöhnliche Verkettung von Umständen, die einen atypischen Kausalverlauf bilden, sind nicht erstattungsfähig. Dieser Ansicht, die Adäquanztheorie im Rahmen des immateriellen Schadenersatzes gem. Art. 82 DS-GVO anzuwenden, ist zu folgen.

b) Praxishinweise

Hinsichtlich der Darlegungs- und Beweislast ergeben sich für die Kausalität keine Ausnahmen vom allgemeinen zivilrechtlichen Grundsatz, wonach der Anspruchsteller die anspruchsbegründenden Umstände darlegen und ggf. beweisen muss. Aus den recherchierten Entscheidungen, die diesem Beitrag zugrunde liegen, ergeben sich keine nennenswerte Praxishinweise. Auch eine diskutierte Beweislastumkehr gilt bei der Kausalität nicht.[62]

5. Regelung des Art. 82 Abs. 3 DS-GVO

Die aus Art. 82 Abs. 3 DS-GVO abzuleitende genaue Regelung ist noch nicht abschließend geklärt. Nach dem Wortlaut des Art. 82 Abs. 3 DS-GVO wird der Verantwortliche bzw. Auftragsverarbeiter von der Haftung befreit, "wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist."

Unklar ist dabei zunächst, ob es sich bei dieser Regelung um eine Möglichkeit der Haftungsbefreiung bzw. "Exkulpationsmöglichkeit"[63] handelt oder um eine Beweislastregelung. Die Rechtsprechung des EuGH ist diesbzgl. uneindeutig. In der Rechtssache "NAP" hat sich der EuGH wie folgt für eine Haftungsbefreiung ausgesprochen: Der Verantwortliche kann sich von der Haftung gem. Art. 82 Abs. 3 DS-GVO befreien, "indem er nachweist, dass es keinen Kausalzusammenhang zwischen der etwaigen Verletzung der Verpflichtung zum Datenschutz [...] und dem entstanden Schaden gibt."[64] Demnach handelt es sich bei der Regelung des Art. 82 Abs. 3 DS-GVO um eine Haftungsbefreiungsmöglichkeit hinsichtlich des Kausalzusammenhangs.

In den Urteilen "MDK Nordrhein", "Juris" und "Bulg. Handelsregister" hat der EuGH den Art. 82 Abs. 3 DS-GVO hingegen als eine Beweislastregelung bezüglich des Verschuldens ausgelegt.[65] Daher ergibt sich aus dieser Regelung, wie bereits oben erörtert, dass das Verschulden des Verantwortlichen im Rahmen des Schadenersatzes nach der DS-GVO zugunsten des Anspruchstellers vermutet wird. Der Ansicht zur Beweislastregelung ist zu folgen. Der Grund liegt darin, dass dem Verantwortlichen bzw. Auftragsverarbeiter, wenn er Anspruchsgegner ist, ohnehin die Möglichkeit zusteht, sich durch Gegenvortrag und Gegenbeweisangebote hinsichtlich aller anspruchsbegründenden Umstände zu entlasten. Aus Sicht der deutschen Rechtsordnung bedarf es auf EU-Ebene also gar keiner gesonderten Entlastungs- oder Exkulpationsregelung in der DS-GVO.

Im Ergebnis handelt es sich bei der Regelung des Art. 82 Abs. 3 DS-GVO entgegen der Ansicht des BGH im Scraping-Fall[66] nicht um eine Exkulpationsmöglichkeit. Vielmehr wird in Art. 82 Abs. 3 DS-GVO einzig eine Beweislastumkehr normiert, wonach das Verschulden des Verantwortlichen bzw. Auftragsverarbeiters bzgl. des Verstoßes vermutet wird.[67]

In den gegenständlichen Urteilen hatte der EuGH nur Sachverhalte zu bewerten, in denen eine Anwendung des Art. 82 Abs. 3 DS-GVO nicht gegeben waren. So hat der Gerichtshof konkret festgestellt, dass der Verantwortliche nicht allein dadurch von seiner Haftung befreit wird, weil Dritte im Sinne des Art. 4 Nr. 10 DS-GVO durch einen Cyberangriff den Zugang zu personenbezogenen Daten erlangt oder diese offengelegt hätten. Hierfür bedarf es des Nachweises durch den Verantwortlichen, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.[68]

Darüber hinaus kann sich der Verantwortliche gem. Art. 82 Abs. 3 DS-GVO nicht allein dadurch entlasten, dass ein Datenschutzverstoß von einem ihm unterstellten und Weisungen unterliegenden Mitarbeiter im Sinne des Art. 29 DS-GVO verursacht wurde. Vielmehr bedarf es zusätzlich des Nachweises, dass kein Kausalzusammenhang zwischen der Datenschutzverletzung und dem Schaden besteht.[69]

IV. Die Rechtsfolge des immateriellen Schadenersatzes

Im Folgenden findet sich eine Analyse der Rechtsprechung in Hinblick auf die Berechnung des immateriellen Schadens gem. Art. 82 DS-GVO. Bei der Schadensberechnung handelt es sich nicht um ein Tatbestandsmerkmal, sondern um die Rechtsfolge des immateriellen Schadenersatzes. Auch wenn auf die Berechnung der Schadenshöhe grundsätzlich die nationalen Vor-

61 Bergt, in: Kühling/Buchner, DS-GVO – Kommentar, 4. Aufl. 2024, Art. 82, Rn. 45; Schwartmann/Keppeler/Jacquemain, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO – Kommentar, 3. Aufl. 2024, Art. 82, Rn. 41 ff.; Schmidt, ZD 2024, 320.

62 Quaas, in: Wolff/Brink, Datenschutzrecht – Kommentar, 2. Aufl. 2022, Art. 82 DS-GVO, Rn. 27; Schwartmann/Keppeler/Jacquemain, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO – Kommentar, 3. Aufl. 2024, Art. 82, Rn. 44; Thüsing/Zhou, ZD 2024, 4; a. A.: Bergt, in: Kühling/Buchner, DS-GVO – Kommentar, 4. Aufl. 2024, Art. 82, Rn. 47 f.

63 Singraven/Bissels, ArbRAktuell 2024, 241 (243); Schneider, CR-online.de Blog 2024, CRBLOG0007609 (9. Gebot); Bergt, in: Kühling/Buchner, DS-GVO – Kommentar, 4. Aufl. 2024, Art. 82, Rn. 51.

64 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 72; siehe auch Singraven/Bissels, ArbRAktuell 2024, 243.

65 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 93 f.; EuGH, Urt. v. 11.04.2024, Az: C-741-/21, Rn. 46; EuGH, Urt. v. 04.10.2024, Az: C-200/23, Rn. 161 f.; siehe auch: OLG Karlsruhe, Urt. v. 07.11.2023, Az: 19 U 23/23, ZD 2024, 408, Rn. 55 ff.

66 BGH, Urt. v. 18.11.2024, Az: VI ZR 10/24, Rn. 21.

67 Quaas, in: Wolff/Brink, Datenschutzrecht – Kommentar, 2. Aufl. 2022, Art. 82, Rn. 51; Gola/Piltz, in: Gola/Heckmann, DS-GVO/BDSG – Kommentar, 3. Aufl. 2022, Art. 82, Rn. 24; a. A.: Bergt, in: Kühling/Buchner, DS-GVO – Kommentar, 4. Aufl. 2024, Art. 82, Rn. 51 ("Exkulpation").

68 EuGH, Urt. v. 14.12.2023, Az: C-340/21, Rn. 74.

69 EuGH, Urt. v. 11.04.2024, Az: C-741-/21, Rn. 51.

schriften anzuwenden sind,[70] hat sich aus europarechtlicher Perspektive der EuGH hierzu verschiedentlich geäußert. Dabei hat der Gerichtshof allgemeine Leitlinien aufgestellt, die die nationalen Gerichte bei der Schadensberechnung anzuwenden haben, und spezielle Fragen zur Schadenshöhe beantwortet.

Zunächst ist festzuhalten, dass die Berechnung des Schadens einzig in die Zuständigkeit der Mitgliedstaaten fällt. Denn die DS-GVO enthält keine Regel zur Bemessung des Schadenersatzes. Die Mitgliedstaaten haben vielmehr autonom "die verfahrensrechtlichen Modalitäten der Rechtsbehelfe (inkl. die Kriterien für die Ermittlung der Schadenshöhe) festzulegen", vorausgesetzt dass die nationalen Normen keinen geringeren Schutz gewährleisten als die DS-GVO (Äquivalenzgrundsatz) und dass dadurch die Ausübung des europäischen Datenschutzes nicht praktisch unmöglich oder übermäßig erschwert wird (Effektivitätsgrundsatz).[71]

Aus ErwG 146 S. 6 DS-GVO ergibt sich weiter die Vorgabe, dass ein "vollständiger und wirksamer Schadenersatz für den erlittenen Schaden" sichergestellt werden soll. Daher liegt der Zweck der Ersatzpflicht des Art. 82 Abs. 1 DS-GVO nach Ansicht des EuGH lediglich in einer Ausgleichsfunktion und nicht in einer darüber hinausgehenden abschreckenden Funktion[72] oder einer Straffunktion.[73] Aus dem gleichen Rechtsgrund dürfen auch die Kriterien des Art. 83 Abs. 2 DS-GVO für die Berechnung von Geldbußen nicht auf die Schadensberechnung des Art. 82 Abs. 1 DS-GVO angewendet werden, da beide Normen unterschiedliche Regelungszwecke verfolgen.[74] Aus diesem Befund lässt sich ableiten, dass sich die Schwere des Verstoßes gegen die DS-GVO[75] oder die Anzahl der Verstöße[76] sowie die Schwere des Verschuldens[77] nicht auf die Höhe des Schadenersatzes auswirken dürfen.[78] Im Urteil "Scalable Capital" hat der EuGH überdies konkret festgestellt, dass bei der Berechnung des Schadens gem. Art. 82 Abs. 1 DS-GVO eine Körperverletzung nicht zwangsläufig schwerer wiegt als ein immaterieller Schaden nach der DS-GVO.[79] Von Relevanz für die Praxis ist schließlich die Klarstellung des EuGH, dass ein nationales Gericht auch einen Schadenersatz in geringer Höhe zusprechen kann, wenn der eingetretene Schaden nicht schwer wiegt.[80]

Es bleibt abzuwarten, ob in Anbetracht dessen, dass gem. Art. 82 DS-GVO nur eine Ausgleichsfunktion bewirkt werden soll, die nationalen Gerichte die Höhe der gewährten Schadenshöhe tendenziell geringer ausurteilen werden.

V. Fazit

Die vorstehende Analyse der einschlägigen Rechtsprechung zum immateriellen Schadenersatz gem. Art. 82 Abs. 1 DS-GVO hat aufgezeigt, dass sich der EuGH und die deutschen Gerichte zu verschiedenen Fragen und offenen Punkten hinreichend geäußert haben. Die Erkenntnisse zum Tatbestand und zur Rechtsfolge können daher wie folgt zusammengefasst werden:

Ein immaterieller Schadenersatz gem. Art. 82 DS-GVO ist gegeben, wenn vier kumulative Voraussetzungen erfüllt sind: 1.) Es muss ein Verstoß gegen einschlägiges Datenschutzrecht vorliegen. 2.) Dieser Verstoß muss durch den Verantwortlichen bzw. Auftragsverarbeiter schuldhaft begangen worden sein, wobei das Verschulden vermutet wird. 3.) Es muss ein Schaden eingetreten sein. Dieser Schaden kann in einem Kontrollverlust oder in der begründeten Befürchtung des Anspruchstellers liegen, dass seine personenbezogenen Daten künftig missbraucht werden. Die hypothetische Möglichkeit der unbefugten Kenntnisnahme durch Dritte reicht für die begründete Befürchtung jedoch nicht aus. 4.) Es muss ein Kausalzusammenhang zwischen Schaden und Verstoß gegeben sein.

In der Rechtsfolge wird mit dem immateriellen Schadenersatz eine Ausgleichsfunktion und keine abschreckende oder Straffunktion verfolgt. Die Schwere des Verstoßes oder die Anzahl der Verstöße sowie die Schwere des Verschuldens dürfen sich nicht auf die Schadenshöhe auswirken. Bei einem geringen Schaden kann auch nur ein geringer immaterieller Ersatz ausgesprochen werden.

Auch wenn diese zusammengefassten Erkenntnisse die praktische Anwendung des immateriellen Schadenersatzes gem. Art. 82 DS-GVO erleichtern, hat die Rechtsprechung des EuGH nichtsdestotrotz Fragen offengelassen. Unklar ist z.B. wie der Begriff "Kontrollverlust", der nach Ansichten des EuGH und des BGH einen immateriellen Schaden darstellen kann, zu definieren ist. Dies ist insbesondere relevant, da mit der verzögerten Auskunft gem. Art. 15 DS-GVO ein Kontrollverlust begründet werden könnte. Diese Frage hat das Amtsgericht Arnsberg dem EuGH erst kürzlich vorgelegt.[81]

Für die zukünftige Anwendung des immateriellen Schadenersatzes ist auch eine Konkretisierung und weitergehende Erläuterung der begründeten Befürchtung der missbräuchlichen Verwendung als Schaden und dessen Darlegung und Beweisangebot von Bedeutung. Dies gilt insbesondere vor dem Hintergrund, dass dieses Tatbestandsmerkmal auf eine Vielzahl von Sachverhalten zutrifft, die ihrerseits das Potenzial zu (unerwünschten) Masseverfahren hat. Entsprechende Ausführungen hat der BGH zwar im Scraping-Fall gegeben. Allerdings bezogen sich diese lediglich auf den Kontrollverlust. Ob diese Ausführungen zur Darlegung und ggf. zum Beweis auf die begründete Befürchtung übertragbar sind, ist unklar.

Dr. Oliver Daum
ist Rechtsanwalt aus Kiel und Fachanwalt für IT-Recht. Zugleich ist er zertifizierter Datenschutzbeauftragter (IHK) und zertifizierter IT-Sicherheitsbeauftragter (IHK). Seine Tätigkeitschwerpunkte sind IT-Recht, Datenschutz, Datensicherheit, das Recht der Künstlichen Intelligenz, Arbeitsrecht und E-Sport.

70 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 59.

71 EuGH, Urt. v. 04.05.2023, Az: C-300/21, Rn. 53 f.

72 EuGH, Urt. v. 20.06.2024, Az: C-182/22 u. C-1859/22, Rn. 24; a.A.: LG Köln, Urt. v. 28.09.2022, Az: 28 O 21/22, ZD 2023, 159, Rn. 34.

73 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 85.

74 EuGH, Urt. v. 11.04.2024, Az: C-741-/21, Rn. 59; a.A.: LG München I, Urt. v. 09.12.2021, Az: 31 O 16606/20, ZD 2022, 243, Rn. 41.

75 EuGH, Urt. v. 21.12.2023, Az: C-667/21, Rn. 86; a.A.: LAG Düsseldorf, Urt. v. 26.04.2023, Az: 12 Sa 18/23, BeckRS 2023, 24880, Rn. 118.

76 EuGH, Urt. v. 11.04.2024, Az: C-741-/21, Rn. 64.

77 EuGH, Urt. v. 20.06.2024, Az: C-182/22 u. C-1859/22, Rn. 28; a. A.: OLG Hamburg, Urt. v. 10.01.2024, Az: 13 U 70/23, BeckRS 2024, 804, Rn. 9.

78 Siehe jedoch OLG Dresden, Urt. v. 30.11.2021, Az: 4 U 1158/21, ZD 2022, 159, Rn. 12, wonach Schwere des Verstoßes, Grad des Verschuldens etc. in der Schadensberechnung zu berücksichtigen sind.

79 EuGH, Urt. v. 20.06.2024, Az: C-182/22 u. C-1859/22, Rn. 39.

80 EuGH, Urt. v. 20.06.2024, Az: C-182/22 u. C-1859/22, Rn. 46.

81 VG Arnsberg, Beschl. v. 31.07.2024, Az: 42 C 434/23, beck-aktuell v. 03.09.2024, https://rsw.beck.de/aktuell/daily/meldung/detail/ag-arnsberg-42C43423-DS-GVO-auskunft-verweigert-rechtsmissbrauch; Leibold, RDi 2024, 578 ff.

Dr. Clemens Birkert/David Pfau

Die KI-VO – Herausforderungen für Unternehmen: Ausgewählte Praxisfragen und erste Lösungsansätze

Mit Inkrafttreten der Verordnung über Künstliche Intelligenz („KI-VO") am 1. August 2024 stehen die rechtlichen Rahmenbedingungen für die verantwortungsvolle Entwicklung und Verwendung Künstlicher Intelligenz in der EU fest. Genauso wie beim Inkrafttreten der Datenschutz-Grundverordnung („DS-GVO") hat der europäische Gesetzgeber in der KI-VO eine Übergangsfrist von zwei Jahren vorgesehen, bis die Vorgaben auch gelten (vgl. Art. 113 S. 2 KI-VO). Anders als bei Einführung der DS-GVO sind aber zahlreiche Vorschriften von der zweijährigen Übergangsfrist ausgenommen. Angesichts des unannehmbaren Risikos, das mit der Nutzung von KI auf bestimmte Weise einhergehe[1], gelten etwa die Verbotstatbestände sowie die allgemeinen Bestimmungen schon ab dem 2. Februar 2025 (vgl. Art. 113 S. 3 lit. a) KI-VO). Daneben greifen zahlreiche allgemeine Vorgaben aus dem deutschen und europäischen Recht, die nach ihrem Gesetzestext zwar überwiegend nicht an den Begriff der Künstlichen Intelligenz anknüpfen, für Unternehmen aber dennoch erhebliche Praxisrelevanz haben können. Unternehmen, die mit KI-Anwendungen erste Erfahrungen sammeln wollen, sollten sich daher zeitnah mit den rechtlichen Rahmenbedingungen auseinandersetzen. Ausgewählte Praxisfragen, die in Pilotprojekten eine besonders große Rolle spielen, sollen im Folgenden mit ersten Lösungsansätzen dargestellt werden.

I. Initiale Einordnung als Anbieter oder Betreiber

Der Umfang des maßgeblichen Pflichtenprogramms der KI-VO hängt entscheidend von der Rolle desjenigen ab, der mit einem KI-System umgeht. Die KI-VO definiert in Art. 3 KI-VO mit dem Anbieter, Produkthersteller, Betreiber, Bevollmächtigten, Einführer und Händler verschiedene Rollen, die gesammelt als Akteure bezeichnet werden (vgl. Art. 3 Nr. 8 KI-VO). Nicht definiert wird die Rolle des Nutzers oder des Endabnehmers.

Unternehmen, die KI-Systeme nur als interne Arbeitserleichterung einsetzen möchten (etwa in Form eines Chatbots oder eines Recherchetools), werden im Regelfall vermeiden wollen, als Anbieter eingeordnet zu werden. Denn während der Betreiber in der KI-VO nur von einer recht überschaubaren Zahl an Normen adressiert wird,[2] treffen den Anbieter eines KI-Systems umfangreiche Pflichten.[3] Die Frage, wer diese Rolle in der Praxis übernimmt, spielt daher eine erhebliche Rolle.

1. Anbieter

Nach der Legaldefinition ist der „Anbieter" eine natürliche oder juristische Person oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt (vgl. Art. 3 Nr. 3 KI-VO). Grundvoraussetzung ist demnach, dass der Anbieter bei der Entwicklung des KI-Systems oder KI-Modells beteiligt ist. Der Begriff der Entwicklung wird in der KI-VO nicht definiert. Die Rolle des Entwicklers entspricht im Wesentlichen der des Herstellers im Produktsicherheits- und Produkthaftungsrecht.[4] Umfasst sein können sowohl privatrechtliche als auch öffentlich-rechtliche Akteure, unabhängig von ihrer Rechtsform. Unerheblich ist auch, ob der Anbieter seinen Sitz in der EU oder in einem Drittland hat[5] und ob die Handlung entgeltlich oder unentgeltlich durchgeführt wird[6]. Die Entwicklungsleistungen müssen auch nicht selbst vorgenommen werden. Ausreichend ist, dass ein Dritter mit der Entwicklung beauftragt wird.

Der Anbieter muss das KI-System oder das KI-Modell anschließend in Verkehr bringen oder in Betrieb nehmen. Inverkehrbringen meint „die erstmalige Bereitstellung eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck auf dem Unionsmarkt" (vgl. Art. 3 Nr. 9 KI-VO). Inbetriebnahme ist definiert als „die Bereitstellung eines KI-Systems in der Union zum Erstgebrauch direkt an den Betreiber oder zum Eigengebrauch entsprechend seiner Zweckbestimmung" (vgl. Art. 3 Nr. 11 KI-VO). Nicht umfasst sind Handlungen im rein privaten, nicht beruflichen Kontext. Bei diesen greift die Haushaltsausnahme in Art. 2 Abs. 10 KI-VO.

Das Inverkehrbringen oder die Inbetriebnahme muss unter eigenem Namen oder eigener Handelsmarke erfolgen. Bietet der Anbieter ein KI-System im Geschäftsverkehr an, erfolgt dies in der Regel ausdrücklich, beispielsweise durch entsprechende Angaben auf der Webseite, in einer Produktbeschreibung oder in Begleitdokumenten. Bei einer Inbetriebnahme zum Eigenbetrieb wird man dagegen im Einzelfall prüfen müssen, ob ein Unternehmen tatsächlich eine Lösung unter eigenen Namen oder mit eigener Handelsmarke in Betrieb nimmt oder erkennbar die Lösung eines Dritten nutzt.

2. Betreiber

Der „Betreiber" verwendet ein KI-System in eigener Verantwortung (Art. 3 Nr. 4 Hs. 1 KI-VO). Ausgenommen ist die

1 So ErwG 179 S. 2 KI-VO.

2 Vgl. dazu Borges, CR 2024, 565, 572.

3 Vgl. Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 63; Borges, CR 2024, 565, 572; von Weiser, GRUR-Prax 2024, 485, 487.

4 So auch Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 63 mit Erläuterungen zu den relevanten Definitionen.

5 Art. 2 Abs. 1 lit. a) KI-VO.

6 Art. 3 Nr. 3 a.E. KI-VO.

Verwendung des KI-Systems im Rahmen einer persönlichen und nicht beruflichen Tätigkeit (Art. 3 Nr. 4 Hs. 2 KI-VO). Anders als beim Anbieterbegriff wurde die Rollenbezeichnung des Betreibers noch während des Gesetzgebungsverfahrens geändert. So wurde derjenige, der ein KI-System in eigener Verantwortung verwendet, im ursprünglichen Kommissionsentwurf aus dem Jahr 2021 noch als „Nutzer" bezeichnet. Diese Begriffsbezeichnung wurde aufgrund ihrer Nähe zum Nutzerbegriff in anderen Digitalrechtsakten stark kritisiert. Während der Nutzer in diesen funktionell überwiegend die geschützte Partei bezeichnet, sollte der Begriff in der KI-VO vielmehr Anknüpfungspunkt für Pflichten sein (vgl. etwa Art. 27, 50 Abs. 3 und Abs. 4, Art. 71 Abs. 3 KI-VO). Um diese Differenzierung auch sprachlich zum Ausdruck zu bringen, hat das Parlament in den Trilogverhandlungen den Begriff „Betreiber" durchgesetzt.[7]

Auch Betreiber können unabhängig von ihrer Rechtsform sowohl privatrechtliche als auch öffentlich-rechtliche Akteure sein. Anders als bei der Anbieterrolle knüpft die Definition jedoch nur an KI-Systeme an, nicht auch an KI-Modelle mit allgemeinem Verwendungszweck (dazu unter I.3). Denn letztere können faktisch nur verwendet werden, sofern sie in ein KI-System integriert werden.[8]

Der Betreiber muss das KI-System „verwenden", was zunächst einen bewussten Einsatz in Bezug auf die wesentlichen Arbeitsschritte des KI-Systems voraussetzt.[9] Nicht ausreichend ist die bloße Verwendung der Ausgabe („Output") eines KI-Systems, die von einem Dritten zur Verfügung gestellt wird (etwa Mediencontent einer Marketingagentur, die einen KI-Bildgenerator eingesetzt hat). Die Verwendung muss zudem „in eigener Verantwortung" erfolgen. Dies setzt nicht voraus, dass die technischen Einzelschritte, wie beispielsweise das Hosting des KI-Systems, die Bereitstellung der Weboberfläche oder die Erstellung einer Ausgabedatei, vom Betreiber selbst durchgeführt werden. Soweit Drittdienstleister eingesetzt werden, ist für die Zurechnung zur Verantwortungssphäre des Betreibers (hier zugleich Auftraggeber) aber erforderlich, dass das KI-System im Auftrag und auf Rechnung des Auftraggebers betrieben wird. Dies kann auch dann der Fall sein, wenn der Dienstleister sämtliche Arbeitsschritte in der Cloud durchführt und dabei etwa als Auftragsverarbeiter agiert (im vorgenannten Beispiel etwa eine Marketingagentur, die den KI-Bildgenerator strikt nach Weisung bedient). Zwischen Dienstleister und Auftraggeber muss dann eine Vereinbarung zur Auftragsverarbeitung mit dem Pflichtinhalt aus Art. 28 Abs. 3 DS-GVO geschlossen werden.

3. KI-System oder KI-Modell

Sachlicher Bezugspunkt bei der Bestimmung der Anbieterrolle ist „ein KI-System oder ein KI-Modell", bei der Rolle des Betreibers dagegen nur ein „KI-System". Diese sprachliche Differenzierung kommt in der Diskussion zum Pflichtenprogramm nach der KI-VO häufig zu kurz, ist aber mitunter entscheidend für die Rollenzuweisung und von enormer Praxisrelevanz: Während KI-Systeme in der KI-VO mit wenigen Ausnahmen umfassend reguliert werden, sind für bestimmte KI-Modelle, die einen allgemeinen Verwendungszweck aufweisen, nur wenige Vorgaben normiert.

Ein KI-System ist nach der sperrigen Definition in Art. 3 Nr. 1 KI-VO „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können"[10]. Umfasst sein können etwa digitale Assistenten (z.B. Microsoft 365 Copilot, ChatGPT, Google Gemini), KI-Tools zur Text- (z.B. Jasper AI, copy.ai und neuroflash) oder Bilderstellung (z.B. Adobe Firefly, Midjourney, Stable Diffusion) sowie Anwendungen zur Unterstützung von Programmiertätigkeiten (z.B. GitHub Copilot). Die Abgrenzung zur herkömmlichen Software erfolgt insbesondere über die Merkmale „autonomer Betrieb" sowie die Fähigkeit zur Ableitung. Beide Merkmale bieten genug Unschärfe, um Sachverständigen und Gerichten in den kommenden Jahren viel Diskussionsstoff zu liefern.[11]

Ein „KI-Modell mit allgemeinem Verwendungszweck" (engl. General Purpose AI oder kurz GPAI), wird in Art. 3 Nr. 63 KI-VO definiert als KI-Modell, „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, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann [...]"[12]. Der Begriff „KI-Modell" selbst wird nicht separat definiert. Vereinfacht gesagt bildet ein KI-Modell die technische Grundlage für KI-Systeme.[13] Bekannte KI-Modelle sind etwa GPT (OpenAI), BERT (Google), AlphaGo (DeepMind), Gemini (Google), DALL-E (OpenAI) oder LLaMA (Meta). Diese Modelle können zum KI-System werden, soweit sie durch Hinzufügung weiterer Komponenten (etwa einer Nutzerschnittstelle) in eine Applikationsumgebung integriert und dadurch interaktiv gemacht werden.

Zu gewissen Verwirrungen kann die Definition eines „KI-Systems mit allgemeinem Verwendungszweck" in Art. 3 Nr. 66 KI-VO führen. Dies ist ein KI-System, „das auf einem KI-Modell mit allgemeinem Verwendungszweck beruht und in der Lage ist, einer Vielzahl von Zwecken sowohl für die direkte Verwendung als auch für die Integration in andere KI-Systeme zu dienen". Auch wenn der Begriff in der KI-VO definiert wird, knüpft die KI-VO keine unmittelbaren Rechtsfolgen an diesen. Entscheidend für die Rollenzuweisung ist, dass es sich insofern um ein KI-System handelt, nicht nur um ein bloßes KI-Modell.

7 Zur Kritik vgl. auch Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 81.

8 Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 82.

9 So auch Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 84.

10 Art. 3 Nr. 1 KI-VO.

11 Ausführlich dazu Keppeler/Thomas, ITRB 2024, 320, die das Merkmal der „Anpassungsfähigkeit" und des „autonomen Betriebs" als „Rettungsanker" bei der Abgrenzung zur herkömmlichen Software herausarbeiten.

12 Art. 3 Nr. 63 KI-VO.

13 Vgl. dazu ErwG 97 KI-VO: „KI-Modelle mit allgemeinem Verwendungszweck können auf verschiedene Weise in Verkehr gebracht werden, unter anderem über Bibliotheken, Anwendungsprogrammierschnittstellen (API), durch direktes Herunterladen oder als physische Kopie. Diese Modelle können weiter geändert oder zu neuen Modellen verfeinert werden. Obwohl KI-Modelle wesentliche Komponenten von KI-Systemen sind, stellen sie für sich genommen keine KI-Systeme dar. Damit KI-Modelle zu KI-Systemen werden, ist die Hinzufügung weiterer Komponenten, zum Beispiel einer Nutzerschnittstelle, erforderlich. KI-Modelle sind in der Regel in KI-Systeme integriert und Teil davon.".

4. Grenzfälle: API-Einbindung, eigene Datenbanken und Finetuning

Im Regelfall werden Unternehmen KI-Anwendungen nicht (vollständig) selbst entwickeln, sondern die Lösung eines Drittanbieters lizenzieren wollen. Eine solche Drittlösung kann ein reines KI-Modell sein, das über eine Programmierschnittstelle (engl. Application Programming Interface, kurz API) in eine eigene Anwendung des Unternehmens eingebunden wird. Alternativ kann ein fertiges KI-System lizenziert werden, das schon selbst eine Applikationsumgebung des Drittanbieters enthält und dem Unternehmen zum lokalen Betrieb auf dessen eigener Unternehmenshardware (On-Premise-Betrieb) oder in Form eines Cloud-Computing-Modells über das Internet (Software-as-a-Service) bereitgestellt wird. Im ersten Fall tritt der Drittanbieter in der Regel als Anbieter des KI-Modells, im zweiten als Anbieter des KI-Systems auf.

Schwieriger zu beantworten ist die Frage, welche Rolle das Unternehmen in beiden Fällen einnimmt. Erhält das Unternehmen ein fertiges KI-System und nutzt dieses ohne Veränderungen (etwa eine Übersetzungslösung oder einen Bildgenerator), tritt es bei der Nutzung im Regelfall als reiner Betreiber auf (zu den Ausnahmen siehe unter II.). Soweit das Unternehmen aber beispielsweise seinen Beschäftigten einen KI-Chatbot zur Verfügung stellen möchte und dafür ein generatives Sprachmodell mit allgemeinem Verwendungszweck bei einem Drittanbieter lizenziert, soll dieser Chatbot im Regelfall individuell an den Einsatz im Unternehmen angepasst werden, um etwa Auskunft über unternehmensinterne Vorgänge geben zu können. Hierfür kann die Anpassung des Sprachmodells erforderlich sein. Im Fall des Chatbots dürfte es ausreichen, unternehmenseigene Datensätze mit dem Sprachmodell zu verknüpfen. Technisch kann dies durch die sog. „Retrieval-Augmented Generation" (RAG) erfolgen, bei der zu referenzierende Daten u.a. in Worteinbettungen umgewandelt und in einer Vektorendatenbank indexiert werden. Die RAG-Technologie erweitert somit die Fähigkeiten des Sprachmodells, indem sie externe Informationen in Echtzeit einbezieht und die Eingaben kontextualisiert, ohne das Sprachmodell selbst zu verändern.[14] Alternativ kann das Unternehmen ein Finetuning des vortrainierten Modells durchführen. Der Begriff des Finetunings wird durch die KI-VO nicht definiert[15] und kann eine Vielzahl an Methoden bezeichnen, um Sprachmodelle zu individualisieren.[16] Dabei können die Parameter des vortrainierten Modells auf neue, spezifische Daten trainiert und angepasst werden.

In beiden Fällen muss begrifflich zwischen der Anbieterrolle für das KI-Modell und der für das KI-System differenziert werden. Da bei RAG keine Veränderung am KI-Modell selbst vorgenommen wird, entwickelt das Unternehmen kein eigenständiges KI-Modell und ist daher auch nicht als Anbieter des KI-Modells einzuordnen. Auch beim Finetuning wird sich dies – abhängig von der Art und Weise der Anpassung – vertreten lassen. Hier stellt sich jedoch regelmäßig die Frage, ab wann Änderungen der Parameter so schwerwiegend sind, dass im Ergebnis von einem neu oder wesentlich weiterentwickelten KI-Modell gesprochen werden und damit das Unternehmen als Anbieter des weiterentwickelten KI-Modells betrachtet werden muss. Das Merkmal „wesentliche Veränderung" definiert die KI-VO nur im Zusammenhang mit KI-Systemen (vgl. Art. 3 Nr. 23 KI-VO). Die dortige Wertung lässt sich jedoch nach der hier vertreten Ansicht auch auf die Anpassung von KI-Modellen übertragen, so dass im Einzelfall geprüft werden muss, ob die Zweckbestimmung des Modells derart weitreichend geändert wurde, dass eine Neubewertung am Maßstab der KI-VO erforderlich wird. Soweit durch ein Finetuning beispielsweise nur besondere Begrifflichkeiten des Unternehmens übernommen werden sollen, wird die Grundstruktur des Modells nicht verändert und damit kein neues KI-Modell entwickelt.

Damit eng verbunden ist die Frage, unter welchen Voraussetzungen das Unternehmen initial als Anbieter des gesamten KI-Systems einzuordnen ist. Stellt man auf den Wortlaut der Anbieterdefinition in Art. 3 Nr. 3 KI-VO ab, müsste das Unternehmen die Schwelle zum Entwickeln eines (neuen) KI-Systems überschreiten. Da die KI-VO selbst bei Hochrisiko-KI-Systemen eine Rollenänderung nur bei wesentlichen Veränderungen vorsieht (Art. 25 Abs. 1 lit. b) KI-VO, dazu unter II.2.), kann bei KI-Systemen unterhalb der Hochrisikoschwelle erst recht argumentiert werden, dass unwesentliche Änderungen nicht zu einer Rollenzuweisung nach Art. 3 Nr. 3 KI-VO führen.[17] Jedenfalls wenn ein Sprachmodell in eine vollständig eigenentwickelte Unternehmensanwendung integriert wird, entsteht aber originär ein KI-System, dessen Anbieter dann das Unternehmen ist.

Bezieht das Unternehmen dagegen ein KI-System mit allgemeinem Verwendungszweck für allgemeine Assistenztätigkeiten (etwa Recherche, Textzusammenfassung, Texterstellung) und passt es an, wird nach der hier vertretenen Ansicht RAG oder Finetuning nur in Ausnahmefällen dazu führen, dass das Unternehmen als Anbieter des KI-Systems einzuordnen ist. Häufig wird hier ein Argumentationsspielraum verbleiben, der bei Nichterfüllung der Anbieterpflichten aber zugleich mit einer gewissen Rechtsunsicherheit für Unternehmen verbunden ist.

II. Unbeabsichtigte Rollenänderungen nach Art. 25 KI-VO

Modifiziert wird die allgemeine Rollenzuweisung durch Art. 25 Abs. 1 KI-VO, der für Händler, Einführer, Betreiber oder sonstige Dritte (nachfolgend: „Beteiligte") eine besondere Verantwortlichkeitszuweisung vorsieht. Die Norm soll Rechtssicherheit in den Fällen gewährleisten, in denen ein bereits in Verkehr gebrachtes oder in Betrieb genommenes KI-System derart verändert wird, dass die originäre Rollenzuweisung nicht mehr sachgemäß erscheint und daher eine andere Person alle einschlägigen Pflichten des Anbieters erfüllen sollte.[18] Die Modifikationen sind von erheblicher Praxisrelevanz.

1. Anbringen eines Namens oder einer Handelsmarke

Eine Rollenänderung tritt nach Art. 25 Abs. 1 lit. a) KI-VO für Beteiligte ein, die ein bereits in Verkehr gebrachtes oder in Be-

14 Vgl. Blum/Rappenglück, CR 2024, 626, 632.

15 Vgl. dazu nur ErwG 97 S. 5.

16 Dazu Blum/Rappenglück, CR 2024, 626, 631.

17 Andererseits stellt ErwG 97 KI-VO klar: „KI-Modelle mit allgemeinem Verwendungszweck können auf verschiedene Weise in Verkehr gebracht werden, unter anderem über Bibliotheken, Anwendungsprogrammierschnittstellen (API), durch direktes Herunterladen oder als physische Kopie. Diese Modelle können weiter geändert oder zu neuen Modellen verfeinert werden.".

18 Vgl. ErwG 84 KI-VO.

trieb genommenes Hochrisiko-KI-System mit ihrem Namen oder ihrer Handelsmarke versehen. Name meint in diesem Zusammenhang die Kennzeichnung einer Person mit einer Identitätskennzeichnung, im deutschen Recht etwa bekannt aus dem Namensrecht in § 12 BGB oder der Firmenbezeichnung in § 17 HGB. Handelsmarke meint eine Unternehmenskennzeichnung im Sinne des Markenrechts. Das KI-System wird mit einem Namen oder einer Handelsmarke versehen, wenn das Kennzeichen innerhalb des KI-Systems oder der Begleitmaterialien (z.B. Betriebsanleitung) angebracht wird.[19] Unerheblich ist dabei, ob der Beteiligte mit dem Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hatte, eine vertragliche Vereinbarung getroffen hat, die eine andere Aufteilung der Pflichten vorsieht. Die Rollenänderung in Art. 25 Abs. 1 lit. a) KI-VO ist nicht disponibel.

Die Rollenzuweisung ist für das Inverkehrbringen mit eigener Handelsmarke nachvollziehbar, da für einen Außenstehenden durch das Anbringen des Namens oder der Handelsmarke der Anschein entsteht, dass das KI-System insgesamt von dem kennzeichnenden Unternehmen stammt. Wenig überzeugend ist die Ausweitung dagegen beispielsweise, wenn ein Unternehmen eine KI-Anwendung nur intern in Betrieb nimmt und etwa bei der Einbindung einer KI-Chatlösung für Beschäftigte in das Intranet seine Handelsmarke anbringt. Denn in diesem Fall wird regelmäßig aus den Umständen des Einzelfalls für die Beschäftigten erkennbar sein, dass der Arbeitgeber nur ein unverändertes KI-System eines Drittanbieters zur Verfügung stellt.

Aus Praxissicht ist es bei einer Inbetriebnahme ratsam, das KI-System möglichst getrennt von eigenen Anwendungen zur Verfügung zu stellen und die Beschäftigten klar darauf hinzuweisen, dass die Anwendung eines Drittanbieters verwendet wird. Dies kann etwa in der Präambel zu den Nutzungsbedingungen oder in einem Praxisleitfaden erfolgen. Auf das Anbringen eines eigenen Namens oder einer Handelsmarke innerhalb des KI-Systems selbst sollte verzichtet werden.

2. Wesentliche Veränderung eines Hochrisiko-KI-Systems

Eine Rollenänderung tritt nach Art. 25 Abs. 1 lit. b) KI-VO für den Beteiligten auch dann ein, wenn er eine wesentliche Veränderung eines Hochrisiko-KI-Systems, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, so vornimmt, dass es weiterhin ein Hochrisiko-KI-System bleibt. Dies führt zu einem Wechsel der Anbieterrolle, da dem ursprünglichen Anbieter das veränderte System nicht mehr zugerechnet werden kann.

Eine wesentliche Veränderung setzt voraus, dass die Veränderung in der vom bisherigen Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war. Des Weiteren muss die Veränderung die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 der KI-VO beeinträchtigen oder zu einer Änderung der Zweckbestimmung führen, für die das KI-System bewertet wurde (vgl. Art. 3 Nr. 23 KI-VO). Die Zweckbestimmung eines KI-Systems richtet sich nach dem tatsächlichen Einsatzgebiet der vom KI-System erzeugten Ausgabe („Output“).[20] Die Einordnung erfolgt nach der Konzeption der KI-VO durch den Anbieter des KI-Systems, der den Einsatzbereich antizipieren muss.[21]

Die Rollenänderung folgt in dieser Konstellation zum einen daraus, dass der ursprüngliche Anbieter wesentliche Änderungen nicht antizipieren kann und daher schutzbedürftig ist, da sein Ursprungssystem nach den Vorgaben der KI-VO ausgestaltet war. Zum anderen wird über die Figur des Quasi-Anbieters eine Haftung desjenigen statuiert, der in der nachgelagerten Wertschöpfungskette die wesentliche Änderung vorgenommen hat.[22] In der Praxis sollte daher genau geprüft werden, ob Anpassungen an Hochrisiko-KI-Systeme zu einer wesentlichen Änderung führen (dazu schon oben unter I.4.).

3. Zweckänderung eines KI-Systems, die zur Einstufung als hochriskant führt

Eine ähnlich gelagerte Rollenänderung tritt nach Art. 25 Abs. 1 lit. c) KI-VO für Beteiligte ein, die die Zweckbestimmung eines KI-Systems, das nicht als hochriskant eingestuft und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das KI-System zu einem Hochrisiko-KI-System wird. Anders als in der vorherigen Fallgruppe resultiert die Einordnung als Hochrisiko-KI-System erst aus der Vornahme der Zweckänderung durch die Beteiligten. Von der Fallgruppe umfasst ist auch eine Zweckänderung, die sich auf ein KI-System mit allgemeinem Verwendungszweck bezieht.

Sinn und Zweck der Norm ist die gewünschte Verantwortungsverschiebung auf den Beteiligten, der durch seine Veränderung das KI-System erstmals hochriskant macht. Eine Zurechnung der Verantwortung auf den ursprünglichen Anbieter wäre in diesem Fall unbillig, da sich die Veränderung außerhalb seiner Zweckbestimmung bewegt. Die Einhaltung der Vorgaben für Hochrisiko-KI-Systeme nach Art. 16 ff. KI-VO kann von diesem daher nicht eingefordert werden.

Noch nicht abschließend geklärt ist die Frage, wie eine solche Zweckänderung durch Beteiligte in der (Unternehmens-)Praxis zuverlässig ausgeschlossen werden kann. Da die Zweckbestimmung des KI-Systems nach dem tatsächlichen Einsatzgebiet des vom KI-System erzeugten Outputs erfolgt,[23] sollten Unternehmen jedenfalls darauf achten, dass die vom Anbieter vorgegebene Zweckbeschreibung an die das KI-System einsetzenden Beschäftigten weitergegeben wird. Soweit naheliegend ist oder später erkennbar wird, dass Beschäftigte die KI-Anwendung für andere Zwecke einsetzen, sollten technische und/oder organisatorische Maßnahmen ergriffen werden, um die zweckwidrige Anwendung zu verhindern. Da im Regelfall nicht allein durch technische Filter auf Input- oder Output-Ebene ausgeschlossen werden kann, dass sich eine Zweckänderung im Unternehmen etabliert, sollten technische Maßnahmen durch eine klare Zweckbeschreibung in Nutzungsrichtlinien oder Praxisanleitungen ergänzt und naheliegende Anwendungsszenarien außerhalb der ursprünglichen Zweckausrichtung ausdrücklich verboten werden.

19 Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 25 KI-VO Rn. 12.

20 Ausführlich dazu Borges, CR 2024, 565, 568 ff.

21 Borges, CR 2024, 565, 569.

22 Vgl. Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 25 KI-VO Rn. 12.

23 Ausführlich dazu Borges, CR 2024, 565, 568 ff.

4. Produkthersteller als Anbieter nach Art. 25 Abs. 3 KI-VO

Eine Modifikation bzgl. Hochrisiko-KI-Systemen, bei denen es sich um Sicherheitsbauteile von Produkten handelt, die unter die in Anhang I Abschnitt A KI-VO genannten Harmonisierungsvorschriften der Union fallen, enthält Art. 25 Abs. 3 KI-VO. Von dem Verweis umfasst sind u.a. Maschinen, Spielzeug, Funkanlagen, Druckgeräte und Medizinprodukte, die in den in Anhang I genannten Harmonisierungsrechtsvorschriften der Union genannt werden. „Sicherheitsbauteil" meint dabei einen Bestandteil, der eine Sicherheitsfunktion erfüllt oder dessen Ausfall oder Störung die Gesundheit und Sicherheit von Personen oder Eigentum gefährdet.[24]

Bei diesen speziellen Systemen gilt der Produkthersteller als Anbieter des Hochrisiko-KI-Systems und unterliegt den Pflichten nach Art. 16 KI-VO, soweit das Hochrisiko-KI-System zusammen mit dem Produkt unter dem Namen oder der Handelsmarke des Produktherstellers in Verkehr gebracht oder ein zuvor in Verkehr gebrachtes Produkt unter dem Namen oder der Handelsmarke des Produktherstellers in Betrieb genommen wird. Die Zuweisung der Rolle als Anbieter nach der KI-VO resultiert in diesem Fall aus dem kumulierten Risiko, das sich aus der jeweiligen Produktgruppe an sich und dem Einsatz hochriskanter KI-Systeme als Sicherheitsbauteil ergibt.

5. Rechtsfolgen einer Rollenänderung

Kommt es nach Art. 25 Abs. 1 KI-VO zu einer Rollenänderung, gilt der bisherige Anbieter, der das KI-System ursprünglich in Verkehr gebracht oder in Betrieb genommen hat, nicht mehr als Anbieter dieses spezifischen KI-Systems (vgl. Art. 25 Abs. 2 S. 1 KI-VO). Sofern er die Änderung des KI-Systems in ein Hochrisiko-KI-System nicht ausdrücklich ausgeschlossen hat, muss er jedoch mit dem neuen Anbieter eng zusammenarbeiten, diesem die erforderlichen Informationen zur Verfügung stellen und den vernünftigerweise zu erwartenden technischen Zugang und sonstige Unterstützung leisten, die für die Erfüllung der in der KI-VO festgelegten Pflichten erforderlich sind (vgl. Art. 25 Abs. 2 S. 2 KI-VO).[25] Davon abweichend führt die Verantwortungszuweisung in Art. 25 Abs. 3 KI-VO zwar zur Einordnung des Produktherstellers als Quasi-Anbieter. Anders als bei der Rollenänderung nach Art. 25 Abs. 1 i.V.m. Abs. 2 KI-VO, behält aber auch der Erstanbieter seine Rolle als Anbieter im Sinne der KI-VO. In diesem Fall treten die neuen Anbieterpflichten des Produktherstellers neben die weiterhin bestehenden Anbieterpflichten des Erstanbieters.

III. Berechtigtes Interesse (Art. 6 Abs. 1 S. 1 lit. f) DS-GVO) beim Training von KI-Modellen durch Scraping und Crawling

Im Zeitalter datengetriebener Geschäftsmodelle stellt das Training von KI-Modellen eine Kernkomponente der Entwicklung innovativer Anwendungen dar. Dies ist zum aktuellen Zeitpunkt noch für die wenigen Anbieter von KI-Systemen relevant, kann jedoch mit Blick auf die zunehmende Individualisierung von KI-Systemen auch für die breite Masse der Unternehmen an Relevanz gewinnen. Im Spannungsfeld zwischen Innovationsförderung und Schutz der Persönlichkeitsrechte steht dabei neben der erörterten Rollenverteilung nach der KI-VO die Frage im Mittelpunkt, auf welche datenschutzrechtlichen Grundlagen die Verarbeitung der Daten gestützt werden kann.

1. KI-Training mittels Scraping und Crawling

Gem. Art. 3 Nr. 29 KI-VO sind „Trainingsdaten" Daten, die eingesetzt werden, um ein KI-System zu trainieren, indem die lernbaren Parameter des Systems angepasst werden. Trainingsdaten werden also genutzt, um ein KI-Modell in ein leistungsfähiges intelligentes Werkzeug zu verwandeln.[26] Um KI-Modelle mit Trainingsdaten zu versorgen, werden häufig Informationen aus dem Internet verwendet, die speziell aufbereitet wurden.[27] Hierfür kommen verschiedene Ansätze zur Datengewinnung infrage: Eine weit verbreitete Methode ist das gezielte Extrahieren von einzelnen Inhalten wie Texten, Bildern oder Videos aus Webseiten (sog. Scraping).[28] Eine andere Herangehensweise, bei der häufig nur Verweise auf Inhalte gespeichert werden, anstatt die Dateien selbst zu sichern, ist das sog. Crawling.[29] In der Regel werden beide Herangehensweisen kombiniert, um brauchbare Trainingsdaten zu erhalten.

Das Sammeln von Daten ist eine Grundvoraussetzung für die Entwicklung von KI-Modellen. Der Erfolg eines KI-Modells hängt maßgeblich von der Qualität der Trainingsdaten und dem Zugang zu diesen ab.[30] Vereinfacht lässt sich sagen: Wird eine größere Menge an Daten für das Training eingesetzt, erhöht dies in der Regel die Leistungsfähigkeit und reduziert mögliche unerwünschte Ausprägungen des Modells.[31] Daraus ergeben sich allerdings auch Implikationen für das Datenschutzrecht. Umso mehr Daten gesammelt werden, desto höher ist das Risiko, dass diese Personenbezug aufweisen.[32] Dieses Risiko ist bereits bei dem Sammeln von Trainingsdaten zu berücksichtigen. Es dürfte aber schwer zu kontrollieren sein, da die „Sammler" der Daten meist unabhängig von den Entwicklern der KI-Modelle agieren[33].

2. Praxistaugliche Rechtsgrundlagen für das Training von KI

Da diese Prozesse im Rahmen des Trainings von KI-Modellen Datenverarbeitungen im Sinne der DS-GVO darstellen können, stellt sich die Frage, auf welche Rechtsgrundlage des Art. 6 Abs. 1 DS-GVO sie gestützt werden können.

Die Verarbeitung von Trainingsdaten kann auf eine Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DS-GVO) gestützt werden, sofern diese u. a. freiwillig, informiert und eindeutig erteilt wurde.[34] Theoretisch könnte damit auch jegliches Training von KI-Modellen auf eine solche Einwilligung der betroffenen Personen

24 Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 149.

25 Vgl. auch ErwG 86 KI-VO.

26 Dieker, ZD 2024, 132, 132.

27 Hacker, GRUR 2020, 1025, 1026.

28 Pukas, GRUR 2023, 614, 614.

29 Jandt/Steidle, Datenschutz im Internet, 1. Aufl. 2018, A.I.3. Rn. 28.

30 Paal, ZfDR 2024, 129, 130.

31 Paal, ZfDR 2024, 129, 130.

32 Dieker, ZD 2024, 132, 133; Paal, ZfDR 2024, 129, 131.

33 Zech, NJW 2022, 502, 504.

34 Paal, ZfDR 2024, 129, 148.

gestützt werden. In der Praxis dürfte die Einwilligung aber meist ungeeignet sein, insbesondere bei automatisierten Datenerhebungen wie dem Scraping und Crawling.[35] Angesichts der Anzahl und der herausfordernden Bestimmbarkeit der betroffenen Personen fehlt im Regelfall schon die Möglichkeit, die Betroffenen entsprechend Art. 13 und 14 DS-GVO über die Verarbeitung zu informieren. Die erforderliche Kontaktaufnahme wäre kaum realisierbar.[36] Erschwerend kommt hinzu, dass eine Einwilligung jederzeit widerrufen werden kann, was umfangreiche und komplexe Löschpflichten nach sich ziehen würde.[37] Auch sind bei der Nutzung von KI-Systemen die genauen Verarbeitungsprozesse oft nicht vollständig nachvollziehbar.[38] Die DS-GVO fordert für eine wirksame Einwilligung jedoch eine transparente Information des Betroffenen über alle Verarbeitungsvorgänge, damit dieser die Folgen seiner Einwilligung einschätzen kann. Diese fehlende Transparenz, kombiniert mit rechtlichen und praktischen Hürden, macht die Einwilligung als Grundlage für die Verarbeitung personenbezogener Daten in solchen Szenarien weitgehend unpraktikabel.[39]

Entsprechendes gilt im Ergebnis für die Vertragsdurchführung als Rechtsgrundlage. Art. 6 Abs. 1 S. 1 lit. b) DS-GVO erlaubt eine Datenverarbeitung, soweit sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Im Regelfall wird weder dem Scraping noch dem Crawling ein Vertrag zugrunde liegen. Selbst wenn das Scraping und Crawling auf solche Online-Plattformen beschränkt wird, bei denen die Nutzungsverträge eine entsprechende Erlaubnis (etwa in Form einer Datenklausel) enthalten, müssten diese Datenverarbeitungsvorgänge nach jüngster Rechtsprechung für die Durchführung des Kernbereichs des Nutzungsvertrags objektiv unerlässlich sein. Andernfalls droht nach Ansicht der Rechtsprechung eine Umgehung der engen rechtlichen Vorgaben der Einwilligung.[40] Auch bei Online-Plattformen werden Scraping und Crawling aber wohl nicht für den Kernbereich des Nutzungsvertrages objektiv erforderlich sein.

3. Berechtigtes Interesse beim KI-Training

Die Verarbeitung personenbezogener Daten durch Datensammler und Entwickler von KI-Modellen kann nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO gerechtfertigt sein, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und keine übergeordneten Rechte der betroffenen Personen entgegenstehen. Dies erfordert zum einen eine Prüfung, ob tatsächlich ein berechtigtes Interesse des Verantwortlichen vorliegt. Dies kann rechtlicher, wirtschaftlicher oder ideeller Natur sein.[41] Für kommerzielle Datensammler und Anbieter von KI-Modellen liegt dieses Interesse meist in der unternehmerischen Freiheit und der Verbesserung von KI-Modellen, während bei nicht-kommerziellen Akteuren häufig die Wissenschafts- oder Informationsfreiheit im Vordergrund steht.[42] Außerdem muss die Verarbeitung zur Verfolgung des berechtigten Interesses erforderlich sein, wobei das mildeste Mittel zu wählen ist.[43] Jedenfalls zur Schaffung eines grundlegenden Trainingsdatenpools dürfte die Erforderlichkeit begründbar sein.[44] Scraping und Crawling werden häufig als die effektivsten Methoden zur Datensammlung angesehen.[45] Ob anonymisierte oder synthetische Daten eine ausreichende Alternative darstellen, hängt vom konkreten Ziel des KI-Modells ab und lässt sich nicht pauschal beantworten.[46] Die vollständige Anonymisierung von Datensätzen ist in der Praxis aber oft schwer umsetzbar und stellt selbst eine rechtfertigungsbedürftige Verarbeitung dar.[47]

Darüber hinaus muss das Interesse des Datensammlers mit den Rechten und Interessen der betroffenen Personen abgewogen werden und überwiegen. Dabei spielen Faktoren wie die Art der gesammelten Daten, deren künftiger Verwendungszweck, die Wahrscheinlichkeit einer Identifikation der betroffenen Personen und die möglichen Folgen der Verarbeitung für die Betroffenen eine zentrale Rolle.[48] Besonders strenge Maßstäbe gelten, wenn schutzwürdige Gruppen wie Kinder betroffen sind.[49] Werden Daten freiwillig veröffentlicht, kann dies das Schutzinteresse der Betroffenen dagegen mindern, allerdings nur dann, wenn die Veröffentlichung eindeutig auf der Entscheidung der betroffenen Personen beruht.[50]

Im Ergebnis ist es damit grundsätzlich möglich, eine Verarbeitung personenbezogener Daten auf berechtigte Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f) DS-GVO zu stützen. Ob die Interessen der Datensammler und Entwickler von KI-Modellen mit Blick auf den konkreten Datensatz aber überwiegen, ist eine Frage des Einzelfalls und mit Rechtsunsicherheit verbunden. Verantwortliche Stellen sollten vor diesem Hintergrund genau prüfen, welche Daten erfasst und zum anschließenden Training verwendet werden. Soweit möglich, sollten die verschiedenen Arten von Daten und Betroffenen in Fallgruppen zusammengefasst werden. Es sollten dann jene Fallgruppen identifiziert werden, bei denen von einem Überwiegen der eigenen Interessen ausgegangen wird und die geplanten Verarbeitungsvorgänge auf diese Fallgruppen beschränkt werden. Dieser Prozess sollte entsprechend dokumentiert werden (vgl. Art. 5 Abs. 2 DS-GVO).

IV. Transparenzpflichten bei der Verwendung KI-generierter Inhalte

Die Nutzung Künstlicher Intelligenz bei der Erstellung und Bearbeitung von Audio-, Bild-, Video- und Textinhalten hat in

35 Paal, ZfDR 2024, 129, 148.

36 Paal, ZfDR 2024, 129, 148; LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 14.

37 LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 14.

38 Dieker, ZD 2024, 132, 133.

39 Vgl. LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 15; Dieker ZD 2024, 132, 134.

40 Vgl. dazu ausführlich EuGH, Urteil v. 04.07.2023, Az. C-252/21, GRUR 2023, 1131, 1139.

41 Paal, ZfDR 2024, 129, 149.

42 Paal, ZfDR 2024, 129, 150; Dieker, ZD 2024, 132, 134.

43 LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 22.

44 Vgl. Paal, ZfDR 2024, 129, 150.

45 Dieker, ZD 2024, 132, 134.

46 Dieker ZD 2024, 132, 134.

47 Dieker ZD 2024, 132, 134.

48 Dieker ZD 2024, 132 (134); vgl. LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 23.

49 LfDI BW, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Vers. 2, S. 23.

50 Vgl. Hessel/Dillschneider, RDi 2023, 458 (461); Franke, RDi 2023, 565, 567.

den letzten Jahren stark zugenommen. Mit der KI-VO wurden klare Transparenzpflichten für KI-erzeugte oder -manipulierte Inhalte eingeführt. Die Pflichten richten sich gemäß Art. 50 Abs. 2 KI-VO an Anbieter sowie gemäß Art. 50 Abs. 4 KI-VO an Betreiber von KI-Systemen, wobei im Folgenden nur die für Betreiber geltenden Transparenzvorgaben dargestellt werden. Ziel des Art. 50 Abs. 4 KI-VO ist es, eine Irreführung der Öffentlichkeit zu verhindern und die Nachvollziehbarkeit digitaler Inhalte zu gewährleisten.[51]

1. Aktueller Regelungsrahmen bei der Kennzeichnung von KI-generierten Inhalten

Bis zum Inkrafttreten der KI-VO gab es auf europäischer Ebene keine einheitlichen Vorgaben zur Kennzeichnung von Inhalten, die mit KI erstellt oder verändert (nachfolgend: „KI-generiert") wurden. Einzelne nationale Vorschriften, freiwillige Verpflichtungen bestimmter Branchen oder Vorgaben von Plattformen bieten lediglich punktuelle Ansätze. Dies führt zu einer mangelnden Transparenz, die besonders im Zusammenhang mit täuschend echten KI-generierten Inhalten, wie etwa Deepfakes, problematisch ist. Eine Studie zeigt, dass allein im Jahr 2023 über 95.000 Deepfake-Videos online verfügbar waren, von denen ein Großteil für die Verbreitung manipulativer oder schädlicher Inhalte genutzt wurde.[52] Die Dunkelziffer dürfte deutlich größer sein. Die mittlerweile einfache Zugänglichkeit solcher Technologien verschärft die damit verbundenen Risiken.[53]

2. Kennzeichnungspflichten bei Deepfakes

Wenn Bild-, Ton- oder Videoinhalte künstlich erzeugt oder manipuliert wurden und diese zugleich Deepfakes darstellen, muss der Betreiber dies gemäß Art. 50 Abs. 4 UAbs. 1 S. 1 KI-VO offenlegen. Voraussetzung für die Annahme einer solchen Kennzeichnungspflicht ist zunächst, dass die Erzeugung oder Manipulation durch ein KI-System i.S.d. Art. 3 Nr. 1 KI-VO erfolgt. Einfache Bildbearbeitungsprogramme, die beispielsweise Lichtverhältnisse optimieren, ohne KI-Funktionalitäten nach der Legaldefinition zu enthalten, unterliegen daher von vornherein nicht den Kennzeichnungspflichten nach Art. 50 KI-VO.[54]

Unterstellt man das Vorliegen eines entsprechenden KI-Systems, muss dieses System wiederum Bild-, Ton- oder Videoinhalte erzeugen oder manipulieren. Ein „Erzeugen" im Sinne der Norm liegt vor, wenn ein Medieninhalt künstlich erstellt wird, beispielsweise durch den Einsatz von KI-basierten Bildgeneratoren.[55] Eine „Manipulation" liegt vor, wenn ein ursprünglich authentischer Medieninhalt nachträglich gezielt verändert wird, etwa durch Technologien wie dem audiovisuellen „Gesichtertausch".[56]

Die so erzeugten oder manipulierten Inhalte müssen zudem einen „Deepfake" darstellen. Nach der Definition in Art. 3 Nr. 60 KI-VO bezeichnet ein Deepfake „einen durch KI erzeugten oder manipulierten Bild-, Ton- oder Videoinhalt, der wirklichen Personen, Gegenständen, Orten, Einrichtungen oder Ereignissen ähnelt und einer Person fälschlicherweise als echt oder wahrheitsgemäß erscheinen würde". Ein Deepfake kann damit nur bei Darstellungen vorliegen, die den Eindruck von Authentizität erwecken sollen. Wenn es sich bei dem Inhalt um „Teil eines offensichtlich künstlerischen, kreativen, satirischen, fiktionalen oder analogen Werks oder Programms"[57] handelt, ist die Pflicht zur Kennzeichnung abgeschwächt. Die Kennzeichnungspflicht gilt zudem nicht in den Ausnahmefällen des Art. 50 Abs. 4 UAbs. 2 S. 2 KI-VO, etwa im Bereich der gesetzlich erlaubten Prävention oder Verfolgung von Straftaten.

Zur Veranschaulichung werden im Folgenden drei Beispiele im Kontext des Art. 50 Abs. 4 UAbs. 1 KI-VO beleuchtet. Für diesen Zweck wird unterstellt, dass ein Unternehmen ein Bildbearbeitungsprogramm einsetzt, welches ein KI-System im Sinne der KI-VO darstellt:

Im ersten Beispiel schneidet ein Unternehmen automatisiert Teile eines Bildes in einem Bildbearbeitungsprogramm mit einem „KI-Lasso" aus. Dabei wird das Abbild des Gesichtes eines Beschäftigten unverändert aus der Umgebung herausgelöst und daraus ein Profilbild mit weißem Hintergrund erstellt. Da der Eingriff nicht zu einer vollständigen Neuerstellung eines Bildes führt, sondern eine Änderung des Ursprungsmaterials herbeiführt, kann argumentiert werden, dass keine Erzeugung im Sinne des Art. 50 Abs. 4 UAbs. 1 KI-VO vorliegt. Da ein ursprünglich authentischer Medieninhalt (hier: das Ursprungsfoto) nachträglich verändert wird (hier: durch Änderung des Hintergrunds), könnte aber eine Manipulation vorliegen. Eine Kennzeichnungspflicht erfordert aber zusätzlich, dass es sich um einen Deepfake i.S.d. Art. 3 Nr. 60 KI-VO handelt. Soweit auf dem neu erstellten Foto die auf dem Porträt abgebildete Person unverändert dargestellt ist und durch die Änderung des Hintergrunds der Kontext nicht so verändert wird, dass dem Bild dadurch ein neuer Aussagegehalt zukommt, dürfte kein Deepfake vorliegen und keine Kennzeichnungspflicht bestehen. Etwas anderes könnte anzunehmen sein, wenn das Abbild des Beschäftigten nicht vor einen weißen Hintergrund, sondern vor das Bild eines anderen Ortes gesetzt wird und suggeriert würde, die Person habe sich tatsächlich an dem abgebildeten Ort aufgehalten (etwa bei einer vermeintlichen Vor-Ort-Berichterstattung eines Reporters).

In einem zweiten Beispiel soll eine Anzeige zur Bewerbung des örtlichen Weihnachtsmarktes erstellt werden. Dazu wird ein KI-generiertes Bild von Weihnachtsmarkständen eingefügt, die aus einem Foto eines großen, überregionalen Weihnachtsmarktes herausgelöst und anschließend nahtlos in die Kulisse des regionalen Weihnachtsmarktes integriert wurden. Das Endergebnis ist fotorealistisch und soll den Eindruck vermitteln, dass es sich bei der Darstellung um den diesjährigen örtlichen Weihnachtsmarkt handelt. In diesem Fall wird ein Deepfake i.S.d. Art. 50 Abs. 4 UAbs. 1 KI-VO von einer KI erzeugt. Es besteht eine Kennzeichnungspflicht.

In einem dritten Beispiel sollen Videos und Fotos für virtuelle Welten durch KI erstellt und in einem Computerspiel verwendet werden. Diese Inhalte sind zwar durch eine KI erzeugt. Soweit die virtuelle Welt als fiktiv erkennbar ist und keine real existierenden Orte, Objekte oder Einrichtungen

51 Vgl. ErwG 133 VO 2024/1689.
52 Kumkar/Griesel, KIR 2024, 117, 118.
53 Vgl. Kumkar/Griesel, KIR 2024, 117, 117.
54 Vgl. ErwG 12 VO 2024/1689; Kumkar/Griesel, KIR 2024, 117, 119.
55 Kumkar/Griesel, KIR 2024, 117, 119.
56 Kumkar/Griesel, KIR 2024, 117, 119.
57 Art. 50 Abs. 4 UAbs. 1 S. 3 KI-VO.

abbilden soll, sind die Inhalte bereits nicht geeignet, den Eindruck von Echtheit zu erwecken. Es handelt sich nicht um ein Deepfake, sodass auch keine Kennzeichnungspflicht nach Art. 50 Abs. 4 UAbs. 1 KI-VO besteht.

3. Kennzeichnungspflichten bei Textinhalten

Für KI-generierte Textinhalte kann nach Art. 50 Abs. 4 UAbs. 2 S. 1 KI-VO eine Kennzeichnungspflicht bestehen. Danach müssen „Betreiber eines KI-Systems, das Text erzeugt oder manipuliert, der veröffentlicht wird, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, [...] offenlegen, dass der Text künstlich erzeugt oder manipuliert wurde." Entscheidend bei der Prüfung einer Kennzeichnungspflicht für Texte ist zunächst das Merkmal der „Öffentlichkeit" und die Frage, welche Inhalte „Angelegenheiten des öffentlichen Interesses" betreffen. Die KI-VO konkretisiert dies nicht. Nach allgemeinem Sprachgebrauch ist „Öffentlichkeit" - im Gegensatz zur Privatsphäre - der Bereich, der einem zahlenmäßig nicht überschaubaren Personenkreis zugänglich ist, wie etwa Print- oder soziale Medien. Bei Letzteren kann – zumindest bei großen Plattformen mit zahlreichen Mitgliedern – auch die Plattformöffentlichkeit genügen.[58] Nicht von einer Kennzeichnungspflicht umfasst sind damit Textinhalte, die nur einem beschränkten Personenkreis zugänglich gemacht werden, wie Beiträge im Intranet. Angelegenheiten von öffentlichem Interesse dürften angesichts des bezweckten Schutzes der öffentlichen Meinungsbildung jedenfalls gesellschaftsrelevante Themen zu Politik, Wirtschaft und Kultur sein.[59]

Auch für diese Kennzeichnungspflicht greifen nach Art. 50 Abs. 4 UAbs. 2 S. 2 KI-VO Ausnahmen: „Diese Pflicht gilt nicht, [...] wenn die durch KI erzeugten Inhalte einem Verfahren der menschlichen Überprüfung oder redaktionellen Kontrolle unterzogen wurden und wenn eine natürliche oder juristische Person die redaktionelle Verantwortung für die Veröffentlichung der Inhalte trägt." Ausnahmetatbestände sind aufgrund des gesetzlich festgelegten Regel-Ausnahme-Prinzips grundsätzlich eng auszulegen.[60] Gleichzeitig sollte aus Praxissicht eine ausufernde Kennzeichnungspflicht vermieden werden. Welche Anforderungen an die menschliche Überprüfung oder redaktionelle Kontrolle zu stellen sind, wird in den kommenden Jahren durch Aufsichtsbehörden und Gerichte konkretisiert werden müssen. Nach der hier vertretenen Auffassung ist es ausreichend, dass der KI-generierte Text zumindest kursorisch korrekturgelesen wird. Von einer redaktionellen Verantwortungsübernahme dürfte bei Veröffentlichungen im Internet beispielsweise schon dann ausgegangen werden, wenn ein Hinweis zur Autorenschaft am Artikel angebracht ist.

Zur Veranschaulichung sollen auch hier zwei Beispiele aus der Praxis aufgeführt werden: In einem ersten Beispiel nutzt ein Redakteur einer Tageszeitung ein KI-System, um die Überschrift und eine knappe Zusammenfassung eines Artikels zu politischen Ereignissen, etwa zu anstehenden Neuwahlen, zu erstellen. Die Überschrift und die Zusammenfassung werden seitens der Redaktion überblicksartig auf Plausibilität geprüft. In diesem Fall werden KI-erzeugte Textinhalte verwendet, um die Öffentlichkeit über eine Angelegenheit von öffentlichem Interesse zu informieren. Soweit der Artikel auf der Webseite der Tageszeitung in deren Verantwortung publiziert wird und vor Veröffentlichung einer – wenn auch nur überblicksartigen – menschlichen Prüfung unterzogen wurde, greift nach der hier vertretenen Ansicht die gesetzliche Ausnahme in Art. 50 Abs. 4 UAbs. 2 S. 2 KI-VO. Eine Kennzeichnungspflicht besteht dann nicht.

In einem zweiten Beispiel will ein Unternehmen Produkte in einem Online-Shop mit Beispielstexten bewerben. Diese Beispielstexte werden mittels eines KI-Systems generiert und nicht durch einen Menschen kontrolliert. Da in diesem Beispiel aber keine Angelegenheiten des öffentlichen Interesses betroffen sind, sondern die Veröffentlichung ausschließlich dem kommerziellen Eigeninteresse des Unternehmens dient (hier: anschauliche Darstellung der Produkte im Online-Shop), besteht keine Kennzeichnungspflicht für die Texte nach Art. 50 Abs. 4 UAbs. 2 S. 1 KI-VO.

4. Handlungsempfehlung für die Praxis

Betreiber von KI-Systemen, welche KI-generierte Inhalte nutzen, sollten hierfür klare Abläufe schaffen. Für den Umgang mit KI-generierten Inhalten bieten sich interne Praxisleitfäden an. Beschäftigte, die mit solchen Inhalten umgehen, sollten zudem für die soeben dargestellten, zentralen Weichenstellungen bei der Ermittlung einer Kennzeichnungspflicht sensibilisiert werden. Die Voraussetzungen, insbesondere das Merkmal des Deepfakes, sind anschaulich zu erläutern. Bei Texten ist es erforderlich, die Veröffentlichungszwecke in die Prüfung miteinzubeziehen und Vorgaben für eine menschliche Prüfung zu formulieren. Zuletzt sollte ein Prozess implementiert werden, um in Grenzfällen die Kennzeichnungspflichten im Einzelfall zu bewerten.

V. Fazit

Der nach der KI-VO einzuhaltende Pflichtenkatalog richtet sich insbesondere nach der initialen Einordnung als Anbieter oder Betreiber. Während Anbieter Adressaten zahlreicher Verpflichtungen in der KI-VO sind, ist das Pflichtenprogramm für Betreiber recht überschaubar. Im Regelfall werden Unternehmen, die KI-Systeme nur als Arbeitserleichterung einsetzen wollen, die Einordnung als Anbieter vermeiden wollen. Dies setzt voraus, dass sie sich intensiv mit dem Rollenverständnis der KI-VO auseinandersetzen. Werden fremde KI-Systeme individualisiert, sollte vorab geprüft werden, ob dies Einfluss auf die Rollenzuweisung nach der KI-VO hat. Entsprechendes gilt beim Anbringen eines Namens oder einer Handelsmarke sowie bei Veränderungen oder Zweckänderungen eines KI-Systems.

Sofern KI-Modelle mit durch Scraping oder Crawling erlangten Daten trainiert werden, werden regelmäßig personenbezogene Daten verarbeitet. Dann ist nach dem Erlaubnisvorbehalt der DS-GVO eine Rechtsgrundlage für die Datenverarbeitung erforderlich. Eine Einwilligung oder die gesetzliche Rechtsgrundlage der Erforderlich-

58 Vgl. Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 113.

59 Vgl. auch: Wendehorst, in: Martini/Wendehorst, KI-VO: Verordnung über die Künstliche Intelligenz, 1. Aufl. 2024, Art. 3 KI-VO Rn. 113.

60 Beispielhaft zum Informationsfreiheitsgesetz: BVerwG, Urteil v. 27.11.2014 – 7 C 20/12, NVwZ 2015, 669, 671.

keit für die Vertragsdurchführung sind im Regelfall keine praktikablen Rechtsgrundlagen. Soweit überwiegende berechtigte Interessen der datenverarbeitenden Stelle herangezogen werden, muss im Einzelfall geprüft und dokumentiert werden, dass deren eigene Interessen tatsächlich überwiegen. Sollten besondere Datenkategorien im Sinne der DS-GVO (etwa Gesundheitsdaten) einbezogen werden, scheidet diese Rechtsgrundlage dagegen aus.

Für KI-generierte Inhalte sieht die KI-VO umfassende Kennzeichnungspflichten vor. Bei Bild-, Ton- und Videoinhalten bestehen derartige Pflichten, soweit die Inhalte durch KI erzeugt oder manipuliert sind und es sich um Deepfakes handelt. Bei KI-generierten Texten besteht eine Kennzeichnungspflicht, soweit der Inhalt durch KI erzeugt oder manipuliert wird und mit den Inhalten die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informiert werden. Für die Kennzeichnungspflichten sieht die KI-VO weitreichende Ausnahmen vor, die in der Praxis eine große Rolle spielen werden. Betreiber von KI-Systemen sollten klare Regeln für Beschäftigte definieren, damit diese die neuen Pflichten und Ausnahmen kennen und die Vorschriften in der Praxis umsetzen können.

Dr. Clemens Birkert
ist Rechtsanwalt und Partner bei OPPENLÄNDER Rechtsanwälte in Stuttgart. Er ist spezialisiert auf Fragen des IT- und Datenschutzrechts sowie der Künstlichen Intelligenz.

David Pfau
ist Geschäftsführer bei conreri und im Herausgeberbeirat der Zeitschrift für Europäisches Daten- und Informationsrecht (EuDIR)

Paula Cipierre, LL.M.

Konzepte zur Umsetzung der rollen- und kontextspezifischen Anforderungen an die KI-Kompetenz gemäß Art. 4 KI-VO

Eine der ersten Vorschriften der EU-KI-Verordnung (KI-VO), die bereits zum 2. Februar 2025 anwendbar wird, ist die der KI-Kompetenz gemäß Art. 4 KI-VO.[1] Demnach müssen alle Unternehmen, die in der EU Künstliche Intelligenz (KI) entwickeln oder betreiben, sicherstellen, dass ihr Personal und alle anderen Personen, die in ihrem Auftrag mit KI hantieren, über ein ausreichendes Maß an KI-Kompetenz verfügen. Der Gesetzgeber definiert KI-Kompetenz als die Fähigkeit, KI-Systeme sachkundig einzusetzen sowie sich der Chancen, Risiken und möglichen Schäden von KI-Systemen bewusst zu sein. Dabei umfasst die Maßgabe der KI-Kompetenz zwei Aspekte: Grundkenntnisse der KI-Kompetenz einerseits und rollen- und kontextspezifisches Wissen andererseits.

Der folgende Aufsatz bietet zunächst einen Überblick über die Grundanforderungen an die KI-Kompetenz, die sich sowohl aus der Maßgabe in Art. 4 als auch der Definition von KI-Kompetenz in Art. 3 Nr. 56 KI-VO ergeben (I.). Nachfolgend geht der Artikel auf die rollen- und kontextspezifischen Anforderungen von Art. 4 KI-VO ein (II.). Anhand einer Fallstudie, in der ein KI-basierter Chatbot im Kundenservice eingesetzt werden soll, wird durchgespielt, auf welche Art und Weise und inwiefern sich die Anforderungen an die KI-Kompetenz je nach Hintergrund und Rolle der Beschäftigten, dem Kontext, in dem KI-Systeme eingesetzt werden und der Perspektive der Betroffenen unterscheiden (III.). Der Aufsatz schließt mit Praxistipps für die Umsetzung (IV.) und einer kurzen Zusammenfassung (V.).

I. Grundkenntnisse der KI-Kompetenz

1. Maßgabe und relevante Definitionen

Laut Art. 4 KI-VO müssen „Anbieter und Betreiber von KI-Systemen [...] Maßnahmen [ergreifen], um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen [...]".

Dabei definiert der Gesetzgeber KI-Kompetenz in Art. 3 Nr. 56 als „die Fähigkeiten, die Kenntnisse und das Verständnis, die es Anbietern, Betreibern und Betroffenen unter Berücksichtigung ihrer jeweiligen Rechte und Pflichten im Rahmen dieser Verordnung ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden".

Ein „Anbieter" ist laut Art. 3 Nr. 3 „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich".

Demgegenüber ist ein „Betreiber" nach Art. 3 Nr. 4 legaldefiniert als „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet".[2]

Betroffene werden in der KI-VO nicht weiter definiert. Allerdings lässt sich aus den ErwGn (ErwG) ableiten, dass hiermit beispielsweise natürliche Personen gemeint sind, deren personenbezogene Daten von KI-Systemen verarbeitet werden (ErwG 10), die mit KI-Systemen interagieren (ErwG 27) oder die von mit Hilfe von KI getroffenen Entscheidungen betroffen sind (ErwG 20).

Zusammenfassend lässt sich festhalten, dass alle Unternehmen, die in der EU KI entwickeln oder betreiben, dafür Sorge zu tragen haben, dass ihre Beschäftigten und andere Personen, die in ihrem Auftrag mit KI-Systemen hantieren, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei KI-Kompetenz definiert wird als die Fähigkeit, sachkundig mit KI-Systemen umzugehen sowie sich der Chancen, Risiken und möglichen Schäden von KI bewusst zu sein.[3]

2. Grundanforderungen der KI-Kompetenz

Aus der Maßgabe und Definition von KI-Kompetenz lassen sich mindestens vier Grundanforderungen an die KI-Kompetenz ableiten.[4]

a) Definition von KI-Systemen

Erstens müssen Beschäftigte dazu imstande sein, KI-Systeme von regulären Softwaresystemen zu unterscheiden. Genau wie bei der Unterscheidung zwischen regulären Daten und personenbezogenen Daten in der EU-Datenschutz-Grundverordnung (DS-GVO), wonach der Begriff des personenbezogenen Datums weitläufig gefasst ist, ist auch die Unterscheidung zwischen Softwaresystemen und KI-Systemen in der KI-VO alles andere als trivial:[5] Beschäftigte müssen mit der Definition von KI-Systemen laut KI-VO vertraut sein, wonach ein KI-System legaldefiniert ist als „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus

1 Für einen Überblick der verschiedenen Umsetzungsfristen der KI-VO, s. Schwarmann/Keber/Zenner-Schwartmann/Kurth, KI-VO: Leitfaden für die Praxis, Teil I, Kap. 1 Rn. 1 ff.

2 Für weiterführende Erläuterung zur Unterscheidung zwischen Anbietern und Betreibern, s. Schwartmann/Keber/Zenner-Keber/Zenner, KI-VO: Leitfaden für die Praxis, Teil II, Kap. 1 Rn. 19 ff.

3 Zu den Anforderungen an KI-Kompetenz, s. auch Wendt/Wendt, Das neue Recht der Künstlichen Intelligenz, § 5 Rn. 46 ff.

4 Für eine ausführliche Behandlung der Grundanforderungen an die KI-Kompetenz, s. Cipierre, RDV 5/2024.

5 Zum Verhältnis zwischen KI-VO und DS-GVO, s. Schwartmann/Keber/Zenner-Schwartmann/Köhler, KI-VO: Leitfaden für die Praxis, Teil II Kap. 3 Rn. 3 ff.

den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können". Das einzige belastbare Ausschlusskriterium findet sich in ErwG 12, wonach Softwaresysteme nicht als KI-Systeme gelten, sofern sie auf „ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruhen". Gleichzeitig werden die meisten Softwaresysteme zunehmend KI-Komponenten enthalten. Arbeitgeber sind daher wohlberaten, ein laufend aktualisiertes KI-Inventar zu führen, um den Überblick über den Einsatz von KI-Systemen im Unternehmen zu behalten und Beschäftigte bei der Unterscheidung zwischen regulären Softwaresystemen und KI-Systemen zu unterstützen.

b) Rolle von Unternehmen mit Hinblick auf KI-Systeme

Zweitens sollten Beschäftigte die Rolle ihres Unternehmens mit Hinblick auf das jeweilige KI-System verstehen, insbesondere ob das Unternehmen als Anbieter oder Betreiber des KI-Systems fungiert. Wie bereits zu Anfang des Aufsatzes erwähnt, gilt laut Art. 3 Nr. 3 KI-VO eine Person oder Organisation als Anbieter eines KI-Systems, sofern sie „ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich". Demgegenüber ist eine Person oder Organisation Betreiber eines KI-Systems, wenn sie „ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet". In anderen Worten, Anbieter von KI-Systemen entwickeln KI-Systeme selber und kontrollieren daher auch die Daten, auf denen die KI-Systeme unterliegenden KI-Modelle trainiert werden. Betreiber hingegen kaufen KI-Systeme lediglich ein, oder lizenzieren diese von Anbietern, ohne die KI-Systeme dabei aber selber zu entwickeln oder maßgeblich weiterzuentwickeln. Dementsprechend unterscheiden sich auch die Anforderungen an die KI-Kompetenz von Anbietern und Betreibern von KI-Systemen, da Anbieter mitunter eine deutlich höhere technische KI-Kompetenz von Beschäftigten ausweisen müssen, insbesondere mit Hinblick auf die angemessene Auswahl von Trainingsdaten und KI-Modellen. Gleichzeitig sind die Grenzen zwischen Anbietern und Betreibern von KI-Systemen fließend: Sofern eine Organisation ein KI-System unter ihrem eigenen Namen oder seiner Handelsmarke in Verkehr bringt, gilt diese nicht mehr als Betreiber sondern als Anbieter des Systems. Sich dessen bewusst zu sein sollte ebenso Teil der grundlegenden KI-Kompetenz sowohl von Beschäftigten als auch Organisationen sein, die KI-Systeme betreiben.

c) Bewusstsein für die Chancen, Risiken und mögliche Schäden von KI

Drittens müssen Beschäftigte ein Bewusstsein entwickeln für die Chancen, Risiken und möglichen Schäden, die mit dem Einsatz von KI-Systemen einhergehen. Dies könnte als das Herzstück der KI-Kompetenz gemäß KI-Verordnung bezeichnet werden, da es hierbei nicht nur darum geht KI-Systeme sachkundig, sondern auch verantwortungsbewusst einzusetzen. Die Zentralität dieser Maßgabe wird in ErwG 20 hervorgehoben, wonach KI-Kompetenz „allen einschlägigen Akteuren in der KI-Wertschöpfungskette die Kenntnisse vermitteln [sollte], die erforderlich sind, um die angemessene Einhaltung und die ordnungsgemäße Durchsetzung der Verordnung sicherzustellen".

d) Unterscheidung von Hochrisiko-KI-Systemen

Viertens und letztens sollten Beschäftigte wissen, wann immer sie mit Hochrisiko-KI-Systemen hantieren. Nicht nur sind mit der Entwicklung und dem Betrieb von Hochrisiko-KI-Systemen besonders hohe Auflagen verbunden.[6] Auch hebt die KI-VO im Hinblick auf Hochrisiko-KI-Systeme die besondere Bedeutung von KI-Kompetenz hervor. So sind Betreiber von Hochrisiko-KI-Systemen laut Art. 26 Nr. 2 KI-VO gefragt, „natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht [über Hochrisiko-KI-Systeme zu übertragen]" und ihnen „die erforderliche Unterstützung zukommen" zu lassen. Darüber hinaus betont der Gesetzgeber in ErwG 91, dass Betreiber von Hochrisiko-KI-Systemen sicherzustellen haben, „dass die Personen, denen die Umsetzung der Betriebsanleitungen und die menschliche Aufsicht gemäß dieser Verordnung übertragen wurde, über die erforderliche Kompetenz verfügen, insbesondere über ein angemessenes Niveau an KI-Kompetenz, Schulung und Befugnis, um diese Aufgaben ordnungsgemäß zu erfüllen".

3. Zwischenfazit

Alle Organisationen, die KI-Systeme in der EU anbieten oder betreiben, müssen dafür Sorge tragen, dass ihre Beschäftigten und alle Personen, die in ihrem Auftrag mit KI-Systemen hantieren, über ein ausreichendes Maß an KI-Kompetenz verfügen. Der Gesetzgeber definiert KI-Kompetenz als die Fähigkeit, KI-Systeme sachkundig einzusetzen und sich ihrer Chancen, Risiken und möglichen Schäden bewusst zu sein. Dabei umfassen die Grundanforderungen an die KI-Kompetenz gemäß Art. 4 KI-VO mindestens ein Verständnis 1) der Definition von KI-Systemen, 2) der Rolle, die eine Organisation im Hinblick auf das KI-System einnehmen kann und insbesondere ob die Organisation als Anbieter oder Betreiber des KI-Systems fungiert, 3) der Chancen, Risiken und möglichen Schäden, die mit der Entwicklung und Implementierung von KI-Systemen einhergehen sowie 4) der Unterscheidung zwischen regulären KI-Systemen und Hochrisiko-KI-Systemen gemäß KI-VO.

II. Rollen- und kontextspezifische Anforderungen

Über die Grundkenntnisse hinaus stellt der Gesetzgeber rollen- und kontextspezifische Anforderungen an die KI-Kompetenz. So verlangt Art. 4 KI-VO, dass Beschäftigte nicht nur über ein ausreichendes Maß an KI-Kompetenz verfügen, sondern auch, dass dabei „ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind". In anderen Worten, was KI-Kompetenz in der Praxis bedeutet, ist

6 S. zu den Pflichten von Anbietern und Betreibern von Hochrisiko-KI-Systemen weiterführend Schwarmann/Keber/Zenner-Kremer/Haar, KI-VO: Leitfaden für die Praxis, Teil II, Kap. 1 Rn. 364 ff.

kontextspezifisch und ist insbesondere abhängig vom Hintergrund der Beschäftigten und dem Kontext, im dem die KI-Systeme eingesetzt werden. Darüber hinaus muss auch die Perspektive der von KI-Systemen Betroffenen in Erwägung gezogen werden. Was bedeutet dies in der Praxis?

1. Hintergrund der Beschäftigten

Art. 4 KI-VO betont, dass bei der Vermittlung von KI-Kompetenz die technischen Kenntnisse, die Erfahrung, die Ausbildung sowie die Schulung von Beschäftigten in Betracht gezogen werden müssen. Dies macht insofern Sinn, als dass bei Beschäftigten mit einem technischen Hintergrund zumindest zu vermuten ist, dass diese bereits über ein besseres Grundverständnis der Funktionsweise von Softwaresystemen verfügen und dementsprechend auch von Hause aus kompetenter mit KI-Systemen umgehen können. Gleichzeitig gehen mit technischen Rollen oft auch höhere Ansprüche an die KI-Kompetenz einher, beispielsweise wenn Beschäftigte KI-Systeme selbst von Grund auf entwickeln oder weiterentwickeln.

2. Kontext der KI-Systeme

Der Kontext, in dem KI-Systeme eingesetzt werden, ist insbesondere für eine Beurteilung der Chancen, Risiken und möglichen Schäden, die mit dem Einsatz von KI-Systemen einhergehen, relevant. Sofern es sich bei einem KI-System um ein Hochrisiko-KI-System gemäß KI-VO handelt, so gehen mit dessen Entwicklung und Inbetriebnahme per Definition höhere Risiken für die Grundrechte, die Sicherheit oder die Gesundheit von Betroffenen einher. Dementsprechend gewichtiger sind die Anforderungen an die KI-Kompetenz. Eine kontextspezifische Risikoanalyse ist aber auch über Hochrisiko-KI-Systeme hinaus unabdingbar: Sofern beispielsweise KI-Systeme mit allgemeinem Verwendungszweck (engl.: General-Purpose Artificial Intelligence Systems, kurz: GPAIS) zum Einsatz kommen, erschließt sich ihr Risiko fast ausschließlich aus dem Kontext ihrer Anwendung.[7]

3. Perspektive der Betroffenen

Über den Hintergrund von Beschäftigten und den Kontext, in dem ein KI-System eingesetzt werden soll, hinaus, verlangt Art. 4 KI-VO, dass Anbieter und Betreiber sich auch in die Rolle derjeniger versetzen, die von der Entwicklung oder dem Einsatz von KI-Systemen betroffen sind. Damit verfolgt KI-Kompetenz gemäß Art. 4 KI-VO einen ähnlichen Ansatz wie Datenschutz-Folgenabschätzungen (DSFAs) in Art. 35 DS-GVO. Auch bei letzterer sind Verantwortliche für die Datenverarbeitung in ihrer Risikobeurteilung gefragt, den Standpunkt der Personen einzunehmen, deren Daten sie zu verarbeiten planen. Die entsprechende Anforderung in der KI-VO könnte man daher auch als „Empathieklausel" beschreiben und verlangt zumindest insofern ein Umdenken von Beschäftigten, als dass diese nicht nur die betrieblichen Interessen des Arbeitgebers im Auge behalten, sondern sich auch in die Lage der von KI-Systemen betroffenen Personen versetzen müssen.

III. Fallstudie: KI im Kundenservice

Was ein rollen- und kontextgerechter Umgang mit KI-Kompetenz bedeutet, wird im Folgenden anhand einer Fallstudie illustriert, in der ein Unternehmen einen KI-basierten Chatbot einsetzen möchte, um den Kundenservice zu verbessern. Diese Fallstudie wird zunächst aus Perspektive der Grundanforderungen an die KI-Kompetenz analysiert: Welche Chancen, Risiken und mögliche Schäden gehen mit der Entwicklung und Implementierung des KI-basierten Chatbots einher? In einem Folgeschritt werden aus der Analyse rollen- und kontextspezifische Anforderungen an die KI-Kompetenz abgeleitet.

1. Chancen, Risiken und mögliche Schäden von KI

Eine Chance, die das Unternehmen mit dem Einsatz des KI-basierten Chatbots verbindet, ist die Verfügbarkeit den Kundenservice zu erhöhen, da der KI-basierte Chatbot ganzjährig 24 Stunden am Tag erreichbar wäre. Darüber hinaus könnte der KI-basierte Chatbot, je mehr er mit denselben Kunden interagiert, deren individuelle Präferenzen immer besser „kennenlernen" und ihnen so einen individuelleren Service bieten.

Ein Risiko, was mit dem Einsatz des KI-basierten Chatbots einhergeht, ist, dass der Chatbot Kundenanfragen falsch oder unangemessen beantwortet, beispielsweise Rabatte anbietet, die das Unternehmen gar nicht machen wollte, oder sich in einem Gespräch auf Themen einlässt, die für den geschäftlichen Austausch belanglos sind.

Mögliche Schäden umfassen, dass Kunden mit Falschinformationen ausgestattet werden oder in Gespräche mit dem Chatbot involviert werden, die unangemessen oder gar beleidigend sind. Dies wiederum könnte dem Ruf und der Marke des Unternehmens schaden und schlimmstenfalls zu Haftungsansprüchen führen.

2. Rollen- und kontextspezifische Anforderungen

Welche rollen- und kontextspezifischen Anforderungen an die KI-Kompetenz ergeben sich aus diesem Szenario? Dies kommt unter anderem darauf an, ob das Unternehmen als Anbieter oder Betreiber des KI-Systems fungiert.

Sollte das Unternehmen als Anbieter des KI-Systems agieren, so müssen die Hintergründe und Rollen der Beschäftigten angemessen für den gesamten Lebenszyklus eines KI-Systems sein. Einige Beschäftigte werden betriebswirtschaftliche Kompetenzen aufweisen müssen, z.B. die Fähigkeit, das spezifische Anwendungsproblem zu definieren, welches das KI-System lösen soll, und Erfolgskriterien festzulegen. Ebenso werden aber auch Beschäftigte mit technischen Kenntnissen gebraucht, z.B. der Statistik und Data Science sowie des maschinellen Lernens, um zu bestimmen, welche Daten erforderlich und welche KI-Modelle geeignet sind, um das KI-System zu bauen. Darüber hinaus muss bei der Entwicklung des KI-Systems der Kontext in Betracht gezogen werden, in dem das KI-System eingesetzt werden soll. Wie konkret soll das KI-System, in dem Fall ein KI-basierter Chatbot für den Kundenservice, auf eine besondere Branche, z.B. den Textilfachhandel, zugeschnitten sein? Je unspezifischer das KI-System ist, desto flexibler ist der Anwendungsbereich. Gleichzeitig erhöht sich damit aber auch das Risiko, dass das KI-System nicht konkret genug oder auch unangemessen auf Kundenanfragen reagiert.

Der Anbieter des KI-Systems könnte sich dafür entscheiden, den Anwendungsbereich des KI-basierten Chatbots bewusst offenzuhalten, gegebenenfalls gar ein GPAI-System auf den

7 Zur Zweckbestimmung eines GPAI-Systems, s. auch Schwartmann/Zenner, EuDIR 1/2025.

Markt zu bringen. In dem Fall obliegt es dem Betreiber, das KI-System nach zu trainieren, also ein sogenanntes „Finetuning" vorzunehmen, um einen kontextgerechten Einsatz zu gewährleisten. Sofern der Betreiber des KI-Systems das KI-System dann aber unter seinem eigenen Namen oder Handelsmarke in Betrieb nimmt wird er laut Art. 3 Nr. 3 KI-VO selbst zum Anbieter des Systems. Darüber hinaus könnte der Betreiber laut Art. 25 Nr. 1 lit. c) zum Anbieter eines Hochrisiko-KI-Systems mutieren, sofern er die Zweckbestimmung des KI-Systems so verändert, „dass das betreffende KI-System zu einem Hochrisiko-KI-System im Sinne von Artikel 6 wird".[8] Sich des fließenden Übergangs zwischen Anbietern und Betreibern von KI-Systemen bewusst zu sein, sollte, wie oben bereits erwähnt, aus genau diesem Grunde Teil der Grundkenntnisse der KI-Kompetenz sein.

Zu guter Letzt gehört zu den rollen- und kontextspezifischen Anforderungen an die KI-Kompetenz auch die Pflicht, die Perspektive der Betroffenen in Betracht zu ziehen: Welche Erwartungen und Bedürfnisse haben die Kunden? Wie kann anbieterseitig sichergestellt werden, dass auch diejenigen, die mit dem KI-System interagieren, dies sachkundig tun und sich der Chancen, Risiken und möglichen Schäden des KI-Systems bewusst sind? Natürlich können Anbieter und Betreiber von KI-Systemen Dritte, die mit ihren KI-Systemen interagieren, nur eingeschränkt schulen. Allerdings sollten sie, im Einklang mit den Bestimmungen aus Art. 50 KI-VO, Nutzerinnen und Nutzern gegenüber zumindest transparent machen, dass es sich jeweils um ein KI-System handelt und die Funktionsweise sowie Limitationen des KI-Systems in einer das KI-System begleitenden Gebrauchsanleitung erläutern. Auf diese Art und Weise wird auch die KI-Kompetenz derjenigen, die mit dem KI-System interagieren, gestärkt.

IV. Praxistipps für die Umsetzung

KI-Kompetenz gemäß Art. 4 KI-VO ist eine umfassende Schulungsanforderung, die sowohl der Vermittlung von Grundkenntnissen als auch einer rollen- und kontextspezifischen Sensibilisierung von Beschäftigten bedarf. Diese Anforderung wird bereits zum 2. Februar 2025 anwendbar.

Um die Umsetzung von Art. 4 KI-VO handhabbar zu halten, bietet sich ein mehrstufiger Ansatz an: Zunächst sollten Unternehmen in eine Basisschulung investieren, welche die Grundlagen der KI-Kompetenz vermittelt und auf alle Beschäftigten ausgerichtet ist. Diese Schulung sollte prägnant sein, sowohl auf ein nicht-technisches als auch nicht-juristisches Publikum ausgerichtet sein und primär darauf abzielen, ein Grundverständnis zu schaffen 1) von KI-Systemen, so wie sie die KI-VO definiert, 2) der Rolle, die ein Unternehmen im Hinblick auf ein KI-System einnehmen kann, 3) der Chancen, Risiken und möglichen Schäden, die mit KI-Systemen einhergehen sowie 4) der Unterscheidung zwischen regulären KI-Systemen und Hochrisiko-KI-Systemen.

In einem nächsten Schritt sollten sich Unternehmen Gedanken darüber machen, inwiefern und in welchen Anwendungsbereichen rollen- und kontextspezifische Schulungen angeboten werden sollten. Im Einklang mit dem risikobasierten Ansatz der KI-VO empfiehlt sich dabei, weiterführende Schulungen für Personengruppen zu priorisieren, die im Auftrag des Unternehmens mit Hochrisiko-KI-Systemen hantieren, nicht zuletzt, weil mit einem sachfremden Einsatz von Hochrisiko-KI-Systemen auch das Risiko besonders gravierender Schäden und entsprechend hoher Strafzahlungen einhergeht. Darüber hinaus sollten Unternehmen überlegen, ob sie weiterführende Schulungen für bestimmte Rollenprofile anbieten sollten, insbesondere für Softwareentwickler und Data Scientists, die nicht nur ein rechtliches und normatives, sondern auch ein technisches Verständnis der Anforderungen haben sollten, die mit der verantwortungsvollen Entwicklung und Implementierung von KI-Systemen einhergeht.[9]

In Ermangelung weiterer Richtlinien vom Gesetzgeber empfiehlt sich, Schulungen der KI-Kompetenz Teil der jährlichen Compliance-Schulungen werden zu lassen, die Unternehmen bereits durchführen müssen, um beispielsweise die gesetzlichen Anforderungen an Datenschutz und Informationssicherheit zu erfüllen. Dies wiederum sollte die Bereitstellung von Nachweisen erleichtern, sollte die Aufsichtsbehörde danach fragen. Zwar sind keine direkten Strafen für die Nichteinhaltung von Art. 4 KI-VO aufgeführt. Doch Unternehmen sollten sich darüber im Klaren sein, dass bei Schäden, die durch eine fehlerhafte oder gar fahrlässige Entwicklung und Implementierung von KI-Systemen entstehen, eine Kausalitätsvermutung zwischen der fehlenden Schulung und dem entstandenen Schaden aufgestellt werden kann.[10] Gleichzeitig wird gerade durch die Schulung von Beschäftigen im sachkundigen und verantwortungsvollen Umgang mit KI-Systemen auch das Risiko von Fehlverhalten minimiert. Eine Investition in die KI-Kompetenz ist daher durchaus nicht nur aus regulatorischer, sondern auch aus geschäftlicher Perspektive von Vorteil.

V. Zusammenfassung

Art. 4 KI-VO ist eine umfassende Schulungsanforderung, die zum 2. Februar 2025 in Kraft tritt. Dabei verlangt Art. 4 KI-VO sowohl den sachkundigen Umgang mit KI-Systemen als auch ein Grundverständnis ihrer Chancen, Risiken und möglichen Schäden. Ob jemand KI-kompetent ist, erschließt sich letztlich aus der Anwendung: Denn die Anforderungen an die KI-Kompetenz variieren, je nach Hintergrund der Beschäftigten, dem Kontext, in dem KI-Systeme eingesetzt werden sowie die Art und Weise, auf die Dritte von KI-Systemen betroffen sind. Die KI-VO trägt diesem Umstand Rechnung, indem sie nicht nur Grundkenntnisse der KI-Kompetenz fordert, sondern auch rollen- und kontextspezifische Weiterbildungen. Eine Investition in die KI-Kompetenz von Beschäftigten lohnt sich dabei nicht aus regulatorischer, sondern auch geschäftlicher Perspektive, da KI-Systeme nur dann erfolgreich entwickelt und implementiert werden können, sofern Beschäftigte sachkundig und im Einklang mit rechtlichen und ethischen Anforderungen mit ihnen umzugehen wissen.

Paula Cipierre, LL.M.
ist Director of Data Ethics & Innovation bei der ada Learning GmbH.

8 Zur Zweckänderung im Sinne von Art. 25 Abs. 1 lit. c) KI-VO, s. auch Schwartmann/Zenner, EuDIR 1/2025.

9 Zur Operationalisierung von KI-Kompetenz, s. auch Hense/Mustać, AI Act kompakt: Compliance, Management & Use Cases in der Unternehmenspraxis, Teil I, Kap. 1 Abschn. 1 Abs. e) UAbs. (1) ff.

10 Zur Rechtsfolge bei Nichtbeachtung, s. auch Fleck, KIR 3/2024.

Ass. iur. Priska Katharina Büttel/Ass. iur. Nicolas Ziegler

Wirtschaftsschutz durch Cybersicherheitsregulierung*

Eine Analyse der deutschen Umsetzung der NIS-2-RL durch das NIS2UmsuCG

Mit der Richtlinie (EU) 2022/2555 vom 14.12.2022 (NIS-2-RL) hat die Europäische Union einen Kernbestandteil des europäischen Cybersicherheitsrechts neu aufgelegt. Während die Vorgängerregulierung (RL (EU) 2016/1148) noch auf den Schutz Kritischer Infrastrukturen fokussiert war, weitet die NIS-2-Richtlinie (NIS-2-RL) den Anwendungsbereich auf einen umfassenderen Wirtschaftsschutz aus. Die deutsche Umsetzung im BSIG durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) gestaltet sich äußert kompliziert, verwirrend und langwierig. Dieser Beitrag will einen Überblick der zentralen Inhalte über den gesamten Gesetzgebungsprozess hinweg verschaffen und die fachliche Diskussion schlaglichtartig beleuchten.

I. Die NIS-2-Richtlinie

1. Reformbedarf der Sicherheit von Netz- und Informationssystemen

Als Vorläufer der NIS-2-RL galt von 2016 bis Ende 2022 die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL).[1] In der Cybersicherheitsstrategie der EU-Kommission von 2020 kündigte diese aufgrund der seit 2016 gestiegenen Bedrohungslage im Cyberraum an, die NIS-RL überarbeiten zu wollen.[2] Neben der allgemeinen Erhöhung des Cybersicherheitsniveaus war das Ziel vor allem eine Harmonisierung des Anwendungsbereichs, da Art. 5 NIS-RL den Anwendungsbereich im Wesentlichen einer Ermittlung wesentlicher Dienste durch die Mitgliedstaaten überlassen hatte, was zu einem Flickenteppich[3] an Cybersicherheitsregulierung in den Mitgliedstaaten geführt hat.[4]

2. Die NIS-2-RL im Kontext europäischer Cybersicherheitsregulierung

Auf Basis der Cybersicherheitsstrategie der Union von 2020 hat sich in den letzten Jahren zunehmend ein europäisches Cybersicherheitsrecht herausgebildet. Dies soll nicht der Ort für eine Systematisierung oder einen Gesamtüberblick sein, aber an einem Vergleich zu zwei weiteren Rechtsakten der vorigen Jahre lässt sich das Regulierungskonzept der NIS-2-RL verdeutlichen: Gemeinsam mit der Richtlinie über die Resilienz kritischer Einrichtungen (CER-RL)[5] regelt die NIS-2-RL ganze Unternehmen und Einrichtungen. Die CER-RL regelt dabei die physische, die NIS-2-RL die digitale Seite der Sicherheit. Dazu im Kontrast steht der Cyber Resilience Act (CRA),[6] der im Wege eines produktbezogenen Ansatzes Produkte mit digitalen Elementen reguliert.[7]

II. Überblick zum Gesetzgebungsverfahren des NIS2UmsuCG

Als Richtlinie muss die NIS-2-RL nach Art. 288 Abs. 3 AEUV in deutsches Recht umgesetzt werden. Nach Art. 41 Abs. 1 NIS-2-RL hatte dies bis zum 17.10.2024 zu erfolgen. Die deutsche Umsetzung soll mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) erfolgen.

1. Entwurfsfassungen und Diskussionspapiere

Vor dem finalen Regierungsentwurf zirkulierten zahlreiche Varianten von Referentenentwürfen des BMI und weitere Diskussionspapiere zur vorgelagerten Verbändeanhörung. Eine erste, den Referentenentwurf vorbereitende Synopse mit Stand vom 03.04.2023 wurde im Frühjahr 2023 geleakt.[8] Ein erster Referentenentwurf lag am 03.07.2023 vor, ehe am 27.09.2023 ein Diskussionspapier mit den wirtschaftsbezogenen Regelungen für eine vorgezogene Verbändeanhörung veröffentlicht wurde. Hierbei kam es bereits zu zahlreichen entscheidenden Änderungen. Ein erster offiziell veröffentlichter Referentenentwurf datiert auf den 07.05.2024.[9] Am 03.06.2024 fand im BMI eine offizielle Verbändeanhörung statt, woraufhin Referentenentwürfe vom 24.06. und 19.07.2024 mit jeweils nur geringfügigen Änderungen folgten. Der Beschluss des Regierungsentwurfs erfolgte am 24.07.2024 im Bundeskabinett[10] und wurde am 02.10.2024 als Bundestagsdrucksache veröffentlicht.[11]

* Der Aufsatz baut auf den Vortrag des Autoren Ziegler auf der 48. DAFTA am 15.11.2024 auf. Sämtliche Links wurden zuletzt aufgerufen am 20.12.2024.

1 RL (EU) 2016/1148.

2 JOIN(2020) 18 final, S. 5.

3 Siehe zur deutschen Systematik unter der NIS-RL ausführlich bei Vogel/Ziegler, International Cybersecurity Law Review, 2023 vol. 4, 1 (6 ff.).

4 Vgl. JOIN(2020) 18 final, S. 5. Trotzdem ist die NIS-2-RL nach Art. 5 mindestharmonisierend und lässt weitergehende nationale Regelungen zu.

5 RL (EU) 2022/2557; weiterführend zur RL bei Hornung, CR 2024, 229 ff.

6 VO (EU) 2024/2847.

7 Zum Regulierungskonzept des CRA ausführlich bei Heckmann/Ziegler, in: Heckmann/Paschke CRA, 2025, Art. 1 Rn. 10 ff., 16 ff. (i.E.).

8 Abrufbar unter https://ag.kritis.info/wp-content/uploads/2023/07/NIS2UmsuCG-Referentenentwurf-BMI-CI1-Bearbeitungsstand-03042023.pdf.

9 Abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE.pdf?__blob=publicationFile&v=7.

10 BMI, Pressemitteilung v. 24.07.2024, vgl. auch https://www.bmi.bund.de/nis2.

11 BT-Drs. 20/13184.

Damit befand sich das NIS2UmsuCG außergewöhnlich lange im Entwurfsstadium. Hierfür gibt es im Wesentlichen zwei Gründe: Erstens waren aufgrund des Regelungsgegenstands der Informationssicherheit der Bundesverwaltung in § 29 BSIG-E sämtliche Bundesministerien bei der Ressortabstimmung beteiligt, die sich aufgrund der nicht unerheblichen Haushaltswirksamkeit des Vorhabens verzögerte. Zweitens versuchte die Ampel-Koalition weitere Cybersicherheitsvorhaben des Koalitionsvertrags,[12] das Schwachstellenmanagement[13] und eine Neuaufstellung des BSI als unabhängige(re)[14] Behörde mit einer dem BKA ähnlichen Zentralstellenfunktion im Bund-Länder-Verhältnis mit der Umsetzung der Richtlinie zu verbinden. Über diese Punkte wurde man sich aber bis zuletzt in der AG BSI, einem Gesprächsformat des BMI mit den fachlich befassten Bundestagsabgeordneten der Koalition, nicht einig.[15]

2. Parlamentarisches Verfahren

Das NIS2UmsuCG wurde im Bundestag in erster Lesung am 11.10.2024 beraten. Der Bundestagsausschuss für Inneres hat am 04.11.2024 eine öffentliche Anhörung von Sachverständigen durchgeführt. Alles in allem haben die Sachverständigen viel Kritik vorgebracht.[16] Im Fokus der Kritik standen insbesondere die Regelung zum CISO Bund in § 48 BSIG-E, die großflächigen Ausnahmen vom Anwendungsbereich des § 29 BSIG-E für die Bundesverwaltung,[17] begriffliche Differenzen zur NIS-2-RL, die Verpflichtung zum Einsatz von Systemen zur Angriffserkennung (SzA) in § 31 Abs. 2 BSIG-E, die Ausgestaltung der Risikomanagementpflichten in § 30 BSIG-E sowie die verpasste Gelegenheit zur umfassenden Überarbeitung des Cybersicherheitsrechts inkl. der oben beschriebenen weiteren Cybersicherheitsvorhaben.

Für das weitere parlamentarische Verfahren war der 05. oder 06.12.2024 für die zweite und dritte Lesung im Bundestag geplant, ein Beschluss im Bundesrat am 14.02.2025 und ein Inkrafttreten des Gesetzes im März 2025.[18] Durch den Bruch der Koalition der 20. Legislaturperiode am 06.11.2024 ist unklar, ob das NIS2UmsuCG noch in dieser Legislatur beschlossen wird.[19] Bei Fertigstellung des Manuskripts am 20.12.2024 wurde der Entwurf noch nicht beschlossen. Die Beschlüsse des Innenausschusses im Nachgang der Sachverständigenanhörung flossen am 29.11.2024 noch in eine Formulierungshilfe der Bundesregierung ein.[20]

3. Unionsrechtliche Folgen der verspäteten Umsetzung

Die Umsetzung der NIS-2-RL ist neben Deutschland in einer Mehrheit der Mitgliedstaaten noch nicht erfolgt.[21] Schon recht kurz nach Ablauf der Umsetzungsfrist leitete die EU-Kommission am 28.11.2024 mit dem Versand der Mahnschreiben[22] an insgesamt 23 Mitgliedstaaten, darunter auch Deutschland, nach Art. 258 Abs. 1 Hs. 2 AEUV das Vorverfahren für ein Vertragsverletzungsverfahren ein.[23]

Angesichts der üblichen Verfahrensdauer vor dem EuGH dürfte die Umsetzung noch vor der Verhängung finanzieller Sanktionen nach Art. 260 Abs. 2 AEUV erfolgen. Von wesentlich höherer Relevanz sind die Folgen der Nichtumsetzung für die Betroffenen im Anwendungsbereich der NIS-2-RL. Nach Art. 41 Abs. 1 S. 3 NIS-2-RL ist keine Umsetzungsfrist für die Betroffenen vorgesehen. Sobald die RL in nationales Recht umgesetzt ist, müssen die Pflichten daher befolgt werden. Da die NIS-2-RL im Kern vom Staat durchzusetzende Anforderungen an private Akteure enthält, scheidet eine vom EuGH anerkannte[24] unmittelbare Wirkung der RL aus, da es sich in diesem Fall um eine dem Sanktionsgedanken der unmittelbaren Wirkung widersprechende umgekehrte vertikale Wirkung handeln würde.[25] Die Nichtumsetzung durch die Mitgliedstaaten wirkt daher im Ergebnis wie eine Übergangsfrist. Dies dürfte im Wesentlichen auch der Grund für die europaweit schleppende Umsetzung einerseits und die verhältnismäßig schnelle Einleitung eines Vertragsverletzungsverfahrens andererseits sein.

III. Auswirkungen auf private Akteure

Im Fokus des NIS2UmsuCG liegt die Verpflichtung privater Akteure zu Cybersicherheitsmaßnahmen. Gemäß den Zielen der NIS-2-RL spannt die deutsche Umsetzung einen regulatorischen Schirm über größere Teile der Wirtschaft.

1. Umfassende Überarbeitung des BSIG

Mit dem NIS2UmsuCG bezweckt der Gesetzgeber u.a. die Vorgaben der NIS-2-RL in nationales Recht umzusetzen – eine Herkulesaufgabe eigener Schöpfung, denn allein das BSIG, der Kern des NIS2UmsuCG, wächst von bislang 15 auf 65 Paragrafen. Dementsprechend liegt der Fokus der nachfolgenden Betrachtung auf der Umsetzung der NIS-2-RL durch den BSIG-E.

2. Anwendungsbereich

Der von der NIS-2-RL vorgegebene Anwendungsbereich wird in Art. 3 der RL geregelt. Im Kern wird zwischen wesentlichen Einrichtungen nach Art. 3 Abs. 1 und wichtigen Einrichtungen nach Art. 3 Abs. 2 NIS-2-RL anhand von Sektorenzugehörigkeit und der Überschreitung von Unternehmenskennzahlen wie Bilanz, Umsatz und der Anzahl von Beschäftigten unterschieden. Die konkreten Schwellenwerte orientieren sich nach Art. 2 Abs. 1 UAbs. 1 NIS-2-RL an der Empfehlung der Kommission vom 06.05.2003 betreffend die Definition der Kleinstun-

12 SPD/Bündnis 90/Die Grünen/FDP, Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, S. 16.

13 Zur Notwendigkeit der Erarbeitung BVerfGE 158, 170 (186 ff., Rn. 34 ff.).

14 Siehe zu den Hintergründen der Debatte um die Unabhängigkeit des BSI bei Schallbruch, DuD 2021, 229 ff. und Ziegler, Schrödingers BSI-Präsidentin?, VerfBlog v. 23.08.2023.

15 Vgl. für einen letzten inhaltlichen Stand vor dem Ende der Koalition bei Stiebel, BSI-Unabhängigkeit rückt näher, Tagesspiegel Background Cybersecurity v. 05.09.2024.

16 Vgl. zur gesamten Anhörung https://www.bundestag.de/dokumente/textarchiv/2024/kw45-pa-inneres-cyber-1026336.

17 Siehe hierzu GDD, Stellungnahme zu BT-Drs. 20/13184, S. 4.

18 BMI, Entwurf eines Zeitplans zur Umsetzung der NIS-2-RL, Stand 23.07.2024.

19 Siehe für einen Überblick der Gründe für und gegen eine Verabschiedung bei Rebhan, NIS-2-Gesetz frühestens im Herbst 2025 erwartet, Tagesspiegel Background Cybersecurity v. 28.11.2024.

20 Abrufbar unter https://ag.kritis.info/wp-content/uploads/2024/12/241202-FH-NIS2UmsuCG-mit-Aend.BT-Druck.pdf.

21 Eine vollständige Umsetzung erfolgte (Stand 28.11.2024) bisher nur in Litauen, Italien, Kroatien und Belgien.

22 Siehe zu Funktion und Inhalt bei Karpenstein, in: Grabitz/Hilf/Nettesheim, 83. EL Juli 2024, AEUV Art. 258 Rn. 32 ff.

23 EU-Kommission, Pressemitteilung v. 28.11.2024, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/inf_24_5988.

24 St. Rspr. seit EuGH, Rs. C-33/70, ECLI:EU:C:1970:118 (1213) – S.A.C.E.

25 Vgl. Frenz, Europarecht, 3. Aufl. 2012, Rn. 51.

ternehmen sowie der kleinen und mittleren Unternehmen.[26] Im Vergleich zur NIS-RL erweitert sich der Anwendungsbereich erheblich, was gerade Ziel der Überarbeitung der RL zur Sicherstellung eines funktionsfähigen Binnenmarkts ist.[27] Die Ausdehnung des Anwendungsbereichs auf größere Teile der Wirtschaft erfolgt, „um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind".[28] Mit der Überarbeitung des Rechtsrahmens der Sicherheit von Netz- und Informationssystemen zur NIS-2-RL erfolgt damit eine Entwicklung vom Infrastrukturschutz[29] hin zu einem umfassenderen Wirtschaftsschutz. Dies wird dadurch unterstrichen, dass die noch immer fehlende Fixierung der Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 BSIG vollständig im § 28 Abs. 2 BSIG-E aufgeht.[30]

Die Regelung der Betroffenen von Informationssicherheitspflichten setzt das NIS2UmsuCG in § 28 BSIG-E um. Die Prognosen der dadurch Betroffenen unterstreichen den Charakter des Wirtschaftsschutzes.[31] Der Anwendungsbereich des § 28 BSIG-E kennt im Kern[32] drei Kategorien: Die besonders wichtigen Einrichtungen nach § 28 Abs. 1. BSIG-E, die wichtigen Einrichtungen nach § 28 Abs. 2 BSIG-E sowie die Betreiber kritischer Anlagen nach § 28 Abs. 7 BSIG-E.

a) Besonders wichtige Einrichtungen

§ 28 Abs. 1 BSIG-E regelt die besonders wichtigen Einrichtungen. Insbesondere erfasst sind davon nach § 28 Abs. 1 Nr. 4 BSIG-E natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen entgeltlich Waren oder Dienstleistungen anbieten, die einem der in Anlage 1 zum BSIG-E bestimmten Wirtschaftssektoren zugeordnet werden können und als Großunternehmen mindestens 250 Mitarbeiter beschäftigen oder einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen. Betroffen sind demnach nur Einrichtungen, die über den KMU-Schwellenwerten der Empfehlung 2003/361/EG liegen.

Mit der Bezeichnung „besonders wichtige Einrichtungen" weicht die deutsche Umsetzung von Art. 3 Abs. 1 NIS-2-RL („wesentliche Einrichtungen") ab. Hintergrund der Abweichung dürfte sein, dass man die Unterscheidung von „wesentlichen" und „wichtigen" Einrichtungen in Art. 3 NIS-2-RL irreführend fand.[33] Mit der in § 28 BSIG-E gewählten Unterscheidung besteht zwar keine Verwechslungsgefahr mehr, der zentrale Grund der Neufassung der RL, die europaweite Harmonisierung der Anwendungsbereiche[34] wird damit jedoch konterkariert.[35]

b) Wichtige Einrichtungen

Die wichtigen Einrichtungen werden in § 28 Abs. 2 BSIG-E definiert. Nach § 28 Abs. 2 Nr. 3 BSIG-E sind das v.a. Unternehmen, die einem der Sektoren in Anlage 1 und 2 zum BSIG-E unterfallen und die hinsichtlich der Beschäftigen sowie Jahresumsatz und Bilanzsumme den Kategorien des kleinen oder mittleren Unternehmens im Sinne der KMU-Definition unterfallen.[36] Durch die Verwendung von „oder" zwischen § 28 Abs. 2 Nr. 3 lit. a) und b) BSIG-E weicht die deutsche Umsetzung überschießend vom „und" in Art. 2 im Anhang zur Empfehlung 2003/361/EG ab, wodurch der Anwendungsbereich breiter ausfallen kann.[37]

c) Kritische Anlagen

Neben den durch Art. 3 NIS-2-RL vorgegebenen Kategorien etabliert Art. 28 Abs. 7 BSIG-E eine dritte Kategorie, die Betreiber kritischer Anlagen, die den bisherigen Begriff der Kritischen Infrastrukturen (KRITIS) ersetzen. Unter den Betreibern kritischer Anlagen sind natürliche oder juristische Personen zu verstehen, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausüben. Die kritische Anlage wird in § 2 Nr. 22 BSIG-E als Anlage definiert, die für die Erbringung einer kritischen Dienstleistung erheblich ist. Die kritische Dienstleistung wiederum wird in § 2 Nr. 24 BSIG-E legaldefiniert. Danach handelt es sich um kritische Dienstleistungen, wenn die Allgemeinheit versorgt werden soll, der Ausfall oder eine Beeinträchtigung der Dienstleistung „zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde" und einem der Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung unterfällt. Eine genaue Bestimmung der betroffenen Anlagen erfolgt nach § 56 Abs. 4 BSIG-E im Verordnungswege.

Mit dem Begriff der kritischen Anlagen wird im Ergebnis die bisherige KRITIS-Systematik nach dem BSIG i.V.m. BSI-KritisV neben der neuen, durch die NIS-2-RL vorgegebenen, Systematik fortgesetzt. Hierfür soll die BSI-KritisV fortgelten oder angepasst werden. Entgegen dem bisherigen nationalen Recht[38] fehlt zukünftig eine rechtliche Lösung für das gemeinsame Betreiben kritischer Anlagen durch mehrere juristische Personen.[39] Auch wenn die Betreiber kritischer

26 Empfehlung der Kommission 2003/361/EG vom 06.05.2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl. L 124 v. 20.05.2003, S. 36.

27 Art. 1 Abs. 1 NIS-2-RL; ErwG 3 S. 5 f. und ErwG 6 S. 1 NIS-2-RL.

28 ErwG 6 S. 1 NIS-2-RL.

29 Der nach Art. 170 Abs. 1 AEUV (hier für Telekommunikationsinfrastruktur) ebenfalls ein legitimes Regelungsziel europäischen Rechts darstellt, vgl. Leisterer, Internetsicherheit in Europa, 2018, S. 56 f.

30 Siehe hierzu bei Kipker/Dittrich, MMR 2023, 481 (482); Monschke/Copeland, CCZ 2022, 152.

31 Während der aktuellen KRITIS-Regulierung des BSIG zum Stichtag 30.09.2024 1127 Betreiber mit 2086 Anlagen unterfallen, vgl. https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html, wird eine Erweiterung auf ca. 29.000 Betreiber erwartet, BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 84 sowie BT-Drs. 20/12184, S. 103.

32 Integriert in diese Kategorien adressiert § 28 BSIG-E auch qualifizierte Vertrauensdiensteanbieter, Top Level Domain Registries oder DNS-Diensteanbieter. Auf diese wird im Einzelnen nicht weiter eingegangen. Die Darstellung hier konzentriert sich auf die zugrunde liegende Systematik zur Bestimmung des Anwendungsbereichs. Wesentlicher Unterschied bei den eben genannten Betreibern ist nur, dass für diese die Schwellenwerte der Unternehmenskennzahlen nicht gelten und eine Anwendbarkeit unabhängig davon begründet werden kann. Für Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber öffentlicher Telekommunikationsnetze gelten nur andere Unternehmenskennzahlen, § 28 Abs. 1 Nr. 3 und Abs. 2 Nr. 2 BSIG-E.

33 Schmidt, RDi 2024, 550 (552); Kipker/Dittrich, MMR 2023, 481 (481).

34 Siehe hierzu bereits oben bei I. 1.

35 Kritisch daher bzgl. grenzüberschreitender Sachverhalte, Schmidt, RDi 2024, 550 (552)

36 Art. 2 des Anhangs zu Empfehlung 2003/361/EG.

37 Ob diese Ausweitung jedoch „deutlich" ausfällt, wie von BDI, Stellungnahme zum NSI2UmsuCG v. 31.10.2024, S. 12 vertreten, bleibt fraglich.

38 § 1 Abs. 2 S. 3 BSI-KritisV, neu gef. m.W.v. 01.01.2022 durch VO v. 06.09.2021 (BGBl. I S. 4163).

39 Umfassend zum Institut der gemeinsamen Betreiber bei Leßner/Mayr, MMR 2024, 148 (149 ff.).

Anlagen nach § 28 Abs. 1 Nr. 1 BSIG-E als Unterfall der besonders wichtigen Einrichtungen gelten sollen, rechtfertigen die deutlich erhöhten Anforderungen an kritische Anlagen[40], diese als eigenständige dritte Unternehmenskategorie zu sehen.[41]

d) Konzerneinbindung und Einschränkungen des Anwendungsbereichs (§ 28 Abs. 3 BSIG-E)

Hinsichtlich der konkret zu Risikomanagementmaßnahmen verpflichteten Einrichtungen geht die NIS-2-RL und der BSIG-E vom Idealbild einer juristischen Person als Betreiber eines Diensts oder einer Anlage aus.[42] Hier fehlt es an einer Konzernregelung für verbundene Unternehmen. Zur Bestimmung der Unternehmensschwellenwerte für den Anwendungsbereich werden nach § 28 Abs. 3 S. 2 BSIG-E i.V.m. Art. 3 der Empfehlung 2003/361/EG jedoch durch einen Konzern verbundene Unternehmen berücksichtigt.[43] Dadurch kann ein grds. nicht reguliertes Unternehmen aufgrund der Anrechnung von Unternehmenskennzahlen verbundener Unternehmen in den Anwendungsbereich fallen. Diese Prüfung ist individuell für jedes Konzernunternehmen vorzunehmen und eine „Infektionswirkung" gegenüber dem gesamten Konzern besteht nicht.[44] Ob der Anwendungsbereich des BSIG-E auch eröffnet ist, wenn konzerninterne IT-Dienstleistungen in einem Unternehmen konzentriert werden,[45] ist unklar: Während der BSIG-E schweigt, schließt ErwG 35 S. 5 NIS-2-RL den Anwendungsbereich hier aus.

§ 28 Abs. 3 Nr. 1 BSIG-E nimmt gegenüber der NIS-2-RL eine dort nicht vorgesehene Einschränkung des Anwendungsbereichs vor, wonach nur „auf die der Einrichtungsart zuzuordnende Geschäftstätigkeit" abzustellen ist. Nach der Konzeption des Entwurfs kommt es also nicht darauf an, ob man die Unternehmenskennzahlen überschreitet, sondern ob man sie auch im Rahmen der hauptsächlichen Geschäftstätigkeit überschreitet.[46] Zwar sieht ErwG 16 der NIS-2-RL einen Ausgleich unbilliger Härten bei der Konzernanrechnung vor, worauf die Begründung zum NIS2UmsuCG auch anspielt. Da dies jedoch keine Entsprechung im Normtext der RL gefunden hat und § 28 Abs. 3 Nr. 1 BSIG-E den ErwG zudem überdehnt, ist die Umsetzung des Anwendungsbereichs an dieser Stelle europarechtswidrig.[47]

e) Sektorenregelungen

Die Anlagen 1 und 2 zum BSIG-E übernehmen die Anhänge I und II der NIS-2-RL. In Anlage 1 sind Sektoren besonders wichtiger und wichtiger Einrichtungen geregelt, in Anlage 2 weitere Sektoren wichtiger Einrichtungen. Im Vergleich zur NIS-RL werden zahlreiche neue Sektoren reguliert,[48] was ein wesentlicher Faktor für die enorme Ausweitung des Anwendungsbereichs ist.[49] Ein – hier nur beispielhaft beleuchtetes – Problem ist die Verweisung auf einschlägiges Fachrecht zur konkreten Bestimmung der Betroffenen. In Spalte D der Anlagen 1 und 2 zum BSIG-E wird auf Definitionen des den Sektor regulierenden Rechts verwiesen. Nicht immer eignet sich dieses aber zur Bestimmung des Anwendungsbereichs von Cybersicherheitsregulierung. Besonders deutlich erkennbar ist dieses Problem beim Sektor der Produktion, Herstellung und Handel mit chemischen Stoffen in Nr. 3.1.1. der Anlage 2 zum BSIG-E. Für den Anwendungsbereich wird hier auf den Hersteller- und Importeursbegriff[50] in Art. 3 Nr. 9 und 11 der REACH-VO[51] verwiesen. Durch die pauschale Verweisung auf Wirtschaftsakteure der europäischen Chemikalienregulierung ergibt sich ein kaum überschaubarer Anwendungsbereich von rund 22.500 Unternehmen in Deutschland.[52] Ebenfalls besonders breit ausgefallen ist der Sektor des verarbeitenden Gewerbes und die Herstellung von Waren in Anlage 2 Nr. 5 zum BSIG-E. Insbesondere die Unterkategorien der Herstellung von Datenverarbeitungsgeräten (Nr. 5.2), der Maschinenbau (Nr. 5.4) und der Fahrzeugbau (Nr. 5.5 sowie 5.6) begründen bei vielen deutschen Unternehmen eine Betroffenheit, da die statistische Systematik der Wirtschaftszweige (NACE), auf die verwiesen wird, breit aufgefächert ist. An diesen beiden Beispielen zeigt sich, dass sich der Anwendungsbereich keineswegs pauschal überschlagen lässt und von einem zielgerichteten Wirtschaftsschutz kaum gesprochen werden kann.

3. Risikomanagementmaßnahmen

Grundsätzlich erfindet der Gesetzgeber das Rad hinsichtlich der Risikomanagementmaßnahmen bis auf wenige Aspekte nicht neu; zusammengefasst geht es um das Ergreifen geeigneter und verhältnismäßiger technischer, operativer und organisatorischer Maßnahmen zur Beherrschung von IT-Sicherheitsrisiken und die Verhinderung oder Minimierung der Auswirkungen von Sicherheitsvorfällen.[53] Es geht also primär um das Implementieren eines einrichtungsbezogenen Cybersicherheitsrisikomanagementsystems (Informationsmanagementsystem – ISMS).[54] Das NIS2UmsuCG verfolgt dabei einen gefahrenübergreifenden Ansatz, d.h. es zielt darauf ab, die Netz- und Informationssysteme sowie auch die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen.[55]

Art. 21 Abs. 2 NIS-2-RL enthält einen detaillierten Maßnahmenkatalog, dessen Anforderungen als Mindeststandard implementiert werden müssen und der in § 30 Abs. 2 S. 2 BSIG-E umgesetzt wird. Inhaltlich halten die verbindlich zu implementierenden Maßnahmen (überwiegend) keine großen Überraschungen parat: Es müssen Konzepte in Bezug auf die Risikoanalyse und die IT-Sicherheit erstellt werden,

40 Geregelt insb. in § 31 BSIG-E.

41 Schmidt, RDi 2024, 550 (551); Füllsack/Lenger, K&R 2024, 31 (32); a.A. wohl Kipker/Dittrich, MMR 2023, 481 (482).

42 Leßner/Mayr, MMR 2024, 148 (149); Hessel/Callewaert/Schneider, RDi 2024, 208 (209 f.).

43 Ausführlich bei Leßner, MMR 2024, 226 (227 f.).

44 Hessel/Callewaert/Schneider, RDi 2024, 208 (210).

45 Einschlägig wäre in Anlage 1 zum BSIG-E Nr. 6.1.5, 6.1.10. und 6.1.11.

46 Vgl. BT-Drs. 20/13184, S. 136.

47 So auch Schmidt, RDi 2024, 550 (552) und Hessel/Callewaert/Schneider, RDi 2024, 208 (210).

48 Siehe zu den neuen Sektoren bereits bei Vogel/Ziegler, International Cybersecurity Law Review, 2023 vol. 4, 1 (15 f.).

49 Vgl. COM(2020) 823 final, S. 5 sowie ErwG 6 NIS-2-RL.

50 Hierbei dürfte es sich um einen Umsetzungsfehler handeln, da Anhang II Nr. 3 der NIS-2-RL auf Art. 3 Nr. 14 REACH-VO, also Händler, verweist.

51 VO (EG) 1907/2006.

52 Siehe zur Berechnung ausführlich Hessel/Zimmermann, Arbeitspapier zum Anhang II Nr. 3 der NIS-2-Richtlinie: NIS2 und REACH, S. 2, 5 ff.

53 Ritter, RDV 2023, 152 (155).

54 Schmidt, RDi 2024, 550 (553).

55 Siehe § 30 Abs. 1 S. 1 BSIG-E sowie Art. 26 Nr. 3 lit. b) NIS2UmsuCG zur Änderung von § 165 TKG, der den „gefahrenübergreifenden Ansatz" näher erläutert; Ritter, RDV 2023, 152 (155).

die Bewältigung von Sicherheitsvorfällen und die Aufrechterhaltung des Betriebs – etwa durch Back-up-Management, Notfallwiederherstellungskonzepte und ein vernünftiges Krisenmanagement – sichergestellt werden, Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen ergriffen werden, wobei auch der Umgang mit Schwachstellen explizit Erwähnung findet, und Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen überlegt werden. Darüber hinaus sind Cyberhygienemaßnahmen – was mit diesem Begriff konkret gemeint ist, bleibt indes unklar[56] – und IT-Sicherheitsschulungen ebenso erforderlich wie ein vernünftiges Zugriffsmanagement, Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung sowie die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung und sicheren (Notfall-)Kommunikationssystemen. Materiell können die Vorgaben etwa durch eine Zertifizierung nach ISO 27001 erfüllt werden.[57] Die Bedeutung von Standards wird dadurch verstärkt, dass auf Ebene der Rechtsprechung eine verlässliche Beurteilung der Angemessenheit ergriffener Maßnahmen infolge der ausfüllungsbedürftigen und daher schwer subsumtionsfähigen Rechtsbegriffe ohne Rückgriff auf beispielsweise das BSI IT-Grundschutz-Kompendium oder ISO 27001 kaum möglich ist.[58]

Neu sind jedoch zwei Dinge: Erstens soll das BSIG zukünftig anstelle der Verwendung unbestimmter Rechtsbegriffe in § 8a Abs. 1 BSIG (angemessene technische und organisatorische Maßnahmen nach dem Stand der Technik) eine Maßnahmenliste ergänzen. Dadurch entsteht die Mentalität einer To-Do-Liste, bei deren Abarbeiten falsche Sicherheit suggeriert wird und deren fragwürdige Prioritäten nicht zu jeder Einrichtung passen.[59] Zweitens wird die Cybersicherheit der Lieferkette explizit einbezogen. Der Gesetzgeber hat erkannt, dass Abhängigkeiten von und insbesondere Cyberangriffe über die IT-Lieferkette (Supply-Chain-Angriffe) zu den größten Bedrohungen zählen.[60] Art. 21 Abs. 2 NIS-2-RL verweist ausdrücklich auf sicherheitsbezogene Aspekte der Beziehungen zwischen Einrichtungen und ihren unmittelbaren (Dienste-)Anbietern.[61] Art. 21 Abs. 2 lit. d) NIS-2-RL wurde unverändert in § 30 Abs. 2 Nr. 4 BSIG-E übernommen. Erforderlich ist, dass betroffene Einrichtungen ebenfalls innerhalb der Lieferkette die Sicherheit prüfen und gewährleisten, beispielsweise mittels vertraglicher Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement sowie der Berücksichtigung von Empfehlungen des BSI.[62] Auch müssen Einrichtungen bei der Erwägung geeigneter Risikomanagementmaßnahmen die Ergebnisse der koordinierten Risikobewertungen kritischer Lieferketten i.S.d. Art. 22 Abs. 1 NIS-2-RL berücksichtigen.[63]

Dass die NIS-2-RL (und damit auch das NIS2UmsuCG) spezifische Regelungen in Bezug auf die Lieferkette enthält, ist vor dem Hintergrund von Vorfällen wie dem CrowdStrike-Vorfall im Juli 2024 – ein fehlerhaftes Update eines Softwareprodukts der Firma CrowdStrike hatte weltweit zu Ausfällen an mehr als 8,5 Millionen Windows-Geräten geführt, was allerdings durch das Testen von Software-Updates im Kundenunternehmen hätte vermieden werden können[64] – nur zu nachvollziehbar. Die praktische Umsetzung dieser Vorgabe hingegen wirft mit Blick auf Standardsoftware Fragen auf; möglich erscheint beispielsweise eine Lösung über eine Vorgabe mittels Durchführungsrechtsakt, spezielle und nach europäischen Cybersicherheitsschemata zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen.[65]

4. Meldepflichten

Die in § 32 BSIG-E statuierte Meldepflicht sieht ein mehrstufiges System vor: Bei erheblichen Sicherheitsvorfällen ist zunächst spätestens innerhalb von 24 Stunden nach Kenntniserlangung von dem Vorfall eine frühe Erstmeldung zu erstatten. Diese ist wiederum spätestens innerhalb von 72 Stunden nach Kenntniserlangung in einer Folgemeldung zu bestätigen oder zu aktualisieren, wobei hier auch eine erste Bewertung des Vorfalls einschließlich seines Schweregrads, möglicher Auswirkungen und ggf. der Kompromittierungsindikatoren beizufügen ist. Spätestens einen Monat nach dieser zweiten Meldung ist – sofern der Vorfall nicht noch andauert[66] – eine Abschlussmeldung vorzunehmen, die neben einer ausführlichen Beschreibung des Vorfalls, seines Schweregrads und seiner (ggf. grenzüberschreitenden) Auswirkungen auch mögliche Ursachen sowie getroffene und laufende Abhilfemaßnahmen erforschen muss. Daneben müssen auf Ersuchen des BSI relevante Statusaktualisierungen in Zwischenmeldungen gemeldet werden (§ 32 Abs. 1 Nr. 3 BSIG-E).

Wann ein erheblicher Sicherheitsvorfall i.S.d. § 32 BSIG-E vorliegt, soll sich aus § 2 Nr. 11 BSIG-E ergeben, wobei angesichts der unscharfen Formulierung auf eine Konkretisierung durch eine zu erlassende Rechtsverordnung zu hoffen ist.[67] In Art. 23 Abs. 3 NIS-2-RL findet sich eine etwas ausführlichere Legaldefinition, die durch Art. 3 der DurchführungsVO der Kommission[68] konkretisiert wird.

5. Pflichten der Geschäftsführung

a) Vorgaben der NIS-2-RL

Unter dem Stichwort Governance fordert Art. 20 Abs. 1 NIS-2-RL, „dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Art. 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können". Weiter heißt es in Abs. 2: „Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger

56 Ritter, RDV 2023, 152 (155).

57 BT-Drs. 20/13184, S. 150: Ein ISO 27001-Zertifikat belegt – jedenfalls grundsätzlich – die Umsetzung der Mindestanforderungen nach § 44 Abs. 1 S. 1 und Abs. 2 S. 1 BSIG-E, wodurch wiederum die Erfüllung der Vorgaben nach § 30 BSIG-E gewährleistet ist, § 44 Abs. 3 S. 1 BSIG-E.

58 Schmidt, RDi 2024, 550 (553); siehe zu dieser Herausforderung auch Keppeler/Poncza/Schneider, CR 2023, 787 (787).

59 Wobei die kritisierte Umsetzung in einem Maßnahmenkatalog ja bereits durch Art. 21 NIS-2-RL vorgezeichnet war. Siehe für einen besseren Alternativvorschlag anstelle einer 1:1 Übernahme des Maßnahmenkatalogs bei Kipker, Stellungnahme zu BT-Drs. 20/13184, S. 25.

60 BT-Drs. 20/13184, S. 2, 89 f.

61 Werry/Éles, MMR 2024, 829 (830).

62 Schmidt, RDi 2024, 550 (553); BT-Drs. 20/13184, S. 139.

63 BT-Drs. 20/13184, S. 139.

64 Hötzel/Völkl, BC 2024, 402 (402).

65 Ritter, RDV 2023, 152 (155).

66 In diesem Fall handelt es sich nicht um eine Abschluss-, sondern um eine Fortschrittsmeldung, § 32 Abs. 1 S. 1 BSIG-E.

67 Siehe auch GDD, Stellungnahme vom 29.10.2024, Ausschuss-BT-Drs. 20(4)522, S. 6.

68 C(2024) 7151 final.

Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben."

Art. 32 Abs. 6 UAbs. 1 NIS-2-RL verpflichtet die Mitgliedstaaten außerdem, sicherzustellen, dass eine natürliche Person, „die für eine wesentliche Einrichtung verantwortlich ist oder [...] als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt.". Mithin sind als Leitungspersonen handelnde natürliche Personen für die Einhaltung der NIS-2-Anforderungen verantwortlich – und gemäß Art. 32 Abs. 6 UAbs. 1 S. 2 NIS-2-RL für etwaige Pflichtverstöße haftbar zu machen. Mit Regelungen wie u.a. der persönlichen Haftung der Geschäftsführung wird bezweckt, auf diese einen gewissen Druck zur Umsetzung der erforderlichen Cybersicherheitsmaßnahmen auszuüben.[69] Nichtsdestotrotz wird vertreten, dass eine teleologische Auslegung der Verpflichtungen der NIS-2-RL sowie auch des NIS2UmsuCG unter Verhältnismäßigkeitsgesichtspunkten als eine absolute Pflicht zur Ergreifung der aufwendigen Maßnahmen nur dann bestehen soll, wenn diese der Aufrechterhaltung der Geschäftstätigkeit des jeweiligen Unternehmens dienen.[70]

b) Umsetzungs-, Überwachungs- und Schulungspflicht für die Geschäftsleitung

Umgesetzt wird dieser Kurs, leicht abgewandelt, in § 38 BSIG-E.

aa) Billigungs- und Überwachungspflicht (§ 38 Abs. 1 BSIG-E)

Zunächst bestimmt § 38 Abs. 1 BSIG-E, dass Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen verpflichtet sind, die Risikomanagementmaßnahmen umzusetzen und die Umsetzung zu überwachen. Auffällig ist die Wortwahl im NIS2UmsuCG. Der deutsche Gesetzgeber verpflichtet Leitungsorgane – mit Blick auf die entsprechenden Vorgaben der NIS-2-RL überschießend – mithin nicht nur zu einer (bloß) formellen Zustimmung, sondern aktiv zur Umsetzung der Maßnahmen.[71] Der Referentenentwurf erklärte Cybersicherheit eindeutig zur „Chefsache"[72]; sinnvoll ist dies schon deswegen, weil die Geschäftsleitung über die notwendigen Entscheidungskompetenzen – nicht nur in Budgetfragen – verfügt.[73] Ob die Regelung des § 38 Abs. 1 BSIG-E überhaupt erforderlich ist, wird teils mit Verweis auf die allgemeinen gesellschaftsrechtlichen Sorgfaltspflichten – die im Übrigen nicht nur für Geschäftsleiter (besonders) wichtiger Einrichtungen, sondern auch diejenigen anderer Unternehmen treffen – bezweifelt.[74]

In der Entwurfsfassung vom 03.07.2023 enthielt § 38 Abs. 1 S. 2 BSIG-E noch den Zusatz, dass die Beauftragung eines Dritten zur Erfüllung der Verpflichtungen nach S. 2 unzulässig ist[75]; im aktuellen Regierungsentwurf ist hiervon keine Rede mehr.[76] Eine Delegation der Pflicht, die Risikomanagementmaßnahmen zu billigen und ihre Umsetzung zu überwachen – sei es intern oder extern – ist somit nicht (mehr) ausgeschlossen, was in der weit überwiegenden Anzahl der Fälle nicht nur sachgerecht, sondern mit Blick auf die Notwendigkeit der Hinzuziehung entsprechender (externer) Expertise schlicht notwendig sein dürfte.[77]

bb) Schulungspflicht

Weiterhin „sollen" sie gemäß Abs. 3 regelmäßig an Schulungen teilnehmen, „um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können". Während sich für die Geschäftsleitung im Vergleich zum RefE vom 03.07.2023 keine Änderungen ergeben – die Schulungspflicht blieb bestehen – enthielt letzterer auch für Mitarbeiter der Geschäftsleitung einen eindringlichen Vorschlag dahingehend („[...] deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen [...]"). Die letztlich vage Formulierung hinsichtlich der Schulungspflicht lässt indes eine handhabbare Konkretisierung hinsichtlich des nötigen Umfangs der Schulungen, die etwaige Erforderlichkeit eines Nachweises und genaue Vorgaben bzgl. der Regelmäßigkeit vermissen, was einerseits das Risiko unzureichender Umsetzung der Pflicht, andererseits auch mangelnde Rechtssicherheit aus Sicht der betroffenen Geschäftsleitungen mit sich bringt.[78]

c) Haftung der Geschäftsleitung

Die Entwicklung der Regelung zur Haftung der Geschäftsleiter war wechselhaft und wurde – verständlicherweise – kritisch beobachtet: Die Entwurfsfassung vom 03.07.2023 enthielt noch eine Haftungsnorm, mit der erstmals eine eigenständige und umfassende Haftungsnorm für Complianceverstöße im Rahmen der Cybersecurity geschaffen worden wäre. Der deutsche Gesetzgeber hatte es sich ursprünglich zum Ziel gesetzt, in dieser Sache überschießend umzusetzen und dabei den durch die NIS-2-RL vorgegebenen Spielraum auszunutzen.[79] § 38 Abs. 2 BSIG-E sieht in der aktuellen Fassung nur noch vor, dass Leitungsorgane von ihren Einrichtungen für Pflichtverletzungen nach den anwendbaren Regeln des Gesellschaftsrechts haftbar gemacht werden können. Relevante Schäden betreffen beispielsweise Kosten für die Zahlung von Lösegeld nach einem Ransomware-Angriff, Schäden infolge von Betriebsunterbrechungen, Reputationsschäden oder Rechts- und Regulierungskosten – auch in Zusammenhang mit Bußgeldern und Schadenersatzforderungen nach der DS-GVO.[80]

Kritisiert wird – soweit sie in der jeweiligen Fassung vorhanden ist – der auslegungsbedürftige Wortlaut der Norm, der Legaldefinition der Geschäftsleitung in § 2 Nr. 13 BSIG-E[81] und die Stellung des § 38 BSIG-E im bestehenden gesellschafts-

69 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (667) mit Verweis auf ErwG 137 S. 2 NIS-2-RL.

70 Keppeler/Poncza/Schneider, CR 2023, 787 (790).

71 So auch Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (667).

72 Keppeler/Poncza/Schneider, CR 2023, 787 (790).

73 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (668).

74 DAV, Stellungnahme 35/2024, S. 2; a.A. Kipker, Stellungnahme vom 31.10.2024, Ausschuss-BT-Drs. 20(4)523 G, S. 30.

75 RefE vom 03.07.2023, S. 46.

76 BT-Drs.20/13184, S. 41.

77 So auch DAV, Stellungnahme 35/2024, S. 4.

78 Ebenso Kipker, Stellungnahme vom 31.10.2024, Ausschuss-BT-Drs. 20(4)523 G, S. 31.

79 Vgl. Diskussionspapier des BMI vom 27.09.2023.

80 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (670).

81 Schaller/Lindberg ZD-Aktuell 2024, 01931.

rechtlichen Kontext.[82] So ist die Geschäftsleitung – insbesondere die GmbH-Geschäftsführung und der AG-Vorstand – zur ordnungsgemäßen Unternehmensleitung verpflichtet und unterliegt der Legalitäts- und Legalitätskontrollpflicht.[83] Die Legalitätspflicht beinhaltet, dass die Geschäftsleitung die Einhaltung geltender Rechtsvorschriften sowie anderer Verpflichtungen sowie eine ordnungsgemäße Buchführung sicherzustellen hat.[84] Die Vorstandsmitglieder haben zudem sowohl einander als auch nachgeordneten Einheiten des Unternehmens gegenüber die Einhaltung der Gesetze und Rechtsvorschriften zu kontrollieren (Legalitätskontrollpflicht).[85] Zu den Sorgfaltspflichten der Geschäftsleitung zählt – auch unabhängig von der NIS-2-RL oder dem BSIG-E – infolge der erheblichen Bedeutung von IT-Systemen für die Funktionsfähigkeit moderner Unternehmen grundsätzlich ein aktives Cybersicherheitsmanagement.[86]

Abseits konkret gesetzlich vorgeschriebener Entscheidungen und der damit verknüpften Legalitätspflicht besteht indes ein weiter unternehmerischer Handlungsspielraum („Business Judgement Rule"), der jedenfalls für den AG-Vorstand in § 93 Abs. 1 S. 2 AktG explizit zum Ausdruck kommt[87], aber auch für andere Geschäftsleitungen als ungeschriebener Grundsatz anerkannt ist.[88] Eine Grenze dieser Entscheidungsfreiheit wird dort zu ziehen sein, wo die (aktive) Entscheidung gegen angemessene Cybersicherheitsmaßnahmen getroffen wird, da eine solche angesichts der gegebenen besorgniserregenden Bedrohungslage[89] schlicht nicht von der unternehmerischen Ermessensausübung gedeckt sein kann.[90] Die bloße Untätigkeit genügt im Zusammenhang mit der Business Judgement Rule zwar grundsätzlich nicht.[91] Mit Blick auf den verbindlichen Maßnahmenkatalog des § 30 Abs. 2 S. 2 BSIG-E ist die Geschäftsleitung allerdings hinsichtlich des „Ob" gebunden, sodass ein Unterlassen der Implementierung eines Cybersicherheits-Mindeststandards selbst bei (tatsächlich) verschwindend geringem Eingriffsrisiko nicht mehr durch die Business Judgement Rule gedeckt wäre.[92]

Bei Pflichtverstößen normieren u.a. § 43 Abs. 2 GmbHG und § 93 Abs. 2 S. 1 AktG eine Innenhaftung ihrer Leitungsorgane. Damit existiert bereits nach geltender Rechtslage eine (Innen-)Haftung der Geschäftsleitung für Verstöße gegen Cybersicherheitspflichten, wenn auch durch § 38 Abs. 2 S. 1 BSIG-E die Leitungsorgane (noch) stärker in den Fokus gerückt werden.[93] Zu beachten ist, dass in § 38 BSIG-E mindestens für AG, GmbH sowie GmbH & Co. KG keine eigenständige Haftungsgrundlage statuiert ist, sondern lediglich die Voraussetzung einer Haftung nach dem anwendbaren Gesellschaftsrecht beschrieben wird.[94] Was die übrigen Gesellschaftsformen betroffener Unternehmen angeht, steht und fällt eine eigenständige Haftung nach der Auslegung des § 38 Abs. 2 S. 1 BSIG-E. Die Entwurfsbegründung sieht darin einen eigenständigen Auffangtatbestand zur Haftung.[95] Als eigenständige Haftungsgrundlage kann § 38 Abs. 2 S. 1 BSIG-E damit nur dann herangezogen werden, wenn – so S. 2 – „die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach S. 1 enthalten". Gegen einen eigenständigen Haftungstatbestand spricht aber der verweisende Charakter und das Fehlen jeglicher Formulierung von haftungsleitenden Maßstäben. Erst § 38 Abs. 2 S. 2 BSIG-E lenkt die Suche nach einem Haftungstatbestand wieder ins BSIG. Diese Rückverweisung geht aber ins Leere, da S. 1 ja gerade keinen eigenen Haftungstatbestand zu formulieren scheint und der restliche BSIG-E keinerlei weitere Haftungsnormen für die Geschäftsleitung enthält.[96] Je nach Sichtweise dient § 38 Abs. 2 BSIG-E danach der Umsetzung eines grenzüberschreitenden (Mindest-)Haftungsregimes innerhalb der EU[97] oder es ist fraglich, ob die NIS-2-RL an dieser Stelle überhaupt vollständig umgesetzt wurde.[98]

6. Sanktions- und Durchsetzungsregime

Zuständig als Aufsichtsbehörde für die Durchführung der Befugnisse in Teil 7 des BSIG ist nach § 59 BSIG-E das BSI.

a) Bußgelder

§ 65 BSIG-E enthält in Abs. 1-4 diverse Ordnungswidrigkeitstatbestände, die mit Geldbußen in Höhe von bis zu zehn Millionen Euro oder 2 % des gesamten weltweiten Vorjahresumsatzes geahndet werden können.[99] Die Höhe orientiert sich dabei an der DS-GVO oder dem DSA.

§ 65 Abs. 10 BSIG-E verhindert eine Kumulierung von Geldbußen, welche die Datenschutzaufsichtsbehörden auf Grundlage der DS-GVO verhängen, wenn sich der Verstoß gegen die DS-GVO und gegen das BSIG aus demselben Verhalten ergeben. Der Ausschluss der Kumulation ist aber einseitig: Der Wortlaut des § 65 Abs. 10 BSIG-E schließt die Kumulation von Geldbußen nur aus, wenn die Datenschutzbehörden zuerst tätig werden. Verhängt das BSI die Geldbuße zuerst, gilt dies jedoch nicht. Unabhängig von der einfachrechtlichen Lage dürfte eine Doppelsanktion aus (unions-) verfassungsrechtlichen Gründen trotzdem ausscheiden. Sowohl das Doppelbestrafungsverbot nach Art. 50 GRCh als auch nach Art. 103 Abs. 3 GG umfassen Verwaltungssanktionen durch Ordnungswidrigkeiten.[100] Auffangend kann auch dem Rechtsstaatsgebot ein eingeschränktes Verbot der Doppelsanktionierung entnommen werden.[101] Da es zwischen GRCh und GG in diesem Fall materiell zu keinem Unterschied kommt, kann die Frage der Anwendbarkeit des Grundrechtsschutzes im Bereich der mindestharmonisierenden NIS-2-RL hier offenbleiben.[102]

82 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (668).

83 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (668): Das Haftungskonzept der §§ 93 Abs. 2 S. 1 AktG, 43 Abs. 2 GmbHG findet jedenfalls teilweise auch auf andere Gesellschaftsformen Anwendung.

84 Wicke, in: Wicke, GmbHG, § 43 Rn. 6; Koch, in: Koch, AktG, § 93 Rn. 9 ff.

85 Koch, in: Koch, AktG, § 93 Rn. 17 m.w.N.

86 von dem Bussche, in: Kipker, Cybersecurity, Kap. 6 Rn. 45 ff.

87 Koch, in: Koch, AktG, § 93 Rn. 26.

88 Wicke, in: Wicke, GmbHG, § 43 Rn. 6.

89 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 90.

90 Grieger, WM 2021, 8 (12).

91 Koch, in: Koch, AktG, § 93 Rn. 35.

92 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (669).

93 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (668).

94 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (669).

95 BT-Drs. 20/13184, S. 146.

96 Schmidt, RDi 2024, 550 (555).

97 Grosmann/Gerecke/Aschenbrenner, CR 2024, 665 (669).

98 Schmidt, RDi 2024, 550 (555).

99 Bspw. wenn Risikomanagementmaßnahmen i.S.d. § 30 Abs. 1 S. 1 BSIG-E nicht, nicht vollständig oder nicht rechtzeitig umgesetzt werden, § 65 Abs. 2 Nr. 2 i.V.m. Abs. 5 Nr. 1 lit. a) bzw. Abs. 6 BSIG-E.

100 Vgl. Aust, in: Huber/Voßkuhle, 8. Aufl. 2024, GG Art. 103 Rn. 230.

101 BVerfGE 28, 264 (276 ff.).

102 BVerfGE 152, 216 (248, Rn. 81).

b) Aufsichts- und Durchsetzungsmaßnahmen

Erst bei der Aufsicht ergeben sich größere Unterschiede zwischen den wichtigen und besonders wichtigen Einrichtungen: Für besonders wichtige Einrichtungen sieht § 61 BSIG-E umfassende Aufsichts- und Durchsetzungsmaßnahmen vor. So kann das BSI u.a. die Durchführung von Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen anordnen (Abs. 1) oder – nach Anhörung der betroffenen Einrichtungen und Wirtschaftsverbände – fachliche und organisatorische Anforderungen für die prüfenden Stellen festlegen (Abs. 2). Kontrollen können hier auch ohne weitere Verdachtsmomente durchgeführt werden. Für wichtige Einrichtungen sieht der § 62 BSIG-E einschränkend vor, dass nur bei berechtigter Sorge, dass z.B. Verpflichtungen i.S.d. § 30 Abs. 1 S. 1 BSIG-E nicht erfüllt werden, die Einhaltung der Risikomanagementpflichten überprüft werden und ggf. Maßnahmen nach § 61 getroffen werden können. Durchsetzbar sind die Anordnungen des BSI mit Zwangsgeldern i.H.v. bis zu 100.000,– Euro (§ 63 BSIG-E).

7. Fachgesetzliche Umsetzung

Die Zersplitterung des deutschen IT-Sicherheitsrechts wird mit dem NIS2UmsuCG nicht aufgehoben und trotz der enormen Aufwertung des BSIG wird dieses kein „IT-Sicherheitsgesetzbuch". Daher erfolgt die Umsetzung der NIS-2-RL auch in Fachgesetzen, die bereits schon Cybersicherheitsanforderungen enthalten. Neben dem BSIG ändert das NIS2UmsuCG als Artikelgesetz weiterhin u.a. das BNDG, TDDDG, AtomG, EnWG, das Messstellenbetriebsgesetz, SGB V, SGB VI, SGB XI, das TKG sowie zahlreiche Verordnungen. Obwohl jeweils dieselben Vorschriften der NIS-2-RL umgesetzt werden, kommt es nach derzeitigem Stand jedoch gerade zwischen dem BSIG-E, TKG und EnWG zu unnötig voneinander abweichenden Begrifflichkeiten.[103] Das EnWG und TKG setzen Art. 34 f. NIS-2-RL auch nicht vollständig um. So fehlt etwa im TKG eine Umsetzung der Bußgeldanforderungen der NIS-2-RL. Im EnWG erfolgt mit der Streichung von § 11 Abs. 1a bis 1g und Einführung eines neuen § 5c eine Bündelung von IT-Sicherheitsvorschriften im Energiebereich.

8. Zusammenspiel BSIG und KRITIS-DachG

Neben dem NIS2UmsuCG und dem darin zentralen BSIG-E muss zwingend auch der Entwurf zum KRITIS-DachG angesprochen werden, der in Umsetzung der CER-RL den physischen Schutz kritischer Anlagen bezweckt, während das BSIG weiterhin die Cybersicherheit regelt. Erst in der Zusammenschau kann ein umfassender Schutz kritischer Anlagen gelingen.[104] Der offizielle Referentenentwurf zum KRITIS-DachG wurde am 21.12.2023 veröffentlicht, der Regierungsentwurf am 06.11.2024 im Kabinett verabschiedet.[105] Beide Werke sind systematisch zusammenhängend zu betrachten.[106]

Nach anfänglichen begrifflichen Spannungen zwischen dem RefE des KRITIS-DachG und dem NIS2UmsuCG sind die Regierungsentwürfe nun aufeinander abgestimmt: Die Beibehaltung der bisherigen KRITIS-Systematik im BSIG-E dient der Herstellung von Kohärenz zum KRITIS-DachG. Im Regierungsentwurf zum KRITIS-DachG werden die oben eingeführten Begriffe zur Bestimmung kritischer Anlagen i.S.v. § 28 Abs. 7 BSIG-E in § 2 Nr. 1 – 4, § 4 Abs. 1 KRITIS-DachG wortlautgleich oder zumindest inhaltsgleich definiert, wodurch sich ein einheitlicher Anwendungsbereich ergibt. Die durch die Kategorie der kritischen Anlagen erhöhte Komplexität[107] des Anwendungsbereichs des BSIG ist für einen kohärenten KRITIS Schutz daher erforderlich.

Ausdruck der engen Verbindung der beiden Gesetze ist auch die Einrichtung einer gemeinsamen Meldestelle für Sicherheitsvorfälle zwischen BSI und dem das KRITIS-DachG durchführenden Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.[108] Da das KRITIS-DachG erst nach dem Koalitionsbruch das parlamentarische Verfahren erreicht hat, ist eine Umsetzung noch in dieser Legislatur unwahrscheinlicher als beim NIS2UmsuCG. Auch bzgl. der Umsetzung der CER-RL hat die EU-Kommission ein Vertragsverletzungsverfahren eingeleitet.[109]

IV. Regelung staatlicher Informationssicherheit

Auch wenn der Wirtschaftsschutz im Vordergrund der NIS-2-RL steht, adressiert die Richtlinie auch staatliche Stellen. Für den Anwendungsbereich stellt Art. 2 Abs. 1 UAbs. 1 NIS-2-RL klar, dass die Sektoren in den Anhängen I und II sowohl bei privaten als auch bei öffentlichen Einrichtungen maßgeblich sind.[110] Im Anhang I benennt die NIS-2-RL in Nr. 10 den Sektor „Öffentliche Verwaltung" als Sektor mit hoher Kritikalität. Kompetenzgemäß kann das NIS2UmsuCG im Bereich der staatlichen Informationssicherheit nur die Bundesverwaltung regeln. Die Umsetzung im Bereich der Länder- und Kommunalverwaltung obliegt den Bundesländern.[111] Von der in Art. 2 Abs. 5 lit. a) NIS-2-RL vorgesehenen Öffnungsklausel des Anwendungsbereichs für Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene, also Kommunen, will keines der Bundesländer Gebrauch machen.[112]

1. Systematik im neuen BSIG

Das NIS2UmsuCG nimmt die öffentliche Verwaltung nicht als Sektor auf, sondern etabliert mit § 29 BSIG-E ein eigenes Regelungsregime. Die Binnensystematik des § 29 BSIG-E gliedert sich folgendermaßen: § 29 Abs. 1 BSIG-E definiert die Einrichtungen der Bundesverwaltung, für die das BSIG zukünftig Anforderungen formuliert. Das sind nach § 29 Abs. 1 Nr. 1 BSIG-E insbesondere die Bundesbehörden. Ohne ersichtlichen Grund ausgenommen werden aber „Institutionen der

103 GDD, Stellungnahme zu BT-Drs. 20/13184, S. 4.

104 Kipker/Dittrich ZRP 2023, 230 (230).

105 Als BT-Drs. 20/13961 wurde das KRITIS-DachG am 05.12.2024 in erster Lesung beraten.

106 So schon Kipker/Dittrich MMR 2023, 481 (483).

107 „KRITISch" zur Komplexität AG Kritis, Stellungnahme zum RegE NIS2UmsuCG v. 2.10.2024, S. 5.

108 § 32 BSIG-E; § 18 KRITIS-DachG-E.

109 EU-Kommission, Pressemitteilung v. 28.11.2024, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/inf_24_5988.

110 Die Begründung des Regierungsentwurfs weist als relevanten Anwendungsbereich die wirtschaftliche Betätigung der öffentlichen Hand aus, BT-Drs. 20/13184, S. 135.

111 Eine rechtzeitige Umsetzung der NIS-2-RL gelang lediglich Bayern durch Änderung des Bayerischen Digitalgesetzes (BayDiG), BayGVBl. 2024, S. 474, und Sachsen durch Änderung des Sächsischen Informationssicherheitsgesetzes, SächsGVBl. 2024, S. 590. Im Übrigen divergiert die Umsetzung zwischen dem Einsatz von Rechtsverordnungen und Verwaltungsvorschriften. Vgl. zum Umsetzungsstand zum Zeitpunkt des Fristablaufs nach Art. 41 Abs. 1 NIS-2-RL bei Hilbricht, Wer die Frist geschafft hat – und wer nicht, Tagesspiegel Background Cybersecurity v. 17.10.2024.

112 Vgl. zu den Hintergründen dieser Entscheidung und zur kommunalen Informationssicherheit allgemein bei Martini/Botta, LKV 2024, 293 ff. und Ziegler, DSRITB 2023, 349 ff.

sozialen Sicherung" und die Bundesbank. § 29 Abs. 2 S. 1 BSIG-E beinhaltet, dass Einrichtungen der Bundesverwaltung grds. die Anforderungen besonders wichtiger Einrichtungen i.S.v. § 28 Abs. 1 BSIG-E zu erfüllen haben. Für die Kernnorm, die Pflicht zum Ergreifen von Risikomanagementmaßnahmen nach § 30 BSIG-E, macht § 29 Abs. 2 S. 2 BSIG-E jedoch eine folgenschwere Rückausnahme. Zu technischen und organisatorischen Schutzmaßnahmen verpflichtet werden dort allein die Bundesministerien und das Bundeskanzleramt. Sämtliche nachgeordneten Behörden in den Geschäftsbereichen der Ministerien werden pauschal und ohne Differenzierung eines Risikoprofils ausgenommen.[113] Weitere Ausnahmen regelt § 29 Abs. 3 BSIG-E für sicherheitsrelevante Bundesbehörden. Nach § 29 Abs. 3 S. 2 BSIG-E soll dabei zumindest das Auswärtige Amt „ergebnisäquivalente" Maßnahmen durch Verwaltungsvorschrift regeln. Dem in der Gesetzesbegründung zutreffend diagnostizierten „Defizit bei der Umsetzung von Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit"[114] und der erhöhten Bedrohungslage aufgrund jüngster geopolitischer Entwicklungen[115] wird dieses Regelungsregime im Ergebnis in keiner Weise gerecht.[116] Ausdrücklich aus Kostengründen hat der Bundestagsinnenausschuss eine Änderung am § 29 BSIG-E aber abgelehnt.[117]

2. CISO Bund

Eine eher bei Gelegenheit geplante und nicht zwingend durch die NIS-2-RL vorgesehene neue Stelle ist ein Chief Information Security Officer für den Bund (CISO Bund). Die Errichtung einer zentral zuständigen Stelle für die Koordination der Cybersicherheit in der Bundesverwaltung war bereits Ziel der Cybersicherheitsagenda des BMI aus dem Juni 2022.[118] Nach § 48 BSIG-E soll dieses Amt in der Form eines Koordinators für Informationssicherheit geschaffen werden. Die Vorschrift regelt jedoch lediglich, dass eine Bestellung überhaupt erfolgen soll, die organisationelle Anbindung soll dem Bestellungsakt durch das Kabinett vorbehalten bleiben.[119] Im Gegensatz zu den Referentenentwürfen fehlt im Regierungsentwurf jedoch eine gesetzliche Festlegung von Aufgaben und Befugnissen.[120] Insbesondere die Unabhängigkeit in der Wahrnehmung seiner Aufgaben, die für die Arbeit eines CISO fachlich erforderlich ist,[121] wird nicht gesetzlich verankert. In seiner Ausgestaltung im RegE vermochte § 48 BSIG-E kaum einen sinnvollen Beitrag zur Cybersicherheit der Bundesverwaltung zu leisten.[122] Diese Kritik hat die Fassung vom 29.11.2024 aufgegriffen und umgesetzt.

V. Fazit

Resümierend gilt es zwei Erkenntnisse nochmals hervorzuheben: Erstens ist der Staat ein schlechtes Vorbild und will selbst nicht einhalten müssen, was er zukünftig von der Wirtschaft verlangt. Diese pharisäische Haltung wirkt vor dem Hintergrund, dass Cyberbedrohungen keineswegs nur die Wirtschaft betreffen und die Digitalisierung öffentlicher Stellen im Gegensatz dazu notorisch schleppend verläuft, bestenfalls ironisch:

76 % der Befragten des letzten Bitkom-Wirtschaftsschutzberichts sehen die Verwaltung insgesamt deutlich schlechter auf Cyberangriffe vorbereitet als die Wirtschaft.[123] Zweitens ergibt sich aus den Darstellungen oben ein nur schwer zu überblickender und rechtsunsicherer Anwendungsbereich. Sollte das NIS2UmsuCG in der 20. Legislatur nicht mehr beschlossen werden und der Diskontinuität anheimfallen, bestünde für einen neuen Umsetzungsanlauf enormes Verbesserungspotenzial, welches die Literatur mittlerweile klar herausgearbeitet hat. Es bleibt zu hoffen, dass dieses ausgeschöpft wird.

Ass. iur. Priska Katharina Büttel
ist Wissenschaftliche Mitarbeiterin am Lehrstuhl für Recht und Sicherheit der Digitalisierung (Prof. Dr. Dirk Heckmann), TU München, School of Social Sciences and Technology. Sie forscht im Bereich des Digitalrechts.

Ass. iur. Nicolas Ziegler
ist Wissenschaftlicher Mitarbeiter am Lehrstuhl für Recht und Sicherheit der Digitalisierung (Prof. Dr. Dirk Heckmann), TU München, School of Social Sciences and Technology. Er forscht im Bereich des Staats- und Verwaltungsrechts sowie dem (IT)-Sicherheitsrecht.

113 Was im konkreten Fall des BSI zum paradoxen Ergebnis führt, dass die nationale Cybersicherheitsbehörde keinerlei Verpflichtung zum Bemühen von Cybersicherheit in eigenen Angelegenheiten unterliegt.

114 BT-Drs. 20/13184, S. 138.

115 BSI, Die Lage der IT-Sicherheit in Deutschland 2024, S. 44 ff., zur Gefährdungslage der Bundesverwaltung explizit auf S. 73 ff.

116 So auch die einhellige Auffassung der Sachverständigen in der Anhörung des Innenausschusses vom 04.11.2024.

117 Gesamtübersicht Formulierungshilfe v. 29.11.2024, S. 3, abrufbar unter: https://ag.kritis.info/wp-content/uploads/2024/12/241202-Uebersicht_Aenderungen.pdf.

118 BMI, Cybersicherheitsagenda, 2022, S. 10.

119 BT-Drs. 20/13184, S. 155.

120 §§ 49 und 50 sämtlicher Referentenentwürfe.

121 Was verfassungsrechtlich jedoch Probleme hinsichtlich Art. 20 Abs. 1, 2 GG aufwirft.

122 So auch die Kritik bei AG Kritis, Stellungnahme zum RegE NIS2UmsuCG v. 02.10.2024, S. 7 und Schmidt RDi 2024, 550 (556).

123 Bitkom, Wirtschaftsschutz 2024, 28.08.2024, S. 20, abrufbar unter https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf.

KURZBEITRÄGE

Künstlich intelligente Strafverfolgung – Warum das Legalitätsprinzip den Einsatz von KI erzwingt

Markus Hartmann*

Das ifo-Institut und die F.A.Z. haben Anfang Mai 2024 das Ergebnis einer Befragung von 180 VWL-Professorinnen und Professoren zur Lage des Wirtschaftsstandorts Deutschland veröffentlicht.[1] In der Gesamtnote erhält Deutschland eine nur befriedigende Schulnote von 3,4. Dabei äußerten die Befragten vielfach die Sorge, dass die Substanz zunehmend erodiere und der Standort Deutschland an Attraktivität verliere. Als Gründe genannt werden die umfassende Bürokratie, fehlende öffentliche Investitionen, der Mangel an Fachkräften, hohe Energiepreise und mangelhafte Digitalisierung. Aus Sicht des Rechtspraktikers besonders interessant ist der Befund, dass demgegenüber das hohe Maß an Rechtssicherheit als ein wesentlicher positiver Umstand angeführt wird.

Rechtssicherheit auf den Bereich der Strafverfolgung – und darum soll es hier ausschließlich gehen – heruntergebrochen, heißt unter anderem, dass derjenige, der eine substanziierte Strafanzeige stellt, sich darauf verlassen kann, dass die Staatsanwaltschaft der Anzeige effektiv nachgeht, den Sachverhalt, wie es § 160 StPO vorsieht, erforscht und verpflichtet ist, wegen aller verfolgbaren Straftaten einzuschreiten, sofern dafür zureichende tatsächliche Anhaltspunkte vorliegen.[2] Es hängt weder von der persönlichen Bereitschaft des Staatsanwalts ab, ob ermittelt wird[3], noch von den für die Aufklärung des Sachverhalts zur Verfügung stehenden Ressourcen.[4]

Das ist im Kern der Gedanke des Legalitätsprinzips: Die Staatsanwaltschaft muss bei einem Anfangsverdacht einschreiten und bei hinreichendem Tatverdacht – sofern nicht die gesetzlich normierten Ausnahmen etwa aus den in §§ 153 ff. StPO normierten Opportunitätsgründen greifen – Anklage erheben. Das Bundesverfassungsgericht sieht das Legalitätsprinzip im Rechtsstaatsprinzip verankert.[5] Es ist damit für das Strafrecht eine wesentliche Ausprägung der Rechtssicherheit[6], denn sämtlichen Verdachtsfällen ist ohne Ansehung der Person und ohne Rücksicht auf äußere Einflüsse nachzugehen.[7] Unerheblich sind daher auch eigene Strafwürdigkeitserwägungen der Strafverfolger. Entscheidend ist vielmehr die Entscheidung des demokratisch legitimierten Gesetzgebers über die Strafbarkeiten und deren Ausformung durch die Gerichte. Für die Strafverfolgungsbehörden ist damit eine substanzielle Aufklärungsanstrengung obligatorisch.[8]

Rechtssicherheit ist aber keine rein dogmatische Begrifflichkeit. Entscheidend ist vielmehr, ob und in welchem Maße das Legalitätsprinzip in der Wirklichkeit der Ermittlungsverfahren umgesetzt wird. Hier sind in der Vergangenheit viele unterschiedliche Fallgruppen diskutiert worden. In der Verfolgung der organisierten Schwerkriminalität wird mitunter die Ermittlung zu einzelnen Straftaten zurückgestellt, um den Gesamtzusammenhang einer kriminellen Organisation wirksam aufklären zu können und verdeckte Ermittlungen zu schützen.[9] Im Bereich der Wirtschaftskriminalität ist der Deal, d.h. das Aushandeln des Ausgangs eines Ermittlungs- bzw. Strafverfahrens ein Instrument zur Eingrenzung des Ermittlungsaufwands.[10] Das tatsächliche Hauptmotiv solcher – wohlmeinend formuliert – Flexibilisierungen des Ermittlungsvorgehens ist oft jedoch die Orientierung an den faktisch für die Strafverfolgung zur Verfügung stehenden Ressourcen im Sinne eines wirtschaftlichen Mitteleinsatzes.[11] Eine unmittelbare Rechtsgrundlage für diesen Gedanken ergibt sich aus der Strafprozessordnung nicht. Diese beschränkt sich vielmehr auf einen abschließenden Katalog von Ausnahmen und Durchbrechungen, der einer generalisierenden Herleitung übergreifender Prinzipien nicht zugänglich ist.[12] Wenn das Legalitätsprinzip aus dem Rechtsstaatsprinzip herzuleiten ist, dürfte es vielmehr Aufgabe des Haushaltsgesetzgebers sein, die für seine Einhaltung erforderlichen Ressourcen den Strafverfolgungsbehörden zur Verfügung zu stellen.[13]

Allein der Ruf nach einem Mehr – mehr Polizistinnen und Polizisten, mehr Staatsanwältinnen und Staatsanwälte – ist jedoch zu kurz gegriffen. Denn bei aller Begeisterung über ei-

* Markus Hartmann ist Leitender Oberstaatsanwalt bei der Generalstaatsanwaltschaft in Köln und Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Der Beitrag fasst seine Thesen für das Symposium der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema "Automatisierte Datenanalyse und KI – Innovative Polizeiarbeit mit Diskriminierungspotenzial?" am 12.09.2024 in Berlin zusammen.

1 Https://www.ifo.de/fakten/2024-05-03/oekonomenpanel-reformvorschlaege-fuer-deutschland.

2 KK-StPO/Diemer, 9. Aufl. 2023, StPO § 152 Rn. 4; MüKoStPO/Kölbel/Ibold, 2. Aufl. 2024, StPO § 160 Rn. 32.

3 MüKoStPO/Kölbel/Ibold, 2. Aufl. 2024, StPO § 160 Rn. 31 f.

4 KK-StPO/Diemer, 9. Aufl. 2023, StPO § 152 Rn. 4.

5 KK-StPO/Diemer, 9. Aufl. 2023, StPO § 152 Rn. 3. BVerfG 2 BvR 8/82=NStZ 1982, 430.

6 HK-GS/Thilo Pfordte, 5. Aufl. 2022, StPO § 152 Rn. 1.

7 MüKoStPO/Kölbel/Ibold, 2. Aufl. 2024, StPO § 160 Rn. 31.

8 MüKoStPO/Kölbel/Ibold, 2. Aufl. 2024, StPO § 160 Rn. 31.

9 Vgl. Abschnitt II. 2. 6 des Gem.RdErl. d. Justizministeriums NRW u.d. Innenministeriums NRW v. 17.02.1986 zur Verfolgung von Straftaten – Inanspruchnahme von Informanten, Einsatz von V-Personen und Verdeckten Ermittlern und sonstigen nicht offen ermittelnden Polizeibeamten.

10 Nestler, JA 2012, 88, 95.

11 Übersicht zur Diskussion bei Nestler JA 2012, 88 ff.

12 MüKoStPO/Kölbel/Ibold, 2. Aufl. 2024, StPO § 160 Rn. 43.

13 KK-StPO/Diemer, 9. Aufl. 2023, StPO § 152 Rn. 4.

nen sinnvollen und nötigen Personalaufwuchs skaliert dieser schlecht. Es ist zu aller erst die Frage zu stellen, ob die Betriebsorganisation der Strafverfolgungsbehörden den Ansprüchen des Legalitätsprinzips hinreichend Rechnung trägt. Anders formuliert: Eine geänderte, zunehmend digitale Wirklichkeit muss auch in den Ermittlungsbehörden weiträumig rezipiert werden.

Besonders deutlich wird dies in den internetkonnexen Kriminalitätsfeldern. Der Endgegner des Legalitätsprinzips im Bereich etwa von Straftaten des 13. Abschnitts des Besonderen Teils des Strafgesetzbuchs ist nicht die durch die Digitalisierung hervorgerufene Komplexität der forensischen Betrachtung des einzelnen Falls. Hier haben die Strafverfolgungsbehörden durch die Einrichtung von spezialisierten Kommissariaten, Cybercrime-Kriminalinspektionen[14] und spezialisierten Task Forces bei den Staatsanwaltschaften die Voraussetzungen für wirksame Ermittlungen geschaffen. Der Fokus auf die Einhaltung des Legalitätsprinzips in einem konkreten Verfahren blendet oftmals jedoch die Perspektive des Legalitätsprinzips in Bezug auf alle zu einem Zeitpunkt anhängigen Verfahren aus. Die Strafverfolgung hat kein Qualitäts-, wohl aber ein Quantitätsproblem.

Dieses lässt sich ganz konkret fassen: Bei Ermittlungen wegen des Verdachts der Verbreitung und des Besitzes kinderpornografischer Inhalte fördert jede Durchsuchung eine Vielzahl digitaler Beweismittel zu Tage, deren Auswertung regelmäßig Hinweise auf umfangreiche Kommunikationsgeflechte ergeben, denen nachzugehen ist. Internetkonnexe Straftaten sind datengetrieben. Die umfassende, dem Legalitätsprinzip genügende Auswertung potenziert die relevanten tatsächlichen Anhaltspunkte für weitere Ermittlungen. Je besser, je genauer die Arbeit der Strafverfolgungsbehörden ausfällt, je mehr neue Fälle werden bekannt. Die Strafverfolgung erstickt an ihrem eigenen Erfolg.

Dies gilt nicht nur für die Fälle des Kindesmissbrauchs und der entsprechenden Darstellungen. Wirtschaftskriminalität ist ebenso ein datengetriebenes Deliktsfeld. Steuerstraftaten sind durch die Durchsicht schriftlicher Unterlagen weit schlechter aufzuklären, als durch die aggregierte Verdichtung relevanter Datenpunkte. Im Bereich der organisierten Kriminalität hat die Aufklärung relevanter Messengerdienste wie „EncroChat“[15] die besondere Bedeutung digitaler, datenorientierter Ermittlungen sehr deutlich gemacht.

Wenn die Strafverfolgung dem Anspruch des Legalitätsprinzips aktuell und vor allem mittel- bis langfristig gerecht werden will, wenn sie ihrer zentralen Rolle für die Rechtssicherheit genügen soll, geht kein Weg an der Erkenntnis vorbei, dass der Einsatz von Künstlicher Intelligenz und Automatisierung nicht fakultativ, kein „nice to have“ ist. Die Strafverfolgung muss KI & Co. einsetzen, um ihrem Auftrag von Verfassungs wegen nachzukommen.

Gegenwärtig sind vor allem drei Bereiche zu nennen:

1. Die Strafverfolgung muss den Kontakt zu ihren Kunden verbessern. Wer heute mit offenen Augen die Webseiten der Staatsanwaltschaften besucht, findet viel zu oft Faxnummern und viel zu selten KI-unterstützte Assistenten vor, die Rechtsuchende qualitätssichernd durch einfache Justizkontakte wie die Erstattung einer Strafanzeige oder die Einholung einer Besuchserlaubnis für Angehörige eines Untersuchungsgefangenen führen. Hier wird sehr viel Potenzial in Bezug auf die Kundenzufriedenheit verschenkt.

2. Die Auswertung digitaler Beweismittel muss umfassend und wo immer möglich abschließend automatisch und KI-gestützt durchgeführt werden. Nur so lassen sich die erforderlichen Effizienzgewinne erzielen. KI ist nie fehlerfrei. Die Sorge darum, ob 90 % oder 95 % aller beweisrelevanten Daten in einem Datenbestand durch die KI erkannt werden, darf jedoch – völlig unabhängig davon, dass auch die manuelle menschliche Auswertung kaum fehlerfreier sein dürfte – nicht den Blick darauf verstellen, dass der Kampf um den letzten Prozentpunkt in einem Verfahren bei endlichen Ressourcen zwingend bedeutet, eine Vielzahl von Verfahren zeitgleich überhaupt nicht bearbeiten zu können.

In diesem Bereich ist in der jüngeren Zeit schon viel bewegt worden. Polizeiliche und justizielle Arbeitsgruppen haben etwa im Bereich der Kindesmissbrauchsdarstellungen Fallgruppen für den Einsatz von Künstlicher Intelligenz diskutiert, die einer weitgehenden Automatisierung zugänglich sind. In der ZAC NRW ist ein Team von KI-Entwicklern und Juristen damit befasst, eigene Künstliche Intelligenzen für eine Vielzahl von konkreten Anwendungsfällen zu trainieren. Gleiches gilt für polizeiliche Einrichtungen. Auch wenn diese Entwicklungen zuversichtlich stimmen, wird es mit Blick auf die Komplexität der Materie eines erheblichen Einsatzes von Ressourcen bedürfen, die Technologien umfassend praxisreif zu machen.

3. KI und Automatisierung müssen als Unterstützung der staatsanwaltlichen, auch der richterlichen Entscheidung in Betracht gezogen werden. Eine ehrliche Betrachtung der in einer Staatsanwaltschaft regelmäßig zu bearbeitenden Sachverhalte offenbart, dass insbesondere im Bereich der sogenannten Bagatellkriminalität viele Fallgestaltungen automatisch vorverfügt werden können. Vielleicht lohnt es, die Debatten rund um die Verfolgung von Straftaten wie Beförderungserschleichung[16] oder „Ladendiebstahl“ weniger rechtlich als technologisch zu betrachten. Entscheidend ist weniger die Einstufung als Ordnungswidrigkeit oder als Straftat, sondern vielmehr, dass solche Massensachverhalte effizient bearbeitet werden können. Damit kann die Strafverfolgung wertvolle und in Zeiten des demografischen Wandels zunehmend knappe Ressourcen für die tatsächlichen juristischen Kernaufgaben freistellen.

Es bleibt eine wesentliche Frage: Dürfen wir das? Sicher ist auf Basis nationalen und europäischen Rechts, dass die menschliche Entscheidung durch eine KI nicht ersetzt werden darf.[17] Unterhalb des entscheidungsersetzenden Einsatzes besteht jedoch ein breites Spek-

14 Vgl. für die Polizei NRW https://www.land.nrw/pressemitteilung/mehr-polizei-im-netz-cybercrime-kriminalinspektionen-gehen-den-start.

15 Übersicht zum Thema bei Gebhard/Michalke, NJW 2022, 655 ff.

16 Vgl. https://rsw.beck.de/aktuell/daily/meldung/detail/schwarzfahren-straftat-ordnungswidrigkeit-reform-vorschlag.

17 Hartmann, RDV 2023, 300 ff.

18 Schwartmann/Keber/Zenner/Benedikt/Hartmann, KI-VO-Leitfaden, 2. Teil 1. Kap. Rn. 236.

trum an technisch möglichen und rechtlich zulässigen Anwendungsfällen. Dies zeigt nicht zuletzt der Blick in die aktuelle europäische KI-Regulierung auf: Die grundsätzliche Aufnahme der Anwendungsfälle der Strafverfolgung in den Katalog des Anhangs III KI-VO macht deutlich, dass der Einsatz von KI in der Strafverfolgung ein – wenngleich im Einzelfall (im Sinne der KI-VO) hochriskantes – grundsätzlich zulässiges Szenario ist.[18]

KI in der Strafjustiz ist kein Selbstläufer und auch nicht risikolos. Die Strafverfolgung muss sich öffnen für den Dialog mit Wissenschaft und Wirtschaft, um die technologischen Kompetenzen zu gewinnen und eine kritische Begleitung zu ermöglichen. Wo immer möglich sollten Entwicklungen als Open Source veröffentlicht werden, damit Kontrolle durch die Fachwelt möglich wird. Die Justiz benötigt fachlich qualifizierte Bedienstete – und damit möglicherweise auch ganz neue Berufsbilder. Der Gesamtprozess der sinnvollen Implementierung von KI erfordert Geld und politische Unterstützung. Diese Aufzählung ließe sich fortsetzen. Eines ist jedoch schon jetzt deutlich: Ohne diese Ausprägungen eines festen Willens zur technologischen Veränderung wird die Strafverfolgung ihren gesetzlichen Auftrag schon in absehbarer Zeit nicht mehr erfüllen können.

Praxisfälle zum Datenschutzrecht XXXII: Haftung des Verantwortlichen für Fehler des Auftragsverarbeiters und Anforderungen an die Dienstleisterkontrolle

RAin Yvette Reif, LL.M.*

I. Sachverhalt

Das Unternehmen U betreibt einen Onlineshop und bediente sich in diesem Zusammenhang eines Auftragsverarbeiters A mit Sitz in der europäischen Union, der für es u.a. folgende Daten verarbeitete: Vor- und Nachname sowie Kontaktinformationen (Postadresse, E-Mail) der Kunden des Shops, Informationen zur Bestellhistorie und Kontoverbindungen (IBAN, BIC) derjenigen Kunden, die für ihren Einkauf per Lastschrift bezahlt haben. Der Vertrag von U mit dem Auftragsverarbeiter A endete zum 01.12.2019. Am 30.11.2019 teilte A dem Unternehmen U per E-Mail mit, dass die im Auftrag verarbeiteten Daten entsprechend der zwischen den Parteien bestehenden Vereinbarung nach Art. 28 Abs. 3 DS-GVO am Folgetag gelöscht würden. Tatsächlich wurden die Daten allerdings erst mehr als drei Jahre später von A gelöscht, nachdem A einem Hackerangriff zum Opfer gefallen war und in der Folge Kontaktinformationen und Kontoverbindungen von Kunden des Unternehmens U im Darknet zum Verkauf angeboten worden waren. Über den Datenschutzvorfall informierte A auf der unternehmenseigenen Website.

Der Kunde des Onlineshops K ist entsetzt über den mangelhaften Schutz seiner personenbezogenen Daten, wendet sich an seinen Vertragspartner U und begehrt Schadenersatz nach Art. 82 DS-GVO. U ist der Ansicht, dass ein Schadenersatzanspruch ihm gegenüber ausscheidet, da der Fehler in der Sphäre des Auftragnehmers liege. Auftraggeberseitig habe man sich auf die Zusage des Dienstleisters verlassen, dass die Daten, wie zugesagt, unmittelbar nach der Beendigung des Auftrages gelöscht würden. Hätte sich der Auftragnehmer an diese Zusage gehalten, wäre es zu der Veröffentlichung der Daten von K im Darknet nicht gekommen. Kunde K solle sich insofern an den Auftragnehmer A halten mit dem von ihm geltend gemachten Anspruch.

Besteht ein materieller bzw. immaterieller Schaden unterstellt, ein Anspruch aus Art. 82 DS-GVO von K gegenüber U und/oder A?[1]

II. Musterlösung

1. Allgemeines

Der Schadenersatzanspruch nach Art. 82 Abs. 1 DS-GVO erfordert einen DS-GVO-Verstoß des Anspruchsgegners, einen materiellen oder immateriellen Schaden des Anspruchstellers sowie einen Kausalzusammenhang zwischen Verstoß und Schaden.[2] Es handelt sich um eine verschuldensabhängige Haftung, allerdings stellt Art. 82 Abs. 3 DS-GVO eine widerleg-

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

1 Der Sachverhalt für diesen Praxisfall ist angelehnt an OLG Dresden, Urt. v. 10.09.2024 – 4 U 602/24 (vgl. auch die im selben Zusammenhang ergangenen weiteren Urteile des OLG Dresden v. 10.09.2024 – 4 U 683/24; v. 17.09.2024 – 4 U 506/24; v. 15.10.2024 – 4 U 422/24; v. 15.10.2024 – 4 U 940/24; v. 05.11.2024 – 4 U 729/24).

2 Pohle/Adelberg, ZD 2024, 312 (312).

bare Verschuldensvermutung zu Lasten des Anspruchsgegners auf.[3] Sein Verschulden wird danach zunächst unterstellt und er nur dann frei von der Haftung, wenn er nachweisen kann, dass er „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist". Diese Verschuldensvermutung ist auch der Grund, warum Art. 82 DS-GVO aus Sicht des Anspruchsstellers im Verhältnis zu anderen möglichen Rechtsgrundlagen für einen Schadenersatzanspruch wegen Datenschutzverstößen, wie insbes. § 280 Abs. 1 und § 823 BGB, welche durch die Regelung in Art. 82 DS-GVO nicht verdrängt werden, vorzugswürdig ist. Mehrere an der Datenverarbeitung Beteiligte haften gegenüber der betroffenen Person gesamtschuldnerisch und unterschiedliche Verantwortungsbeiträge im Hinblick auf den entstandenen Schaden sind lediglich im Innenverhältnis der an der Verarbeitung Beteiligten auszugleichen (Art. 82 Abs. 4 und 5 DS-GVO).

2. Schadenersatzanspruch gegenüber U

U beruft sich gegenüber seinem Kunden K darauf, dass der Fehler, der zu der Veröffentlichung der Daten von K im Darknet geführt habe, nicht in seiner Sphäre liege, sondern in derjenigen des Auftragsverarbeiters A und K sich deshalb an diesen wenden müsse.

Zwar sind nach Art. 82 DS-GVO auch Schadenersatzansprüche der betroffenen Person gegenüber dem Auftragsverarbeiter möglich, so dessen Abs. 1 explizit: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter." Dennoch ist fraglich, ob U als Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO seinen Kunden hier an A verweisen darf.

Den Fall, dass sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt sind und diese gemäß Art. 82 Abs. 2 und 3 DS-GVO für einen durch die Verarbeitung verursachten Schaden verantwortlich sind, regelt Art. 82 Abs. 4 DS-GVO explizit und geht insofern zugunsten der betroffenen Person von einer gesamtschuldnerischen Haftung von Verantwortlichem und Auftragsverarbeiter aus. Der Geschädigte kann also grundsätzlich frei entscheiden, wen von den Beteiligten er in Anspruch nimmt und jeder Beteiligte haftet im Außenverhältnis zu ihm auf die volle Summe.[4] Ein Ausgleich mit Blick auf die jeweiligen Verschuldensbeiträge erfolgt lediglich im Innenverhältnis der Beteiligten.[5] Der Geschädigte muss sich nicht darauf verweisen lassen, dass einer der Beteiligten nur einen geringen Anteil an der Schadensentstehung gehabt hat.[6]

Da Art. 82 Abs. 4 DS-GVO dem ausdrücklichen Wortlaut nach nur eingreift, sofern die Beteiligten „gemäß den Abs. 2 und 3" für einen durch die Verarbeitung verursachten Schaden verantwortlich sind, ergibt sich zwar die Frage, ob sich ein als Auftraggeber für die Datenverarbeitung Verantwortlicher ggf. nach Art. 82 Abs. 3 DS-GVO exkulpieren kann mit der Folge, dass auch im Außenverhältnis nur der Auftragsverarbeiter haftet. Der Wortlaut des Art. 82 Abs. 4 DS-GVO scheint für eine solche Exkulpationsmöglichkeit zu sprechen. Gegen eine solche Exkulpationsmöglichkeit spricht jedoch, dass es gerade zu den Grundprinzipien der Auftragsverarbeitung zählt, dass trotz Auslagerung der Datenverarbeitung die auslagernde Stelle als Verantwortlicher Ansprechpartner gegenüber der betroffenen Person bleibt.[7] Im Fall der Exkulpation müsste die betroffene Person nicht nur gegen ihr unbekannte Auftragsverarbeiter vorgehen, mit denen sie in keinerlei vertraglichen Beziehungen steht und die ggf. im Ausland niedergelassen sind, sondern trüge auch noch das Risiko einer möglichen Insolvenz des jeweiligen Auftragsverarbeiters.[8] Ein Abschieben der Haftung auf den Auftragsverarbeiter würde einem „wirksamen Schadenersatz" i.S.v. Art. 82 Abs. 4 DS-GVO (vgl. auch ErwG 146 S. 6 DS-GVO) entgegenstehen.[9]

Im Ergebnis kann die Beantwortung der Frage im vorliegenden Fall dahinstehen, da Unternehmen U hier die Voraussetzungen an eine Exkulpation nach Art. 82 Abs. 3 DS-GVO nicht erfüllt. Denn die Haftung entfällt nach dieser Bestimmung nur, sofern der Verantwortliche bzw. Auftragsverarbeiter nachweisen kann, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Notwendig ist der Nachweis, dass sämtliche Sorgfaltsanforderungen erfüllt wurden und dem Verantwortlichen bzw. Auftragsverarbeiter nicht die geringste Fahrlässigkeit vorzuwerfen ist.[10] Den Auftraggeber trifft im Rahmen von Art. 28 DS-GVO aber nicht nur die Pflicht, den Auftragsverarbeiter sorgfältig auszuwählen, sondern zudem auch eine Verpflichtung zur sorgfältigen Überwachung desselben.[11] Zu einer sorgfältigen Überwachung wird es regelmäßig gehören, dass sich der Auftraggeber der Auftragsverarbeitung die Löschung verarbeiteter Daten nach Auftragsbeendigung nicht nur zusichern lässt, sondern eine entsprechende Bestätigung nach Durchführung der Löschung verlangt.[12] Dies ist vorliegend nicht geschehen, so dass U nicht sämtliche Sorgfaltspflichten erfüllt hat und die Voraussetzungen von Art. 82 Abs. 3 DS-GVO nicht vorliegen.[13]

Auch die übrigen Voraussetzungen eines Schadenersatzanspruches nach Art. 82 DS-GVO gegenüber U sind vorliegend gegeben, insbes. lässt sich der Schaden des K, der nach dem Sachverhalt zu unterstellen war, kausal auf die verspätete Löschung der Daten zurückführen. Wären die Daten am 1.12.2019 durch A gelöscht worden, hätten sie nicht durch den Hackerangriff abgegriffen werden und später im Darknet auftauchen können. Wie dargestellt, muss sich U mangels Exzess des A die verspätete Löschung durch Letzteren zurechnen lassen. Im Übrigen ist auch die eigene Pflichtverletzung des U (mangelhafte Kontrolle der Löschung) als kausal für den Schaden anzusehen, denn eine sachgerechte Kontrolle hätte den Schaden verhindern können.

U haftet damit gegenüber der betroffenen Person K auf Schadenersatz nach Art. 82 DS-GVO und dies in voller Höhe des Schadens, der K entstanden ist, und nicht nur anteilig entspre-

3 Pohle/Adelberg, ZD 2024, 312 (312).

4 Kühling/Buchner/Bergt, DS-GVO BDSG, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 57.

5 Kühling/Buchner/Bergt, DS-GVO Art. 82 Rn. 57.

6 Kühling/Buchner/Bergt, DS-GVO Art. 82 Rn. 57.

7 So zu Recht Simitis/Hornung/Spiecker gen. Döhmann/Boehm, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 82 Rn. 26; ähnlich auch OLG Dresden, Urt. v. 10.09.2024 – 4 U 602/24 in der Entscheidung, an die dieser Praxisfall angelehnt ist.

8 Kühling/Buchner/Bergt, DS-GVO Art. 82 Rn. 55; Simitis/Hornung/Spiecker gen. Döhmann/Boehm, DS-GVO Art. 82 Rn. 26.

9 OLG Dresden, Urt. v. 10.09.2024 – 4 U 602/24.

10 Vgl. etwa Kühling/Buchner/Bergt, DS-GVO Art. 82 Rn. 54; Taeger/Gabel/Moos/Schefzig, DS-GVO – BDSG – TTDSG, 4. Aufl. 2022, DS-GVO Art. 82 Rn. 80 („Verschuldensquote von 0 %").

11 OLG Dresden, Urt. v. 10.09.2024 – 4 U 602/24.

12 AA OLG Stuttgart, Beschl. v. 15.10.2024 – 4 U 49/24.

13 OLG Dresden, Urt. v. 10.09.2024 – 4 U 602/24; aA OLG Stuttgart, Beschl. v. 15.10.2024 – 4 U 49/24.

chend seinem Verantwortungsbeitrag. Der Umstand, dass hier die Hauptverantwortung für den Schaden des K wohl beim Auftragnehmer A zu suchen ist, erlangt nur im Innenverhältnis zwischen U und A Bedeutung, d.h., U hat einen dessen Verantwortungsanteil entsprechenden Regressanspruch gegenüber A.

3. Schadenersatzanspruch gegenüber A

Gemäß Art. 82 DS-GVO haftet auch ein Auftragsverarbeiter gegenüber der betroffenen Person auf Schadenersatz (vgl. Abs. 1). Nach Abs. 2 S. 2 der Bestimmung gilt dies allerdings nur, „wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat". Die eingeschränkte Haftung des Auftragsverarbeiters trägt dem Umstand Rechnung, dass es eben nicht er, sondern sein Auftraggeber ist, der die Verantwortlichkeit für die Datenverarbeitung trägt. Der Auftraggeber legt als Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO Zwecke und wesentliche Mittel der Datenverarbeitung fest, während der Auftragsverarbeiter mit den im Auftrag verarbeiteten personenbezogenen Daten nur auf Weisung des Verantwortlichen umgehen darf (Art. 28 Abs. 3 S. 2 lit. a) DS-GVO). Lediglich wenn der Auftragsverarbeiter selbst über Zwecke und Mittel der Verarbeitung entscheidet und sich entgegen der Vereinbarung selbst zum Verantwortlichen aufschwingt, haftet er auch als ein solcher (sog. Exzess, vgl. Art. 28 Abs. 10 DS-GVO). Dies ist hier nicht der Fall. Zwar hat A gegen seine Pflichten verstoßen, indem er die Daten nicht zum angekündigten Zeitpunkt gelöscht hat. Er hat aber nicht über Zwecke und Mittel der Datenverarbeitung bestimmt. Eine Haftung von A kommt hier demnach nur als Auftragsverarbeiter und unter Beachtung der Rahmenbedingungen von Art. 82 Abs. 2 S. 2 DS-GVO in Betracht.

Der Vorwurf gegenüber A besteht vorliegend darin, entgegen der bestehenden Vereinbarung nach Art. 28 Abs. 3 DS-GVO sowie seiner eigenen Zusicherung per E-Mail vom 30.11.2019 nicht gelöscht zu haben. Bei der Nichtlöschung der im Auftrag verarbeiteten Daten handelt es sich um eine der Sphäre des Auftragsverarbeiters zuzuordnende Pflichtverletzung. Die Löschung der Daten (bzw. alternativ deren Rückgabe) nach Abschluss der Erbringung der Verarbeitungsleistung gehört zu den klassischen zentralen Pflichten des Auftragsverarbeiters, was sich auch an Art. 28 Abs. 3 S. 2 lit. g) DS-GVO zeigt, wonach zu den Mindestinhalten eines Auftragsverarbeitungsvertrages u.a. eine Vereinbarung dahingehend zählt, was mit den verarbeiteten Daten nach Beendigung der Beziehung zu geschehen hat. Nach Sinn und Zweck von Art. 82 DS-GVO hat der Auftragsverarbeiter für einen Schaden der betroffenen Person, welcher aus der Verletzung dieser Löschverpflichtung entsteht, entsprechend einzustehen. Dies gilt unabhängig davon, ob eventuell die Voraussetzungen von Art. 82 Abs. 2 S. 2 DS-GVO nicht unmittelbar erfüllt sind, da die Löschverpflichtung des A keine „speziell den Auftragsverarbeitern auferlegte Pflicht aus dieser Verordnung" (Art. 82 Abs. 2 S. 2 Alt. 1 DS-GVO), sondern eine Pflicht ist, die auf dem Auftragsverarbeitungsvertrag beruht, und mangels entsprechender Weisung durch U auch nicht weisungswidrig gehandelt wurde durch A (Art. 82 Abs. 2 S. 2 Alt. 2 DS-GVO). Bei der Aufnahme des Auftragsverarbeiters als möglichen Anspruchsgegner im Rahmen von Art. 82 DS-GVO ging es dem Verordnungsgeber darum, dass auch der Auftragsverarbeiter von der betroffenen Person in Anspruch genommen werden können soll, sofern er „auftragsverarbeiterspezifischen Pflichten"[14] nicht nachgekommen ist. Die gesamtschuldnerische Haftung zwischen Auftraggeber und -nehmer der Auftragsverarbeitung trägt maßgeblich dazu bei, dass „ein wirksamer Schadenersatz für die betroffene Person sichergestellt ist" (Art. 82 Abs. 4 DS-GVO). Die Verletzung der Löschpflicht kommt damit als den Schadenersatz nach Art. 82 DS-GVO begründende Pflichtverletzung des A in Betracht.

Für eine Exkulpation des A gemäß Art. 82 Abs. 3 DS-GVO bestehen keine Anhaltspunkte, so dass auch von der Schuldhaftigkeit der Pflichtverletzung durch A auszugehen ist. Ohne die Pflichtverletzung seitens A wäre der Schaden des betroffenen K nicht entstanden, so dass des Weiteren die Kausalität zwischen Pflichtverletzung und Schaden zu bejahen ist.

Nach alledem hat K auch gegen A einen Anspruch auf Schadenersatz nach Art. 82 DS-GVO. K kann sich entscheiden, ob er U und/oder A in Anspruch nehmen will. Er kann den gesamten Schaden gegen einen der Beteiligten geltend machen oder aber jeweils anteiligen Schadenersatz von beiden Parteien verlangen.

III. Weiterführende Hinweise

Rund um den Schadenersatzanspruch nach Art. 82 DS-GVO bestanden nach dem Inkrafttreten der DS-GVO diverse ungeklärte Fragen. Inzwischen haben eine Reihe von EuGH-Entscheidungen zu der Vorschrift wichtige Punkte geklärt. Die zentralen Aussagen des EuGH finden sich nachfolgend zusammengefasst:

- Ein bloßer Verstoß gegen die DS-GVO reicht nicht, um einen Anspruch aus Art. 82 DS-GVO zu begründen (EuGH, Urt. 04.05.2023 – C-300/21; Urt. v. 14.12.2023 – C-456/22; Urt. 11.04.2024 – C-741/21; Urt. v. 20.06.2024 – C-590/22 PS). Betroffene Personen müssen auch nachweisen, dass ihnen ein materieller oder immaterieller Schaden entstanden ist (EuGH, Urt. v. 25.01.2024 – C-687/21; Urt. v. 20.06.2024 – C-590/22 PS).
- DS-GVO-Schadenersatz ist nicht vom Erreichen einer Erheblichkeitsschwelle abhängig (EuGH, Urt. v. 04.05.2023 – C-300/21; Urt. v. 14.12.2023 – C-456/22; Urt. 11.04.2024 – C-741/21; Urt. v. 20.06.2024 – C-590/22 PS).
- Die Furcht vor Datenmissbrauch bzw. ein zeitlich begrenzter Verlust der Kontrolle über die eigenen personenbezogenen Daten kann einen immateriellen Schaden begründen; der Schaden muss aber ordnungsgemäß nachgewiesen werden (EuGH, Urt. v. 14.12.2023 – C-340/21; Urt. v. 11.04.2024 – C-741/21; Urt. v. 20.06.2024 – C-590/22 PS; Urt. v. 04.10.2024 – C-200/23).
- DS-GVO-Schadenersatz hat „Ausgleichsfunktion", keine Straf- oder Abschreckungsfunktion[15] (EuGH, Urt. v. 21.12.2023 – C-667/21; Urt. v. 25.01.2024 – C-687/21; Urt. v. 20.06.2024 – C-182/22 und C-189/22; Urt. v. 20.06.2024 – C-590/22 PS).

14 Spindler/Schuster/Spindler/Horváth, Recht der elektronischen Medien, 4. Aufl. 2019, DS-GVO Art. 82 Rn. 10.

15 Vgl. in diesem Zusammenhang auch BGH, Urt. v. 18.11.2024 – VI ZR 10/24: 100 Euro Schadenersatz für Kontrollverlust bei Scraping angemessen.

RECHTSPRECHUNG

HIGHLIGHTS FÜR DEN BETRIEBLICHEN DATENSCHUTZ

EuGH setzt der Verarbeitung von Daten für personalisierte Werbung Grenzen („Schrems III")

(EuGH, Urteil vom 4. Oktober 2024 – C-446/21 –)

Relevanz für die Praxis

Die Entscheidung erlangt praktische Relevanz für alle Anbieter von Online-Diensten, die ihr Angebot zumindest auch über die Anzeige verhaltensbasierter Werbung finanzieren. Rechtlich stellt sich für die entsprechenden Anbieter zum einen die Frage, ob die Einholung einer Einwilligung nach Art. 7 DS-GVO erforderlich ist oder eine Rechtfertigung auch über ein Vertragskonstrukt denkbar ist. Zum anderen ist entscheidend, welche Bedingungen die Datenverarbeitung erfüllen muss. Der EuGH hat in der vorliegenden Entscheidung die Anforderungen an eine rechtmäßige Verarbeitung mit Blick auf den Grundsatz der „Datenminimierung" und auf die Verarbeitung besonderer Kategorien personenbezogener Daten näher konkretisiert und den Handlungsspielraum der Anbieter eingeschränkt.

Der EuGH hat klargestellt, dass der Grundsatz der „Datenminimierung" den Betreibern verbietet, sämtliche personenbezogenen Daten, die durch den betroffenen Online-Dienst selbst und außerhalb der Plattform erworben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach Zweckbestimmung zu verarbeiten. Es muss vielmehr eine Prüfung der Verhältnismäßigkeit je nach Datum und Zweckbestimmung erfolgen.

Besondere Vorsicht ist zudem im Kontext von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO geboten. Eine hierunter fallende Information darf zwar dann verarbeitet werden, wenn die betroffene Person die Information einer breiten Öffentlichkeit zugänglich gemacht hat (Art. 9 Abs. 2 lit. e) DS-GVO). Dies berechtigt Verantwortliche aber nicht, dieselbe Information auch an anderer, nicht öffentlicher Stelle, wie bspw. einem privaten Facebook-Profil, zu sammeln. Die öffentliche Bekanntgabe hebt den Schutz des spezifischen Datums durch Art. 9 DS-GVO nicht in Gänze auf. Die Sammlung von inhaltsgleichen Daten an anderen Stellen bleibt dennoch verboten.

1. **Art. 5 Abs. 1 lit. c) der Verordnung (EU) 2016/679 […] (Datenschutz-Grundverordnung) 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 lit. 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 ggf. 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.**

Zur zweiten Frage:

Mit seiner zweiten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 5 Abs. 1 lit. c) DS-GVO 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. […]

Als Erstes ist darauf hinzuweisen, dass das Ziel der DS-GVO, wie aus ihrem Art. 1 und aus ihren ErwGn 1 und 10 hervorgeht, insbesondere darin besteht, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres in Art. 8 Abs. 1 der Charta und in Art. 16 Abs. 1 AEUV verankerten Rechts auf Privatleben – bei der Verarbeitung personenbezogener Daten zu gewährleisten (Urt. v. 07.03.2024, IAB Europe, C-604/22, EU:C:2024:214, Rn. 53 und die dort angeführte Rechtsprechung).

Zu diesem Zweck enthalten die Kapitel II und III der Verordnung die Grundsätze für die Verarbeitung personenbezogener Daten bzw. die Rechte der betroffenen Person, die bei jeder Verarbeitung personenbezogener Daten beachtet werden müssen. Vorbehaltlich der in Art. 23 der Verordnung vorgesehenen Ausnahmen muss jede Verarbeitung personenbezogener Daten insbesondere zum einen im Einklang mit den in Art. 5 der Verordnung aufgestellten Grundsätzen zur Verarbeitung solcher Daten im Einklang stehen und die in Art. 6 der Verordnung genannten Rechtmäßigkeitsvoraussetzungen erfüllen sowie zum anderen die in den Art. 12 bis 22 DS-GVO genannten Rechte der betroffenen Person beachten (Urt. v. 11.07.2024, Meta Platforms Ireland [Verbandsklage], C-757/22, EU:C:2024:598, Rn. 49 und die dort angeführte Rechtsprechung).

Wie der Gerichtshof bereits klargestellt hat, gelten die in Art. 5 DS-GVO niedergelegten Grundsätze für die Verarbeitung personenbezogener Daten kumulativ (Urt. v. 20.10.2022, Digi, C-77/21, EU:C:2022:805, Rn. 47).

Gemäß Art. 5 Abs. 1 lit. a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Diese Daten müssen gemäß Art. 5 Abs. 1 lit. b) DS-GVO für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

Des Weiteren bestimmt Art. 5 Abs. 1 lit. c) DS-GVO, in dem der sogenannte Grundsatz der „Datenminimierung" verankert ist, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein" müssen (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 109 sowie die dort angeführte Rechtsprechung).

Mit diesem Grundsatz wird, wie der Gerichtshof bereits entschieden hat, der Grundsatz der Verhältnismäßigkeit zum Ausdruck gebracht (vgl. in diesem Sinne Urt. v. 22.06.2021, Latvijas Republikas Saeima [Strafpunkte], C-439/19, EU:C:2021:504, Rn. 98 und die dort angeführte Rechtsprechung, sowie vom 30.01.2024, Direktor na Glavna direktsia „Natsionalna politsia" pri MVR – Sofia, C-118/22, EU:C:2024:97, Rn. 41).

Gemäß dem in Art. 5 Abs. 2 DS-GVO genannten Grundsatz der Rechenschaftspflicht muss der Verantwortliche nachweisen können, dass die personenbezogenen Daten unter Einhaltung der in Abs. 1 dieses Artikels genannten Grundsätze erhoben und verarbeitet werden (vgl. in diesem Sinne Urt. v. 20.10.2022, Digi, C-77/21, EU:C:2022:805, Rn. 24). Außerdem obliegt es nach Art. 13 Abs. 1 lit. 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 für die Verarbeitung zu informieren (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 95).

Als Zweites 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 (Urt. v. 24.02.2022, Valsts ieņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C-175/20, EU:C:2022:124, Rn. 79).

Die Folgen für die Interessen und das Privatleben der betroffenen Person sind nämlich umso schwerer und die Anforderungen an die Rechtmäßigkeit der Speicherung der betreffenden Daten sind umso höher, je länger diese gespeichert werden (vgl. in diesem Sinne Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 95).

Des Weiteren ist darauf hinzuweisen, dass gemäß Art. 5 Abs. 1 lit. e) DS-GVO 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.

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 Urt. v. 20.10.2022, Digi, C-77/21, EU:C:2022:805, Rn. 53).

Daraus ergibt sich, wie der Gerichtshof bereits entschieden hat, dass selbst eine ursprünglich zulässige Verarbeitung von Daten im Lauf der Zeit gegen die DS-GVO 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 Urt. v. 20.10.2022, Digi, C-77/21, EU:C:2022:805, Rn. 54 und die dort angeführte Rechtsprechung).

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 lit. c) DS-GVO 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.

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 DS-GVO diesen Nutzern garantiert, anzusehen.

Was als Drittes 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 lit. c) DS-GVO 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 (Urt. v. 24.02.2022, Valsts ieņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C-175/20, EU:C:2022:124, Rn. 74).

Ferner muss der Verantwortliche gemäß Art. 25 Abs. 2 DS-GVO 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.

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 so-

zialen 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.

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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, Rn. 118).

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.

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 DS-GVO garantiert werden.

Nach alledem ist auf die zweite Frage zu antworten, dass Art. 5 Abs. 1 lit. c) DS-GVO 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:

Mit der vierten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 9 Abs. 2 lit. e) DS-GVO 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 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.

Insbesondere möchte das vorlegende Gericht wissen, ob Herr Schrems aufgrund der Äußerung, die er bei einer Podiumsdiskussion getätigt hat, keinen Anspruch mehr auf den durch Art. 9 Abs. 1 DS-GVO gewährten Schutz hat und ob Facebook folglich berechtigt war, andere Daten über seine sexuelle Orientierung zu verarbeiten.

Zunächst ist festzustellen, dass die vom vorlegenden Gericht angeführte Podiumsdiskussion, in deren Rahmen Herr Schrems sich zu seiner sexuellen Orientierung äußerte, am 12.02.2019 stattfand und, wie aus der Vorlageentscheidung hervorgeht, Meta Platforms Ireland zu diesem Zeitpunkt bereits personenbezogene Daten zur sexuellen Orientierung von Herrn Schrems verarbeitete, so dass diese Äußerung nach dem Beginn einer solchen Datenverarbeitung erfolgte.

Daraus folgt, dass die vierte Frage des vorlegenden Gerichts so zu verstehen ist, dass sie nur etwaige Verarbeitungen von Daten über die sexuelle Orientierung von Herrn Schrems betrifft, die Meta Platforms Ireland nach dem 12.02.2019 vorgenommen haben soll. Es ist jedoch gemäß der in Rn. 42 des vorliegenden Urteils angeführten Rechtsprechung Sache des vorlegenden Gerichts, zu prüfen, ob nach diesem Zeitpunkt solche Verarbeitungen tatsächlich stattgefunden haben.

Zur Beantwortung dieser Frage ist als Erstes darauf hinzuweisen, dass nach dem 51. ErwG der DS-GVO 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 ErwG ausgeführt, dass derartige personenbezogene Daten nicht verarbeitet werden sollten, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig.

In diesem Zusammenhang stellt Art. 9 Abs. 1 DS-GVO 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.

Für die Zwecke der Anwendung von Art. 9 Abs. 1 DS-GVO 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 genannten 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 DS-GVO vorgesehenen Ausnahmen untersagt.

Wie der Gerichtshof bereits entschieden hat, gilt dieses in Art. 9 Abs. 1 DS-GVO 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 DS-GVO genannten Kategorien fallen, zielt diese Vorschrift nämlich darauf ab, solche Datenverarbeitungen unabhängig von ihrem erklärten Zweck zu verbieten (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C 252/21, Rn. 69 und 70).

Zwar ist nach Art. 9 Abs. 1 DS-GVO die Verarbeitung von Daten u.a. zur sexuellen Orientierung grundsätzlich untersagt, Art. 9 Abs. 2 DS-GVO sieht allerdings in seinen lit. 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 (Urt. v. 21.12.2023, Krankenversicherung Nordrhein, C 667/21, EU:C:2023:1022, Rn. 47).

Insbesondere zur Ausnahme des Art. 9 Abs. 2 lit. e) DS-GVO ist darauf hinzuweisen, dass nach dieser Bestimmung das in Art. 9 Abs. 1 DS-GVO 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".

Da Art. 9 Abs. 2 lit. e) DS-GVO eine Ausnahme vom Grundsatz des Verbots der Verarbeitung besonderer Kategorien personenbezogener Daten vorsieht, ist er eng auszulegen (vgl. in diesem Sinne Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C 252/21, Rn. 76 und die dort angeführte Rechtsprechung).

Folglich ist für die Zwecke der Anwendung der in Art. 9 Abs. 2 lit. e) DS-GVO 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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C 252/21, Rn. 77).

Vorliegend geht aus der Vorlageentscheidung hervor, dass die am 12.02.2019 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.

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 lit. e) der DS-GVO offensichtlich öffentlich gemacht hat.

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 DS-GVO und im Einklang mit den Anforderungen, die sich aus den anderen Bestimmungen der DS-GVO ergeben, verarbeitet werden können (vgl. in diesem Sinne Urt. v. 24.09.2019, 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.

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

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 lit. a) DS-GVO dazu erteilt hat, dass der Betreiber einer Onlineplattform für ein soziales Netzwerk andere Daten über ihre sexuelle Orientierung verarbeitet.

Nach alledem ist auf die vierte Frage zu antworten, dass Art. 9 Abs. 2 lit. e) DS-GVO 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.

Zur Vertiefung

Reif, Praxisfälle zum Datenschutzrecht XXVIII: Die neue Gleichstellungsbeauftragte – Die Rechtsgrundlagen der Verarbeitung von Daten nach Art. 9 DS-GVO= RDV 3/2024

Reif, Praxisfälle zum Datenschutzrecht XVI: Gewinnung von Neukunden mittels personalisierter Werbung = RDV 3/2022

Enge Auslegung des Begriffs des berechtigten Interesses

(EuGH, Urteil vom 4. Oktober 2024 – C-621/22 –)

Relevanz für die Praxis

In diesem Urteil präzisiert der EuGH seine Rechtsprechung zur Rechtfertigung einer Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO. Grundsätzlich verlangt diese das kumulative Vorliegen von drei Voraussetzungen: die Wahrnehmung eines berechtigten Interesses, die Erforderlichkeit der Verarbeitung zur Verwirklichung des berechtigten Interesses und das Überwiegen des berechtigten Interesses gegenüber Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person. Da Art. 6 Abs. 1 UAbs. 1 lit. b) - f) DS-GVO dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist, sind die entsprechenden Tatbestände eng auszulegen. Im Rahmen von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO führt das zunächst dazu, dass das geltend gemachte berechtigte Interesse rechtmäßig sein muss. Außerdem ist im Rahmen der

Prüfung der Erforderlichkeit der Verarbeitung der Grundsatz der Datenminimierung zu prüfen. Eine Verarbeitung ist deshalb nur zur Wahrung des berechtigten Interesses erforderlich, wenn sie absolut notwendig ist. Das ist grundsätzlich nicht der Fall, wenn es möglich wäre, die betroffenen Personen zu informieren und sie zu fragen, ob sie möchten, dass ihre Daten für Werbe- oder Marketingzwecke an Dritte weitergegeben werden.

In der Praxis stellt Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO weiterhin eine wichtige Rechtsgrundlage dar, vor allem wenn es um Verarbeitungen personenbezogener Daten aus wirtschaftlichem Interesse geht. Verantwortliche sollten aber vor dem Hintergrund der eng auszulegenden Erforderlichkeit genau prüfen, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, insbesondere durch Einholen einer Einwilligung.

Art. 6 Abs. 1 UAbs. 1 lit. f) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ist dahin auszulegen, dass 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.

Zu den Vorlagefragen:

Nach Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung 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 DS-GVO erteilt, ist eine solche Verarbeitung gleichwohl gerechtfertigt, wenn sie eine der in Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) genannten Voraussetzungen in Bezug auf die Erforderlichkeit erfüllt.

In diesem Zusammenhang sind die in Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) DS-GVO vorgesehenen Rechtfertigungsgründe eng auszulegen, da sie dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 93 und die dort angeführte Rechtsprechung).

Außerdem braucht nach der Rechtsprechung des Gerichtshofs, wenn festgestellt werden kann, dass eine Verarbeitung personenbezogener Daten aus einem der in Art. 6 Abs. 1 UAbs. 1 lit. b) bis f) DS-GVO vorgesehenen Gründe erforderlich ist, nicht geprüft zu werden, ob diese Verarbeitung auch unter einen anderen dieser Gründe fällt (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 94 und die dort angeführte Rechtsprechung).

Der Gerichtshof hat zudem entschieden, dass nach Art. 5 DS-GVO 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 lit. 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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 95).

Im vorliegenden Fall geht aus den dem Gerichtshof vorliegenden Akten hervor, dass die Mitglieder des KNLTB nicht im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. a) DS-GVO eingewilligt haben, dass der KNLTB sie betreffende personenbezogene Daten gegen Entgelt gegenüber Dritten, namentlich Tennis-Direct und der NLO, offenlegt.

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

Insoweit ist darauf hinzuweisen, dass nach Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO 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.

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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 106 und die dort angeführte Rechtsprechung).

Was erstens die Voraussetzung der Wahrnehmung eines „berechtigten Interesses" betrifft, kann in Ermangelung einer Definition dieses Begriffs durch die DS-GVO, wie der Gerichtshof bereits entschieden hat, ein breites Spektrum von Interessen grundsätzlich als berechtigt gelten (vgl. in diesem Sinne Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 76).

Wie sich auch aus dem 47. ErwG der DS-GVO 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 UAbs. 1 lit. f) dieser Verordnung ist. Dies gilt umso mehr, als dieser ErwG die Zwecke der Direktwerbung im Allgemeinen als Beispiel für berechtigte Interessen anführt, die von einem Verantwortlichen wahrgenommen werden können.

Allerdings verlangt der Begriff „berechtigtes Interesse" im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO, auch wenn er nicht auf gesetzlich verankerte und bestimmte Interessen beschränkt ist, dass das geltend gemachte berechtigte Interesse rechtmäßig ist.

Außerdem obliegt es nach Art. 13 Abs. 1 lit. d) DS-GVO 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 UAbs. 1 lit. f) DS-GVO beruht (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 107).

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 (Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 77 sowie die dort angeführte Rechtsprechung).

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 lit. c) DS-GVO verankert ist und verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" sind (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 109 und die dort angeführte Rechtsprechung).

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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 110 und die dort angeführte Rechtsprechung).

Außerdem können, wie sich aus dem 47. ErwG der DS-GVO 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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 112).

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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 96, und v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 81 sowie die dort angeführte Rechtsprechung).

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 UAbs. 1 lit. f) DS-GVO 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 Casinospielen in den Niederlanden, offenzulegen.

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 UAbs. 1 lit. f) DS-GVO angesehen werden kann (vgl. entsprechend Urt. v. 13.05.2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 73).

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 UAbs. 1 lit. f) DS-GVO 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.

Sollte ein solches Interesse als berechtigt angesehen werden, müsste der Verantwortliche zudem allen anderen ihm obliegenden Pflichten aus der DS-GVO nachkommen, damit die Wahrnehmung dieses Interesses eine Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 UnterAbs. 1 lit. f) DS-GVO rechtfertigen kann.

Was zweitens die Voraussetzung der Erforderlichkeit dieser Verarbeitung zur Verwirklichung des betreffenden Interesses 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.

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 Urt. v. 12.09.2024, HTB Neunte Immobilien Portfolio und Ökorenta Neue Energien Ökostabil IV, C-17/22 und C-18/22, EU:C:2024:738, Rn. 60).

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 Urt. v. 12.09.2024, HTB Neunte Immobilien Portfolio und Ökorenta Neue Energien Ökostabil IV, C-17/22 und C-18/22, EU:C:2024:738, Rn. 61).

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 (Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 116).

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. ErwG der DS-GVO 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.

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. ErwG der DS-GVO 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.

Zur Vertiefung

Benedikt/Pfau, Meta führt bezahlpflichtiges Abonnement ein – PUR-Modelle an der Schnittstelle zwischen Datenschutz, Privatautonomie und unternehmemerischer Freiheit = RDV 1/2024

[Urteil] Prüfungskompetenz von Kartellbehörden bezüglich der Verletzung von Datenschutzvorschriften = RDV 5/2023

WICHTIGES AUS DER RECHTSPRECHUNG

Schadenersatzanspruch allein aufgrund des Kontrollverlustes über die eigenen Daten

(BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –)

Immaterieller Schaden im Sinne des Art. 82 Abs. 1 DS-GVO 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.

Aus den Gründen:

Nach der Rechtsprechung des Gerichtshofes erfordert ein Schadenersatzanspruch im Sinne des Art. 82 Abs. 1 DS-GVO 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, Urt. v. 04.10.2024 – C-507/23, juris Rn. 24 – Pateretāju tieslbu aizsardzlbas centrs; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 34 – juris; v. 25.01.2024 – 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 DS-GVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH, Urt. v. 11.04.2024-C-741/21, NJW2024,1561 Rn. 35-juris; v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 60 f. – MediaMarktSaturn). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadenersatzanspruches nach Art. 82 Abs. 1 DS-GVO ein Verschulden des Verantwortlichen. Art. 82 DS-GVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DS-GVO dem Verantwortlichen (vgl. EuGH, Urt. v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 44 ff. -juris; v. 21.12.2023 – C-667/21, EuZW 2024, 270 Rn. 94 – Krankenversicherung Nordrhein; vgl. ferner ErwG 146 S. 2 DS-GVO).

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 lit. b), Art. 25 Abs. 2, Art. 32 Abs. 1 DS-GVO vorliegt, und deshalb die hierzu erforderlichen Feststellungen nicht getroffen hat (s. hierzu aber unten B.VIII.1).

aa) Dabei bedarf es im Streitfall keiner Entscheidung, ob ein Verstoß gegen die Datenschutz-Grundverordnung im Sinne des Art. 82 Abs. 1 DS-GVO nicht nur die unrechtmäßige Verarbeitung von personenbezogenen Daten erfasst, wie es Art. 82 Abs. 2 S. 1 und ErwG 146 S. 1 DS-GVO nahelegen (vgl. auch EuGH, Urt. v. 04.05.2023 – C-300/21, VersR 2023, 920 Rn. 36 – Österreichische Post: "Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DS-GVO"), 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, Urt. v. 22.11.2023 – 4 U 20/23, juris Rn. 381 ff.; offengelassen auch von OLG Oldenburg, Urt. v. 21.05.2024 – 13 U 100/23, juris Rn. 24; jeweils m.w.N.). Denn angesichts des umfassenden Verarbeitungsbegriffs des Art. 4 Nr. 2 DS-GVO (jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung) wäre auch bei einem engeren Verständnis des Art. 82 Abs. 1 DS-GVO 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.

Entsprechend hat der Gerichtshof bereits entschieden, dass bei Verstößen gegen die Vorschriften der Art. 5 bis 11 DS-GVO, mithin des zweiten Kapitels der Datenschutz-Grundverordnung, die Grundsätze für die Verarbeitung von Daten aufstellen, zugleich eine unrechtmäßige Datenverarbeitung vorliegt (vgl. EuGH, Urt. v. 04.05.2023 – C-60/22, ZD 2023, 606 Rn. 54-57 – Bundesrepublik Deutschland [Elektronisches Gerichtsfach]). Bedenken gegen die Anwendbarkeit des Art. 82 Abs. 1 DS-GVO auf Verstöße gegen Art. 5 DS-GVO bestehen daher nicht (vgl. auch bereits EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024,160 Rn. 42 f. – MediaMarktSaturn; v. 14.12.2023 – 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 DS-GVO) hat der Gerichtshof zu einzelnen Vorschriften bereits angenommen, dass ein Schadenersatzanspruch aus Art. 82 DS-GVO möglich ist (vgl. zu einem Verstoß gegen Art. 32 DS-GVO EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 42 f. – MediaMarktSaturn; v. 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 52 f. – Natsionalnaagentsia za prihodite; für Verstöße gegen Art. 26 und 30 DS-GVO, Urt. v. 04.05.2023 – C-60/22, ZD 2023, 606 Rn. 66 f. – Bundesrepublik Deutschland [Elektronisches Gerichtsfach]).

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 DS-GVO vorgesehene Schadenersatzanspruch ausschließlich eine Ausgleichsfunktion, jedoch keine Abschreckungsoder Straffunktion erfüllt und daher das Vorliegen mehrerer Verstöße nicht zu einer Erhöhung des Schadenersatzes führt (vgl. EuGH, Urt. v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 59 f., 64 f. – juris; OLG Oldenburg, Urt. v. 21.05.2024 -13 U 100/23, juris Rn. 24). […]

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

aa) Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (st. Rspr., EuGH, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 31 – PS GbR; v. 25.01.2024 – C-687/21, CR 2024,160 Rn. 64 – MediaMarkt-Saturn; v. 04.05.2023 – C-300/21, VersR 2023, 920 Rn. 30 und 44 – Österreichische Post). Dabei soll nach ErwG 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadenersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich (st. Rspr., vgl. EuGH, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 25 – PS GbR; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 34 – juris; v. 04.05.2023 – C-300/21, VersR 2023, 920 Rn. 42 – Österreichische Post).

Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DS-GVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (EuGH, Urt. v. 20.06.2024 -C-590/22, DB 2024, 1676 Rn. 26 – PS GbR; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 36 – juris; v. 04.05.2023 – C-300/21, VersR 2023, 920 Rn. 51 – Österreichische Post). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DS-GVO verpflichtet ist, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die 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, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 27 – PS GbR; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 36 – juris).

Schließlich hat der Gerichtshof in seiner jüngeren Rechtsprechung unter Bezugnahme auf ErwG 85 DS-GVO (vgl. ferner ErwG 75 DS-GVO) klargestellt, dass schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Begriff des "immateriellen Schadens" den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (EuGH, Urt. v. 04.10.2024 – C-200/23, juris Rn. 145, 156 i.V.m. 137-Agentsia po vpisvaniyata; v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 33 – PS GbR; vom 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 42 – juris; vgl. zuvor bereits EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 66 – MediaMarktSaturn; v. 14.12.2023 – C-456/22, NZA 2024, 56 Rn. 17-23 – Gemeinde Ummendorf sowie – C-340/21, NJW 2024, 1091 Rn. 82 – Natsionalna agentsia za prihodite). Im ersten Satz des 85. ErwG

der DS-GVO 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 Datenschutz-Grundverordnung fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (EuGH, Urt. v. 04.10.2024 – C-200/23, juris Rn. 145 – Agentsia po vpisvaniyata; v. 14.12.2023 – C-340/21, NJW 2024,1091 Rn. 82 – Natsionalna agentsia za prihodite).

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, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 33 – PS GbR; v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 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.

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 Schadenersatzanspruch zu begründen (vgl. EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 67 – MediaMarktSaturn; v. 14.12.2023 – 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, Urt. v. 20.06.2024 – C-590/22, DB 2024,1676 Rn. 36 – PS GbR; v. 14.12.2023 – 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, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 35 – PS GbR; v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 68 – MediaMarktSaturn).

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.

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, Urt. v. 06.02.2024 – VI ZR 526/20, WM 2024, 761 Rn. 11; v. 13.07.2021 -VI ZR 128/20, VersR 2021, 1252 Rn. 20; v. 18.05.2021 -VI ZR 401/19, VersR 2021, 1046 Rn. 19; jeweils m.w.N.).

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 DS-GVO 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.

(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 Schadenersatzklage muss der Betroffene jedoch nur darlegen, dass und in welcher Weise gerade er von dem Scraping-Vorfall betroffen war und welche Folgen dies für ihn hatte (vgl. zu einer vergleichbaren Situation in Anlegerschutzprozessen BGH, Urt. v. 06.12.2012 – III ZR 66/12, VersR 2013, 359 Rn. 15, bei denen es jedoch zumindest individuelle Anlageberatungsgespräche gab, die zu schildern waren; vgl. ferner BGH, Beschl. v. 21.03.2022 – 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.

Das Risiko der Nichterweislichkeit – auch in Bezug auf das konkrete Ausmaß eines etwaigen Schadens – verbleibt freilich beim Anspruchsteller (vgl. EuGH, Urt. v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 35 – juris).

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

(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 wähl- und grundlos der Öffentlichkeit, wie etwa im Internet, zugänglich zu machen.

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 ermitteln, sich um eine Auskunft der Beklagten kümmern und selbst weitere Maßnahmen ergreifen müssen.

(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.

Die Darlegungslast wird auch nicht dadurch erhöht, dass die Telefonnummer im Vergleich zu den in Art. 9 DS-GVO genannten besonders sensiblen Daten weniger geheimhaltungsbedürftig ist. Dieser Umstand mag sich zwar auf die Höhe eines etwaigen Schadenersatzanspruches 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.

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, Urt. v. 15.08.2023 – 7 U 19/23, juris Rn. 112,117 ff.; OLG Oldenburg, Urt. v. 21.05.2024 – 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 UAbs. 1 lit. a) DS-GVO zu prüfen.

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 DS-GVO; vgl. EuGH, Urt. v. 01.10.2019 – 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 DS-GVO), ob der Kläger seine Einwilligungserklärung auf dieser Grundlage in informierter Weise und unmissverständlich abgegeben hat (Art. 4 Nr. 11 DS-GVO) und ob die Einwilligungserklärung letztlich freiwillig erfolgt ist (Art. 7 Abs. 4, ErwG 42, 43 DS-GVO), wobei auch die beherrschende Stellung der Beklagten auf dem Markt für soziale Netzwerke zu berücksichtigen ist (vgl. EuGH, Urt. v. 04.07.2023 – C-252/21, NJW 2023, 2997 Rn. 140 ff. – Meta Platforms).

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 Substanziierung des klagebegründenden Vortrags nicht in unzulässigerweise 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.

DS-GVO steht wettbewerbsrechtlicher Verfolgung von Datenschutzverstößen nach nationalem Recht nicht entgegen

(EuGH, Urteil vom 4. Oktober 2024 - C-21/23 -)

1. **Die Bestimmungen des Kapitels VIII der Verordnung (EU) 2016/679 […] (Datenschutz-Grundverordnung) sind dahin auszulegen, dass sie einer nationalen Regelung nicht entgegenstehen, die – neben den Eingriffsbefug-**

nissen der zur Überwachung und Durchsetzung dieser Verordnung zuständigen Aufsichtsbehörden und den Rechtsschutzmöglichkeiten der betroffenen Personen – Mitbewerbern des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten die Befugnis einräumt, wegen Verstößen gegen die DS-GVO gegen den Verletzer im Wege einer Klage vor den Zivilgerichten unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken vorzugehen.

2. **Art. 8 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie Art. 9 Abs. 1 der Verordnung 2016/679 sind dahin auszulegen, dass in einem Fall, in dem der Betreiber einer Apotheke über eine Onlineplattform apothekenpflichtige Arzneimittel vertreibt, Daten, die seine Kunden bei der Onlinebestellung dieser Arzneimittel eingeben müssen (wie z.B. Name, Lieferadresse und für die Individualisierung der Arzneimittel notwendige Informationen), Gesundheitsdaten im Sinne dieser Bestimmungen darstellen, auch wenn der Verkauf dieser Arzneimittel keiner ärztlichen Verschreibung bedarf.**

Zur ersten Vorlagefrage:

Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob die Bestimmungen des Kapitels VIII DS-GVO dahin auszulegen sind, dass sie einer nationalen Regelung entgegenstehen, die – neben den Eingriffsbefugnissen der zur Überwachung und Durchsetzung dieser Verordnung zuständigen Aufsichtsbehörden und den Rechtsschutzmöglichkeiten der betroffenen Personen – Mitbewerbern des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten die Befugnis einräumt, wegen Verstößen gegen die DS-GVO gegen den Verletzer im Wege einer Klage vor den Zivilgerichten unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken vorzugehen.

Vorab ist darauf hinzuweisen, dass Kapitel VIII DS-GVO u.a. die Rechtsbehelfe regelt, mit denen die Rechte der betroffenen Person geschützt werden können, wenn die sie betreffenden personenbezogenen Daten Gegenstand einer Verarbeitung gewesen sind, die mutmaßlich gegen die Bestimmungen dieser Verordnung verstößt. Der Schutz dieser Rechte kann somit entweder gemäß Art. 77 bis 79 DS-GVO unmittelbar von der betroffenen Person oder nach Art. 80 DS-GVO von einer befugten Einrichtung – mit oder ohne entsprechenden Auftrag – beansprucht werden (vgl. i.d.S. Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 53).

Zum einen sieht Art. 77 Abs. 1 DS-GVO nämlich vor, dass jede betroffene Person unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde hat. Nach Art. 78 Abs. 1 DS-GVO hat jede natürliche oder juristische Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde, und zwar unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs. Art. 79 Abs. 1 DS-GVO garantiert jeder betroffenen Person das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 DS-GVO.

Zum anderen hat die betroffene Person nach Art. 80 Abs. 1 DS-GVO das Recht, eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht unter bestimmten Voraussetzungen zu beauftragen, in ihrem Namen eine Beschwerde einzureichen oder die in den Art. 77 bis 79 DS-GVO genannten Rechte wahrzunehmen. Außerdem können die Mitgliedstaaten nach Art. 80 Abs. 2 DS-GVO vorsehen, dass jede Einrichtung, Organisation oder Vereinigung unabhängig von einem Auftrag der betroffenen Person in diesem Mitgliedstaat das Recht hat, bei der Aufsichtsbehörde eine solche Beschwerde einzulegen und diese Rechte in Anspruch zu nehmen, wenn ihres Erachtens die nach dieser Verordnung bestehenden Rechte einer betroffenen Person infolge einer Verarbeitung sie betreffender personenbezogener Daten verletzt worden sind.

Im vorliegenden Fall ergibt sich aus den dem Gerichtshof vorliegenden Akten, dass ND, der eine Apotheke betreibt, über Amazon apothekenpflichtige Arzneimittel vertreibt und dass die Kunden bei der Onlinebestellung dieser Arzneimittel Daten wie ihren Namen, ihre Lieferadresse und die für die Individualisierung der Arzneimittel notwendigen Informationen eingeben müssen. Im Ausgangsverfahren wurde die Klage bei einem Zivilgericht jedoch weder nach Art. 79 DS-GVO von diesen Kunden, bei denen es sich um betroffene Personen im Sinne von Art. 4 Nr. 1 DS-GVO handelt, noch gemäß Art. 80 DS-GVO von einer Einrichtung, Organisation oder Vereinigung – mit oder ohne entsprechenden Auftrag einer betroffenen Person – erhoben, sondern von einem Wettbewerber dieses Apothekers unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken aufgrund der Verstöße, die dieser Apotheker gegen die Bestimmungen der DS-GVO begangen haben soll.

Das Ausgangsverfahren wirft also die Frage auf, ob die DS-GVO dem entgegensteht, dass ein Mitbewerber wie DR, der keine betroffene Person im Sinne von Art. 4 Nr. 1 dieser Verordnung ist, befugt ist, bei den nationalen Zivilgerichten eine solche Klage zu erheben.

Hierzu ist darauf hinzuweisen, dass bei der Auslegung einer unionsrechtlichen Vorschrift nicht nur ihr Wortlaut, sondern auch ihr Kontext und die Ziele zu berücksichtigen sind, die mit der Regelung, zu der sie gehört, verfolgt werden (Urt. v. 12.01.2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, Rn. 32).

Zum Wortlaut der Bestimmungen des Kapitels VIII DS-GVO ist festzustellen, dass in keiner dieser Bestimmungen ausdrücklich ausgeschlossen wird, dass ein Mitbewerber eines Unternehmens unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken wegen eines angeblichen Verstoßes dieses Unternehmens gegen die in der DS-GVO vorgesehenen Pflichten bei den Zivilgerichten Klage gegen dieses Unternehmen erheben kann. Aus Art. 77 Abs. 1, Art. 78 Abs. 1 und Art. 79 Abs. 1 DS-GVO, die in Rn. 48 des vorliegenden Urteils angeführt wurden, ergibt sich vielmehr, dass das Recht auf Beschwerde bei einer Aufsichtsbehörde sowie

das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde und gegen einen Verantwortlichen oder Auftragsverarbeiter gemäß diesen Bestimmungen „unbeschadet" jegliches anderen verwaltungsrechtlichen, gerichtlichen oder außergerichtlichen Rechtsbehelfs besteht.

Zum Regelungszusammenhang von Kapitel VIII DS-GVO ist darauf hinzuweisen, dass diese Verordnung in ihrem Kapitel II materielle Bestimmungen enthält, die u.a. die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5) und die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung (Art. 6) umfassen und die uneingeschränkte Achtung insbesondere des in Art. 16 Abs. 1 AEUV und Art. 8 der Charta verankerten Grundrechts der betroffenen Personen auf Schutz personenbezogener Daten sicherstellen sollen. Dass Kapitel VIII DS-GVO keine Bestimmungen enthält, die vorsehen, dass Mitbewerber eines Unternehmens, das gegen diese materiellen Bestimmungen verstoßen haben soll, Klage auf Unterlassung dieser Verstöße erheben können, geht darauf zurück, dass – wie vom Generalanwalt in Nr. 80 seiner Schlussanträge ausgeführt – nur betroffene Personen, nicht aber diese Mitbewerber Adressaten des durch diese Verordnung gewährleisteten Schutzes personenbezogener Daten sind.

Ist der Verstoß gegen diese materiellen Bestimmungen jedoch geeignet, sich vorrangig auf die von den fraglichen Daten betroffenen Personen auszuwirken, kann er auch Dritte beeinträchtigen. Dies wird dadurch verdeutlicht, dass Art. 82 Abs. 1 DS-GVO für „jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist", ein Recht auf Schadenersatz vorsieht. Der Gerichtshof hat auch bereits festgestellt, dass der Verstoß gegen eine Vorschrift zum Schutz personenbezogener Daten gleichzeitig den Verstoß gegen Vorschriften über den Verbraucherschutz oder unlautere Geschäftspraktiken nach sich ziehen kann (Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 78) und ein wichtiges Indiz für die Beurteilung der Frage, ob ein Missbrauch einer beherrschenden Stellung im Sinne von Art. 102 AEUV vorliegt, darstellen kann (vgl. in diesem Sinne Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 47 und 62).

In diesem Zusammenhang ist darauf hinzuweisen, dass der Zugang zu personenbezogenen Daten sowie deren Verwertung im Rahmen der digitalen Wirtschaft von erheblicher Bedeutung sind. Der Zugang zu personenbezogenen Daten und die Möglichkeit ihrer Verarbeitung sind nämlich zu einem bedeutenden Parameter des Wettbewerbs zwischen Unternehmen der digitalen Wirtschaft geworden. Um der tatsächlichen wirtschaftlichen Entwicklung Rechnung zu tragen und einen lauteren Wettbewerb zu wahren, kann es also erforderlich sein, bei der Durchsetzung des Wettbewerbsrechts und der Regeln über unlautere Geschäftspraktiken die Vorschriften zum Schutz personenbezogener Daten zu berücksichtigen (vgl. in diesem Sinne Urt. v. 04.07.2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 50 und 51).

Außerdem ergibt sich zwar aus Art. 1 Abs. 1 DS-GVO im Licht insbesondere der ErwG 9 und 13 der Verordnung, dass diese eine grundsätzlich vollständige Harmonisierung der nationalen Rechtsvorschriften zum Schutz personenbezogener Daten sicherstellen soll. Mehrere ihrer Bestimmungen eröffnen den Mitgliedstaaten aber ausdrücklich die Möglichkeit, zusätzliche – strengere oder einschränkende – nationale Vorschriften vorzusehen, die ihnen einen Ermessensspielraum hinsichtlich der Art und Weise ihrer Durchführung lassen („Öffnungsklauseln") (Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 57).

Der Gerichtshof hat bereits festgestellt, dass dies für Art. 80 Abs. 2 DS-GVO gilt, der den Mitgliedstaaten einen Ermessensspielraum hinsichtlich seiner Umsetzung lässt und der einer nationalen Regelung, nach der ein Verband zur Wahrung von Verbraucherinteressen gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten ohne entsprechenden Auftrag und unabhängig von der Verletzung konkreter Rechte betroffener Personen Klage insbesondere mit der Begründung erheben kann, dass gegen das Verbot der Vornahme unlauterer Geschäftspraktiken verstoßen worden sei, nicht entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen kann (Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 59 und 83).

Zwar enthalten die Bestimmungen des Kapitels VIII DS-GVO keine solche spezielle Öffnungsklausel, die es den Mitgliedstaaten ausdrücklich erlaubt, den Mitbewerbern eines Unternehmens, das angeblich gegen die materiellen Bestimmungen dieser Verordnung verstößt, die Möglichkeit einzuräumen, auf Unterlassung dieses Verstoßes zu klagen.

Aus dem Wortlaut und dem Kontext der Bestimmungen dieses Kapitels VIII, die in den Rn. 53 bis 58 des vorliegenden Urteils erläutert wurden, ergibt sich jedoch, dass der Unionsgesetzgeber mit dem Erlass dieser Verordnung keine umfassende Harmonisierung der Rechtsbehelfe, die bei einem Verstoß gegen die Bestimmungen der DS-GVO zur Verfügung stehen, vornehmen und insbesondere nicht ausschließen wollte, dass Mitbewerber eines mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten auf der Grundlage des nationalen Rechts unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken Klage erheben können.

Diese Auslegung wird durch die mit der DS-GVO verfolgten Ziele bestätigt. Insbesondere aus dem 10. ErwG dieser Verordnung geht nämlich hervor, dass bei der Verarbeitung personenbezogener Daten ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen gewährleistet und die Hemmnisse für den Verkehr personenbezogener Daten in der Union beseitigt werden sollen. Im 11. ErwG der Verordnung heißt es außerdem, dass ein wirksamer Schutz dieser Daten die Stärkung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen erfordert, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie – in den Mitgliedstaaten – gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Fall ihrer Verletzung. Dem 13. ErwG der Verordnung zufolge ist, damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer Rechtssicher-

heit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten gewährleistet.

Die Möglichkeit für den Mitbewerber eines Unternehmens, unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken bei den Zivilgerichten Klage auf Unterlassung eines von diesem Unternehmen angeblich begangenen Verstoßes gegen die materiellen Bestimmungen der DS-GVO zu erheben, lässt diese Ziele nicht nur unberührt, sondern kann die praktische Wirksamkeit dieser Bestimmungen sogar verstärken und damit das mit dieser Verordnung angestrebte hohe Schutzniveau der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten verbessern.

Denn zum einen hat eine Unterlassungsklage, die von einem Mitbewerber gegen ein Unternehmen unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken wegen eines behaupteten Verstoßes gegen die materiellen Bestimmungen der DS-GVO erhoben wird, keinerlei Einfluss auf das in Kapitel VIII dieser Verordnung vorgesehene Rechtsbehelfssystem oder auf das Ziel, in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen zu gewährleisten und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, zu beseitigen.

Zwar kann eine solche Klage, wenn auch inzident, auf dem Verstoß gegen die gleichen Bestimmungen der DS-GVO beruhen wie jene, auf die betroffene Personen oder eine Einrichtung, Organisation oder Vereinigung im Sinne von Art. 80 dieser Verordnung gemäß deren Art. 77 bis 79 eine Beschwerde oder einen Rechtsbehelf stützen können.

Doch dient erstens eine von einem Mitbewerber erhobene Unterlassungsklage – im Unterschied zu den Art. 77 bis 80 DS-GVO – nicht dem Ziel, die Grundrechte und Grundfreiheiten der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten zu schützen; vielmehr soll, im Interesse insbesondere dieses Mitbewerbers, ein lauterer Wettbewerb sichergestellt werden.

Zweitens besteht die Möglichkeit eines Mitbewerbers, unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken bei den Zivilgerichten eine solche Klage zu erheben, zusätzlich zu den Rechtsbehelfen gemäß den Art. 77 bis 79 DS-GVO, die uneingeschränkt erhalten bleiben und von den betroffenen Personen sowie gegebenenfalls von den Einrichtungen, Organisationen oder Vereinigungen im Sinne von Art. 80 DS-GVO jederzeit ergriffen werden können.

Insbesondere ist, wie von der deutschen Regierung ausgeführt, durch eine Koexistenz von datenschutzrechtlichen und wettbewerbsrechtlichen Rechtsbehelfen keine Gefahr für die einheitliche Durchsetzung der DS-GVO zu befürchten. Aus den Art. 77 bis 80 DS-GVO ergibt sich, dass diese Verordnung weder eine vorrangige oder ausschließliche Zuständigkeit vorsieht noch einen Vorrang der Beurteilung der genannten Behörde oder des genannten Gerichts zum Vorliegen einer Verletzung der durch die Verordnung verliehenen Rechte (vgl. in diesem Sinne Urt. v. 12.01.2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, Rn. 35). Folglich wirkt sich die Erhebung einer Unterlassungsklage durch einen Mitbewerber des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten bei den Zivilgerichten nicht auf das durch Kapitel VIII DS-GVO geschaffene Rechtsbehelfssystem aus. Außerdem wird, wie ebenfalls von der deutschen Regierung dargelegt, durch das in Art. 267 AEUV vorgesehene Vorabentscheidungsverfahren gewährleistet, dass die materiellen Bestimmungen der DS-GVO, die die Aufsichtsbehörde und die auf der Grundlage der Art. 77 bis 80 DS-GVO angerufenen Gerichte auf der einen Seite und die von einem solchen Mitbewerber unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken angerufenen Gerichte auf der anderen Seite möglicherweise auf den gleichen Verstoß anwenden, einheitlich ausgelegt werden.

Drittens wird, wie vom Generalanwalt im Wesentlichen in Nr. 104 seiner Schlussanträge ausgeführt, die Verwirklichung des Ziels, in der Union ein gleichmäßiges Datenschutzniveau für die betroffenen Personen zu gewährleisten und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, zu beseitigen, nicht dadurch gefährdet, dass auch anderen als den betroffenen Personen und den Einrichtungen, Organisationen und Vereinigungen gemäß Art. 80 DS-GVO die Möglichkeit eingeräumt wird, sich auf die materiellen Bestimmungen der DS-GVO zu berufen. Selbst wenn einzelne Mitgliedstaaten diese Möglichkeit nicht vorsähen, würde dies nämlich nicht zu einer Fragmentierung der Umsetzung des Datenschutzes in der Union führen, weil die materiellen Bestimmungen der DS-GVO für alle Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO gleichermaßen verbindlich sind und ihre Einhaltung durch die in dieser Verordnung vorgesehenen Rechtsbehelfe sichergestellt wird.

Zum anderen ist zum Ziel der Gewährleistung eines wirksamen Schutzes der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und zur praktischen Wirksamkeit der materiellen Bestimmungen der DS-GVO festzustellen, dass – wie in Rn. 65 des vorliegenden Urteils ausgeführt – eine von einem Mitbewerber des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten erhobene Unterlassungsklage zwar nicht diesem Ziel dient, sondern einen lauteren Wettbewerb sicherstellen soll; sie trägt jedoch unbestreitbar zur Einhaltung dieser Bestimmungen und damit dazu bei, die Rechte der betroffenen Personen zu stärken und ihnen ein hohes Schutzniveau zu gewährleisten (vgl. in diesem Sinne Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 74).

Im Übrigen könnte sich eine solche Unterlassungsklage eines Mitbewerbers, ähnlich wie Klagen von Verbänden zur Wahrung von Verbraucherinteressen, für die Gewährleistung dieses Schutzes als besonders wirksam erweisen, da sie es ermöglicht, zahlreiche Verletzungen der Rechte der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen zu verhindern (vgl. in diesem Sinne Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 75).

Daraus folgt, dass die in Rn. 60 des vorliegenden Urteils vorgenommene Auslegung im Einklang mit den Anforderungen steht, die sich aus Art. 16 Abs. 1 AEUV und Art. 8 der Charta ergeben, und damit mit dem Ziel der DS-GVO, einen

wirksamen Schutz der Grundfreiheiten und Grundrechte natürlicher Personen und insbesondere ein hohes Schutzniveau für das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten zu gewährleisten (vgl. in diesem Sinne Urt. v. 28.04.2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, Rn. 73).

Im vorliegenden Fall ist es Sache des vorlegenden Gerichts, zu prüfen, ob der mutmaßliche Verstoß gegen die im Ausgangsverfahren in Rede stehenden materiellen Bestimmungen der DS-GVO, sofern er erwiesen ist, auch einen Verstoß gegen das Verbot der Vornahme unlauterer Geschäftspraktiken gemäß den einschlägigen nationalen Regelungen darstellt.

Nach alledem ist auf die erste Frage zu antworten, dass die Bestimmungen des Kapitels VIII DS-GVO dahin auszulegen sind, dass sie einer nationalen Regelung nicht entgegenstehen, die – neben den Eingriffsbefugnissen der zur Überwachung und Durchsetzung dieser Verordnung zuständigen Aufsichtsbehörden und den Rechtsschutzmöglichkeiten der betroffenen Personen – Mitbewerbern des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten die Befugnis einräumt, wegen Verstößen gegen die DS-GVO gegen den Verletzer im Wege einer Klage vor den Zivilgerichten unter dem Gesichtspunkt des Verbots der Vornahme unlauterer Geschäftspraktiken vorzugehen.

Keine Handlungspflicht der Datenschutzaufsichtsbehörde

(EuGH, Urteil vom 26. September 2024 – C-768/21 –)

Art. 57 Abs. 1 lit. a) und f) Art. 58 Abs. 2 sowie Art. 77 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sind dahin auszulegen, dass die Aufsichtsbehörde im Fall der Feststellung einer Verletzung des Schutzes personenbezogener Daten nicht verpflichtet ist, nach diesem Art. 58 Abs. 2 eine Abhilfemaßnahme zu ergreifen, insbesondere eine Geldbuße zu verhängen, wenn ein solches Einschreiten nicht geeignet, erforderlich oder verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten.

Zur Vorlagefrage:

Zur Bearbeitung von Beschwerden verleiht Art. 58 Abs. 1 DS-GVO jeder Aufsichtsbehörde weitreichende Untersuchungsbefugnisse. Stellt eine solche Behörde am Ende ihrer Untersuchung einen Verstoß gegen die Bestimmungen dieser Verordnung fest, ist sie verpflichtet, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen, wobei gemäß der Klarstellung im 129. ErwG dieser Verordnung alle Maßnahmen insbesondere im Hinblick auf die Gewährleistung der Einhaltung der Verordnung geeignet, erforderlich und verhältnismäßig sein sollten und die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind. Zu diesem Zweck werden in Art. 58 Abs. 2 DS-GVO die verschiedenen der Aufsichtsbehörde zur Verfügung stehenden Abhilfebefugnisse aufgezählt (vgl. in diesem Sinne Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 57 und die dort angeführte Rechtsprechung).

So hat die Aufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO u.a. die Befugnis, einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn Verarbeitungsvorgänge zu einem Verstoß gegen die Bestimmungen dieser Verordnung geführt haben (lit. b)), den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach der Verordnung zustehenden Rechte zu entsprechen (lit. c)), den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der Verordnung zu bringen (lit. d)), oder eine Geldbuße gemäß Art. 83 DS-GVO zu verhängen, zusätzlich zu oder anstelle von den in Art. 58 Abs. 2 DS-GVO genannten Maßnahmen, je nach den Umständen des Einzelfalls (lit. i)).

Demnach ist das Beschwerdeverfahren als ein Mechanismus konzipiert, der geeignet ist, die Rechte und Interessen der betroffenen Personen wirksam zu wahren (Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 58).

Im vorliegenden Fall geht aus dem Vorabentscheidungsersuchen hervor, dass der HBDI die Beschwerde, mit der ihn der Kläger des Ausgangsverfahrens befasst hatte, inhaltlich prüfte und ihn über das Ergebnis der Untersuchung unterrichtete. Im Einzelnen bestätigte der HBDI, dass in der Sparkasse eine Verletzung der personenbezogenen Daten des Klägers des Ausgangsverfahrens stattgefunden habe und diese darin bestanden habe, dass eine ihrer Mitarbeiterinnen unbefugten Zugriff auf diese Daten gehabt habe. Hinsichtlich der Zugriffsrechte der Mitarbeiter der Sparkasse wies der HBDI die Beschwerde des Klägers des Ausgangsverfahrens allerdings zurück. Außerdem gelangte er zu dem Ergebnis, dass kein Anlass bestehe, gemäß Art. 58 Abs. 2 DS-GVO gegen die Sparkasse einzuschreiten.

Insoweit ist darauf hinzuweisen, dass die DS-GVO der Aufsichtsbehörde ein Ermessen hinsichtlich der Art und Weise einräumt, wie sie der festgestellten Unzulänglichkeit abhilft, da Art. 58 Abs. 2 DS-GVO der Aufsichtsbehörde die Befugnis verleiht, verschiedene Abhilfemaßnahmen zu ergreifen. So hat der Gerichtshof bereits entschieden, dass es der Aufsichtsbehörde obliegt, unter Berücksichtigung aller Umstände des konkreten Falles das geeignete und erforderliche Mittel zu wählen, und sie verpflichtet ist, mit aller gebotenen Sorgfalt ihre Aufgabe zu erfüllen, die darin besteht, über die umfassende Einhaltung der DS-GVO zu wachen (vgl. in diesem Sinne Urt. v. 16.07.2020, Facebook Ireland und Schrems, C-311/18, EU:C:2020:559, Rn. 112).

Dieses Ermessen wird jedoch durch das Erfordernis begrenzt, durch einen klar durchsetzbaren Rechtsrahmen ein gleichmäßiges und hohes Schutzniveau für personenbezogene Daten zu gewährleisten, wie sich aus den ErwG 7 und 10 der DS-GVO ergibt.

Was speziell Geldbußen nach Art. 58 Abs. 2 lit. i) DS-GVO anbelangt, geht aus Art. 83 Abs. 2 dieser Verordnung hervor,

dass diese je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von den Maßnahmen nach Art. 58 Abs. 2 der Verordnung verhängt werden. Art. 83 Abs. 2 DS-GVO stellt außerdem klar, dass die Aufsichtsbehörde bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag in jedem Einzelfall die in Art. 83 Abs. 2 lit. a) bis k) dieser Verordnung genannten Merkmale, wie etwa Art, Schwere und Dauer des Verstoßes, gebührend zu berücksichtigen hat.

Der Unionsgesetzgeber hat somit ein Sanktionssystem vorgesehen, das es den Aufsichtsbehörden ermöglicht, die Sanktionen zu verhängen, die je nach den Umständen des konkreten Falles am besten geeignet und gerechtfertigt sind (vgl. in diesem Sinne Urt. v. 05.12.2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, Rn. 75 und 78), wobei sie, wie in den Rn. 37 und 38 des vorliegenden Urteils ausgeführt, das Erfordernis zu berücksichtigen haben, über die umfassende Einhaltung der DS-GVO zu wachen und durch einen klar durchsetzbaren Rechtsrahmen ein gleichmäßiges und hohes Schutzniveau für personenbezogene Daten zu gewährleisten.

Somit kann weder aus Art. 58 Abs. 2 DS-GVO noch aus Art. 83 dieser Verordnung abgeleitet werden, dass die Aufsichtsbehörde verpflichtet wäre, in jedem Fall, wenn sie eine Verletzung des Schutzes personenbezogener Daten feststellt, eine Abhilfemaßnahme zu ergreifen, insbesondere eine Geldbuße zu verhängen, da ihre Verpflichtung unter derartigen Umständen darin besteht, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen. Daher steht, wie der Generalanwalt in Nr. 81 seiner Schlussanträge ausgeführt hat, dem Beschwerdeführer, dessen Rechte verletzt wurden, kein subjektives Recht zu, dass die Aufsichtsbehörde gegen den für die Verarbeitung Verantwortlichen eine Geldbuße verhängt.

Dagegen ist die Aufsichtsbehörde zum Einschreiten verpflichtet, wenn das Ergreifen einer oder mehrerer der in Art. 58 Abs. 2 DS-GVO vorgesehenen Abhilfemaßnahmen unter Berücksichtigung aller Umstände des konkreten Falles geeignet, erforderlich und verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung dieser Verordnung zu gewährleisten.

Insoweit ist nicht ausgeschlossen, dass die Aufsichtsbehörde ausnahmsweise und unter Berücksichtigung der besonderen Umstände des konkreten Falles vom Ergreifen einer Abhilfemaßnahme absehen kann, obwohl eine Verletzung des Schutzes personenbezogener Daten festgestellt wurde. Ein solcher Fall könnte namentlich dann vorliegen, wenn die festgestellte Verletzung nicht angedauert hat, beispielsweise wenn der Verantwortliche, der grundsätzlich geeignete technische und organisatorische Maßnahmen im Sinne von Art. 24 dieser Verordnung umgesetzt hatte, in Anbetracht der ihm insbesondere nach Art. 5 Abs. 2 und Art. 24 DS-GVO obliegenden Pflichten, sobald er von dieser Verletzung Kenntnis erlangt hat, die geeigneten und erforderlichen Maßnahmen ergriffen hat, damit die Verletzung abgestellt wird und sich nicht wiederholt.

Die Auslegung, wonach die Aufsichtsbehörde, wenn sie eine Verletzung des Schutzes personenbezogener Daten feststellt, nicht in jedem Fall verpflichtet ist, eine Abhilfemaßnahme nach Art. 58 Abs. 2 DS-GVO zu ergreifen, wird durch die mit Art. 58 Abs. 2 und Art. 83 dieser Verordnung verfolgten Ziele bestätigt.

Hinsichtlich des mit Art. 58 Abs. 2 DS-GVO verfolgten Ziels ergibt sich aus dem 129. ErwG, dass mit dieser Bestimmung sichergestellt werden soll, dass die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung erfolgt und dass Situationen, in denen gegen die Verordnung verstoßen wird, durch das Eingreifen der nationalen Aufsichtsbehörden wieder mit dem Unionsrecht in Einklang gebracht werden (Urt. v. 14.03.2024, Újpesti Polgármesteri Hivatal, C-46/23, EU:C:2024:239, Rn. 40).

Daraus folgt, dass das Ergreifen einer Abhilfemaßnahme ausnahmsweise und unter Berücksichtigung der besonderen Umstände des konkreten Falles nicht geboten sein kann, sofern der Situation, die einen Verstoß gegen die DS-GVO begründete, bereits abgeholfen wurde, die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durch den hierfür Verantwortlichen gewährleistet ist und ein solches Nichteinschreiten der Aufsichtsbehörde nicht geeignet ist, das in Rn. 38 des vorliegenden Urteils genannte Erfordernis eines klar durchsetzbaren Rechtsrahmens zu beeinträchtigen.

Was das mit Art. 83 DS-GVO, der die Verhängung von Geldbußen betrifft, verfolgte Ziel angeht, so besteht dieses nach dem 148. ErwG dieser Verordnung darin, die Vorschriften der Verordnung konsequenter durchzusetzen. In demselben Erwägungsgrund heißt es jedoch, dass die Aufsichtsbehörden im Fall eines geringfügigeren Verstoßes oder falls die voraussichtlich zu verhängende Geldbuße eine unverhältnismäßige Belastung für eine natürliche Person bewirken würde, davon absehen dürfen, eine Geldbuße zu verhängen, und stattdessen eine Verwarnung erteilen können (vgl. in diesem Sinne Urt. v. 05.12.2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, Rn. 76).

Im vorliegenden Fall geht aus dem Vorabentscheidungsersuchen hervor, dass die Sparkasse dem HBDI gemäß Art. 33 DS-GVO die Verletzung des Schutzes der personenbezogenen Daten des Klägers des Ausgangsverfahrens durch den unberechtigten Zugriff einer ihrer Mitarbeiterinnen auf diese Daten meldete. Außerdem gab die Sparkasse an, Disziplinarmaßnahmen gegen diese Mitarbeiterin ergriffen zu haben und die Speicherdauer der Zugriffsprotokolle überprüfen zu lassen. Infolgedessen sah der HBDI davon ab, eine Abhilfemaßnahme nach Art. 58 Abs. 2 DS-GVO zu ergreifen, und insbesondere davon, eine Geldbuße zu verhängen.

Da Beschlüsse einer Aufsichtsbehörde über eine Beschwerde einer vollständigen inhaltlichen Überprüfung durch ein Gericht unterliegen (Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 70), ist es Sache des vorlegenden Gerichts, zu prüfen, ob sich der HBDI mit aller gebotenen Sorgfalt mit der betreffenden Beschwerde befasst hat und beim Erlass des im Ausgangsverfahren in Rede stehenden Bescheids die Grenzen des Ermessens, das ihm Art. 58 Abs. 2 DS-GVO einräumt, eingehalten hat (vgl. entsprechend Urt. v. 07.12.2023, SCHUFA Holding [Restschuldbefreiung], C-26/22 und C-64/22, EU:C:2023:958, Rn. 68 und 69 sowie die dort angeführte Rechtsprechung).

Auskunft nach Art. 15 DS-GVO kann auch durch Self-Service-Tool erfüllt werden

(OLG Frankfurt a.M., Beschluss vom 2. Juli 2024 – 6 U 41/24 –)

Der Auskunftsanspruch nach § 15 Abs. 2 DS-GVO kann durch die Bereitstellung eines Self-Service-Tools erfüllt werden. […]

Aus den Gründen:

1. Das Landgericht ist zutreffend davon ausgegangen, dass die Beklagte durch die Bereitstellung eines Self-Service-Tools sowie das Schreiben vom 18.04.2023 (Anlage K 3) den Auskunftsanspruch des Klägers nach § 15 II DS-GVO erfüllt hat.

Die Bereitstellung des Selbstbedienungstools führt dazu, dass der Kläger die Auskünfte an seinem Wohnsitz abrufen kann, wenn er dies will. Der Auskunftserfolg tritt damit auch dann am rechten Ort ein, wenn man – mit der Berufungsbegründung – zugrunde legt, dass Erfüllungsort der Sitz des Klägers ist.

Anderes ergibt sich (entgegen der Berufungsbegründung) auch nicht aus ErwG 63 zur DS-GVO. […] Der ErwG 63 besagt […] nirgends, dass der Fernzugang (hier: Selbstbedienungstool) nur dann erfüllungstauglich wäre, wenn der Nutzer mit dieser Art der Erfüllung einverstanden ist. Auch gebietet er keine solche Folgerung. Die Bereitstellung eines angemessenen Fernzugangs über ein Self-Service-Tool wird daher als ausreichend angesehen, um den Anspruch auf Bereitstellung einer Kopie der personenbezogenen Daten gemäß Art. 15 Abs. 3 S. 1 DS-GVO zu erfüllen (OLG Dresden, Urt. v. 05.12.2023, Az. 4 U 1094/23, Rn. 65, juris; OLG München, Vfg. v. 29.01.2024, 14 U 4826/23 – nicht veröffentlicht; LG Bonn, Urt. v. 08.03.2023, Az.: 17 O 165/22, GRUR-RS 2023, 3854 Rn. 59 ff.; LG Bonn, Urt. v. 03.02.2023, Az.: 2 O 170/22, GRUR-RS 2023, 4566, Rn. 54 ff.; LG Bonn, Urt. v. 03.02.2023, Az.: 18 O 127/22, GRUR-RS 2023, 4565, Rn. 56 f.; LG Paderborn, Urt. v. 19.12.2022, Az.: 3 O 99/22, GRUR-RS 2022, 39349, Rn. 162 ff.; LG Paderborn, Urt. v. 13.12.2022, Az.: 2 O 212/22, GRUR-RS 2022, 41028 Rn. 176 ff.; LG München I, Urt. v. 02.09.2021, Az.: 23 O 10931/20, juris Rn. 23 f.; Krämer/Burghoff, ZD 2022, 428, 432; Paal, in: Paal/Pauly DS-GVO, 3. Aufl. 2021, Art. 15 Rn. 38 iVm Rn. 14; Franck, in: Gola/Heckmann DS-GVO, 3. Aufl. 2022, Art. 15 Rn. 40.), sie ist sogar die gewünschte Form der Übermittlung

Soweit eine einzelne Stimme (Schmidt-Wudy, BeckOK Datenschutzrecht, Art. 15 DS- GVO Rn. 84) der Auffassung ist, ein Fernzugriffssystem ersetze nur dann die Übersendung der Auskunft bzw. Datenkopie im Wege der Schickschuld per Post oder auf elektronischem Wege, wenn sich der Anspruchsteller hiermit einverstanden erkläre, fehlt es hierfür ebenso an einer tragfähigen Begründung wie in der Entscheidung des LAG Niedersachsen (NZA-RR 2020, 571, RNr. 46), die ohne Begründung diese Literaturstelle zitiert.

Die Verweisung auf den Fernzugang kann im Einzelfall zwar dazu führen, dass der betroffenen Person faktisch die Auskunft verweigert wird: Beispielsweise haben auch Menschen, die „analog leben" oder/und keine nennenswerten Fähigkeiten im Umgang mit IT-gestützten Portalen haben, ein Recht auf Auskunft nach Art. 15 DS-GVO, dieses könnte untergraben werden, wenn man sie auf das ihnen unzugängliche Selbstbedienungstool verwiese. Darüber muss vorliegend jedoch nicht entschieden werden, denn wer sich bei der Beklagten registriert, lebt denknotwendig nicht (mehr) analog und lässt auch nicht erwarten, im Umgang mit IT-gestützten Portalen unbeschlagen zu sein.

Kontrollpflicht des Verantwortlichen gegenüber dem Auftragsverarbeiter

(OLG Dresden, Urteil vom 15. Oktober 2024 – 4 U 940/24 –)

1. **Dem datenschutzrechtlich Verantwortlichen obliegt gegenüber dem Auftragsverarbeiter mit Beendigung des Verarbeitungsvertrags eine Kontrollpflicht über die Löschung der beim Verarbeiter angefallenen personenbezogenen Daten.**
2. **Auf einen Exzess kann er sich nicht berufen, wenn er dieser Kontrollpflicht nicht genügt.**
3. **Der Empfang von Spam-Nachrichten ohne weitere Folgen begründet keinen immateriellen Schaden.**

Aus den Gründen:

2. Die Beklagte ist der Klagepartei dem Grunde nach gemäß Art. 82 DS-GVO zum Schadenersatz verpflichtet.

Der Verantwortliche und Auftragsverarbeiter haftet im Grundsatz nach Art. 82 DS-GVO für das Handeln seiner Auftragsverarbeiter und deren Mitarbeiter jedenfalls dann, wenn dem Mitarbeiter erst durch die ihm vom Verantwortlichen oder Auftragsverarbeiter übertragene Tätigkeit die Gelegenheit gegeben wurde, auf die Rechtsgüter der betroffenen Person einzuwirken. Der Verantwortliche haftet auch, wenn der Auftragsverarbeiter die Weisungen des Verantwortlichen ausführt und dadurch ein Schaden entsteht. Missachtet der Auftragsverarbeiter eine rechtmäßige Weisung des Verantwortlichen, haftet der Verantwortliche auch hierfür (Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), 8. EL 2024, Art. 82 EUV 2016/679, Rn. 30a). Zwar besteht in diesem Fall auch eine Haftung des Auftragsdatenverarbeiters. Der Verantwortliche kann den Betroffenen aber nicht auf dessen vorrangige Inanspruchnahme verweisen, weil dies einem "wirksamen Schadenersatz" im Sinne des Art. 82 Abs. 4 DS-GVO (vgl. auch ErwG 146 S. 6) entgegenstünde. Ein Abschieben der Haftung auf den Auftragsverarbeiter widerspricht auch dem Grundgedanken der Auftragsverarbeitung, wonach der Verantwortliche zwar ohne Weiteres Dritte einschalten darf, aber gegenüber der betroffenen Person verantwortlich bleibt. Der Auftragsverarbeiter ist letztlich – mit einigen formalen und inhaltlichen Anforderungen, die aus der fehlenden arbeitsrechtlichen Weisungsbefugnis und tatsächlichen Kontrollmöglichkeit herrühren – wie ein sonstiger Mitarbeiter zu behandeln (vgl. Bergt, in: Kühling/Buchner, DS-GVO, 4. Aufl., 2024, Art. 82 Rn. 55 m.w.N.).

a) Die Beklagte hat gegen die ihr obliegende Pflicht zur sorgfältigen Überwachung des von ihr beauftragten externen Auftragsdatenverarbeiters verstoßen, Art. 28, 32 DS-GVO.

Art 28 Abs. 1 DS-GVO regelt unmittelbar nur die Anforderungen an die Auswahl des Auftragsverarbeiters durch den Verantwortlichen. Dieser darf nur solche Auftragnehmer als Auftragsverarbeiter beauftragen, "die hinreichende Garantie dafür bieten, dass geeignete technische und organisatorische Maßnahmen" im Einklang mit der DS-GVO durchgeführt werden. Dies führt aber nicht nur zu einer Pflicht zur sorgfältigen Auswahl, sondern auch zu einer Pflicht zur sorgfältigen Überwachung des Auftragsverarbeiters durch den Verantwortlichen. Diese Pflicht zur Überwachung des Auftragsverarbeiters – im Anschluss an dessen Auswahl – ist in Art. 28 Abs. 1 DS-GVO zwar nicht ausdrücklich geregelt, ergibt sich jedoch aus der Formulierung der Norm ("arbeitet [...] nur mit"). Abs. 3 lit h) setzt eine solche Kontrollpflicht voraus, was auch die ordnungsgemäße Datenlöschung betrifft. Zugleich enthält er eine Verpflichtung der Vertragsparteien, die Details zu den Prüfrechten auszugestalten und hierdurch eine effektive Kontrolle durch den Verantwortlichen sicherzustellen (Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/ Bundesdatenschutzgesetz (BDSG), 8. EL 2024, Art. 28 EUV 2016/679, Rn. 61). De facto ist die Pflicht zur Überwachung daher auch ohne konkrete zeitliche Vorgaben als Dauerpflicht zu verstehen (vgl. Plath, in: Plath, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Rn. 17 m.w.N.). Durch diese vertragliche Ausgestaltung werden aber nicht nur die Pflichten des Auftragsdatenverarbeiters, sondern auch die korrespondierenden Prüfpflichten des Unternehmers konkretisiert. Ob dies auch dann gilt, wenn dem Auftragsdatenverarbeiter Pflichten auferlegt werden, die über das nach der DS-GVO gebotenen Schutzniveau hinausgehen, bedarf hier entgegen der Auffassung der Beklagten im Schriftsatz vom 09.09.2024 keiner Entscheidung, weil die durch Ziff. 9 des Nachtrags geregelten Pflichten nicht über diese Mindestanforderungen hinausgehen. Wie die Beklagte im Schriftsatz vom 09.09.2024 insofern zu Recht geltend macht, ist der Auftragsverarbeiter nämlich nach Vertragsende – als Ausfluss der allgemeinen Grundsätze der "Rechtmäßigkeit", (Art. 5 Abs. 1 lit. a)) DS-GVO), der "Datenminimierung" (Art. 5 Abs. 1 lit. (c) DS-GVO) sowie der Speicherbegrenzung (Art. 5 Abs. 1 e) DS-GVO) – verpflichtet, alle noch vorhandenen personenbezogenen Daten entweder zu löschen oder zurückzugeben (vgl. Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 22, 23, beck-online mit Verweisen auf Spoerr, in: BeckOK DatenschutzR, DS-GVO Art. 28 Rn. 78). Dies entspricht Art. 9 des Nachtrags.

Die Anforderungen an Auswahl und Überwachung dürfen dabei in der Praxis zwar nicht überspannt werden. Wählt ein Unternehmen z.B. einen führenden und am Markt als zuverlässig bekannten IT-Dienstleister aus, so darf es grundsätzlich auf dessen Fachwissen und Zuverlässigkeit vertrauen, ohne dass etwa eine – vollkommen praxisfremde – Vor-Ort-Kontrolle erforderlich wäre (Schaffland/Wiltfang aaO.). Gesteigerte Anforderungen ergeben sich indes, soweit z.B. große Datenmengen oder besonders sensible Daten gehostet werden sollen (Plath, a.a.O., Rn. 18). Diese gesteigerten Kontrollpflichten gelten auch außerhalb der Verarbeitung personenbezogener Daten nach Art. 9, 10 DS-GVO. Ungeachtet der Frage, ob die von dem zwischen der Beklagten und dem Autragsdatenverarbeiter geschlossenen Vertrag erfassten Daten auch Daten über das Nutzerverhalten und hieraus zu erstellende Profile beinhalteten, betraf die Verarbeitung vorliegend jedenfalls nicht unbedeutende Datenmengen, deren Verlust potenziell vielen Millionen Nutzern Schaden zufügen konnte. Infolgedessen war die Beklagte auch nach Vertragsbeendigung zu einer Überwachung ihres Auftragsdatenverarbeiters dahingehend angehalten, dass dieser die ihm zur Verfügung gestellten Daten tatsächlich löscht und hierüber eine aussagekräftige Bescheinigung ausstellt. [...]

d) Die Beklagte kann sich nicht nach Art. 82 Abs. 3 DS-GVO entlasten.

Der Verantwortliche oder der Auftragsverarbeiter wird nach dem Wortlaut dieser Vorschrift von der Haftung gemäß Abs. 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. "Nicht verantwortlich" bedeutet, dass den Verantwortlichen bzw. den Auftragsverarbeiter keinerlei Verschulden an dem Ereignis trifft, das den Schaden auslöste (Bergt, in: Kühling/ Buchner, DS-GVO/BDSG, 3. Aufl., Art. 82 Rn. 49; im Ergebnis auch Spindler, DB 2016, 937 ff. (947) Schaffland/Wiltfang, a.a.O, Rn. 28). "In keinerlei Hinsicht" bedeutet, dass der Verantwortliche bzw. der Auftragsverarbeiter nachweist, er habe alle Sorgfaltspflichten erfüllt und damit ihm nicht die geringste Fahrlässigkeit vorgeworfen werden kann (Becker, in: Plath, DS-GVO/BDSG/ TTDSG, 4. Aufl., Art. 82 DS-GVO Rn. 5). Hält er alle erforderlichen technischen und organisatorischen Datensicherungsmaßnahmen ein und kommt es dennoch zu einem unbefugten Datenzugriff, kann ihm dies nicht angelastet werden (Becker in Plath, DS-GVO/BDSG/TTDSG, 4. Aufl., Art. 82 DS-GVO Rn. 5; Frenzel, in: Paal/Pauly, DS-GVO/BDSG, 3. Aufl., Art. 82 Rn. 15; Bergt, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., Art. 82 Rn. 54; Schaffland/Wiltfang, a.a.O, Rn. 29). Die Haftung des Verantwortlichen für das Verhalten eines Auftragsverarbeiters erstreckt sich grundsätzlich nicht auf die Fälle, in denen der Auftragsverarbeiter personenbezogene Daten für eigene Zwecke verarbeitet hat oder diese Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte (EuGH, Urt. v. 05.12.2023 – C-683/21 –, juris Rn. 85).

Vorliegend hat der Auftragsdatenverarbeiter zwar sowohl gegen allgemeine Regeln der DS-GVO als auch gegen seine vertraglichen Pflichten verstoßen. Ungeachtet vertraglicher Verpflichtungen ist der Auftragsverarbeiter bereits nach der DS-GVO im Rahmen der Auftragsverarbeitung grundsätzlich nicht berechtigt, die im Auftrag verarbeiteten Daten für eigene Zwecke bzw. für die Zwecke Dritter zu verarbeiten. Darüber hinaus hat der Auftragsverarbeiter die Rückgabe- und Löschpflichten nach Beendigung des Auftrags zu beachten (vgl. Plath, in: Plath, DS-GVO/BDSG/TTDSG, 4. Aufl. 2023, Rz. 17 m.w.N.). Vorliegend ist unstreitig, dass Datensätze der Beklagten bei der Firma O... zum einen unzulässigerweise von der Produktiv- in eine Testumgebung überführt wurden, deren Sphäre verlassen haben und anschließend im Darknet zum Verkauf angeboten wurden, nachdem Mitarbeiter dieser Firma entgegen ihrer Zusicherung aus dem Jahre 2023 nicht alle Da-

tensätze der Beklagten wie vertraglich vereinbart unverzüglich nach Vertragsende gelöscht hatten, sondern zumindest einer der Datensätze schließlich entweder von Hackern erbeutet, oder von Mitarbeitern unbefugt weitergegeben wurden.

Wie oben ausgeführt, käme die Beklagte allerdings nur dann in den Genuss der Haftungsprivilegierung nach Art. 82 Abs. 3 DS-GVO, wenn ihr selbst keinerlei Fahrlässigkeit vorzuwerfen wäre. Dies ist vorliegend angesichts des eigenen Pflichtenverstoßes der Beklagten nicht der Fall. Dem kann auch nicht das fehlende Zugriffsrecht der Beklagten nach Ablauf des Auftragsverarbeitungsverhältnisses entgegen gehalten werden; wie aufgezeigt standen hier nämlich der Beklagten die in Ziff. 9, 10 des Nachtrags geregelten nachwirkenden Kontrollmöglichkeiten offen.

3. Der Kläger kann aus den angeführten Verstößen der Beklagten gegen die DS-GVO keinen Anspruch auf Ersatz immateriellen Schadens herleiten. Der Klagepartei obliegt die Darlegungs- und Beweislast für den bei ihr eingetretenen Schaden sowie den Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung der Daten und dem Schaden. Dieser Beweis ist nicht erbracht worden.

Art. 82 Abs. 2 DS-GVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt die drei Voraussetzungen für die Entstehung des Schadenersatzanspruchs, nämlich eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DS-GVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (so EuGH, Urt. v. 04.05.2023 – C – 300/21, Rn. 36 – juris). Der europäische Gerichtshof stützt sich auf den 146. ErwG, der auf "Schäden" abstellt, "die einer Person aufgrund einer Verarbeitung entstehen". Zwar muss der Schaden nicht eine gewisse Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urt. v. 20.06.2024 – C-590/22, Rn. 28 – juris; EuGH, Urt. v. 04.05.2023 – C-300/21, 49, 50 – juris). Allerdings muss der Schaden tatsächlich und sicher entstanden sein (vgl. EuGH, Urt. v. 04.04.2017 – C-337/15, Rn. 91 – juris). Hierbei hat der Europäische Gerichtshof in einem behaupteten Verlust des Vertrauens in eine Institution keinen ersatzfähigen immateriellen Schaden gesehen (vgl. EuGH, Urt. v. 04.04.2017 – C-337/15, Rn. 95 – juris).

Der Kontrollverlust der Daten und deren Veröffentlichung im Darknet hat im vorliegenden Fall zu keinem immateriellen Schaden im Sinne von Art. 82 DS-GVO bei der Klagepartei geführt. […]

Nach der Rechtsprechung des EuGH (EuGH, Urt. v. 20.06.2024 – C-590/22 – juris; Urt. v. 14.12.2023 – C-340/21 – juris) kann der Kontrollverlust grundsätzlich einen immateriellen Schaden begründen. Aus dieser beispielhaften Aufzählung im ErwG Nr. 85 der "Schäden", die den betroffenen Personen entstehen können geht hervor, dass der Unionsgesetzgeber unter den Begriff "Schaden" insbesondere auch den bloßen "Verlust der Kontrolle" über ihre eigenen Daten infolge eines Verstoßes gegen die DS-GVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (vgl. EuGH, Urt. v. 14.12.2023 – C-340/21, Rn. 82 – juris). Allerdings muss eine Person, die von einem Verstoß gegen die DS-GVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DS-GVO darstellen (vgl. EuGH, a.a.O. Rn. 84). Wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, ist aber gleichwohl zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. EuGH a.a.O., Rn. 85). An dem Erfordernis eines kausalen Schadens hat der Europäische Gerichtshof festgehalten.

Dies deckt sich mit der Funktion des aus Art. 82 Abs. 1 DS-GVO folgenden Anspruchs auf Schadenersatz, einen konkreten Schaden auszugleichen (EuGH, Urt. v. 20.06.2024 – C-590/22, Rn. 24 – juris). Ließe man einen für den Betroffenen folgenlosen Kontrollverlust als immateriellen Schaden zu, müsste die Höhe des Schadenersatzes konsequent Null betragen. Denn für die Bemessung des Ersatzes des immateriellen Schadens kommt es letztlich im Hinblick auf die Ausgleichsfunktion des Art. 82 Abs. 1 DS-GVO nur auf die konkreten Auswirkungen für die betroffene Person an, nicht aber bspw. auf Strafzwecke, Schwere des Verschuldens, Schwere des Verstoßes gegen die DS-GVO oder die Anzahl der Verstöße gegen die Datenschutz-Grundverordnung im Hinblick auf einen Vorgang (vgl. OLG Hamm, Urt. v. 21.06.2024 – 7 U 154/23, Rn. 48 – juris Bezug nehmend auf EuGH, Urt. v. 20.06.2024 – C-590/22, Rn. 28 ff – juris; EuGH, Urt. v. 11.04.2024 – C-741/21, Rn. 64 – juris;).

Dafür sprechen zudem systematische Gründe. So wird in der Auslegung anderer Normen, die einen immateriellen Schaden voraussetzen, dieser als eine negative innere Tatsache des Geschädigten angesehen, z.B. die Trauer über den Verlust eines nahen Angehörigen; hingegen wird der Verlust des nahen Angehörigen als solcher nicht als Schaden anerkannt (EuGH, Urt. v. 10.12.2015 – C-350/14, Rn. 27 – juris). Wenn aber schon der Verlust eines Angehörigen an sich zur Begründung eines immateriellen Schadens nicht ausreicht, dann ist dies aus Wertungsgesichtspunkten erst recht nicht beim Verlust der Kontrolle über Daten der Fall (OLG Hamm, Urt. v. 21.06.2024 – 7 U 154/23, Rn. 49 – juris).

Die betroffene Person muss die Tatsachen, die dazu führen können, dass ein "tatsächlich erlittener immaterieller Schaden" infolge der Verletzung des Schutzes personenbezogener Daten anerkannt werden kann, genau und nicht nur allgemein darlegen, auch wenn er nicht eine im Voraus festgelegte Schwelle von besonderer Schwere erreicht. Entscheidend ist, dass es sich nicht um eine bloße subjektive Wahrnehmung handelt, die veränderlich ist und auch vom Charakter und von persönlichen Faktoren abhängt, sondern um die Objektivierung einer, wenn auch geringfügigen aber nachweisbaren Beeinträchtigung der physischen oder psychischen Sphäre oder des Beziehungslebens einer Person; die Art der betroffenen personenbezogenen Daten und die Bedeutung, die sie im Leben der betroffenen Person haben und vielleicht auch die Wahrnehmung, die die Gesellschaft zu diesem Zeitpunkt von dieser spezifischen, mit der Datenverletzung verbundenen Beeinträchtigung hat (vgl. Schlussanträge des GA Pitruzella v. 27.04.2023 – C 340/21, Rn. 83 – juris).

Unter Berücksichtigung der Umstände kann hier die Befürchtung der Klagepartei, dass die Daten missbräuchlich

verwendet werden, nicht als begründet angesehen werden. Zu den besonderen Umständen gehört die Art des Datums. Wird die Kontrolle über sensible Daten, wie z.B. Gesundheitsdaten, Daten über die sexuelle Orientierung, Daten über rassische oder ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen, Daten über Bankverbindungen, Vermögenswerte, Einkommen, Beruf oder Berufsgeheimnisse verloren, liegt eine missbräuchliche Verwendung nicht fern (vgl. Art. 9 Abs. 1 DS-GVO). Insbesondere bei Daten, die den persönlichen Lebensbereich betreffen, besteht die Gefahr einer Rufschädigung oder Diskriminierung. Ebenso geht der Verlust der Kontrolle von Daten über Vermögenswerte, Bankverbindungen und Berufsgeheimnisse mit dem Risiko eines materiellen Schadens einher.

Bei der hier gehackten E-Mail-Adresse handelt es sich um ein solches Datum, das – seiner Funktion entsprechend – der Kontaktaufnahme dient und durch andere identifizierbare Personen im alltäglichen und geschäftlichen Leben regelmäßig anderen Personen in großem Umfang zugänglich gemacht wird (vgl. OLG Köln, Urt. v. 07.12.2023 – I-15 U 33/23, Rn. 37 – juris; OLG Hamm, Urt. v. 21.06.2024 – 7 U 154/23, Rn. 51 – juris). Sie stellt gerade kein besonders sensibles Datum dar, sondern eines aus der Sozialsphäre des Klägers. Mit der daneben erbeuteten IP-Adresse kann im Regelfall ein Hacker nichts anfangen, die User-ID könnte in der Verknüpfung mit dem Namen allenfalls einen Rückschluss darauf zulassen, dass die Klagepartei Nutzer eines Musik-Streaming-Dienstes ist. Welche konkrete Befürchtung die Klagepartei hieran anschließt, hat sie ebenso wenig dargelegt wie die negativen Folgen des Bekanntwerdens des Alters oder Geschlechts.

Ein Missbrauch drängt sich unter den gegebenen Umständen nicht auf. Die E-Mail-Adresse – ebenso wie etwa eine Telefonnummer – kann zwar auch missbräuchlich zur Übersendung von Spam sms oder betrügerischen Anrufen genutzt werden, jedoch kann ein materieller Schaden erst dann entstehen, wenn bei einer Spam -mail der mitgesendete link verwendet wird oder die betroffene Person auf einen Anruf reagiert, dem betrügerischen Anrufer Auskunft gibt oder auf dessen Aufforderung Geld überweist. Der Empfang von Spam-Nachrichten o.ä. als solcher – ohne weitere negativen Folgen – stellt für sich genommen keinen immateriellen Schaden dar (vgl. EuGH, Urt. v. 20.06.2024 – C-590/22, Rn. 34-36 – juris; OLG Hamm, Urt. v. 21.06.2024 – 7 U 154/23, Rn. 43 – juris). Die Lästigkeit, die mit den ungebetenen Nachrichten oder Anrufen von angeblichen Bankmitarbeitern, von automatischen Ansagen sowie mit der Zusendung von angeblichen Sendungsbenachrichtigungen oder anderen Spam-Nachrichten einhergeht, kann aber grundsätzlich schon deshalb nicht als begründete Befürchtung eines Missbrauches der Daten angesehen werde, weil davon Personen, deren Daten nicht gehackt wurden, in vergleichbarer Weise betroffen sind. Es ist allgemein – und auch den Senatsmitgliedern aus eigener Erfahrung – bekannt, dass Personen, die keine Streaming-Dienste nutzen, ebenfalls viele Spam-Nachrichten erhalten. Ein Zusammenhang mit dem streitgegenständlichen Datensatzverlust ist nicht nachweisbar. In den Schriftsätzen ist lediglich allgemein von Sorgen, Unwohlsein und Ängsten um einen befürchteten Identitätsdiebstahl wegen der entwendeten Daten die Rede.

Eine darüber hinaus gehende emotionale Beeinträchtigung der Klagepartei ist zur Überzeugung des Senates nicht eingetreten. Die schriftsätzlich allgemein gehaltene Behauptung der Klagepartei, sie sei in einen Zustand großen Unwohlseins und Sorge über einen möglichen Missbrauch geraten, genügt diesen Darlegungsanforderungen nicht. Die Ausführungen sind schon nicht auf die konkrete Person der Klagepartei bezogen, sondern werden in einer Vielzahl von Klagen gleichlautend wiederholt. Allgemeine Sorgen, Ängste und Unwohlsein sind alltägliche Empfindungen, die keine begründete Befürchtung rechtfertigen. Erforderlich ist vielmehr der konkrete Nachweis eines realen und sicheren emotionalen Schadens (vgl. Schlussanträge des GA Pitruzella v. 27.04.2023 – C -340/21, Rn. 82, 83, – juris). Da im Allgemeinen jeder Verstoß gegen eine Norm über den Schutz personenbezogener Daten zu einer negativen Reaktion der betroffenen Person führen kann (vgl. Schlussanträge des GA Campos Sanchez-Bordona v. 06.10.2022 – C 300/21, Rn. 113 – juris) und ein Schadenersatz, der sich aus einem bloßen Unmutsgefühl wegen der Nichtbeachtung des Rechts durch einen anderen ergibt, einem "Schadenersatz ohne Schaden" recht nahe kommt, der nicht von Art. 82 erfasst ist (vgl. EuGH, Urt. v. 04.05.2023 – C – 300/21, Rn. 36 ff – juris), reicht demgegenüber allein der potenzielle oder hypothetische Schaden oder die bloße Beunruhigung wegen des Diebstahls der eigenen personenbezogenen Daten nicht aus (vgl. Schlussanträge des GA Collins v. 26.10.2023 – C 182/22, Rn. 24 – juris). [...]

BUCHBESPRECHUNG

Schwartmann/Köhler (Hrsg.), **Datenrecht – Datenschutz, Datenwirtschaft, Digitalwirtschaft und KI**, C.F. Müller, Heidelberg, 2025, 1107 S., 35,– €

Herb, **Die Digitale Dekade der EU**, **Wegweiser zum neuen Datenrecht und Datenschutzrecht in Deutschland und Europa,** Boorberg Verlag, Stuttgart, 2025, 144 S., 28,– €

Das **Textbuch Datenrecht** von Prof. Dr. Rolf Schwartmann, Leiter der Kölner Forschungsstelle für Medienrecht an der TH Köln, und Moritz Köhler, Wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle für Medienrecht an der TH Köln, bietet mit seinen 1107 Seiten eine umfassende Einführung in das weitläufige und zunehmend bedeutende Gebiet des Datenrechts. Es weist eine klare Struktur auf, die das komplexe Zusammenspiel von Datenschutz, Datenwirtschaft, Digitalwirtschaft und Künstlicher Intelligenz (KI) greifbar macht.

Besonders hervorzuheben ist die thematische Einordnung und die Zusammenstellung relevanter Gesetzestexte des Datenrechts. Während einige Vorschriften wie die des BDSG und der DS-GVO im Volltext enthalten sind, werden andere Gesetze in gezielten Auszügen dargestellt. Diese Methode ermöglicht eine präzise Fokussierung auf die datenrechtlich entscheidenden Normen, etwa aus dem BGB oder StGB, und erleichtert so den Zugang zu den zentralen Regelungen des Datenrechts. Ergänzt wird dies durch die kluge Verknüpfung der europäischen Rechtsakte mit Verweisen zu den Erwägungsgründen, die über Fußnoten organisiert sind und einen erheblichen Mehrwert bieten, da sie die rechtliche Einordnung und Auslegung der jeweiligen Norm erleichtern.

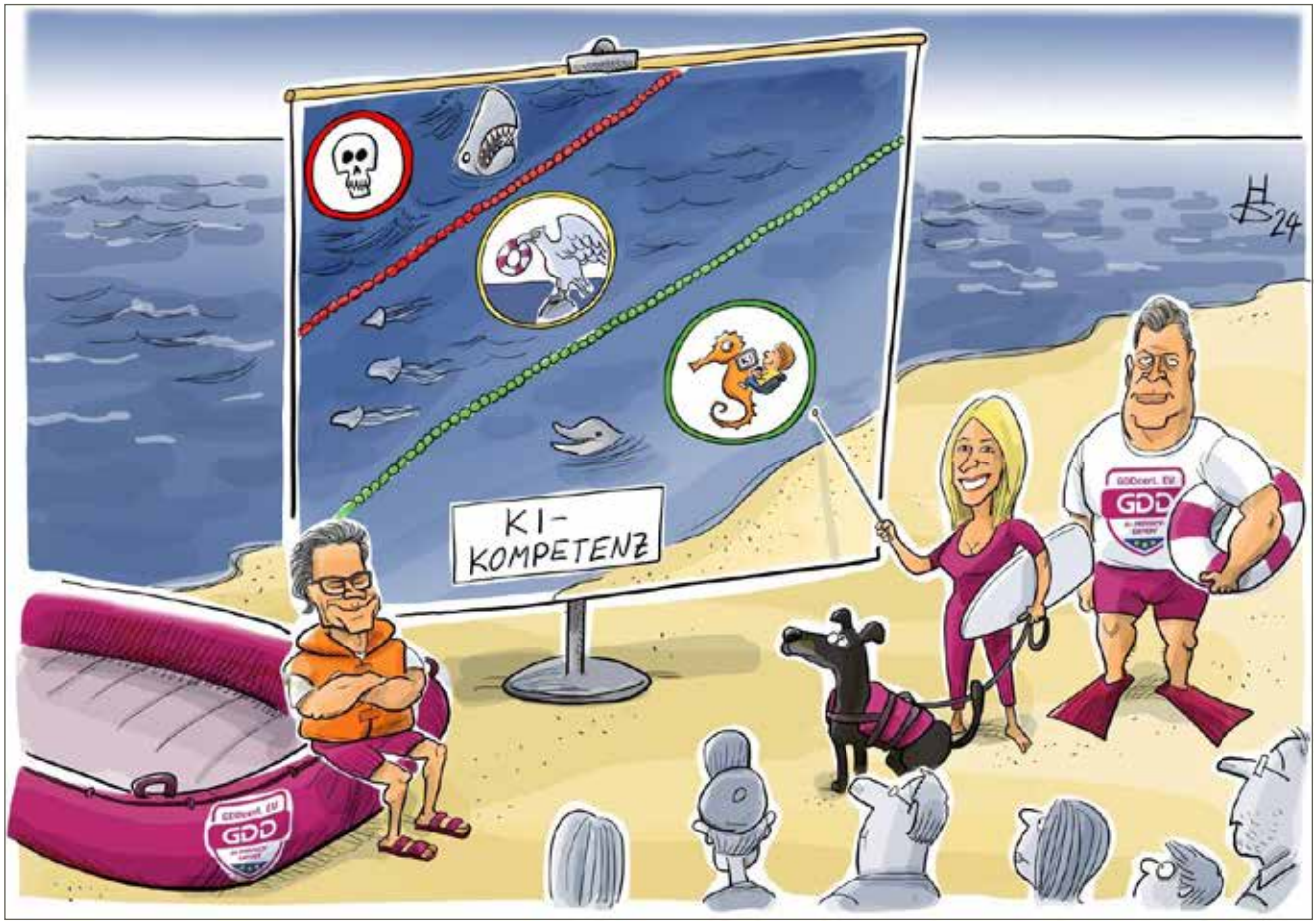
Das Werk liefert einen exzellenten Überblick über die Verzahnungen verschiedener Rechtsakte wie des Data Governance Act (DGA), des Data Act (DA) und der KI-Verordnung mit dem Datenschutzrecht. Dank einer ergänzenden Linksammlung, die über die Website der TH Köln abrufbar ist, bietet sich dem Leser die Möglichkeit, stets aktuell und praxisorientiert zu arbeiten. Für alle, die sich mit diesem komplexen, aber zukunftsweisenden Rechtsgebiet vertraut machen möchten, ist dieses Buch ein unverzichtbares Nachschlagewerk und ein äußerst hilfreicher Begleiter.

Eine gute Ergänzung zum Textbuch Datenrecht ist der kurze Band von Armin Herb. **Die Digitale Dekade der EU.** Der Band adressiert ein großes Thema, aber er versteht sich als Wegweiser zum neuen Datenrecht und Datenschutzrecht in Deutschland und Europa. Er umfasst nur gut 140 Seiten und in seiner Kürze liegt eine Stärke des Buches.

Wie das Textbuch von Schwartmann/Köhler trifft er eine Auswahl und behandelt in fünf Teilen die relevanten Digitalrechtsakte. Nach einer Einführung (Teil I), werden die fünf wichtigsten Verordnungen (DGA, DMA, DSA, DA und AI-Act) jenseits des Datenschutzrechts griffig vorgestellt. Sehr hilfreich sind Kleinigkeiten, wie eine tabellarische Zusammenstellung von Verordnungen, Geltungsdaten und Ausnahmen zur Geltung (S. 15). Teil III befasst sich mit weiteren Rechtsakten, allen voran mit der DS-GVO. In Teil IV werden die deutschen Begleitgesetze zum EU-Recht tabellarisch benannt und kurz eingeordnet. Es ist hilfreich für alle, die sich einen sehr kurzen Überblick über die Zusammenhänge schaffen wollen, um DDG, TMG, TDDDG, TKG und das geplante DGG im Schnelldurchlauf kennenzulernen. In Teil V werden schließlich kurz medienrechtliche Vorschriften, insbesondere der MStV vorgestellt.

Wenn man so will, ergänzen sich die Bücher von Schwartmann/Köhler und Herb insofern gut, als beide das neu entstandene Datenrecht systematisieren und transparent machen. Das Textbuch ist ein perfektes Werkzeug für die Arbeit mit dem Recht und der kurze Leitfaden eine kompakte Gebrauchsanweisung. Beide Anschaffungen lohnen und sie sind auch im Paket (35,– € bzw. 28,– €) mit knapp über 60,– € gut erschwinglich und eine Anschaffung wert.

Maximilian Olker



Das hat KI mit Tieren gemeinsam

KI-Systeme wie ChatGPT sind spezielle Werkzeuge. Ihre Besonderheit besteht darin, dass sie autonom arbeiten und dass das, was sie uns an Inhalten anbieten, weder vorhersehbar noch berechenbar ist. Man kann diese KI-Systeme mit Tieren vergleichen. Auch Spürhunde oder Polizei- oder Zugpferde sind nüchtern betrachtet lebende Werkzeuge. Das Tierschutzrecht gewährt ihnen keine Rechte, verpflichtet aber den Menschen zu deren Schutz und zu einer tiergerechten Behandlung. Was das ist, definiert allerdings der Mensch. Wenn wir Tiere halten oder im Beruf einsetzen, dann müssen wir uns darüber klar sein, dass wir ihr Inneres nicht beherrschen, sondern nur ihren Einsatz kontrollieren können. Tiere verantworten sich im Gegensatz zum Menschen nicht für Fehlverhalten oder haften gar dafür. Genau genommen kann man rechtlich gar nicht von Fehlern eines Tieres sprechen. So ist es auch bei KI-Systemen, wie ChatGPT. Die Sprache macht uns Menschen zu besonderen Geschöpfen, weil wir Geschichten erfinden, erzählen und verbreiten können. Das wiederum können KI-Systeme und sie erwecken so den Eindruck, als seien sie intelligent oder gar menschlich. Anders ein Tier, beißt KI nicht. Wir haben noch kaum negative Erfahrungen mit der neuen Technik gemacht und sehen vielleicht nicht ein, warum wir uns vor Risiken, die man erst bei genauerem Hinsehen, „mit Händen greifen" kann, schützen sollen. Deshalb muss man sich dringend absichern, wenn es um den Einsatz von GPAI geht. Man muss lernen, wann man in hochriskante oder gar verbotene Zonen kommt. Das ist nicht ungewöhnlich. Auch als Tierhalter muss man je nach Risiko einen „Tierführerschein" machen, um seine Eignung für den Umgang mit dem autonomen und potenziell gefährlichen Wesen nachzuweisen.

Bild: nazarkru - stock.adobe.com

Awareness-Schulungen, die bewegen!

Kommen Sie Ihrer Unterweisungspflicht gemäß DS-GVO nach.

- Datenschutz für Beschäftigte
- Datenschutz für Führungskräfte
- Datenschutz Zusatzmodule
- Datenschutz KI
- Datenschutz öD
- Datenschutz im Gesundheitswesen

Jetzt kostenfrei testen: **elearning-mit-zertifikat.de**

UNIVADO

DATAKONTEXT

Löschen nach DS-GVO

Datenschutzrechtliche Anforderungen und Entwicklung von Löschkonzepten

3. April 2025 | online | 10:00 Uhr – 17:00 Uhr
Referenten: Sascha Kremer, Dr. Oliver Stiemerling

Schwerpunktthemen:

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

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

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT