

MMR

Zeitschrift für das Recht
der Digitalisierung,
Datenwirtschaft und IT

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

AUS DEM INHALT

- | | |
|-----------------------|--|
| Prüfungsrecht | 455 ANNE PASCHKE
Künstliche Intelligenz unter Erlaubnisvorbehalt? |
| Haftungsfragen | 457 VALERIE SCHNEIDER / ANNA CARDILLO
White-Label-Modelle im digitalen Umfeld:
Strategische Risiko- und Vertragsanalyse |
| Public-Cloud-Dienste | 462 ALEXANDER KUBIS
Das Schuldverhältnis bei IaaS- und PaaS-Cloud-
Verträgen |
| Leistungsschutzrechte | 466 WOLFGANG FRHR. RAITZ VON FRENTZ / CHRISTIAN L.
MASCH
KI und Urheberrecht im Zivilprozess und im
Schiedsstellenverfahren |
| Verbraucherschutz | 472 SEBASTIAN PECH
Vom Bestellbutton über den Kündigungsbutton zum
Widerrufsbutton |
| Transparenz | 477 MORITZ GRIESEL / HANS BRORSEN
Kennzeichnungspflichten für synthetische
Medieninhalte |
| Digitalrechtsakte | 482 ANKE DIECKHOFF / FELIX HEMPEL
Die Reform der Datenschutzaufsicht |
| | 487 ANNA LENA NOWICKI / LISA FLECKENSTEIN / LUCAS
BLUM / DANIEL WERNER
Diensteanbieter im Fokus der e-Beweismittelsicherungs-
Verordnung |
| | 494 EuGH: Tragweite der Ausnahme für „Pastiches“
im Zusammenhang mit Sampling mAnm HOEREN |
| | 500 EuGH: Exzessivität von Auskunftsanträgen
mAnm SOSNA / MEYER |



Beilage
Leserumfrage mit
Gewinnspiel

www.mmr.de

6/2026

Seiten 455–538
29. Jahrgang · 15. Juni 2026



[linkedin.com/showcase/zeitschriftmmr](https://www.linkedin.com/showcase/zeitschriftmmr)



C.H. BECK



1850202606

3. Kölner Symposium zum Urheber- und Medienrecht

09.07.2026 | 10.07.2026 | KölnSKY

Programm-Highlights:

- › Territoriale Grenzen des Urheberrechts in der dt. und europ. Rechtsprechung
- › Künstliche Intelligenz & Recht: Vervielfältigung und öff. Wiedergabe durch Memorisierung; Haftung für rechtsverletzenden KI-Output aus urheber- und äußerungsrechtlicher Sicht; legislative Reaktion auf generative KI
- › Recht an der eigenen Stimme
- › SLAPP-Klagen
- › Haftungsfreistellungen des DSA im Urheber- und MedienR
- › Panel & Streitgespräch: Expansives Medienstrafrecht

Wissenschaftliche Leitung:

- › Prof. Dr. Ingo Jung, Rechtsanwalt, CBH Rechtsanwälte; Honorarprofessor an der TH Köln
- › Prof. Dr. Karl-Nikolaus Peifer, Universität zu Köln
- › Prof. Dr. Benjamin Raue, Rheinische Friedrich-Wilhelms-Universität Bonn



10 Stunden Fortbildung
gem. § 15 FAO

bis 15.05.2026

1.050 €

danach 1.190 €
jeweils zzgl. MwSt.

Jetzt anmelden →

wolterskluwer.com/koelner-symposium-urh



INHALT

Prüfungsrecht	EDITORIAL 455 ANNE PASCHKE Künstliche Intelligenz unter Erlaubnisvorbehalt?
Haftungsfragen	BEITRÄGE 457 VALERIE SCHNEIDER / ANNA CARDILLO White-Label-Modelle im digitalen Umfeld: Strategische Risiko- und Vertragsanalyse. White-Labeling vor dem Hintergrund des Cyber Resilience Act
Public-Cloud-Dienste	462 ALEXANDER KUBIS Das Schuldverhältnis bei IaaS- und PaaS-Cloud-Verträgen. Pflichtenprogramm und Leistungsstörungenrecht beim PaaS-Cloud-Vertrag im B2B-Bereich
Leistungsschutzrechte	466 WOLFGANG FRHR. RAITZ VON FRENTZ / CHRISTIAN L. MASCH KI und Urheberrecht im Zivilprozess und im Schiedsstellenverfahren. Urheberrechtliche Nutzungen und Durchsetzung daraus folgender Ansprüche
Verbraucherschutz	472 SEBASTIAN PECH Vom Bestellbutton über den Kündigungsbutton zum Widerrufsbutton. Die Widerrufsfunktion für Fernabsatzverträge
Transparenz	477 MORITZ GRIESEL / HANS BRORSEN Kennzeichnungspflichten für synthetische Medieninhalte. Rechtliche Anforderungen und technische Realität
Digitalrechtsakte	482 ANKE DIECKHOFF / FELIX HEMPEL Die Reform der Datenschutzaufsicht. Wer beaufsichtigt die neuen EU-Digitalrechtsakte?
Strafverfolgung	487 ANNA LENA NOWICKI / LISA FLECKENSTEIN / LUCAS BLUM / DANIEL WERNER Diensteanbieter im Fokus der e-Beweismittelsicherungs-Verordnung. Alles neu bei elektronischen Beweismitteln?
Kunstfreiheit	RECHTSPRECHUNG 494 EuGH: Tragweite der Ausnahme für „Pastiches“ im Zusammenhang mit Sampling Urteil vom 14.4.2026 – C-590/23 – Pelham mAnm HOEREN
Datenverarbeitung	500 EuGH: Exzessivität von Auskunftsanträgen Urteil vom 19.3.2026 – C-526/24 – Brillen Rottler mAnm SOSNA / MEYER

Fernabsatzvertrag	506 EuGH: Verbraucherrechtliches Widerrufsrecht bei Unterstützung durch einen Architekten Urteil vom 5.3.2026 – C-564/24 – Eisenberger Gerüstbau GmbH mAnm BRISKE / MÜTER
Vervielfältigungsrecht	512 ÖOGH: Speichermedienvergütungspflicht für Cloud-Speicher nach österreichischem Urheberrecht Urteil vom 16.12.2025 – 4 Ob 15/25x
Formmangel	514 BGH: Dateiformat PDF als zwingendes Recht Urteil vom 10.2.2026 – VI ZR 313/24
Online-Coaching	516 BGH: Teleologische Reduktion des § 1 Abs. 1 Nr. 1 FernUSG Urteil vom 5.2.2026 – III ZR 137/25 mAnm STOFFEL / DIESLER / KLICKERMANN
Code of Conduct	521 BGH: Lösungsfrist bei Zahlungsstörungen Urteil vom 18.12.2025 – I ZR 97/25 mAnm REINELT
Internetveröffentlichung	528 OLG Hamburg: Örtliche Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet Beschluss vom 3.3.2026 – 7 W 26/26
Missbrauchskontrolle	529 KG: Log-in-Pflicht bei Online-Kündigungsschaltfläche unzulässig Urteil vom 18.11.2025 – 5 UKI 10/25
Kündigungsschaltfläche	532 KG: Unzulässige Abfrage von Log-in-Daten bei Kündigung von Dauerschuldverhältnissen Urteil vom 12.11.2025 – 5 U 6/25
Unwahre Tatsachenbehauptung	536 LG Hamburg: Haftung für KI-generierte Persönlichkeitsverletzung Beschluss vom 23.9.2025 – 324 O 461/25
Jugendmedienschutz	536 VG Köln: Beanstandung eines Twitch-Livestream-Angebots Urteil vom 25.11.2025 – 6 K 2650/22 mAnm HENTSCH
	538 Leitsätze

III–IV	Inhalt
V–XXVII	MMR-Fokus
XXVIII	Impressum



Beilage
Leserumfrage mit Gewinnspiel

Sandra Schmitz-Berndt EU-Parlament: Forderung von Nudifier-Verbot in KI-Systemen

MMR-Aktuell 2026, 01252

Nachdem sich die EU-Mitgliedstaaten am 13.3.2026 im Standpunkt des Rates zum Digital-Omnibus-Paket zur KI auf ein Verbot von KI-Praktiken zur Erstellung nicht einvernehmlicher sexueller und intimer Inhalte sowie von Darstellungen sexuellen Kindesmissbrauchs geeinigt haben, fordert auch das EU-Parlament eine Ergänzung der KI-VO um ein spezifisches Nudifier-Verbot, also ein Verbot von KI-Praktiken, die Personen künstlich entkleiden. Der Vorschlag der EU-Kommission zum Digital-Omnibus-Paket zur KI v. 19.11.2025 sah keine Regulierung entsprechender Anwendungen vor.

Die von den Ausschüssen für Binnenmarkt und bürgerliche Freiheiten ausgearbeitete Position, die am 26.3.2026 vom Parlament angenommen wurde, fordert konkret die Aufnahme eines Verbots des Inverkehrbringens, der Inbetriebnahme oder Nutzung eines KI-Systems, das realistische Bilder oder Videos so verändert, manipuliert oder künstlich erzeugt, dass sexuell explizite Handlungen oder die intimen Körperteile einer identifizierbaren natürlichen Person ohne deren Einwilligung dargestellt werden.

Dieses Verbot soll nicht für Anbieter oder Nutzer von KI-Systemen gelten, die wirksame Sicherheitsmaßnahmen eingeführt haben, um die Erstellung solcher Darstellungen zu verhindern und einen fortlaufenden Missbrauch nach dem Inverkehrbringen oder der Inbetriebnahme des Systems zu vermeiden. Das Verbot soll KI-Anbieter aber nicht darin hindern, die o.g. Fähigkeiten zu entwickeln. Art. 5 der KI-VO soll dementsprechend ergänzt werden.

Dieser Ansatz unterscheidet sich von dem Standpunkt des Rates der EU, wonach auf der Output-Seite auch Audioinhalte oder ähnliche Materialien mit entsprechenden Inhalten verboten werden sollen, während nach dem EU-Parlament zunächst nur Bilder und Videos erfasst sein sollen. Auch hinsichtlich der Anforderungen an die Einwilligung der identifizierbaren Person unterscheiden sich die Vorschläge von Rat und Parlament. Der Rat schlägt diesbezüglich vor, die Rechtmäßigkeit von einer „freiwilligen, spezifi-

schon, informierten, unmissverständlich und ausdrücklichen Einwilligung für diese Erzeugung, Manipulation oder Reproduktion“ abhängig zu machen. Unabhängig von den Anforderungen an die spezifische Einwilligung wird dieses Erfordernis Anbieter und Betreiber von KI-Systemen vor Herausforderungen stellen, denn schon bei der Eingabe des Befehls müsste das Vorliegen einer solchen Einwilligung überprüft werden.

Abweichungen bei der Verhandlungsposition finden sich auch im Hinblick auf den Regulierungsgegenstand: Die verbotene Praktik soll sich in der Position des EU-Parlaments auf alle KI-Systeme beziehen, die entsprechendes Material verändern, manipulieren oder erzeugen können.

Der Standpunkt des Rates sieht hier eine Einschränkung dahingehend vor, dass in einem zweiten Absatz erläutert wird, wann ein KI-System als in der Lage gilt, die genannten Inhalte zu erzeugen, zu manipulieren oder zu reproduzieren. Dies soll dann der Fall sein, wenn dies der beabsichtigte Zweck des KI-Systems ist oder die Ausgestaltung, das Training, die Architektur, die Fähigkeiten oder die nutzerseitigen Funktionen die Erzeugung solcher Inhalte „als vernünftigerweise vorhersehbares und reproduzierbares Ergebnis“ ermöglichen, ohne dass wesentliche technische Änderungen erforderlich sind, und das System über keinen Schutzmechanismus verfügt.

Letzteres bedeutet, dass die technische Ausgestaltung einen Missbrauch naheliegend macht, was zB bei Face-Swapping der Fall sein dürfte. Es sollte darauf abzustellen sein, ob ein durchschnittlicher Nutzer das Ergebnis mit den zur Verfügung stehenden Mitteln, sprich dem KI-System, erzeugen kann, ohne dass dies effektiv unterbunden wird. Ergänzend hierzu sieht der Standpunkt des Rates vor, dass das Verbot sich nicht auf andere Formen von Nacktinhalten erstreckt, wie etwa Inhalte ohne Bezug zu identifizierbaren natürlichen Personen, realistische Nacktdarstellungen ohne Sichtbarkeit intimer Körperteile, nicht-realistische künstlerische Aktdarstellungen sowie satirische Werke, die keine identifizierbaren natürlichen Personen realistisch bei sexuellen Handlungen zeigen oder deren intime Körperteile darstellen. Inwieweit ein KI-System überhaupt in der Lage ist, zu beurteilen, ob ein zu erzeugender Inhalt

satirischen Charakter hat, erscheint in diesem Zusammenhang äußerst zweifelhaft.

Es ist daher absehbar, dass insbesondere die konkrete Ausgestaltung eines entsprechenden Verbots in den Trilog-Verhandlungen intensiv diskutiert werden wird, auch wenn wohl weitgehend Einigkeit darüber besteht, dass eine solche Regelung grundsätzlich erforderlich ist.

■ Vgl. auch Schmitz-Berndt MMR-Aktuell 2026, 01179; Schmitz-Berndt MMR-Aktuell 2026, 01212; MMR-Aktuell 2026, 01144; Waegner MMR-Aktuell 2026, 01125 und Etteldorf ZD-Aktuell 2025, 01271.

Dr. Sandra Schmitz-Berndt LL.M., LL.M., ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

BNetzA: KI-Service Desk

MMR-Aktuell 2026, 01261

Die BNetzA hat in Vorbereitung auf ihre voraussichtlich zentrale Rolle bei der Umsetzung der KI-VO ein umfassendes KI-Service Desk entwickelt, um Unternehmen, Behörden sowie Organisationen bei der Umsetzung der KI-VO zu unterstützen. Neben einem KI-Compliance-Kompass, der eine erste Orientierung zur Relevanz der KI-VO für die unterschiedlichen Akteure ermöglicht, bietet das Service Desk Informationen zu vielen weiteren Themen.

So werden mehrere Themenbereiche zur KI-Regulierung abgedeckt: Ziele, Zielgruppen und Zeitplan der Verordnung, das risikobasierte System der Einstufung von KI-Anwendungen, Vorgaben zu Transparenzpflichten, Regelungen zu KI-Modellen mit allgemeinem Verwendungszweck, Anforderungen an Hochrisiko-Systeme, verbotene Praktiken sowie Fragen der Governance, Normung, Marktüberwachung und Notifizierung. Weitere Abschnitte befassen sich mit Energie- und Ressourceneffizienz sowie der Rolle der BNetzA als zentrale Anlaufstelle.

Abgerundet wird die Seite durch FAQ, weiterführende Materialien, ein Factsheet, Blog-Beiträge und Podcast-Hinweise. Insgesamt dient sie als strukturierter Einstiegspunkt in die regulatorischen Anforderungen der KI-VO und die Unterstützungsangebote der BNetzA.

■ Vgl. hierzu auch MMR-Aktuell 2024, 01539.

Jakob Horn/Susan Lipeyko/ Alexander Schmalenberger Einigung mit neuen Fristen – Politische Verständigung über den KI-Omnibus

MMR-Aktuell 2026, 01266

Am 7.5.2025 erzielten das EU-Parlament und der Rat eine politische Einigung über den sog. KI-Omnibus, einen Teil des Digital Omnibus-Pakets der EU-Kommission zur Verbesserung der Digitalrechtsregulierung in der EU. Der KI-Omnibus zielt insbesondere auf die Änderung der erst im August 2024 in Kraft getretenen KI-VO (VO (EU) 2024/1689). Zentrale Themen der politischen Einigung sind die Verschiebung der Geltung wichtiger Vorschriften um bis zu anderthalb Jahre, die Einführung neuer verbotener KI-Praktiken sowie verschiedene Erleichterungen für Unternehmen, die KI-Systeme entwickeln und einsetzen. Der „große Wurf“ ist der KI-Omnibus allerdings nicht. So wurde etwa weder die weitgehend konturlose Definition von KI-Systemen angegangen noch wurden die Vorschriften, die Anbieter und Betreiber von Hochrisiko-KI-Systemen einhalten müssen, substantiell verändert.

I. Kernpunkte der politischen Einigung

1. Neue Fristen

Im Mittelpunkt der Einigung steht eine Verschiebung der Geltung zentraler Vorschriften. So gelten die Vorgaben für alleinstehende Hochrisiko-KI-Systeme (Art. 6 Abs. 2 KI-VO iVm Anhang III KI-VO) erst ab 2.12.2027, also etwa anderthalb Jahre später als bisher vorgesehen (2.8.2026). Für produktintegrierte Hochrisiko-KI-Systeme nach Art. 6 Abs. 1 KI-VO iVm Anhang I KI-VO wird der Geltungsbeginn um ein Jahr verschoben, vom 2.8.2027 auf den 2.8.2028.

Als besonders problematisch werden in der Praxis derzeit die Kennzeichnungspflichten nach Art. 50 Abs. 2 KI-VO (sog. Watermarking) gesehen. Das EU-Parlament hatte in seiner Presseerklärung angekündigt, die Geltung der Kennzeichnungspflichten werde um vier Monate bis zum 2.12.2026 verschoben. Ein Blick in einen geleakten Entwurf zum künftigen Text des KI-Omnibus zeigt jedoch, dass die Verschiebung nicht pauschal für alle KI-Systeme gilt, sondern nur für KI-

Systeme, die bereits vor dem 2.8.2026 in Verkehr gebracht wurden. Für KI-Systeme, die am oder nach dem 2.8.2026 in Verkehr gebracht werden, gelten die Kennzeichnungspflichten sofort.

2. Erweiterte Verbote

In materieller Hinsicht ergänzt die Einigung Art. 5 KI-VO um zwei verbotene KI-Praktiken (Art. 5 Abs. 1 lit. ba und bb KI-VO-E). Im Grundsatz verboten ist das Inverkehrbringen, die Inbetriebnahme oder die Nutzung von KI-Systemen, die ohne wirksame Einwilligung realistische intime Darstellungen identifizierbarer Personen oder Material über sexuellen Kindesmissbrauch erzeugen oder manipulieren. Ob ein KI-System in diese Kategorie fällt, soll nicht ausschließlich davon abhängen, ob der Anbieter das System für diesen Einsatz gedacht hat. Verboten ist auch der Einsatz von KI-Systemen, bei denen solche Ergebnisse nach Design, Training, Architektur oder Nutzerfunktionen vernünftigerweise erwartbar und reproduzierbar sind, sofern keine hinreichenden technischen und organisatorischen Schutzmaßnahmen bestehen (Art. 5 Abs. 1a lit. a KI-VO-E). Betreiber unterfallen dem Verbot, wenn sie ein KI-System gezielt zur Erzeugung oder Manipulation entsprechender Inhalte einsetzen (Art. 5 Abs. 1a lit. b KI-VO-E).

3. Produktintegrierte Hochrisiko-KI und Governance

Gewisse Erleichterungen soll es für KI-Systeme geben, die in ein Produkt integriert sind und deshalb als Hochrisiko-KI-System gelten. Die inhaltlichen Anforderungen für Hochrisiko-KI-Systeme werden jedoch nur geringfügig angepasst. Eine erste Erleichterung in dieser Hinsicht betrifft Produkte, die der EU-Maschinen-VO (VO (EU) 2023/1230) unterliegen. Diese Verordnung wird von Annex I/A in Annex I/B verschoben. Auch wenn die Verschiebung technisch wirkt, hat dies große Auswirkungen, denn auf KI-Systeme, die Annex I/B unterfallen, findet die KI-VO nur eingeschränkt Anwendung. Primär gelten hier die Anforderungen des jeweiligen Harmonisierungsrechtsakts, also zB die EU-Maschinen-VO. Zusätzlich soll es Erleichterungen geben für KI-Systeme, die Annex I/A unterfallen. Sofern die anwendbaren Harmonisierungsvorschriften ein gleichwertiges oder höheres Schutzniveau für Gesundheit, Si-

cherheit und Grundrechte bieten und das Schutzniveau nicht insgesamt unter das der KI-VO sinkt, sollen die Vorschriften der KI-VO eingeschränkt werden (Art. 2 Abs. 13 KI-VO-E). Die Kommission soll hier bis zum 2.8.2027 festlegen, welche KI-Systeme das betrifft.

Weitere Erleichterungen betreffen die Einschränkung der Anwendbarkeit der Vorschriften für Hochrisiko-KI-Systeme, etwa durch eine Schärfung des Begriffs der Sicherheitskomponente. Im Kern sollen nur noch solche Komponenten erfasst werden, deren Versagen Gesundheit oder Sicherheit gefährden (Art. 6 Abs. 1 Nr. 1a, 1b KI-VO-E).

4. Erleichterungen beim Datenschutz

Erleichterungen soll es auch beim KI-spezifischen Datenschutz geben. Zwischen der KI-Entwicklung und dem Datenschutzrecht gibt es eine gewisse natürliche Spannung, weil die Entwicklung und Verbesserung von KI-Modellen die Verarbeitung von Daten voraussetzen. Das Datenschutzrecht will die Verarbeitung personenbezogener Daten demgegenüber möglichst auf das Nötige beschränken. Ein KI-Entwickler steht daher immer vor der Frage, ob und unter welchen Bedingungen Datensätze, die auch personenbezogene Daten enthalten, überhaupt in der KI-Entwicklung eingesetzt werden dürfen. Besonders schwierig gestaltet sich die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie Gesundheitsdaten. Art. 9 DS-GVO erlaubt die Verarbeitung idR nur, wenn eine Einwilligung des Betroffenen vorliegt. Das ist in der Praxis bei großen Datenbeständen kaum zu erreichen. Der KI-Omnibus bringt hier eine gewisse Erleichterung, denn Art. 4a KI-VO-E beinhaltet einen neuen Ausnahmetatbestand. Dieser erlaubt die Verarbeitung von besonderen Kategorien personenbezogener Daten iSd Art. 9 Abs. 1 DS-GVO zum Zwecke der Erkennung und Korrektur von Verzerrungen (bias).

Die Bedeutung des Art. 4a KI-VO-E darf aufgrund der umfassenden Vorgaben jedoch nicht überbewertet werden. So ist die Verarbeitung etwa nur erlaubt, wenn die Verarbeitung anderer Daten (einschließlich synthetischer oder anonymisierter Daten) nicht ausreicht. Zudem ist die Vorschrift nicht vollständig neu,

sondern adaptiert nur den bisherigen Art. 10 Abs. 5 KI-VO. Der wesentliche Unterschied zur Vorgängerregelung liegt darin, dass Art. 10 Abs. 5 KI-VO nur für Hochrisiko-KI-Systeme galt. Die neue Vorschrift kann nun grundsätzlich von allen Anbietern von KI-Systemen und KI-Modellen als Rechtfertigung der Verarbeitung personenbezogener Daten genutzt werden.

5. Erleichterungen bei KI-Kompetenz-Vorgaben

Erleichterungen gibt es auch bei der sich aus dem derzeitigen Art. 4 KI-VO ergebenden Pflicht, für KI-Kompetenz (AI Literacy) der eigenen Mitarbeiter zu sorgen. Während Unternehmen bisher verpflichtet waren, nach besten Kräften für ein angemessenes Maß an KI-Kompetenz zu sorgen, sollen sie künftig nur noch verpflichtet sein, die Entwicklung von KI-Kompetenz zu unterstützen. Die EU-Kommission und die Mitgliedstaaten werden zudem ausdrücklich verpflichtet, die Bemühungen zu unterstützen und zu fördern, etwa durch Bereitstellung praktischer Beispiele für die Erfüllung dieser Pflichten.

In der Praxis dürfte diese Änderung allerdings nur begrenzte Auswirkungen haben. Eine Verletzung der Pflicht, für KI-Kompetenz zu sorgen, war auch bisher nicht mit Sanktionen bewehrt. Ein Verstoß hätte daher bisher nicht unmittelbar mit Bußgeldern oder Verpflichtungen durchgesetzt werden können. Gleichzeitig werden sich im Vertrags- und Deliktsrecht weitere Sorgfaltspflichten entwickeln, die Unternehmen Haftungsrisiken aussetzen, wenn KI nicht mit der notwendigen Umsicht eingesetzt wird. Unternehmen werden daher auch ohne explizite Pflicht ein Interesse haben, für die KI-Kompetenz ihrer Mitarbeiter zu sorgen.

II. Praktische Konsequenzen der Einigung

Unternehmen sollten sich nun mit den neuen Vorgaben beschäftigen und prüfen, ob und was sich für ihre eigenen Governance-Bemühungen ändert. Hilfreich ist hierbei die zusätzliche Zeit bis die Pflichten für Hochrisiko-KI-Systeme gelten. Die zusätzliche Zeit sollte nun genutzt werden, um sich auf die neuen Vorgaben einzustellen. Daneben müssen Unternehmen beachten, dass die Trans-

parenzpflichten nach Art. 50 KI-VO im Grundsatz weiterhin ab dem 2.8.2026 gelten. Nur für die Kennzeichnungspflicht nach Art. 50 Abs. 2 KI-VO gibt es eine kurze Verschiebung für Bestandssysteme.

Daneben müssen Unternehmen sich auf die neuen verbotenen KI-Praktiken einstellen. Insbesondere Anbieter von KI-Systemen, die verbotene Inhalte erzeugen können, müssen sich nun schnellstmöglich damit beschäftigen, wie sie die Erzeugung entsprechender Inhalte wirksam verhindern können. In Betracht kommen insbesondere sicheres Prompt-Design, Output-Kontrollen, Inhaltsklassifizierung und Filtermechanismen, Nutzungsbeschränkungen, Missbrauchserkennung sowie Notice-and-Action- und Korrekturmechanismen. Die entsprechenden Pflichten treffen im Kern alle Anbieter von KI-Systemen, die Bilder, Videos, Audio und vergleichbare Inhalte erzeugen können. Werden hier keine ausreichenden Vorkehrungen gegen die missbräuchliche Verwendung getroffen, drohen empfindliche Bußgelder. Die neuen Regeln zu verbotenen KI-Praktiken sollen bereits ab dem 2.12.2026 in Kraft treten.

■ Vgl. hierzu auch MMR-Aktuell 2026, 01225.

Dr. Jakob Horn, LL.M. (Harvard),

ist Rechtsanwalt im Bereich Technology, Media & Telecoms (TMT) im Berliner Büro von Taylor Wessing.

Susan Lipeyko, Lic. en droit,

ist Rechtsanwältin im Bereich TMT im Münchener Büro von Taylor Wessing.

Alexander Schmalenberger, LL. B.,

ist Rechtsanwalt und Knowledge Lawyer im Bereich TMT im Hamburger Büro von Taylor Wessing.

Sandra Schmitz-Berndt EU: Veröffentlichung von Transparenzberichten aufgrund Verhaltenskodex gegen Desinformation

MMR-Aktuell 2026, 01253

Im Februar und März 2026 haben die Unterzeichner des freiwilligen Verhaltenskodex gegen Desinformation ihre jüngsten Berichte im Online-Transparenzzentrum für den Kodex veröffentlicht. In diesen ersten Berichten nach Anerken-

nung des Kodex als Verhaltenskodex iSd Art. 45 DSA legen die Unterzeichner detailliert dar, welche Maßnahmen sie iRd Verhaltenskodex gegen die Verbreitung von Desinformation ergriffen haben. Mit der Anerkennung des Kodex als Verhaltenskodex zum 1.7.2025 ist dieser zu einem wichtigen Maßstab für die Einhaltung der Verpflichtungen zur Risikominimierung des Art. 35 DSA durch die Unterzeichner geworden. Sehr große Online-Plattformen (VLOPs) und sehr große Online-Suchmaschinen (VLOSEs) unterliegen einer halbjährlichen Berichtspflicht, während andere Unterzeichner jährlich Bericht erstatten müssen. Die im Transparenzzentrum des Kodex veröffentlichten Berichte stammen von Anbietern von Online-Plattformen wie Google, Meta, Microsoft und TikTok sowie von Faktenprüfern, Forschungs- und zivilgesellschaftlichen Organisationen und Vertretern der Werbebranche.

Die Transparenzberichte enthalten Informationen u.a. zu Maßnahmen gegen Desinformation, zur Inhaltmoderation, zu politischer Werbung, zur Kooperation mit Faktenprüfern, Demonetarisierung von Desinformation und Ausführungen zu spezifischen Risiken. Außerdem liefern die Berichte Daten zur Umsetzung der plattformspezifischen Maßnahmen und führen Entwicklungen bei Richtlinien, Tools und Partnerschaften auf.

Der Umfang der Berichte ist aufgrund der Diversität der Berichtspflichtigen sehr unterschiedlich. So ist der Bericht von Facebook relativ kurz gehalten und verweist vielfach darauf, dass wie schon im Juli 2025 angekündigt, seit 6.10.2025 von Meta keine politischen, wahlbezogenen oder gesellschaftspolitischen Werbeanzeigen mehr auf seinen Plattformen erlaubt werden; begründet wird dies damit, dass die durch die Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) eingeführten Anforderungen und rechtlichen Unsicherheiten als nicht praktikabel angesehen werden. Damit erübrigen sich aus Sicht dieses Anbieters vielfach Ausführungen zu einzelnen Maßnahmen. Der Bericht von Facebook zeigt darüber hinaus auch, dass gegen die Entfernung von Inhalten aufgrund eines Verstoßes gegen die plattformeigenen Richtlinien zu schädlicher Gesundheitsfehlinformation, unethischem Verhalten oder zur Beeinflussung von Wahlen oder

eines Zensus in den Mitgliedstaaten nur in einem sehr geringen Bruchteil Widerspruch durch die betroffenen Nutzer eingelegt wurde. So wurde in Deutschland bei über 320.000 entfernten Inhalten nur in etwa 710 Fällen der Entscheidung widersprochen.

Was die Anzahl entfernter Inhalte betrifft, zeigt sich zB bei Twitch ein anderes Bild. Der Anbieter von Twitch selbst gibt an, dass relativ wenige Inhalte aufgrund der Selbstverpflichtung entfernt wurden. Begründet wird dies mit der Plattformstruktur, die es erschwere, schnell große Reichweiten aufzubauen, da Inhalte meist langformatig und oft nur für kurze Zeit verfügbar sind und dies groß angelegten Desinformationskampagnen im Weg stehe. Im Kontext von Wahlen und demokratischen Prozessen wurden im Berichtszeitraum keine entsprechenden Vorfälle festgestellt.

Die Berichte der Suchmaschinen Bing und Google beinhalten hingegen eigene Kapitel zu Maßnahmen im Zusammenhang mit aktuellen Krisen, insbesondere dem Krieg in der Ukraine und dem Konflikt zwischen Israel und der Hamas sowie zu Maßnahmen zum Schutz der Integrität von Wahlen zB in den Niederlanden und Irland. Ebenso verhält es sich bei den Berichten von Faktenprüfern wie zB Newsguard, wobei Newsguard auch auf sein am 24.2.2025 gestartetes Monitoring-Zentrum für Desinformation zu den deutschen Bundestagswahlen Bezug nimmt, das der Analyse gezielter Falschinformationen rund um die vorgezogene Wahl diene.

Zusammenfassend zeigen die Transparenzberichte, dass Desinformationsaktivitäten insbesondere im Kontext von geopolitischen Konflikten, Wahlen und Gesundheitsthemen stehen und es gezielte Einflusskampagnen gibt, die versuchen politische Narrative zu beeinflussen. Als neue Herausforderung für die Bekämpfung von Desinformation wird in verschiedenen Berichten der Aufstieg von KI-generierten Inhalten und ausländischer Einfluss auf große Sprachmodelle genannt.

■ Vgl. auch Setz di Fabio MMR 2024, 467; MMR-Aktuell 2022, 449701 mwN; Meese MMR-Aktuell 2025, 01542 und Wolters MMR 2025, 680.

Dr. Sandra Schmitz-Berndt LL.M., LL.M., ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

Lina Marquard **Discord: Vereinbarkeit der geplanten Altersprüfung mit den „Golden Five“ der Altersverifikation?**

MMR-Aktuell 2026, 01258

Die Online-Plattform Discord ist u.a. für ihre altersbeschränkten Server bekannt, die es Nutzenden erlauben, jugendgefährdende oder pornografische Inhalte zu teilen. Kritisiert wurde dabei, dass der Zugang lediglich von einer Selbstausskunft des Alters abhing (s. klicksafe.de v. 24.8.2023). Dies sollte geändert werden, denn Discord kündigte Anfang Februar 2026 die Einführung einer globalen Altersprüfung ab März 2026 an (Discord, Pressemitteilung v. 9.2.2026). Statt Zustimmung folgte große Empörung in der Community, sodass Discord die Einführung der Altersprüfung auf die zweite Jahreshälfte verschoben hat (Discord, Pressemitteilung v. 24.2.2026). Fernab des Aufruhrs bleibt zu klären, ob die geplante globale Altersprüfung mit den europäischen Vorgaben im Einklang steht.

1. Hintergrund

Discord ist mit weltweit über 90 Mio. aktiven Nutzenden pro Tag eine der bedeutendsten Plattformen für Messaging, Sprach- und Videodienste (Discord, About Page). Die amerikanische Plattform, die ursprünglich für die Gaming-Community entwickelt wurde, erfreut sich auch bei Minderjährigen größerer Beliebtheit. Neben privaten Messengern gibt es bei Discord Server, die von den Nutzenden erstellt werden können. Die Server können in verschiedene Kanäle unterteilt werden, wobei ein Server oder einzelne Kanäle als „altersbeschränkt“ markiert sein können. Es handelt sich dabei um eine Selbstkennzeichnung, wobei auch Discord selbst Server nachträglich als „altersbeschränkt“ einstufen kann. Weitere Funktionen der Plattform lassen sich durch Abschluss eines sog. Nitro-Abonnements freischalten.

In Deutschland gab es zuvor keine zwingende Alterskontrolle auf der Plattform, die über eine einfache Altersabfrage hinausging. Dabei ist Discord dafür bekannt, dass Kanäle und Server betrieben werden, die Inhalte mit der Kennzeichnung NSFW (not safe for work) oder 18+ beinhalten (Discord Support). Manche

Kanäle haben eigene Richtlinien und fordern eine aktive Bestätigung der Teilnehmenden, dass sie über 18 Jahre alt sind. Ein tatsächliches Hindernis für Minderjährige stellen diese Mechanismen allerdings nicht dar.

Um den regulatorischen Maßnahmen entgegenzukommen, entschied sich Discord am 9.2.2026, die globale Altersprüfung anzukündigen, um auf „jugendgerechte“ Standardprofile umzustellen (Discord, Pressemitteilung v. 9.2.2026). Die Empörung der Community ließ nicht lange auf sich warten, es folgten zahlreiche Kündigungen des Nitro-Abonnements und der Hashtag #DeleteDiscord wurde ins Leben gerufen.

Die heftige Reaktion der Community lässt sich vor allem durch das Timing erklären. Erst im Oktober 2025 war ein großes Datenleck bei dem von Discord genutzten Drittanbieter 5CA bekannt geworden. Dabei wurden rund 70.000 Ausweisfotos, die für Einsprüche gegen Altersbeschränkungen bei Discord genutzt wurden, erbeutet (Discord, Pressemitteilung v. 3.10.2025).

Daraufhin veröffentlichte Discord am 24.2.2026 ein ausführliches Statement, in dem Kommunikationsfehler eingeräumt wurden und die globale Altersprüfung auf die zweite Jahreshälfte vertagt wurde. Darin wurde klargestellt, dass die Altersprüfung nur diejenigen treffe, die auf geschlossene Nutzergruppen zugreifen wollen. Die Zahl liege bei 10% aller Nutzenden. Außerdem betonte Discord, dass es nur um die Verifizierung des Alters und nicht der Identität gehe. Grund für die Maßnahmen seien die zunehmenden regulatorischen Anforderungen. England, Australien und nun auch Brasilien sehen verpflichtende Alterskontrollen vor (Discord Blog v. 24.2.2026).

Auch auf nationaler Ebene werden effiziente Altersverifikationen diskutiert. So hat im September 2025 die Bundesdatenschutzbeauftragte (BfDI) Prof. Dr. Louisa Specht-Riemenschneider die „Golden Five“ der Altersverifikation vorgestellt (s. BfDI, Vortrag v. 1.9.2025). Altersverifikationen seien demnach rechtlich möglich (These 1), müssen aber die Grundsätze der Datenminimierung und der Verhältnismäßigkeit wahren (These 2). Für verpflichtende Alterskontrollen sei auf Zero-Knowledge-Lösungen zu setzen (These 3). Die Verhältnismäßigkeit sei erst ab einem gewissen Risikograd gewährt,

6/2026

HERAUSGEBER

RAin **Dr. Astrid Auer-Reinsdorff**, FA IT-Recht, Berlin/Lissabon – **Prof. Dr. Maximilian Becker**, Lehrstuhl für Bürgerliches Recht, Immaterialgüterrecht und Medienrecht, Universität Siegen – **Paula Cippierre**, Global Head of Privacy, HCLTech, Berlin – RA **Dr. habil. Christian Förster**, Partner, Bartsch Rechtsanwälte, Karlsruhe – **Prof. Dr. Nikolaus Forgó**, Professor für Technologie- und Immaterialgüterrecht und Vorstand des Instituts für Innovation und Digitalisierung im Recht, Universität Wien – RAin **Prof. Dr. Sibylle Gierschmann**, LL.M. (Duke University), FA Urheber- und Medienrecht, Hamburg – RA **Prof. Dr. Christian-Henner Hentsch**, M.A., LL.M., Leiter Recht und Regulierung beim game – Verband der deutschen Games-Branche e.V., Berlin/Professor für Urheber- und Medienrecht an der Kölner Forschungsstelle für Medienrecht der TH Köln – **Prof. Dr. Thomas Hoeren**, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. em. Dr. Bernd Holznagel**, ehem. Direktor der Öffentlich-rechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht, Universität Münster – **Prof. Dr. Lena Hornkohl**, LL.M., Tenure Track Professur für Europarecht, Universität Wien/Institut für Europarecht, Internationales Recht und Rechtsvergleichung – RAin **Dr. Andrea Huber**, LL.M. (USA), Berlin – **Prof. Dr. Katharina Kaesling**, LL.M., Juniorprofessur für Bürgerliches Recht, Geistiges Eigentum, insbesondere Patentrecht, sowie Rechtsfragen der KI, TU Dresden – **Prof. Dr. Dennis-Kenji Kipker**, Legal Advisor, Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) e.V., Kompetenzzentrum Informationssicherheit + CERT@VDE/Research Director Cyberintelligence.institute, Frankfurt/M. – **Wolfgang Kopf**, LL.M., Leiter Zentralbereich Politik und Regulierung, Deutsche Telekom AG, Bonn – **Prof. Dr. Oliver Kreutz**, LL.M., Professur für Zivilrecht mit der Vertiefungsrichtung Immaterialgüterrecht, Rechtsfragen der Digitalisierung und Wettbewerbsrecht, Ostfalia – Hochschule für angewandte Wissenschaften – **Prof. Dr. Marc Liesching**, Professor für Medienrecht und Medientheorie, HTWK Leipzig/München – **Prof. Dr. Tobias Lutz**, LL.M., MJur, Juniorprofessor für Privatrecht, Universität Augsburg – **Prof. Dr. Juliane K. Mendelsohn**, Juniorprofessur Fachgebiet Law and Economics of Digitization, TU Ilmenau – **Prof. Dr. Anne Paschke**, Professur für Öffentliches Recht, Technikrecht und Recht der Digitalisierung, Direktorin des Instituts für Rechtswissenschaften, Leiterin der Forschungsstelle Mobilitätsrecht und des Digital Innovation and Transformation Law Hubs (DigiTL Hub), TU Braunschweig – **Prof. Dr. Alexander Roßnagel**, Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Wiesbaden/Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel – **Prof. Dr. Christian Rückert**, Lehrstuhl für Strafrecht, Strafprozessrecht und IT-Strafrecht, Universität Bayreuth – RA **Dr. Raimund Schütz**, Loschelder Rechtsanwälte, Köln – **Prof. Dr. Louisa Specht-Riemenschneider**, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn – RA **Dr. Axel Spies**, Partner, Potomac Law, Washington DC – **Prof. Dr. Björn Steinrötter**, Lehrstuhl für Bürgerliches Recht, IT-Recht und Medienrecht, Universität Potsdam

BEIRAT DER KOOPERATIONSPARTNER

Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Medien (VAUNET), Berlin – RAin **Dr. Christiane Bierehoven**, Vorsitzende der Arbeitsgemeinschaft IT-Recht (davit) im Deutschen Anwaltverein e.V., Berlin – **Susanne Dehmel**, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – **Stefan Schicker**, Vorstandsvorsitzender des Legal Tech Verband Deutschland e.V., Berlin

REDAKTION

Anke Zimmer-Helfrich, Chefredakteurin – **Nina Himmelstoß**, Redakteurin – **Ruth Schrödl**, Redakteurin – **Christine Völker-Albert**, Redakteurin – **Alexandra Link**, Redaktionsassistentin – Wilhelmstr. 9, 80801 München

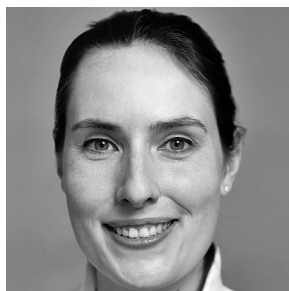
EDITORIAL Künstliche Intelligenz unter Erlaubnisvorbehalt?

Lesedauer: 7 Minuten

Am 28.5.2026 konstituierte sich an der Universität Hamburg die Arbeitsgruppe der Hochschulrektorenkonferenz (HRK) „Künstliche Intelligenz und Prüfungen“. Unter der Leitung von Prof. Dr. Gabi Reinmann (Hamburger Zentrum für universitäres Lehren und Lernen – HUL) soll durch insgesamt 11 Expertinnen und Experten innerhalb eines Jahres eine Handreichung zum Thema „Künstliche Intelligenz und Prüfungen an deutschen Hochschulen“ erstellt werden, „die Hochschulleitungen als Orientierung in strategischen Fragestellungen dienen soll.“ Im „Spannungsfeld zwischen KI-generierten Inhalten in Prüfungsleistungen, neuen Prüfungsformaten, rechtlichen Rahmenbedingungen und der Sicherung des Kompetenzerwerbs im wissenschaftlichen Arbeiten“ sieht die HRK einen besonders großen Handlungs- und Orientierungsbedarf seitens der Hochschulen. Die Arbeitsgruppe deckt insbesondere die Disziplinen Recht, Informatik und Didaktik ab. Ergänzt wird dies durch Expertise zu E-Learning oder Bildungstransfer. Von juristischer Seite wurden Prof. Dr. Sarah Rachut (TU Braunschweig) und Prof. Dr. Dirk Heckmann (TU München) in die Kommission berufen.

Damit ist die Hoffnung verbunden, dass im Mai 2027, viereinhalb (!) Jahre nach der breitflächigen Bereitstellung von Angeboten generativer KI wie ChatGPT (später dann Gemini, Claude und andere mehr), eine hinreichende Rechtssicherheit auch an den Hochschulen herrscht, ob und wie Künstliche Intelligenz in Prüfungen eingesetzt werden kann und unter welchen Bedingungen ein etwaiges Fehlverhalten sanktioniert werden darf. Diese Rechtssicherheit besteht derzeit nicht.

Im Gegenteil: Erste Gerichtsentscheidungen in diesem Kontext, wie jene des VG München (MMR 2024, 521 und VG München MMR 2024, 902) oder des VG Kassel (Urt. v. 25.2.2026 – 7 K 2515/25 und VG Kassel Urt. v. 25.2.2026 – 7 K 2134/24.KS) erwecken den trügerischen Eindruck, der KI-Einsatz in Hochschulprüfungen sei verboten, solange er nicht ausdrücklich – durch die jeweilige Hochschule oder die Prüfenden – erlaubt sei. Nachdem nicht wenige Lehrende die Erbringung von Prüfungsleistungen mit Unterstützung von KI-Anwendungen per se kritisch sehen, werden diese und die Prüfungsämter sich unter „Berufung auf die Rechtsprechung“ bequem zurücklehnen: Man müsse eigentlich gar nichts unternehmen, die Drohung des Nichtbestehens einer Prüfung bei KI-Einsatz muss nicht einmal ausgesprochen werden, sie steht einfach im Raum. Natürlich wisse man um die Bedeutung von KI in zukünftigen (sic!) beruflichen Kontexten.



Professorin Dr. Anne Paschke

Aber, gemacht: Das muss erst einmal in Ruhe erörtert werden. Bis dahin bleibt alles beim Alten. Schnelle Anpassungen an veränderte Verhältnisse sind nicht unbedingt eine Stärke der Verwaltung und im Lehrbetrieb.

Warum dann die Ungeduld? Einfach deshalb, weil die Einschätzung der Rechtslage durch die Verwaltungsgerichte falsch ist, wie die wohl herrschende Lehre in mehreren (Urteils-)Anmerkungen zutreffend konstatiert (Brägelmann RD 2024, 188; Rachut NJW 2024, 1057; vgl. auch Heckmann/Rachut ODW 2024, 85; Birnbaum NVwZ 2024, 607; Brägelmann KIR 2026, 84). So ist etwa der Einsatz von KI-Detektoren zum Aufspüren KI-generierter Inhalte untauglich und unzulässig. Und auch die Grundsätze des Anscheinsbeweises lassen sich auf solche Fälle nicht übertragen, weil sich die Texterzeugung mittels generativer KI nicht mit dem konventionellen Abschreiben bei Hausarbeiten vergleichen lässt.

Vor allem aber stimmt bereits die Grundannahme des VG Kassel nicht, wonach der Einsatz generativer KI in Hochschulprüfungen verboten ist, solange er nicht ausdrücklich erlaubt ist. Ein solches Verbot mit Erlaubnisvorbehalt ist verfassungsrechtlich nicht haltbar (so Heckmann in Anm. 2 zu VG Kassel jurisPR-ITR 9/2026). Es widerspricht bereits dem rechtsstaatlichen Grundsatz hinreichender Bestimmtheit: Was meint überhaupt KI-Einsatz bei einem solchen pauschalen Verbot? Selbst die Nutzung von Suchmaschinen stellt mittlerweile einen KI-Einsatz dar und Unterstützungsleistungen (Teamwork) waren auch bei bisherigen (juristischen) Hausarbeiten (bei denen hunderte Studierende den gleichen Fall ohne Aufsicht bearbeiten) mindestens geduldet, wenn nicht sogar erwünscht. Regelt man das Ob und Wie eines KI-Einsatzes für Hochschulprüfungen (für Recherchen? Brainstorming? Kritisches „Gegenlesen“ von Texten? Stilistische Verbesserungen? Erstellung von Textentwürfen, die anschließend weiterbearbeitet werden? etc) nicht genauer, ist auch die Chancengleichheit – Verfassungsgebot und elementarer Prüfungsgrundsatz – gefährdet: So werden nämlich innerhalb einer Prüfungskohorte unterschiedliche Prüfungsbedingungen schon deshalb provoziert, weil jeder die Grenzen zulässigen KI-Einsatzes mangels verbindlicher Vorgaben unterschiedlich interpretieren und für sich einhalten wird. Vor allem aber fordert der Parlamentsvorbehalt im Sinne der Wesentlichkeitsrechtsprechung des BVerfG, dass wesentliche Entscheidungen bzw. Weichenstellungen im grundrechtssensiblen Bereich durch den Gesetzgeber (und nicht durch einzelne Prüfer oder Prüfungsämter) vorzunehmen sind.

Vorliegend ist neben Art. 3 Abs. 1 GG vor allem Art. 12 Abs. 1 GG betroffen, wie auch die durch das VG Kassel bestätigte Exmatrikulation zeigt. Wenn aber kein KI-Verbot mit Erlaubnisvorbehalt besteht, ist der Einsatz von (generativer) KI im Hochschulkontext grundrechtlich geschützt. Solange jedenfalls, wie eine eigenständige Prüfungsleistung erbracht wird. Was eine eigenständige Prüfungsleistung ist, muss im Zeitalter der Co-Kreation

von KI-Systemen und Menschen neu justiert werden. Dass eine solche nicht vorliegt, wenn Studierende die Prüfungsaufgabe zum Prompt machen und das Ergebnis (weitgehend) eins zu eins als „eigene“ Prüfungsleistung einreichen, versteht sich von selbst.

Generative KI fungiert aber keineswegs nur als „Ghostwriter“, sondern ist zugleich Assistenzsystem, Coach, Recherche-Tool, Datenbank und Sparrings-Partner. Dass etwa das VG Kassel auch hier Rechtsunsicherheit schafft, sieht man am zweiten Leitsatz des Urteils: „Der Einsatz generativer KI in einer Hausarbeit über die bloße Rechtschreibkontrolle hinaus stellt eine nicht mehr eigenständige Anfertigung dar.“ Damit legt das Gericht einen „Eigenständigkeitsbegriff“ zugrunde, der nicht nur nicht zeitgemäß ist, sondern der Eigenständigkeit im prüfungsrechtlichen Sinne überhaupt nicht gerecht wird. Überhaupt hat man den Eindruck, dass die Rechtsprechung nur vom (unerwünschten) Ergebnis her denkt, demgegenüber aber das Prozesshafte im co-kreativen Erkenntnisprozess übersieht.

Dass insoweit Prüfungsformate und konkrete Aufgabenstellungen modifiziert werden müssen, ist logische Konsequenz einer veränderten digitalen Realität, im Berufsleben und eben vorangeschaltet im Studium. Pointiert formuliert: Sollte es tatsächlich gelingen, eine „Musterlösung“ durch ein oder zwei Prompts zu generieren, müssen sich die Prüfenden fragen, ob ihre Aufgabe richtig gestellt ist. KI-Kompetenz ist nicht nur auf Seiten der Studierenden, sondern auch auf Seiten der Prüfenden erforderlich.

Ganz nebenbei: Die „Grundsätze guter wissenschaftlicher Praxis“, auf die sich insbesondere das VG München und das VG Kassel berufen, taugen nicht als „Rechtsgrundlage“. Dass solche im KI-Kontext (noch) nicht existieren, zeigt gerade der Reformprozess der HRK, der am 28.5.2026 angestoßen wurde.

Es ist in der Tat überfällig, dass sich Expertinnen und Experten um die Gestaltung und Ausdifferenzierung bemühen. Das wiederum muss dann aber Vorlage für normative Anpassungen in den Hochschulgesetzen und – fachspezifisch – in den jeweiligen Prüfungsordnungen sein. Wie so etwas detailliert aussehen kann, lässt sich in einem Rechtsgutachten nachlesen, das im Auftrag des Bundesbildungsministeriums erstellt und im Mai 2026 veröffentlicht wurde (Heckmann/Paschke/Rachut, Künstliche Intelligenz in der beruflichen Bildung, abrufbar unter: <https://doi.org/10.24355/dbbs.084-202604280915-0>).

Die Lösungen liegen damit weitgehend schon vor. Man muss sie nur umsetzen und mit Leben füllen.

Braunschweig, im Juni 2026

Professorin Dr. Anne Paschke

ist Professorin für Öffentliches Recht, Technikrecht und Recht der Digitalisierung sowie Direktorin des Instituts für Rechtswissenschaften, Leiterin der Forschungsstelle Mobilitätsrecht und Leiterin des Digital Innovation and Transformation Law Hubs (DigITL Hub) an der TU Braunschweig und Mitherausgeberin der MMR.

VALERIE SCHNEIDER / ANNA CARDILLO

White-Label-Modelle im digitalen Umfeld: Strategische Risiko- und Vertragsanalyse

White-Labeling vor dem Hintergrund des Cyber Resilience Act

Haftungsfragen

Der Cyber Resilience Act (CRA) macht White-Labeling zu einer strategischen Compliance-Frage, indem er die Herstellerepflichten primär an das Inverkehrbringen unter eigener Marke knüpft. White-Label-Anbieter werden dadurch regelmäßig zum Hersteller im Rechtssinn und tragen die Pflichten nach Art. 10 ff. CRA, obwohl die technische Kontrolle häufig beim Produzenten liegt. Diese Asymmetrie erfordert eine systemati-

sche Due Diligence sowie vertragliche Mechanismen zu Dokumentationsbereitstellung, Update- bzw. Sicherheitszusagen und behördlicher Mitwirkung. White-Label-Modelle bleiben damit wirtschaftlich nur tragfähig, wenn sie in eine belastbare Risiko- und Vertragsstrategie eingebettet werden.

Lesedauer: 20 Minuten

I. White-Label-Produkte im digitalen Umfeld

White-Label-Produkte sind ein fester Bestandteil des europäischen Digitalmarkts.¹ Sie ermöglichen Unternehmen ohne eigene Entwicklungsressourcen, marktfähige Produkte anzubieten und vorhandene Technologien unter eigener Marke zu vertreiben. In der Praxis wirft dieses Geschäftsmodell jedoch Verantwortlichkeits- und Haftungsfragen auf.

Diese Fragen stellen sich auch im Zusammenhang mit dem Cyber Resilience Act (CRA). Mit dem CRA verfolgt die EU das Ziel, einheitliche Mindeststandards der Cybersicherheit für alle Produkte mit digitalen Elementen zu schaffen.² Künftig gelten damit umfangreiche Anforderungen an die Sicherheit von Produkten mit digitalen Elementen über den gesamten Lebenszyklus hinweg. Damit verknüpft ist die zentrale Frage der Verantwortlichkeit: Wer trägt die Verantwortung für die Einhaltung welcher Pflichten?

Im White-Label-Kontext stellt sich diese Frage ganz besonders. Denn während die technische Entwicklung und Produktion häufig durch Dritte erfolgt, übernehmen die vermarktenden Unternehmen vor allem Branding, Vertrieb und Kundenbeziehung und treten damit dem Kunden gegenüber auf.³

1. Was sind White-Label-Produkte?

Unter White-Labeling versteht man den Vertrieb eines fremden Produkts oder einer Dienstleistung unter eigener Marke.⁴ Charakteristisch ist, dass Produktion und Markenauftritt getrennt voneinander sind.⁵ Auch wenn die Vorteile des White-Labeling zahlreich sind, stehen dagegen auf der anderen Seite insbesondere der mangelnde Einfluss und die mangelnde Transparenz iRd Herstellungsprozesses für den Anbieter.⁶

Dies wird noch einmal verstärkt, wenn die Produktion von White-Label-Produkten international erfolgt. Insbesondere auf-

grund von kostengünstigeren Produktions- und Entwicklungsstrukturen in Ländern außerhalb der EU entscheiden sich viele Produzenten, ihre Produktion in Drittländer zu verlegen.⁷ IdR geschieht die Vermarktung an den Endkunden durch den Anbieter dann jedoch innerhalb der EU.

Dies wirft Compliance-Fragen auf, insbesondere so bald regulatorische Rahmenwerke wie der CRA Anwendung finden. Denn aus regulatorischer Sicht bedeutet dies, dass der ursprüngliche Produzent idR unmittelbar einem anderen Rechtsregime unterliegt als der Anbieter iRd Vermarktung. Selbst wenn der Anwendungsbereich von EU-Gesetzgebung für die Produzenten eröffnet wäre, wäre gleichzeitig die Rechtsdurchsetzung gegenüber solchen Produzenten deutlich erschwert. Es stellt sich daher die Frage, welche Pflichten aus dem CRA auf die jeweiligen Akteure Anwendung finden.

2. Anwendungsbereich des CRA

Der Anwendungsbereich des CRA erstreckt sich zunächst auf sämtliche Produkte mit digitalen Elementen, die im Unionsmarkt bereitgestellt werden, unabhängig davon, wo sie hergestellt wurden (Art. 2 Abs. 2 CRA). Maßgeblich ist allein, wer im Binnenmarkt als verantwortlicher Akteur auftritt und welche Rolle ihm nach der Verordnung zukommt. Der CRA sieht insofern verschiedene Rollen für alle Wirtschaftsakteure in der Lieferkette vor. Dazu zählen Hersteller, Importeure, Händler sowie ggf. Bevollmächtigte, die an der Bereitstellung digitaler Produkte beteiligt sind.⁸

II. Rollen der Beteiligten im White-Label-Kontext

Gem. Art. 3 Nr. 13 CRA bezeichnet der Begriff „Hersteller“ eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder die Produkte mit digitalen Elementen konzipiert, entwickelt oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet, sei es gegen Bezahlung, zur Monetarisierung oder unentgeltlich. Da der Anbieter ein Produkt konzipieren, entwickeln oder herstellen lässt und es unter der eigenen Marke vermarktet, ist er Hersteller iSd CRA.

Es stellt sich jedoch die Frage, ob auch der Produzent Hersteller iSd Verordnung ist. Festzuhalten ist, dass der technische Produzent jedenfalls das Merkmal der „Entwicklung oder Herstellung“ erfüllt. Daher ist entscheidend, ob das Merkmal der Ver-

¹ Grabowski, Journal of Risk and Financial Management, 21.06.2021, Legal Aspects of „White-Label“ Banking in the European, Polish and German Law.

² Heckmann/Paschke, CRA/Heckmann/Ziegler, 2025, Art. 1 Rn. 10.

³ <https://fastercapital.com/content/Brand-Identity--Maintaining-Brand-Identity-Within-the-OEM-Framework.html?>

⁴ <https://de.squarespace.com/blog/was-ist-white-labeling>.

⁵ Auer-Reinsdorff/Conrad, Hdb. IT- und Datenschutzrecht/Kast, § 15 Rn. 163.

⁶ Montecchi, International Journal of Production Economics, Volume 238, August 2021, 108152, Supply chain transparency: A bibliometric review and research agenda.

⁷ Weigel/Rücker, Praxisguide Strategischer Einkauf, 3. Aufl. 2025, Vorwort.

⁸ Teichmann NJW 2025, 2577 Rn. 5.

marktung unter eigenem Namen nur die zweite Alternative oder beide Herstellungsvarianten erfasst. Bietet der Produzent das Produkt selbst unter eigener Marke im Binnenmarkt an, ist die Zuordnung eindeutig: Neben dem Anbieter gilt auch der Produzent als Hersteller iSd Verordnung, sodass zwei Hersteller nebeneinander bestehen.

Es lässt sich dem CRA nicht entnehmen, dass eine solche Konstellation nicht möglich ist. Daher sind die Herstellerpflichten in dieser Konstellation von beiden Akteuren getrennt zu erfüllen. Wie dies bei bereits CE-zertifizierten Produkten umzusetzen ist, bleibt abzuwarten; zu erwarten ist, dass dies der Produzent als erster Hersteller in der Lieferkette sicherstellt.

Problematischer wird die Konstellation jedoch dann, wenn das Produkt erstmalig durch den Anbieter auf dem EU-Markt angeboten wird. Dann stellt sich die Frage, ob die bloße technische Entwicklung oder Herstellung ohne anschließende Vermarktung im eigenen Namen bereits zur Herstellerstellung führt oder ob das Inverkehrbringen unter eigener Kennzeichnung stets notwendige Voraussetzung für die Herstellereigenschaft ist. Der Wortlaut lässt beide Alternativen zu.

Die Tatbestandsalternativen sind durch „oder“ voneinander getrennt, während der Zusatz der notwendigen Markenanbringung mit einem „und“ angefügt ist.

Für den CRA ergibt sich jedoch eine Parallele zum europäischen Produktsicherheitsrecht.⁹ Auch hier wird u.a. in Art. 3 Abs. 8 VO (EU) 2023/988 der Begriff des Herstellers verwendet und auf die Markenanbringung Bezug genommen. Der „Blue Guide“ stellt insofern klar, dass die Herstellerpflichten nicht an die bloße technische Fertigung, sondern auch an den Markenauftritt angeknüpft sind – auch bei eigener Herstellung.¹⁰

Hersteller im Rechtssinn ist danach derjenige, der ein Produkt unter eigenem Namen oder eigener Marke im Binnenmarkt in Verkehr bringt. Der bloße Produzent bleibt dagegen „unsichtbar“ und trägt keine Herstellerpflichten. Übertragen auf White-Labeling wäre damit der Produzent in dieser Auslegung auch nach dem CRA kein Hersteller.

Auch Sinn und Zweck der Norm stützen diese Auslegung. Der CRA zielt darauf ab, die Widerstandsfähigkeit gegenüber Cyberangriffen in der EU zu stärken und zu gewährleisten, sodass Bürger und Unternehmen von vertrauenswürdigen und zuverlässigen digitalen Diensten profitieren können.¹¹

Zur Umsetzung genügt dabei ein einziger greifbarer Normadressat innerhalb der Union. Die Beschränkung der Markenanbringung auf die zweite Alternative würde jeden Produzenten zum Hersteller machen, selbst ohne EU-Marktauftritt.

Dies ließe die EU-Kontrollzuständigkeit mangels Greifbarkeit ausländischer Produzenten ins Leere laufen, wofür kein Regelungsbedürfnis besteht. Teleologisch ist daher eine enge Anknüpfung an den Vertrieb unter eigener Kennzeichnung geboten. Ließe man den reinen Herstellungsakt genügen, würde zudem die Alternative des Herstellenlassens sinnentleert. Die Pflichten (zB CE-Kennzeichnung) lägen bereits beim Produzenten, sodass für den Anbieter kein Raum zur Pflichterfüllung mehr bliebe.

Die besseren Argumente sprechen daher dafür, die Herstellerstellung an den Vertrieb unter eigener Marke zu knüpfen.¹² Maßgeblich ist nicht die technische Gestaltungsmacht, sondern die rechtliche und wirtschaftliche Verantwortung für das Produkt, die sich durch das Auftreten unter eigener Marke manifestiert.

III. Folge: Asymmetrie zwischen Verantwortung und Kontrolle

Die o.g. Konstellation führt zu einer Asymmetrie zwischen rechtlicher Verantwortung und faktischer Kontrolle: Während der White-Label-Anbieter in beiden dargestellten Konstellationen in die vollen Pflichten des Herstellers nach dem CRA eintritt, hat er idR begrenzte Einflussmöglichkeiten auf die zugrunde liegende Technik. Der Produzent ist zumindest dann, wenn er nicht unter der eigenen Marke auftritt, der unmittelbaren Anwendung der Verordnung entzogen, hat aber auf der anderen Seite den Herstellungsprozess unter seiner Kontrolle. Der White-Label-Anbieter trägt damit die Verantwortung, obwohl er in zentralen sicherheitsrelevanten Fragen von seinem Produzenten abhängig ist.

IV. Lösungsvorschläge für Einhaltung der Herstellerpflichten

Die wesentlichen Schwierigkeiten, die dabei auftreten können, sollen im Folgenden anhand von beispielhaften Pflichten des Herstellers dargelegt werden und es sollen mögliche Lösungsansätze aufgezeigt werden.

1. Sicherheitsanforderungen an Produkte

Gem. Art. 13 Abs. 1 CRA iVm Anhang 1 Teil 1 Abs. 1 CRA müssen Hersteller u.a. gewährleisten, dass Produkte mit digitalen Elementen so konzipiert, entwickelt und hergestellt werden, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten. Der Anbieter kann die Umsetzung dieser Anforderungen allerdings nur schwer sicherstellen oder überprüfen, denn die faktische Umsetzung liegt beim Produzenten. Selbst wenn der Anbieter konkrete Vorgaben macht, drohen Beweisprobleme bei Marktaufsichtsprüfungen, wenn keine vollständige Dokumentation zur Umsetzung vorliegt. Um dem entgegenzuwirken, ist dem Anbieter zu empfehlen, sich vom Produzenten vertraglich zusichern zu lassen, dass die Produkte konform zum CRA konzipiert, entwickelt und hergestellt wurden und dass entsprechende technische Nachweise sowie Sicherheitskonzepte vorgelegt werden. Ferner sollte der Anbieter eine Unterstützungspflicht des Produzenten im Falle von Überprüfungen vereinbaren, damit er sicherstellen kann, dass er allen Anforderungen gerecht wird. Ferner empfiehlt sich auch eine Nachbesserungspflicht, wenn eine Marktaufsichtsbehörde zu dem Ergebnis kommt, dass die zur Verfügung gestellte Dokumentation nicht genügt.

2. Konformitätsbewertung und CE-Kennzeichnung

Art. 13 Abs. 12 und 32 CRA sehen ein Konformitätsbewertungsverfahren vor, das in die EU-Konformitätserklärung (Art. 13 Abs. 12 und 28 CRA) und die CE-Kennzeichnung (Art. 13 Abs. 12 und 29 CRA, Art. 30 Abs. 1 VO (EG) 765/2008) mündet. Mit der CE-Kennzeichnung übernimmt der Anbieter die Verantwortung für die Übereinstimmung mit den einschlägigen Vorschriften.¹³ Hierfür ist er abermals vollständig auf technische Nachweise des Produzenten angewiesen. Bleiben diese unvollständig, kann dies zu einem Marktausschluss führen, da die CE-Konformität nicht nachweisbar ist. Obgleich der Anbieter

⁹ Teichmann CCZ 2025, 165 Rn. 166.

¹⁰ Bekanntmachung der Kommission, Leitfaden für die Umsetzung der Produktvorschriften der EU 2022 („Blue Guide“), Ziff. 3.1.

¹¹ PM des Europäischen Parlaments v. 1.12.2023, CRA: Agreement with Council to boost digital products' security, abrufbar unter: <https://www.europarl.europa.eu/news/en/press-room/20231106IPR09007/cyber-resilience-act-agreement-with-council-to-boost-digital-products-security>.

¹² So auch Albrecht GWR 2022, 313, Rn. 313.

¹³ Martinek/Semler/Flohr, Hdb. des Vertriebsrechts/Hess, § 11 Rn. 87.

die Konformitätsbewertung auf einen Dritten – zB auch auf den Produzenten – auslagern kann¹⁴, bleibt er der Verantwortliche im Rechtsinne, vgl. Art. 30 Abs. 1 VO (EG) 765/2008. Eine vertragliche Vereinbarung kann die Eintrittspflicht nach außen damit nicht beeinflussen. Empfehlenswert ist daher die Konformität mit dem CRA vertraglich ausdrücklich als Beschaffenheit zu vereinbaren.

3. Technische Dokumentation

Art. 13 Abs. 12 CRA iVm Art. 31 CRA verpflichtet den Hersteller ferner, umfassende technische Unterlagen über Entwicklung, Herstellung und Sicherheitsarchitektur zu erstellen und vorzuhalten. Eine solche technische Dokumentation kann faktisch nur beim Produzenten entstehen. Da dem Anbieter ohne vertragliche Grundlage der Zugriff fehlt und bei Mängeln Maßnahmen der Marktaufsichtsbehörden drohen (Art. 58 Abs. 1 lit. f, Abs. 2 CRA), sind Vereinbarungen zur Erstellung, Bereitstellung, Richtigkeit, Vollständigkeit und zur laufenden Aktualisierung essenziell. Es empfiehlt sich, zugleich die Sprache der Dokumentation frühzeitig festzulegen, um die Vorgaben des Art. 31 Abs. 4 CRA zu erfüllen, wonach technische Dokumentation und Korrespondenz in einer Amtssprache des Mitgliedstaats der notifizierten Stelle oder in einer von dieser zugelassenen Sprache abzufassen sind.

4. Update- und Wartungspflichten

Nach Art. 13 Abs. 8 CRA haben Hersteller, die ein Produkt mit digitalen Elementen in den Verkehr bringen, zu diesem Zeitpunkt und während der erwarteten Produktlebensdauer und des Unterstützungszeitraums sicherzustellen, dass Schwachstellen des Produkts einschließlich seiner Komponenten wirksam und im Einklang mit den grundlegenden Cybersicherheitsanforderungen des Anhang I Teil I CRA behandelt werden. Zudem müssen sie gem. Art. 13 Abs. 2 CRA iVm Anhang 1 Teil 1 Abs. 2 lit. c CRA sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, ggf. auch durch automatische Aktualisierungen. Mit anderen Worten: Der Hersteller hat für Updates und Wartungen zu sorgen. Updates liegen allerdings allein im Machtbereich des Produzenten, denn er allein hat Zugriff auf die notwendigen Informationen und Daten. Liefert dieser verspätet oder gar nicht, trifft dies hauptsächlich den Anbieter in seiner Stellung als Hersteller. Dies kann zu Verzögerungen und Rückrufaktionen führen (Art. 54 Abs. 1 CRA), die hohe Kosten und erhebliche Reputationsschäden nach sich ziehen. Zur vertraglichen Weitergabe der Verpflichtungen bieten sich insbesondere sog. Service Level Agreements (SLA) mit Update-Zyklen, Patch-Fristen und Reaktionszeiten an. Bei der Definition des Sicherheitsstandards sollte sich an gängigen Modellen wie ISO/IEC 27001 orientiert werden.¹⁵

Fraglich ist, wie vorgegangen werden kann, wenn der Produzent verspätet oder gar nicht liefert. Denkbar wäre – je nach konkretem Fall – die Zahlungen an den Produzenten in Stufen zu vereinbaren und einen Teil der Zahlung erst nach Ablauf der Lebensdauer des Produkts freizugeben. Da dies allerdings eine enorme Verzögerung der Gegenleistung mit sich bringen würde, ist damit zu rechnen, dass Produzenten dies in die Berechnung des Grundpreises mit einrechnen und dadurch eine erheb-

liche Steigerung der Gesamtkosten entsteht. Auch führt dies zu einer Unsicherheit auf Seiten des Produzenten, da für ihn wiederum die Gefahr besteht, dass die Zahlung am Ende der Leistungszeit nicht erfolgt. Um dem vorzubeugen könnte zB mit Treuhandkonten gearbeitet werden, wobei ein Dritter über die Freigabe der Mittel entscheidet.¹⁶ Alternativ könnte ein Software-Escrow-Modell angedacht werden, wobei der Code hinterlegt wird, sodass der Anbieter im Bedarfsfall darauf zugreifen und damit ggf. selbst in diese Pflichten eintreten kann. Faktisch wird das für den Anbieter idR wenig attraktiv sein, da er allein durch den Code nicht das praktische Wissen erlangt, das erforderlich ist, um seinen Pflichten nachzukommen. Als letztes Mittel – bevor ihm nicht nur ein Rückruf, sondern potenziell noch viel schlimmer der Reputationsschaden droht – kann es aber ein geeignetes Instrument sein.

5. Meldepflichten bei Schwachstellen und Sicherheitsvorfällen

Nach Art. 10 Abs. 11 und 11 CRA muss der Hersteller neue Schwachstellen überwachen und innerhalb von 24 Stunden an die Agentur der EU für Cybersicherheit (ENISA) und an die jeweiligen nationalen Computer Security Incident Response Teams (CSIRT)¹⁷ melden. IdR kann der Anbieter als Markenanbieter diese Überwachung nicht selbst leisten. Er ist darauf angewiesen, dass der Produzent ihn rechtzeitig und vollständig informiert. Bleibt diese Kommunikation aus, riskiert der Anbieter als Markenanbieter Bußgelder und Vertrauensverluste bei Kunden, da Sicherheitsvorfälle nicht ordnungsgemäß gemeldet werden. Auch in diesem Zusammenhang empfiehlt sich, vertraglich Fristen zu bestimmen, innerhalb derer der Anbieter über die Schwachstellen zu informieren ist, sowie Unterstützungs-, Update- und Berichtspflichten in Bezug auf die Behebung dieser Schwachstellen und die Zusammenarbeit mit den Überwachungsbehörden.

6. Risikomanagement und Prozesse

Art. 13 Abs. 2–3 CRA iVm Art. 32 CRA fordert die Implementierung eines kontinuierlichen Risikomanagements. IdR kann der Hersteller diese Bewertung selbst durchführen (s. Art. 32 Abs. 1 lit. a CRA). Für bestimmte Produkte ist jedoch eine Fremdbewertung gem. Art. 32 Abs. 1 lit. b, lit. c, Abs. 4 CRA vorgeschrieben. Trotz des erheblichen Aufwands, der durch die kontinuierlichen Aktualisierungspflichten besteht, schafft die Bewertung ein Bewusstsein für alle potenziellen Risiken und bildet die Grundlage für die Auswahl geeigneter Cybersicherheitsmaßnahmen.¹⁸ Art. 13 Abs. 1 CRA, Anhang 1 Teil 2 Abs. 1 CRA fordert zudem die Erstellung einer sog. Software Bill of Materials (SBOM), die in die technische Dokumentation eingefügt werden muss. Risikobewertung und SBOM können regelmäßig nur vom Produzenten bereitgestellt werden, da er die verwendeten Softwarekomponenten kennt.

Auch diesbezüglich sollten vertragliche Regelungen getroffen werden. Theoretisch kommen Treuhand- oder Hinterlegungslösungen in Betracht, sie erweisen sich jedoch als kaum praktikabel, da die SBOM nach dem CRA fortlaufend zu aktualisieren ist. Die Erstellung und Pflege ist kein abgeschlossener Vorgang, sondern ein kontinuierlicher Prozess über die gesamte Produktlebensdauer. Eine an die Erfüllung geknüpfte Zahlung würde daher praktisch bedeuten, dass Mittel über Jahre blockiert blieben, ohne dass ein klarer Erledigungspunkt erreicht wird. Treuhandkonten könnten hingegen genutzt werden, um ggf. etwaige Zahlungen erst nach Erfüllung der Pflichten freizugeben. Da die SBOM laufend zu aktualisieren ist, wäre dies dann allerdings erst nach Erlöschen der Pflichten denkbar und damit ein längerer Zeitraum, wodurch die o.g. Nachteile (insbesondere erhöhte Kosten) abermals zu erwarten sind.

¹⁴ Hornung/Schallbruch, IT-Sicherheitsrecht/Skierka-Canton, § 8 Rn. 12.

¹⁵ Nordmann LTZ, 2025, 278 Rn. 279.

¹⁶ Buchheim/Möslein/Omlor, Datentreuhand und Recht, 1. Aufl. 2025, § 5 Rn. 19.

¹⁷ <https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map>.

¹⁸ Zirnstein CRI 2024, 66.

7. Transparenzpflichten gegenüber Endnutzern

Hersteller müssen nach Art. 13 Abs. 17–18 CRA, Anhang II CRA Endnutzern Informationen u.a. zu sicherer Konfiguration, Updates, Funktionen und Eigenschaften, Lebensdauer und Art und Dauer des technischen Cybersicherheitsupports bereitstellen. Endkunden sollen so cybersicherheitsrelevante Eigenschaften bei der Auswahl und Nutzung stärker berücksichtigen können.¹⁹ Die Angaben sind meist nur in Zusammenarbeit mit dem Produzenten möglich – insbesondere in Bezug auf die Angaben in Anhang II Nr. 8 und Nr. 9 CRA. Fehlerhafte oder unvollständige Informationen führen zu Haftungsrisiken und können das Vertrauen der Endkunden nachhaltig schädigen. Ein Sicherheitsvorfall aufgrund mangelnder Transparenz kann massive Reputationsverluste nach sich ziehen. Es empfiehlt sich abermals, vertragliche Ansprüche auf diese Informationen zu implementieren.

8. Aufbewahrungs- und Nachweispflichten

Der CRA verpflichtet Hersteller, u.a. in Art. 13 Abs. 10, Abs. 13 und Abs. 18 CRA, die erstellte Dokumentation sowie weitere Informationen, wie die Konformitätserklärung und technische Dokumentation zehn Jahre lang bereitzuhalten. Soweit der Anbieter diese Dokumente nicht selbst verwaltet, kann er bei Insolvenz oder Unerreichbarkeit des Produzenten in Nachweisnot geraten. Es empfiehlt sich also stets eine Kopie der erstellten Dokumentation vertraglich zusichern zu lassen. Berechtigten Geheimhaltungsinteressen des Produzenten kann mit einem Escrow-Set-Update begegnet werden, bei dem die Dokumentation nur bei Unerreichbarkeit oder Insolvenz des Produzenten herausgegeben wird.

9. Haftungs- und Sanktionsrisiken

Verstöße gegen den CRA können erhebliche Rechtsfolgen nach sich ziehen. Dies beinhaltet Bußgelder bis zu 15 Mio. EUR oder 2,5% des weltweiten Jahresumsatzes (Art. 64 Abs. 2 CRA), Produktrücknahmen, Rückrufe oder Verkaufsverbote (Art. 45 CRA). Hinzu tritt die zivilrechtliche Produkthaftung bei Schäden durch Sicherheitslücken. Diese Risiken treffen den Anbieter unmittelbar, auch wenn Pflichtverletzungen auf den Produzenten zurückgehen. Eine vertragliche Absicherung bindet nur im Innenverhältnis. Die vertragliche Abwälzung eines Bußgelds auf Dritte könnte zudem den Abschreckungszweck unterlaufen und daher als unzulässige Umgehung nach § 134 BGB oder § 138 BGB gewertet werden.²⁰ Die Zulässigkeit solcher Gestaltungen ist höchststrichterlich bislang ungeklärt; der BGH hat die Frage im Zusammenhang mit Kartellbußgeldern allerdings dem EuGH vorgelegt.²¹ Eine Schuldübernahme nach § 415 BGB scheidet mangels Zustimmung der Bußgeldbehörde aus. Auch ist für den Produzenten zu beachten, dass Versicherungen idR keine Deckung bieten für vertragliche Ansprüche.²²

10. Zwischenfazit

Der CRA erzeugt im White-Label-Bereich eine strukturelle Verantwortungsverschiebung. Der Anbieter trägt als Hersteller die vollen Pflichten aus dem CRA, obwohl er weder die technische Gestaltungsmacht noch die notwendigen Einblicke in die Sicherheitsarchitektur hat. Diese Asymmetrie birgt erhebliche Haftungs- und Marktfolgen. Für White-Label-Anbieter ist es daher unerlässlich, insbesondere durch vertragliche Absicherungen die Lücke zwischen formaler Herstellerpflicht und tatsächlicher Einflussmöglichkeit zu schließen. Nur so lässt sich vermeiden, dass sie trotz fehlender Kontrolle die gesamte Last von Sanktionen, Rückrufen und Reputationschäden allein tragen. Vertragliche Klauseln müssen sich insbesondere an der Bestimmtheit gem. § 307 Abs. 1 BGB messen. Es reicht – insbesondere im internationalen Kontext – nicht aus,

dem Produzenten pauschal alle Pflichten aus dem CRA aufzuerlegen.

V. Durchsetzbarkeit von Ansprüchen

Gerade wenn der Produzent außerhalb der EU ansässig ist, ergeben sich erhebliche Herausforderungen für die Durchsetzung vertraglicher Ansprüche und Haftungsregelungen. Neben den vertraglichen Regelungen ist daher sicherzustellen, dass diese auch durchsetzbar sind. Nachfolgend werden verschiedene Instrumente dargestellt, mit denen der Anbieter seine Position gegenüber dem Produzenten – insbesondere im internationalen Kontext – stärken kann.

1. Rechtswahl- und Gerichtsstandsklauseln

Da der CRA europarechtlich gilt, während der Produzent häufig außerhalb der EU sitzt, ist eine klare Rechtswahl wichtig. Der Hersteller sollte ausdrücklich die Anwendung europäischen bzw. deutschen Rechts vereinbaren, um auf vertraute Haftungsmaßstäbe, Vertragsauslegung und Beweisregeln zurückgreifen zu können.²³ Gleichzeitig sollte eine Gerichtsstandsklausel iSd § 38 ZPO in den Vertrag eingefügt werden, die idealerweise die ausschließliche Zuständigkeit eines Gerichts am Sitz des Anbieters definiert. Dadurch kann sichergestellt werden, dass Streitigkeiten nach einem vertrauten prozessualen Rahmen entschieden werden.

2. Versicherungspflicht des Produzenten und Abtretungsansprüche

Ein wesentliches Sicherungsinstrument kann in der vertraglichen Pflicht des Produzenten bestehen, die wesentlichen Risiken durch eine entsprechende Versicherung abzusichern, um Leistungsfähigkeit und Liquidität sicherzustellen.²⁴ Bei internationaler Tätigkeit ist zu beachten, dass die Versicherung eine internationale Deckung hat – insbesondere für die EU. Die Versicherung sollte nicht nur Personenschäden, sondern ausdrücklich auch Vermögensschäden infolge von Cybersicherheitsverstößen abdecken. Ergänzend empfiehlt sich ein Nachweis- und Abtretungsanspruch, der den Produzenten zur Vorlage von Versicherungspolice und Zahlungsbelegen verpflichtet und dem Anbieter im Schadensfall den direkten Zugriff auf die Versicherungsleistung ermöglicht, falls der Produzent insolvent oder in einem Drittstaat nicht greifbar ist.

3. Prüfung internationaler Anerkennungs- und Vollstreckungsabkommen

Vertragliche Regelungen reichen nicht aus, wenn gerichtliche Entscheidungen praktisch nicht durchsetzbar sind. Daher sollte vor Vertragsschluss geprüft werden, ob Anerkennungs- und Vollstreckungsabkommen zwischen dem Sitzstaat des Produzenten und der EU bzw. dem Sitzstaat des Anbieters bestehen. Fehlen solche Abkommen, ist die Durchsetzung oft nur über ein erneutes Verfahren im Drittstaat möglich. Zweckmäßig ist zudem die vertragliche Vereinbarung einer Erstattungspflicht für Vollstreckungs-, Anwalts- und Übersetzungskosten, um den wirtschaftlichen Druck auf den Produzenten zu erhöhen. Auch wenn dies weitestgehend idR auch gesetzlich der Fall ist, erhöht dies in der Praxis den ökonomischen Druck auf den Produzenten, sich an die vereinbarten Pflichten zu halten.

¹⁹ Heckmann/Paschke, CRA/Paschke, 1. Aufl. 2025, Art. 13 Rn. 54.

²⁰ Grunewald, NZG 2016, 1121 Rn. 1122.

²¹ BGH Beschl. v. 11.2.2025 – KZR 74/23.

²² <https://www.gdv.de/resource/blob/6132/6a2283f21432edcdf9291a53e9967fd0/01-allgemeine-versicherungsbedingungen-fuer-die-haftpflichtversicherung--ahb--data.pdf>, Ziff. 7.3.

²³ Auer-Reinsdorff/Conrad, Hdb IT- und Datenschutzrecht, 3. Aufl. 2019, Rn. 70–72.

²⁴ Förster MMR 2024, 4 Rn. 13.

4. Internationale Schiedsgerichtsklausel

Besteht kein Anerkennungs- und Vollstreckungsabkommen, empfiehlt sich die Vereinbarung einer internationalen Schiedsgerichtsklausel. Schiedsurteile sind nach dem New-York-Übereinkommen von 1958 in über 170 Staaten anerkannt und vollstreckbar. Empfehlenswert ist die Vereinbarung einer institutionalisierten Schiedsgerichtsbarkeit, etwa nach den Regeln der International Chamber of Commerce (ICC) mit klarer Festlegung von Schiedsort, anwendbarem materiellen Recht und Verfahrenssprache.²⁵

5. Lokale Bevollmächtigte und Zustellungsfähigkeit

Für Konstellationen mit Produzenten außerhalb der EU sollte vertraglich festgeschrieben werden, dass dieser einen zustellungsfähigen Vertreter innerhalb der EU benennt. Dies erleichtert die Zustellung von Schriftstücken, Vollstreckungsmaßnahmen und die Kommunikation mit Behörden erheblich. Zudem kann der Bevollmächtigte als Ansprechpartner für technische oder sicherheitsrelevante Rückfragen dienen.

6. Vertragsstrafen und pauschalisierte Schadensersatzansprüche

Zur Abschreckung dient die Aufnahme von Vertragsstrafen und pauschalisierten Schadensersatzansprüchen der erleichterten Kompensation bei Vertragsverletzungen, ohne dass der Hersteller einen konkreten Schaden nachweisen muss. Den Parteien sollte es jedoch freigestellt werden, einen höheren oder niedrigeren Schaden nachzuweisen. Der Vorteil liegt in der Erleichterung der Durchsetzbarkeit und in der Abschreckung.

7. Lieferstoppklauseln

Ökonomischen Druck kann der Anbieter auch über Lieferstoppklauseln erzeugen, die ihm ermöglichen, bei Verstößen gegen Sicherheitsanforderungen oder mangelhafter Dokumentation die Abnahme zu verweigern oder die Lieferbeziehung fristlos zu beenden. Solche Klauseln wirken präventiv, weil sie unmittelbar an die wirtschaftlichen Interessen des Produzenten anknüpfen.

8. Bankgarantien und Akkreditive

Zweckmäßig können auch Bankgarantien oder Akkreditive sein, wobei die Bezahlung des Produzenten über eine Bankverbindung abgesichert wird, die nur bei Vorlage bestimmter Nachweise erfolgt – etwa einer Sicherheitszertifizierung oder Konformitätserklärung nach dem CRA. Dadurch kann der Anbieter die wirtschaftliche Erfüllung des Vertrags unabhängig von der Bonität oder Erreichbarkeit des Produzenten absichern.

VI. Fazit

Der CRA macht White-Labeling zur strategischen Compliance-Frage. Während bislang der Schwerpunkt der Verantwortung für Sicherheit und Produktkonformität faktisch eher beim technischen Hersteller lag, verschiebt der CRA die rechtliche Verantwortung auf den White-Label-Anbieter. Der Herstellerbegriff überträgt Unternehmen, die Produkte lediglich branden und vertreiben, die vollen Herstellerpflichten nach Art. 13 ff. CRA.

Der Produzent bleibt hingegen regelmäßig außerhalb des Normadressatenkreises, sofern er nicht selbst unter eigenem Namen auf dem europäischen Binnenmarkt auftritt.

Im Ergebnis zeigt sich damit, dass der CRA nicht nur technische und organisatorische Anforderungen stellt, sondern auch eine Neujustierung der Vertragsbeziehungen in internationalen Lieferketten erforderlich macht. Faktisch muss der Anbieter sicherstellen, dass der Produzent sämtliche Sicherheits- und Dokumentationspflichten einhält und ihm diejenigen Dokumentationen und Informationen zur Verfügung gestellt werden, die er selbst benötigt, um seinen Pflichten nachzukommen. Vertragliche Absicherungen – von Versicherungspflichten über Schiedsgerichtsklauseln bis hin zu Escrow-Vereinbarungen – werden daher keine bloßen juristischen Vorsichtsmaßnahmen mehr sein, sondern müssen ein integraler Bestandteil der Vertragsverhandlungen im White-Label-Kontext werden.

Für die Praxis folgt daraus: White-Labeling muss künftig nicht allein als vertriebswirtschaftliche Entscheidung verstanden werden. Unternehmen sind gut beraten, eine regulatorische Due Diligence durchzuführen, die CRA-Pflichten in einer Pflichten-Matrix aufzuteilen und konkrete Anforderungen an die Vertragspartner zu formulieren. Ergänzend zu den so oder so nach dem CRA einzuführenden Prozessen und Maßnahmen sollten Vertragsgestaltungen mit Produzenten u.a. Freistellungen, Rückversicherungspflichten, SLA-gestützte Sicherheitszusagen und Audit-Rechte enthalten.

Insgesamt zeigt sich: Der CRA schließt bewusst Lücken, die im bisherigen Produktsicherheitsrecht White-Label-Modelle privilegierten. Daraus resultiert, dass White-Labeling in Zukunft nur dann ein ökonomisch sinnvolles Modell bleibt, wenn es in eine umfassende Strategie regulatorischer Risikosteuerung eingebettet wird.

Schnell gelesen ...

- Der CRA verlagert die Herstellerverantwortung bei White-Label-Produkten systematisch auf den White-Label-Anbieter und macht diesen voll Compliance-pflichtig.
- Dadurch entsteht ein erheblicher Anpassungsbedarf in internationalen Liefer- und Vertragsbeziehungen, insbesondere hinsichtlich Informations-, Sicherheits- und Haftungsregelungen.
- White-Labeling bleibt wirtschaftlich nur tragfähig, wenn es Teil einer umfassenden regulatorischen Risikosteuerung und vertraglichen Absicherung ist.



Anna Cardillo

ist Rechtsanwältin und Gründungspartnerin der Kanzlei MYLE Rechtsanwaltsgesellschaft mbH im Berlin.



Valerie Schneider

ist Rechtsanwältin und Gründungspartnerin der Kanzlei MYLE Rechtsanwaltsgesellschaft mbH in Berlin.

²⁵ <https://www.iccgermany.de/schiedsgerichtsbarkeit/schiedsgerichtsklausel/>.

Das Schuldverhältnis bei IaaS- und PaaS-Cloud-Verträgen

Pflichtenprogramm und Leistungsstörungenrecht beim PaaS-Cloud-Vertrag im B2B-Bereich

Public-Cloud-Dienste

Trotz der durch § 548a BGB gesetzlich angeordneten Typisierung sämtlicher Public-Cloud-Verträge als Mietverträge ist eine differenzierte vertragsrechtliche Behandlung von Cloud-Verträgen in Abhängigkeit vom jeweiligen Cloud-Modell geboten. Der Beitrag untersucht den typischen Platform-as-a-Service(PaaS)-Vertrag auf der Grundlage eines Verständnisses des PaaS-Modells als Betrieb einer Applikation des Nutzers durch den Cloud-Anbieter unter Annahme und Weiterleitung von Netzwerkanfragen. Als zentrale Vertragspflichten des Cloud-Anbieters werden die Abnahme der Applikationsdefinition,

der fortlaufende Applikationsbetrieb sowie die schnelle und zuverlässige Weiterleitung sämtlicher Netzwerkaufträge herausgearbeitet. Trotz des dienst- oder werkvertraglich geprägten Leistungscharakters lässt sich das Pflichtenprogramm aus dem typischen PaaS-Vertrag gut in die mietrechtlichen Vorgaben des § 535 BGB einpassen. Auf dieser Grundlage zeigt der Beitrag, dass sich auch die typischen Leistungsstörungen des PaaS-Vertrags im Wesentlichen mit den Instrumenten des mietrechtlichen Mängelrechts sachgerecht bewältigen lassen.

Lesedauer: 18 Minuten

I. Einleitung

Seit der Einführung des § 548a BGB zum 1.1.2022 muss für sämtliche Verträge über die Nutzung von Public-Cloud-Produkten de lege lata einheitlich das Mietrecht zur Anwendung gebracht werden.¹ Über die Anordnung einer entsprechenden Geltung der Vorschriften zur Sachmiete hinaus fehlt es allerdings an einer gesetzlichen Konkretisierung des vertragstypischen Pflichtenprogramms und des Leistungsstörungenrechts für solche Verträge. In Anlehnung an die Rechtsprechung, die bereits vor Einführung des § 548a BGB mietrechtliche Vorschriften auf Softwarenutzungsverträge anwendete,² wurde in der Vergangenheit eine weitgehende vertragsrechtliche Gleichbehandlung sämtlicher Cloud-Verträge vorgeschlagen.³ Zum Pflichtenprogramm und Leistungsstörungenrecht beim Infrastructure-as-a-Service(IaaS)-Cloud-Vertrag wurde aufgezeigt,⁴ dass im Hinblick auf die drei typischen Service-Modelle des Cloud-Computing tatsächlich der Software-as-a-Service(SaaS)-Vertrag mit seiner Begründung einer direkten Pflicht zu einer abstrakt bestimmbaren Verarbeitung übergebener Nutzerdaten durch den Cloud-Anbieter wesensmäßig klassischen Softwarenutzungsverträgen entspricht. Die beiden anderen Service-Modelle IaaS und Platform-as-a-Service (PaaS) weisen erhebliche Unterschiede auf und gebieten daher trotz der notwendig mietrechtlichen Typisierung eine differenzierte vertragsrechtliche Betrachtung.

Der vorliegende Beitrag nimmt eine vertiefte Betrachtung des PaaS-Vertrags vor. Hierzu wird zunächst auf technischer Ebene eine umfassende Definition und Abgrenzung des PaaS-Servicemodells herausgearbeitet. Die hierbei zu entwickelnde Auffassung vom PaaS-Dienst als „Betrieb einer Applikation des Nutzers unter Annahme und Weiterleitung von Netzwerkaufträgen durch den Cloud-Anbieter“ bildet die Grundlage der anschließenden vertragsrechtlichen Untersuchung des typischen PaaS-Vertrags. Zunächst wird hierzu unter größtmöglicher Einpassung in die gesetzlichen Leistungspflichten der Sachmiete nach § 535 BGB das Pflichtenprogramm des PaaS-Vertrags ausgearbeitet. Anschließend erfolgt eine Untersuchung des spezifischen Leistungsstörungenrechts. Hierbei wird sich zeigen, dass Bedenken im Hinblick auf die Unterwerfung der Cloud-Verträge unter das Mietrecht⁵ jedenfalls für den PaaS-Vertrag weitgehend unbegründet sind. Die meisten Leistungsstörungen lassen sich gut durch eine entsprechende Anwendung des Mietmängelrechts behandeln. Besonderheiten des PaaS-Vertrags ohne

Entsprechung im Sachmietrecht können durch einen Rückgriff auf das allgemeine Schuldrecht eingefangen werden.

II. Definition und Abgrenzung des PaaS-Modells

Eine Definition und Abgrenzung des PaaS-Modells gegen die anderen Modelle IaaS und SaaS gestaltet sich schwierig, da die bestehenden Standardprodukte im Public-Cloud-Markt durchaus vielfältig sind und die Übergänge zwischen den Service-Modellen mitunter fließend erscheinen.⁶ Hinzu kommt, dass gerade das PaaS-Konzept insgesamt uneinheitlich verwendet wird und die genaue Definition meistens vom Zweck der jeweiligen Darstellung abhängt.⁷ Nach der hier vertretenen Auffassung lassen sich IaaS und SaaS in ihrer reinsten Form als „Extremfälle“ des Cloud-Computing betrachten: IaaS ist danach die reine Bereitstellung von IT-Ressourcen in Form einer virtuellen Maschine für den Cloud-Nutzer. SaaS ist auf der anderen Seite die Bereitstellung einer fertigen Applikation, zu deren Verwendung der Nutzer lediglich seine Eingabedaten übermitteln muss, um den gewünschten Daten-Output zu erhalten.

Es wäre allerdings nicht sachgerecht, sämtliche Zwischenformen des Cloud-Computing zwischen diesen Extremen dem PaaS-Modell zuzuordnen. Es ist jedenfalls noch von einem IaaS-Dienst auszugehen, wenn dem Cloud-Nutzer zusätzlich zur Bereitstellung einer virtuellen Maschine vom Cloud-Anbieter aktiv bedeutende Systemlogs (Logging) sowie Daten über Zustand und Performanz des Systemprozesses hinter der virtuellen Maschine (Monitoring) bereitgestellt werden. Auf der anderen Seite liegt stets noch ein SaaS-Dienst vor, wenn der Nutzer vor dem produktiven Einsatz einer Software noch bestimmte Konfigurationen für seinen speziellen Einsatzkontext vornimmt. Im PaaS-Modell liegt ein strukturell anderes Zusammenwirken von Cloud-Anbieter und Cloud-Nutzer vor. Das wesentliche Defini-

¹ Staudinger, BGB/Steinrötter, 2024, BGB § 548a Rn. 8.

² BGH MMR 2007, 243 Rn. 11 f.

³ Staudinger, BGB/Mäsch, 2025, BGB Anh. zu §§ 305–310 Rn. L50; Redeker, IT-Recht, 8. Aufl. 2023, Rn. 1278 f.; Förster MMR 2025, 19 f.

⁴ Kubis MMR 2026, 377.

⁵ Staudinger, BGB/Steinrötter, 2024, BGB § 548a Rn. 8.

⁶ Förster MMR 2025, 20.

⁷ Rehman, Cloud-Computing-Basics, 2018, S. 20 f.

tionsmerkmal von PaaS ist der Betrieb von Applikationen des Nutzers durch den Cloud-Anbieter auf dessen Infrastruktur.

Der Applikationsbegriff ist hierbei technisch zu verstehen. Ein alternatives Verständnis geht von einem funktionsbezogenen Applikationsbegriff aus. Es gibt kommerzielle Anbieter, die das „Entwickeln“ eigener Applikationen durch das Anlegen eines Datenmodells und die Definition von Relationen und Prozessroutinen zur Datenverarbeitung ermöglichen.⁸ Hierzu werden jedoch technisch gesehen lediglich Konfigurationsdaten hinterlegt, die von der Software des Anbieters bei Aufruf geladen werden, um die gewünschte Funktionalität bereitzustellen. Da hierbei technisch gesehen keine Applikation des Cloud-Nutzers ausgeführt wird, sind nach dem hier vertretenen Verständnis die entsprechenden Dienste und „Plattformen“ dem SaaS-Modell zuzuordnen. IRd PaaS-Modells ist eine echte, technische Applikation des Nutzers zu betreiben.

Der gelingende Einsatz eines PaaS-Produkts im betrieblichen Kontext hat mithin stets zur Voraussetzung, dass der Nutzer eine lauffähige und funktional korrekte Applikation selbst entwickelt oder zu seiner Verfügung anderweitig beschafft hat. Die korrekte Funktionalität in technischer und fachlicher Hinsicht liegt in der alleinigen Verantwortung des Nutzers. Der Cloud-Anbieter übernimmt und betreibt die Applikation stets in der Form und in dem Zustand, in dem sie ihm übergeben wird. Hierzu muss in die Applikation in einer ausführbaren Form vorliegen. Übergabe in diesem Sinne meint die Übermittlung der entsprechenden Daten. Dies kann grundsätzlich recht klassisch in Form einer ausführbaren Programmdatei oder einem „Programmarchiv“ erfolgen. Im Rahmen modernerer Ansätze von Containerisierung und Microservice-Cluster-Architekturen⁹ werden alternativ in der Praxis häufig lauffähige Applikationen auch durch Container-Images sowie Cluster-Definitionen übermittelt. Der Cloud-Anbieter hat iRd PaaS-Modells die Applikation des Nutzers zu betreiben. Dies bedeutet technisch gesehen zunächst die Bereitstellung physischer IT-Infrastruktur und den Betrieb einer geeigneten Laufzeitumgebung für den jeweiligen Applikationstyp. Soweit die Applikation des Nutzers technisch lauffähig ist, hat der Cloud-Anbieter ihren tatsächlichen Betrieb sicherzustellen. Er muss daher hinreichend viel Infrastruktur hierfür bereitstellen und für funktionale und performante Laufzeitumgebungen sorgen.

Applikationen iRd PaaS-Modells übernehmen typischerweise die Funktion eines Webserver. Ihr Zweck als Bestandteil eines Software-Architekturmodells besteht daher zumindest auch darin, eingehende Netzwerkaufträge anzunehmen, zu verarbeiten und zu beantworten. Ob und wie die Applikation eingehende Aufrufe bearbeitet liegt grundsätzlich im Verantwortungsbereich des Nutzers. Allerdings gehört es zum Aufgabenbereich des Cloud-Anbieters im typischen PaaS-Modell, eine Erreichbarkeit der Applikation aus dem Netzwerk (iRd dem Internet) zu garantieren sowie eingehende Aufrufe anzunehmen und an eine Instanz der laufenden Applikation weiterzuleiten. Er hat daher eine hinreichende Ressourcenausstattung sicherzustellen. In technischer Hinsicht erfordert die Annahme und Weiterleitung von Aufrufen auch in Zeiten von Lastspitzen die bedarfsgerechte Anpassung der technischen Infrastrukturleistung (Skalierung) sowie eine gleichmäßige Verteilung der Anfragen auf die verschiedenen Instanzen (Lastverteilung).

In der Praxis verbreitet ist das Angebot zusätzlicher Dienste des Cloud-Anbieters, die dem Nutzer den Einsatz seiner Applikation erleichtern. Hierzu zählen etwa die kontrollierte Ausführung von Update-Routinen ohne Ausfallzeiten beim Betrieb der Applikation sowie Logging und Monitoring des Applikationsbetriebs und ein Versionierungssystem. Solche zusätzlichen Dienstangebote sind jedoch nicht konstitutiv für das PaaS-Modell. Wesentlich ist lediglich der Betrieb einer Applikation des Nutzers durch den Cloud-Anbieter unter Annahme und Weiterleitung sämtlicher Netzwerkaufträge. Das typische Pflichtenprogramm aus dem PaaS-Cloud-Vertrag lässt sich daher allein auf die Absicherung dieses Ziels hin bestimmen.

III. Der PaaS-Cloud-Vertrag

1. Leistungspflichten der Vertragsparteien

a) Pflichten des Cloud-Anbieters

Entsprechend der hier vertretenen Definition des PaaS-Modells wird der Cloud-Anbieter aus dem PaaS-Vertrag primär verpflichtet, eine Applikation des Nutzers während eines vereinbarten Zeitraums zu betreiben und dabei alle eingehenden Aufrufe anzunehmen und weiterzuleiten. Es scheint daher primär eine Dienstleistung oder auch ein werkvertraglicher Erfolg geschuldet zu sein.¹⁰ Die gesetzlich vorgeschriebene Anwendung des Mietrechts erscheint mithin wesentlich problematischer als etwa noch beim IaaS-Vertrag, dessen Primärpflicht in Form der Bereitstellung einer virtuellen Maschine wesensmäßig noch deutlich stärker an die klassische Sachmiete erinnern dürfte.¹¹ Das primäre Pflichtenprogramm des Cloud-Betreibers aus dem PaaS-Vertrag lässt sich daher nur eingeschränkt in das System des § 535 Abs. 1 BGB einpassen. Eine strukturelle Komponente des mietrechtlichen Pflichtenprogramms lässt sich jedoch adaptieren: Wie die Pflichten des Vermieters im Hinblick auf die Sicherung eines bestimmten Zustands der Mietsache nach § 535 Abs. 1 S. 2 BGB gliedern sich auch die Leistungspflichten des Cloud-Anbieters aus dem typischen PaaS-Vertrag in initiale Pflichten zu Beginn der Vertragslaufzeit und Dauerpflichten während der gesamten Vertragsdauer.

Statt mit „Überlassung“ iSd § 535 Abs. 1 S. 1 BGB ist wohl im Grunde der geschuldete Leistungsgegenstand wie schon beim IaaS-Vertrag am besten als „Bereitstellung“ (vgl. § 327 Abs. 1 BGB) zu bezeichnen. Die initiale Leistungspflicht ist jedoch mit der Bereitstellung der Applikation für den Netzwerkzugriff zum vereinbarten Anfangszeitpunkt unvollständig beschrieben. Schon denklogisch kann dieser Leistungspflicht nur entsprochen werden, wenn der Cloud-Anbieter zuvor rechtzeitig ein Datenpaket mit der vollständigen Applikationsdefinition vom Nutzer übernommen hat. Die Abnahme der Applikationsdefinition ist als echte Primärpflicht aus dem PaaS-Vertrag aufzufassen. Zwar wird der Cloud-Nutzer an einer isolierten Durchsetzung des entsprechenden Anspruchs in den seltensten Fällen ein Interesse haben. Seine Nichterfüllung sollte aber für sich genommen einen Übergang zu Sekundärrechten grundsätzlich begründen können.

Soweit dem Cloud-Anbieter bis zum Beginn der vereinbarten Vertragslaufzeit vom Nutzer eine Applikationsdefinition übergeben wird, hat der Cloud-Anbieter als Primärpflicht aus dem PaaS-Vertrag so rechtzeitig den Versuch zu unternehmen, eine Applikationsinstanz auf geeigneter Infrastruktur zu starten, dass im Fall des erfolgreichen Starts eine Verfügbarkeit der Applikation gewährleistet ist. Im Bereich der klassischen Sachmiete wird nach § 535 Abs. 1 S. 1 BGB mit der Überlassung zu Beginn des Mietverhältnisses die Schaffung eines bestimmten Zustands geschuldet.¹² Das gesetzliche Leitbild geht hierbei zutreffend davon aus, dass vor Beginn des Mietverhältnisses keine Mitwir-

⁸ Ein Beispiel hierfür ist die „NowPlatform“ von ServiceNow, abrufbar unter: <https://docs.flexera.com/flexera/EN/SaaSManager/SNSubscriptionLicensing.htm>.

⁹ Vgl. zur Container-Technologie Sharma et al., DevOps, 2023, 51 f. und zur Microservice-Cluster-Architektur Container-Technologie Sharma et al., DevOps, 2023, 107 f.

¹⁰ Riehm RdI 2022, 209 (211 f.).

¹¹ Vgl. hierzu Staudinger, BGB/Steinrötter, 2024, BGB § 548a Rn. 8.

¹² Schmidt-Futterer/Lehmann-Richter, Mietrecht, 17. Aufl. 2026, BGB § 535 Rn. 752.

kung des künftigen Mieters erforderlich ist, um die Mietsache in einen Zustand zu versetzen, der einen vertragsgemäßen Gebrauch ermöglicht.

IRd typischen PaaS-Vertrags liegt jedoch stets eine Mitwirkung des Cloud-Nutzers in Form der Bereitstellung der Applikationsdefinition vor. Weil der Cloud-Anbieter insoweit keine Kontrolle über den Programmcode ausüben kann und soll, kann er aus dem PaaS-Vertrag nicht zur Herbeiführung des Erfolgs einer stabil laufenden Applikation verpflichtet werden. Geschuldet wird daher zu Beginn der Vertragslaufzeit nur eine Handlung in Form eines Startversuchs dahingehend, dass das Scheitern eines stabilen Applikationsbetriebs nur durch Fehler in der Applikationsdefinition des Nutzers verursacht sein darf. Da die Bereitstellung von korrektem Programmcode nach dem PaaS-Modell in den Verantwortungsbereich des Nutzers fällt, treffen den Cloud-Anbieter im Grunde genommen keine weiteren Primärpflichten aus dem Vertrag für den Fall der Übermittlung von fehlerhaftem Programmcode. Es wird aber wohl gegen den Grundsatz von Treu und Glauben nach § 242 BGB verstoßen, wenn die initiale Bereitstellung der Applikation auf Grund von Programmfehlern scheitert und der Cloud-Anbieter daraufhin für einen längeren Zeitraum sein vertragliches Entgelt verlangt, ohne frühzeitig einen entsprechenden Hinweis über das Scheitern des Applikationsstarts an den Nutzer erteilt zu haben.

Im Fall des erfolgreichen initialen Starts einer Applikationsinstanz zu Beginn der Vertragslaufzeit wird aus dem PaaS-Vertrag der permanente Applikationsbetrieb grundsätzlich für die gesamte Vertragslaufzeit geschuldet. Diese zeitliche Komponente lässt insoweit wieder eine entsprechende Anwendung des § 535 Abs. 1 S. 1 BGB zu. Deutlich bedeutender als die Pflicht zum ununterbrochenen Betrieb dem Grunde nach ist allerdings die Pflicht zur Annahme und Weiterleitung aller Netzwerkanfragen an eine laufende Applikationsinstanz durch den Cloud-Anbieter. Es erscheint möglich, diese typische Pflicht aus dem PaaS-Vertrag aus einer entsprechenden Anwendung des § 535 Abs. 1 S. 2 Hs. 2 BGB abzuleiten. Nach dieser Norm hat der Vermieter bei der klassischen Sachmiete für die Erhaltung der Mietsache in einem Zustand zu sorgen, die deren vertragsgemäßen Gebrauch ermöglicht. Analog hierzu trifft den Cloud-Anbieter aus dem PaaS-Vertrag die Pflicht, die Applikation des Nutzers in einer Weise bereitzustellen, die einen vertragsgemäßen Gebrauch ermöglicht.

Typisches Merkmal von Applikationen, die iRd PaaS-Modells betrieben werden, ist die funktionale Stellung als Webserver. Entsprechend setzt der vertragsgemäße Gebrauch einer solchen Applikation regelmäßig voraus, dass ein hohes Aufkommen an Netzwerkanfragen auch in Zeiten von Lastspitzen schnell und zuverlässig angenommen und zur Verarbeitung an eine Instanz der Applikation weitergeleitet wird. Technisch gesehen wird der Cloud-Anbieter hierzu ausreichend skalieren und die Eingangslast gleichmäßig verteilen müssen. Bestimmte Ansprüche in Hinblick auf Skalierung, Lastverteilung oder sonstige Maßnahmen im Bereich der Infrastruktur können aus dem typischen PaaS-Vertrag jedoch gerade nicht abgeleitet werden. Im Hinblick auf die Annahme und Weiterleitung von Netzwerkaufufen an die Applikation während der Vertragslaufzeit besteht die Pflicht des Cloud-Anbieters lediglich in der Herbeiführung des Erfolgs einer schnellen und performanten Verarbeitung der Netzwerkzugriffe. Die Mittel zur Herbeiführung dieses Erfolgs kann der Cloud-Anbieter grundsätzlich frei wählen.

b) Pflichten des Cloud-Nutzers

Die Primärpflicht des Cloud-Nutzers aus dem PaaS-Vertrag ist die Leistung des vereinbarten Entgelts. § 535 Abs. 2 BGB ist insoweit unproblematisch anwendbar. Im Gegensatz zum IaaS-Vertrag ist die Höhe des Entgelts allerdings typischerweise nicht nur

im Hinblick auf die Laufzeit des Vertrags teilweise ex ante nicht bestimmbar. Regelmäßig setzt sich das Entgelt für den PaaS-Vertrag aus einer festen Komponente für den Dienst als solches und einer variablen Komponente, die sich am Umfang der erforderlichen physischen Ressourcen zur Bewältigung der jeweiligen Auslastung orientiert, zusammen. Ein variabler Vergütungsanteil und die damit verbundene Unsicherheit für den Nutzer bei Vertragsschluss sind angemessen und interessengerecht, da jedenfalls der Cloud-Anbieter vorab nicht abschätzen kann, wie viele Ressourcen er während der Vertragslaufzeit einsetzen muss, um seiner Primärpflicht zum Betrieb der Applikation unter Annahme und Weiterleitung sämtlicher Netzwerkaufufe zu genügen. Der variable Entgeltanteil ist jedoch regelmäßig auf eine fixe Gebühr je Ressourceneinheit pro Zeiteinheit vorab festzulegen, und die Leistungspflicht des Nutzers beschränkt sich auf die Vergütung für die tatsächlich (technisch) erforderlichen Ressourcen. Ein höherer Ressourceneinsatz durch den Cloud-Anbieter zur Erfüllung seiner Vertragspflichten ist unerheblich.

Die rechtzeitige Übergabe der Applikationsdefinition durch den Nutzer an den Cloud-Anbieter ist hingegen nicht als Leistungspflicht aus dem PaaS-Vertrag zu betrachten. Da die Übergabe einer solchen Definition denklogisch eine notwendige Voraussetzung für die Bereitstellung und den Betrieb einer Applikation durch den Cloud-Anbieter sind, kann allerdings dieser ohne entsprechende Mitwirkung des Nutzers seine vertragliche Primärpflicht in keiner Weise erfüllen. Rechtlich ist die rechtzeitige Übergabe einer Programmdefinition durch den Nutzer daher als Obliegenheit zu werten, bis zu deren Bewirkung dem Nutzer seine Primäransprüche aus dem PaaS-Vertrag zu versagen sind.¹³ Aufgrund der Nichterfüllung dieser Obliegenheit wird der Cloud-Anbieter zudem im Hinblick auf sein Pflichtenprogramm umfassend nach § 295 S. 1 Alt. 2 BGB (ggf. iVm § 296 S. 1 BGB) einen Annahmeverzug des Cloud-Nutzers begründen können.

2. Leistungsstörungenrecht

Im Hinblick auf die primäre vertragliche Leistungspflicht des Cloud-Nutzers stellt sich die Behandlung von Leistungsstörungen als unproblematisch dar. Zu beachten ist, dass vorrangig die speziellen Vorschriften des Mietrechts zur Anwendung gebracht werden müssen. Eine Vertragsbeendigung wegen unzureichender Leistung auf die jeweilige Zahlungspflicht durch den Cloud-Nutzer ist daher nicht durch Rücktritt nach § 323 BGB, sondern im Wege der Kündigung nach § 543 BGB zu bewirken. IÜ gelten die allgemeinen Grundsätze des Leistungsstörungenrechts bei einer Geldschuld. Vor dem Hintergrund des umfassenderen und komplexeren Pflichtenprogramms aus dem PaaS-Vertrag für den Cloud-Anbieter ist für die Behandlung von Leistungsstörungen eine differenzierte Betrachtung der einzelnen möglichen Pflichtverletzungen geboten.

a) Nicht-Abnahme der Applikationsdefinition

Die Pflicht zur Abnahme der Applikationsdefinition durch den Cloud-Anbieter vom Cloud-Nutzer wurde als echte Primärpflicht aus dem typischen PaaS-Vertrag identifiziert. Da das klassische Sachmietrecht keine auch nur annähernd vergleichbare Pflicht kennt, kommen mietrechtliche Vorschriften zur Behandlung einer Leistungsstörung nicht in Betracht. Auch das Verbraucherrecht der digitalen Produkte der §§ 327 ff. BGB enthält keine Regelungen zu einer vergleichbaren Pflicht, sodass es insofern an jedem gesetzlichen Leitbild fehlt.¹⁴ Mithin wird auf das allgemeine Schuldrecht zurückzugreifen sein.

¹³ Zur Rechtsnatur der Obliegenheit vgl. bereits BGH NJW 1957, 1233 (1234) sowie MüKoBGB/Ernst, 10. Aufl. 2025, BGB vor § 241 Rn. 14.

¹⁴ Zur Funktion der Vorschriften der §§ 327 ff. BGB als gesetzliches Leitbild auch für Verträge im B2B-Bereich vgl. MüKoBGB/Metzger, 10. Aufl. 2025, BGB vor § 327 Rn. 39.

Nicht ganz unproblematisch ist hierbei die Bestimmung der Fälligkeit. Regelmäßig werden die Parteien des PaaS-Vertrags bei einer Vereinbarung über den Leistungsbeginn übereinstimmend den Zeitpunkt vor Augen haben, ab dem der Betrieb der Applikation auf der Infrastruktur des Cloud-Anbieters beginnen soll. Eine explizite Vereinbarung über den Fälligkeitszeitpunkt für die Abnahme der Applikationsdefinition als notwendig zeitlich vorausgehende Leistung wird nur in den seltensten Fällen vorliegen. Gleichwohl lassen die Umstände des typischen PaaS-Vertrags wohl die Annahme zu, dass mit § 271 Abs. 1 BGB nicht sofortige Leistung auf die Abnahmepflicht verlangt werden kann, sondern nur eine Leistungszeit, die so rechtzeitig vor dem Beginn der vereinbarten Betriebszeit liegt, dass der rechtzeitige Start des Applikationsbetriebs sichergestellt ist.

Die Behandlung der Leistungsstörung selbst weist keine besonderen Schwierigkeiten auf. Sofern kein Tatbestand für die Entbehrlichkeit einer Fristsetzung erfüllt ist, kann der Nutzer im Falle des erfolglosen Ablaufs einer Frist zur Erfüllung nach § 323 Abs. 1 BGB vom Vertrag zurücktreten oder nach §§ 280 Abs. 1, Abs. 3, 281 BGB Schadensersatz auf sein Erfüllungsinteresse verlangen, soweit der Cloud-Anbieter sich nach § 280 Abs. 1 S. 2 BGB nicht exkulpieren kann. Im Hinblick auf die Angemessenheit der Frist ist die Schnelligkeit des digitalen Wirtschaftsverkehrs zu beachten. Beim Ausbleiben der Abnahme der Applikationsdefinition muss der Nutzer regelmäßig befürchten, dass seine Applikation nicht rechtzeitig im Netzwerk bereitstehen wird. Er wird daher ggf. sehr schnell Abhilfe schaffen und ggf. anderweitig die notwendigen Ressourcen beschaffen müssen. Eine Entbehrlichkeit der Fristsetzung für einen Rücktritt nach § 323 Abs. 2 Nr. 2 BGB ist gleichwohl nicht typischerweise für den PaaS-Vertrag anzunehmen, da im Regelfall doch größere Zeiträume zwischen dem Betriebsbeginn einer PaaS-Applikation und ihrer produktiven Verwendung liegen. Sie wäre daher nur im Fall einer ausdrücklichen Benachrichtigung des Cloud-Anbieters von einem zeitkritischen Prozess anzunehmen.

b) Kein Programmstart bei Vertragsbeginn

Keine besonderen Probleme ergeben sich im Hinblick auf die rechtliche Behandlung einer Verletzung der Pflicht zum Beginn des Applikationsbetriebs zum vereinbarten Zeitpunkt. Die Bereitstellung in diesem Sinne entspricht der Überlassung der Sache zum Gebrauch gem. § 535 Abs. 1 S. 1 BGB. Folglich sind Leistungsstörungen nach den mietrechtlichen Sondervorschriften zu behandeln. Eine Vertragsbeendigung ist daher bei ausbleibender Leistung im Wege der außerordentlichen Kündigung nach § 543 Abs. 1 BGB iVm Abs. 2 Nr. 1 Alt. 1 BGB zu bewirken. Für einen Anspruch auf Schadensersatz wegen Frustration des Leistungsinteresses enthält das Mietrecht keine eigene Vorschrift, insbesondere ist nach hM § 536a BGB erst nach Übergabe (bzw. hier: Bereitstellung) einschlägig.¹⁵ Ein Anspruch ist daher nach den allgemeinen Vorschriften unter den Voraussetzungen der §§ 280 Abs. 1 und Abs. 3, 281 BGB gegeben. Zu beachten ist wiederum die Schnelligkeit des digitalen Wirtschaftsverkehrs für die Bestimmung der angemessenen Frist zur Leistungsbewirkung, die im Regelfall für beide Rechtsbehelfe erfolglos verstreichen muss.

c) Keine Bearbeitung von Netzwerkaufrufen

Die Pflicht zur Annahme und Weiterleitung von Netzwerkaufrufen an die Applikation aus dem PaaS-Vertrag ist unmittelbar auf die Herbeiführung von Erfolgen und nicht den Erhalt eines Zu-

stands gerichtet. Zur Herbeiführung dieses Erfolgs wird der Cloud-Anbieter zwar auf technischer Ebene einen bestimmten Zustand herstellen und erhalten müssen. Dies kann aber nicht unmittelbar durch den Nutzer aus dem PaaS-Vertrag verlangt werden. Trotz dieses strukturellen Unterschieds zur klassischen Sachmiete lässt sich eine Verletzung der Pflicht zur Annahme und Weiterleitung von Netzwerkaufrufen an die Applikation gut mit dem mietrechtlichen Mängelrecht der §§ 536 ff. BGB behandeln. Dem Tatbestand beider Alternativen des § 536 Abs. 1 S. 1 BGB lässt sich deutlich entnehmen, dass auch im Fall einer vollständigen Untauglichkeit der Mietsache für den vertragsgemäßen Gebrauch das mietrechtliche Mängelgewährleistungsrecht anzuwenden ist. Mithin ist selbst dann, wenn die Überlassung einer bloßen „Hülle“ ohne jede Möglichkeit für den praktischen vertragsgemäßen Gebrauch erfolgt, kein Rückgriff auf Vorschriften des allgemeinen Schuldrechts eröffnet.

Die bloße Bereitstellung der Nutzerapplikation entspricht der Überlassung einer solchen Hülle, solange eine Weiterleitung von Netzwerkaufrufen durch den Cloud-Anbieter pflichtwidrig unterbleibt. Mithin ist der Cloud-Nutzer für den Fall dieser Leistungsstörung in Abhängigkeit vom Zeitpunkt des Störungsbegins nach einer der beiden Varianten des § 536 Abs. 1 S. 1 BGB kraft Gesetzes von seiner Entgelpflicht für die Dauer der Störung befreit. Nach § 536a Abs. 1 BGB steht dem Nutzer ein Anspruch auf Schadensersatz zu, der sich grundsätzlich in Übereinstimmung mit den Grundsätzen zur Sachmiete auf sämtliche Folgeschäden des jeweiligen Mangels erstreckt.¹⁶ Wenig sachgerecht erscheint allerdings die Differenzierung nach Zeitpunkt des Mangelbeginns im Hinblick auf das Vertretenmüssen des Cloud-Anbieters.

Bei der klassischen Sachmiete befindet sich die Mietsache nach Überlassung an den Mieter grundsätzlich in dessen Einfluss-sphäre. Die positive Feststellung einer Verantwortung des Vermieters für nachträglich auftretende Mängel als Voraussetzung für einen Schadensersatzanspruch ist daher interessengerecht. Bei der Abwicklung des PaaS-Vertrags übt jedoch während der gesamten Laufzeit der Cloud-Anbieter die physische Kontrolle über die Hardware und die administrative Kontrolle über die Systemsoftware aus, sodass die wortgetreue Anwendung des § 536a Abs. 1 BGB unbillig erscheint. Für eine sachgerechte Lösung ist daher mindestens eine Vermutungsregel dahingehend aufzustellen, dass bei einem Ausbleiben der Weiterleitung von Netzwerkaufrufen ein Verschulden des Cloud-Anbieters vorliegt. Im konkreten Fall sollten darüber hinaus die Umstände der Vertragsbeziehung daraufhin untersucht werden, ob nicht sogar mindestens konkludent eine Funktionsgarantie für die gesamte Laufzeit durch den Cloud-Anbieter übernommen wurde. In diesem Fall wäre bei der entsprechenden Leistungsstörung der Schadensersatzanspruch nach § 536a Abs. 1 BGB unabhängig vom Zeitpunkt des Störungsbegins verschuldensunabhängig gegeben. Zu beachten ist, dass eine fehlerhafte oder ausbleibende Beantwortung von Netzwerkaufrufen natürlich auch durch Fehler in der Applikation selbst verursacht sein kann. Hierfür ist der Cloud-Anbieter in keinem Fall verantwortlich. Es wäre im Zweifel keine Frage des Vertretenmüssens, sondern, ob überhaupt ein Mangel besteht.

d) Verzögerte Bearbeitung von Aufrufen

Moderne Webanwendungen und ihre Nutzer sind darauf ausgerichtet, dass Netzwerkanfragen an die Server-Applikationen in sehr kurzer Zeit beantwortet werden. Daher sind kurze Antwortzeiten für den vertragsgemäßen Gebrauch iSd entsprechend anzuwendenden § 535 Abs. 1 S. 2 BGB ein essenzielles Zustandsmerkmal des Leistungsgegenstands aus dem PaaS-Vertrag. Soweit eine verzögerte Bearbeitung von Netzwerkaufrufen in der Sphäre des Cloud-Anbieters verursacht wird, liegt da-

¹⁵ BGH NJW 1997, 2813; BGH NJW 1999, 635; Börstinghaus/Siegmund, Miet-/Siegmund, 8. Aufl. 2025, BGB § 536a Rn. 4; aA Schmidt-Futterer/Lehmann-Richter, Mietrecht 17. Aufl. 2026, BGB § 536a Rn. 5.

¹⁶ Schmidt-Futterer/Lehmann-Richter, Mietrecht, 17. Aufl. 2026, BGB § 536a Rn. 101.

her eine Leistungsstörung in Form eines Mangels vor. Je nach Schwere dieses Mangels ist in solchen Fällen die Entgeltspflicht des Nutzers aus dem PaaS-Vertrag nach § 536 Abs. 1 S. 1 BGB aufgehoben oder wird nach dieser Norm iVm Satz 2 nur teilweise aufrechterhalten. Weiterhin ist der Anspruch auf Schadensersatz nach § 536a Abs. 1 BGB eröffnet, insoweit gelten die gleichen Grundsätze wie beim Mangel des vollständigen Ausbleibens der Bearbeitung von Netzwerkaufrufen.

e) Betriebsausfall

Applikationen im PaaS-Modell dienen nicht notwendig ausschließlich der Bearbeitung von Netzwerkanfragen. Möglich und praktisch verbreitet ist die Nutzung für weitere Funktionen, wie etwa die zeitgesteuerte Synchronisation mit anderen Systemen oder der regelmäßige, automatische Import bzw. Export von Daten. Daher liegt jedenfalls auch unabhängig von der Verfügbarkeit der Applikation für Aufrufe über das Netzwerk eine Leistungsstörung vor, soweit und solange während der Laufzeit des PaaS-Vertrags trotz Übergabe einer lauffähigen Applikationsdefinition kein Betrieb mindestens einer Instanz durch den Cloud-Anbieter erfolgt. Dem Nutzer sind in diesem Fall neben dem Primäranspruch auf Erfüllung daher ebenfalls die mietrechtlichen Mängelrechte einzuräumen, namentlich die Entgeltminderung kraft Gesetzes nach § 536 Abs. 1 BGB sowie ein Anspruch auf Schadensersatz nach § 536a Abs. 1 BGB. Praktisch relevant dürfte hier vor allem der Schadensersatz sein: Gerade der Ausfall von Synchronisationsroutinen kann Funktionsstörungen in anderen Systemen nach sich ziehen und mitunter recht schnell zu wirtschaftlich bedeutenden Folgeschäden im

betrieblichen Leistungssystem des Nutzers oder seiner Partnerfirmen führen.

Schnell gelesen ...

- Im PaaS-Cloud-Modell realisiert der Cloud-Anbieter den Betrieb einer Webserver-Nutzerapplikation auf seiner Infrastruktur.
- Primärpflichten des Cloud-Anbieters aus dem PaaS-Vertrag sind die Abnahme der Applikationsdefinition und der Applikationsbetrieb während der gesamten Vertragslaufzeit unter Annahme und Weiterleitung sämtlicher Netzwerkaufträge.
- Trotz des vermeintlichen dienst- oder werkvertraglichen Charakters des PaaS-Vertrags lassen sich Leistungsstörungen gut mit dem mietrechtlichen Mängelgewährleistungsrecht behandeln.
- Störungen bei Annahme und Weiterleitung von Netzwerkaufrufen oder sonstige Ausfälle des Applikationsbetriebs führen zur Entgeltminderung nach § 536 BGB und begründen Schadensersatzansprüche des Nutzers nach § 536a BGB.



Alexander Kubis

ist Rechtsreferendar am OLG Rostock.

Zum Pflichtenprogramm und Leistungsstörungenrecht beim Infrastructure-as-a-Service(IaaS)-Cloud-Vertrag s. bereits Kubis MMR 2026, 377.

WOLFGANG FRHR. RAITZ VON FRENTZ / CHRISTIAN L. MASCH

KI und Urheberrecht im Zivilprozess und im Schiedsstellenverfahren

Urheberrechtliche Nutzungen und Durchsetzung daraus folgender Ansprüche

Leistungsschutzrechte

Das LG München I hat die urheberrechtliche Haftung eines KI-Anbieters für die Vervielfältigung und öffentliche Zugänglichmachung von Inhalten bejaht (MMR 2026, 74 mAnm Gierschmann). Der Beitrag umreißt die aktuellen urheberrechtlichen und prozessualen Fragen bei der Nutzung von Werken iRv KI-Modellen. Zunächst wird die Funktion von KI-Modellen beschrieben. Dann werden die betroffenen Urheber- und Leistungsschutzrechte für die drei Arbeitsphasen – Datensammlung, Training, Ausgabe der Arbeitsergebnisse – dargestellt.

I. Sachverhalt

KI-Systeme¹ basieren auf KI-Modellen.² Bei den sprachbezogenen KI-Modellen (Large Language Models – LLM) und bei den allgemeinen KI-Modellen (Large Multimodal Model), die zB auch Videos abdecken, sind drei Arbeitsschritte zu unterscheiden (siehe Abb. 1).

1. Datensammlung

Bei der Datensammlung werden Informationen gesammelt. Dabei erfolgt häufig zumindest eine vorübergehende Vervielfälti-

Auch wird erörtert, ob die KI-VO Weiterungen der urheberrechtlichen Rechte begründet und ob ergänzender wettbewerbsrechtlicher Leistungsschutz in Betracht kommt. Im Anschluss wird die prozessuale Durchsetzung etwaiger urheberrechtlicher Ansprüche durch die Rechteinhaber dargestellt und die Passivlegitimation erörtert. Schließlich werden urheberrechtliche „Fallstricke“ für die Nutzer beleuchtet.

Lesedauer: 26 Minuten

gung der abgerufenen Inhalte. Die Trainingsdaten muss ein Betreiber nicht umfänglich selbst beschaffen, sondern kann sie

¹ Definition in Art. 3 Nr. 1 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) (KI-VO), ABl. L 2024/1689, 1.

² Definition in Art. 3 Nr. 63 KI-VO; Erläuterungen hierzu in Erwägungsgrund 97 KI-VO.

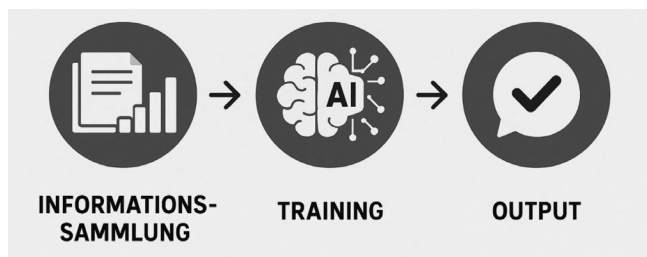


Abb. 1: Grafik erstellt mit Copilot am 28.11.2025.

baukastenartig erwerben, einschließlich synthetischer Daten.³ Ob Drittinhalte (dauerhaft) gespeichert werden, ist von außen regelmäßig nicht erkennbar. In der Literatur wird sowohl auf Studien verwiesen, die eine dauerhafte Speicherung belegen als auch erklärt, dass eine solche Speicherung nicht erfolgt und nur die extrahierten Informationen gespeichert werden. Wie bei Suchmaschinen erfolgt die Datensammlung fortlaufend, dh es kommen stetig neue Trainingsdaten hinzu. Zeitlich laufen bei KI-Modellen im operativen Betrieb die Datensammlung und das Training also parallel.

2. Training

Mit den Trainingsdaten wird das KI-Modell laufend trainiert. Dies ist nachfolgend dargestellt:

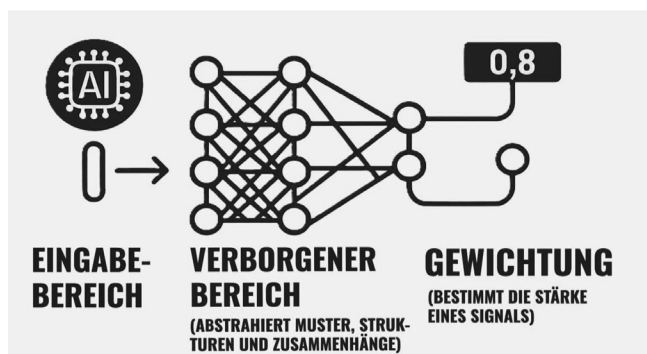


Abb. 2: Grafik erstellt mit Copilot am 3.12.2025.

Das Training erfolgt idR automatisiert. Dabei geht es um die Anwendung von Statistik. Es werden Zusammenhänge bewertet, mit denen später die bei statistischer Betrachtung naheliegenden Antworten zusammengestellt werden. Ein KI-Modell besteht also aus gewichteten Informationen. Zusätzlich erfolgen externe Bewertungen, zB um unerwünschte Ergebnisse zu korrigieren.

³ Hierzu Dornis GRUR 2015, 1717.

⁴ Zur Unterscheidung zwischen Information und Ausdrucksform BGH GRUR 1981, 352 (353); BeckOK Urheberrecht/Rauer/Bibi, 48. Ed. 2025, UrhG § 2 Rn. 155 ff; Raue GRUR 2017, 11 (13).

⁵ Jedoch kann zB beim massenhaften Zugriff auf Informationssammlungen § 87b UrhG greifen, mit der unionsrechtlichen Vorgabe, dass Datenbanken gegen die Entnahme und Weiterverwendung geschützt sind, sodass für die Bejahung eines Eingriffs nicht notwendig herkömmliche Vervielfältigungen oder Handlungen der öffentlichen Wiedergabe iSv §§ 16, 19a UrhG erforderlich sind.

⁶ LG München I MMR 2026, 74 Rn. 180 ff. mAnm Gierschmann.

⁷ S. BeckOK Urheberrecht/Götting, 48. Ed. 2025, UrhG § 16 Rn. 18.

⁸ Hierbei handelt es sich um den originären Rechteinhaber, zB den Urheber, sowie jeden Inhaber derivativer Rechte, wobei das LG Hamburg MMR 2024, 973 auch den Inhaber eines einfachen Nutzungsrechts als Rechteinhaber in diesem Sinne einordnet.

⁹ LG Hamburg MMR 2024, 973.

¹⁰ OLG Hamburg MMR 2026, 140 mAnm Hoeren; die Revision zum BGH (Az: I ZR 281/25) wurde zugelassen.

¹¹ Gausling CR 2021, 609 (611); Müller-ter Jung/Rexin CR 2022, 169 (174); Maa-mar ZUM 2023, 481 (484); Schack NJW 2024, 113 (116).

3. Output

Dem trainierten KI-Modell können die Nutzer Fragen stellen bzw. Aufgaben definieren, die Prompts. Qualität und Genauigkeit der Prompts entscheiden mit über die Qualität der ausgegebenen Resultate. Daher können Prompts eine erhebliche Ausführlichkeit und Komplexität erreichen, zB wenn Dokumente auf bestimmte Inhalte untersucht werden sollen. Je nach Nutzungsvertrag können die vom Nutzer eingebrachten Informationen bzw. Dateien für das allgemeine Training (s. unter I.2.) des KI-Modells verwendet werden. Gerade bei Informationen, für die ein Geheimnisschutz nach dem GeschGehG bestehen soll, oder die einer Berufsverschwiegenheit oder dem Datenschutz unterliegen, ist also nutzerseitig darauf zu achten, dass diese nicht in den allgemeinen Datenbestand des KI-Modells aufgenommen werden.

II. Urheber- und Leistungsschutzrechte

Urheberrechtlich ist nach den o.g. Arbeitsschritten – Sammlung, Training und Arbeitsergebnisse – zu unterscheiden:

1. Datensammlung

a) Vervielfältigung

Die Datensammlung, dh das Abgreifen von Informationen mit der Speicherung der hierzu abgerufenen Internetinhalte, kann § 16 UrhG unterfallen. Sofern die Vervielfältigungen nur vorübergehend sind und der Informationsgewinnung dienen, können sie gem. § 44b UrhG zulässig sein.

■ Anwendbarkeit des UrhG

Voraussetzung für die Anwendung der §§ 16, 44b UrhG ist, dass die Handlungen zumindest auch in Deutschland erfolgen. Dabei führt nicht schon der extratoritoriale Sitz des Anbieters zur Unanwendbarkeit des UrhG. Entscheidend ist, ob Vervielfältigungen zumindest auch in Deutschland erfolgen.

■ Herstellung von Vervielfältigungsstücken

Sodann ist erforderlich, dass Schutzgüter vervielfältigt werden. Dabei ist zu beachten, dass nicht die enthaltenen Informationen vor der Übernahme geschützt sind, sondern die urheberrechtlichen Ausdrucksformen, zB Sprachwerke.⁴ Das bloße „Auslesen“ der Informationen kann daher zustimmungsfrei sein.⁵ Das Urteil des LG München I belegt, dass das UrhG – iRd unionsrechtlichen Vorgaben – elastisch ist und auch neuere Formen der Speicherung erfasst. Damit kann auch die Speicherung in Form „künstlicher Neuronen“ mit unterschiedlichen Gewichten eine Vervielfältigung sein⁶ – so wie zB ein Musikstück, wenn es digital gespeichert wird, auch dann dem Vervielfältigungsrecht unterfällt, wenn es ohne Hilfsmittel nicht sinnlich wahrnehmbar ist.⁷

■ Text und Data Mining

Vervielfältigungsstücke können gem. § 44b UrhG zulässig sein, wenn kein Nutzungsvorbehalt gem. § 44b Abs. 3 UrhG erklärt wurde.

Wirksame Erklärung

Der Nutzungsvorbehalt ist bei im Internet zugänglichen Inhalten nur relevant, wenn er vom Rechteinhaber⁸ ausdrücklich in maschinenlesbarer Form erklärt wurde. Dazu hat sich das LG Hamburg im Ur. v. 27.9.2024⁹ geäußert, dass ein KI-Modell natürliche Sprache verarbeiten könne, sodass ein Nutzungsvorbehalt auch in natürlicher Sprache maschinenlesbar sei gem. § 44b Abs. 3 S. 2 UrhG. Dem hat das OLG Hamburg im Berufungsurteil widersprochen und den Nutzungsvorbehalt in natürlicher Sprache für unwirksam erklärt.¹⁰ Angesichts der Entscheidung des OLG Hamburg sowie der weitgehend übereinstimmenden Literaturauffassung¹¹ ist Rechteinhabern zu empfehlen, den Vorbehalt zB unter Berücksichtigung des Text and Data Mining

Reservation Protocol zu erklären, dh nicht nur in natürlicher Sprache.¹²

Zeitliche Beschränkung

Auch ohne Nutzungsvorbehalt sind Vervielfältigungen nur für die Informationsgewinnung zulässig, § 44b Abs. 2 S. 2 UrhG. Nicht abschließend geklärt ist, wann die Vervielfältigungen gelöscht werden müssen. Bei einer wortlautnahen Anwendung von § 44b Abs. 2 S. 1 UrhG muss die Löschung sogleich nach der Informationsgewinnung erfolgen. Nach einer vermittelnden Auffassung sollen die Vervielfältigungen zulässig sein, solange das betreffende Projekt andauert.¹³

Für die vermittelnde Auffassung bietet Art. 4 Abs. 2 DSM-RL¹⁴ keine sichere Grundlage. Auch wegen der abweichenden Regelung einer längeren Speicherung beim Text und Data Mining zwecks wissenschaftlicher Forschung in § 60d UrhG dürfte sich die wortlautnahe Auslegung durchsetzen. Dafür spricht auch die unsichere Abgrenzung, was ein Projekt ist und wann es abgeschlossen ist, und, dass die Rechteinhaber für die Vervielfältigungen gem. § 44b UrhG keinen Ausgleich erhalten.¹⁵

Rechtmäßige Zugänglichkeit

Zugänglichkeit in § 44b Abs. 2 S. 1 UrhG meint die tatsächliche Zugangsmöglichkeit. Es dürfen also keine Zugangsbeschränkungen umgangen werden. Rechtmäßig zugänglich sind damit die frei im Internet verfügbaren und solche Inhalte, auf die der Anbieter mit einem Zugangsrecht, zB iRe Nutzungsvertrags, zugreift.¹⁶

b) Datenbankherstellerrrecht

Wertvolle Informationen finden sich häufig in Datenbanken. Werden diese vollständig oder in wesentlichen Teilen abgegriffen, kann § 87b UrhG greifen. § 87b UrhG ist unionsrechtskonform dahin auszulegen, dass die Datenbank gegen die Entnahme und Weiterverwendung geschützt ist.¹⁷ Selbst wenn die Datensammlung ohne Vervielfältigung erfolgt, kann also § 87b UrhG einschlägig sein. Die vom EuGH geforderte Beeinträchtigung des Investitionsinteresses¹⁸ wird bei privat – dh nicht steuer- oder beitragsfinanziert angebotenen – Diensten regelmäßig vorliegen. Denn das Interesse an der für das KI-Modell ausgewerteten Datenbank sinkt bzw. entfällt, wenn die Informationen über KI-Systeme zur Verfügung stehen. Der verminderte Zugriff der Nutzer auf die Datenbank kann deren Refinanzierung beeinträchtigen, zB über die Vermarktung entgeltlicher Zugänge und von Werbung.

Auch Eingriffe in das Datenbankherstellerrrecht können gem. §§ 44b, 60d UrhG zulässig sein, die gem. § 87c Abs. 1 Nr. 4, Nr. 5 UrhG für die Vervielfältigung wesentlicher Datenbankteile gelten. Dies entspricht Art. 4 Abs. 1 DSM-RL, der Entnahmen aus Datenbanken iSv Art. 5, 7 Datenbank-RL¹⁹ für Zwecke des Text und Data Mining rechtfrei stellt. Rechtfrei ist dabei allerdings nach Art. 4 Abs. 1 DSM-RL nur die Entnahme, nicht auch die Weiterverwendung iSv Art. 7 Abs. 1 Datenbank-RL.²⁰ Außerhalb der wissenschaftlichen Forschung kommt ein relevanter Eingriff gem. § 87b Abs. 1 UrhG bei KI-Systemen also durchaus in Betracht.

c) Presseleistungsschutzrecht

Bei Presseveröffentlichungen kann § 87g UrhG greifen. Der KI-System-Betreiber ist Anbieter eines Dienstes der Informationsgesellschaft iSv § 87g Abs. 1 UrhG. Auch eine Online-Nutzung liegt regelmäßig vor, da die Trainingsdaten nicht nur für interne Zwecke verwendet werden,²¹ sondern für passende Arbeitsergebnisse an die Nutzer. Im Hinblick auf die gem. § 87g Abs. 1 UrhG geschützten Vervielfältigungen kann § 44b UrhG greifen, wenn sich der Presseverleger die Rechte nicht gem. § 44b Abs. 3 S. 1 UrhG vorbehalten hat, da §§ 44a ff. UrhG gem. § 87i UrhG anwendbar sind.²² Dies betrifft nach § 44b Abs. 2 S. 1 UrhG aber nur die Vervielfältigung, nicht auch die öffentliche Zugänglichmachung gem. § 87g Abs. 1 UrhG.

d) Öffentliche Zugänglichmachung

Angesichts der Zielrichtung, ein passendes Arbeitsergebnis auszuliefern, kann die Erfassung der Trainingsdaten eine öffentliche Zugänglichmachung iSv § 19a UrhG begründen. Zwar erfolgt die Erfassung der Trainingsdaten intern beim Anbieter. Gleichwohl werden die Inhalte verarbeitet, um sie bzw. die enthaltenen Informationen den Nutzern, und damit einer Öffentlichkeit, zugänglich zu machen. Und dies kann für die Anwendung von § 19a UrhG genügen, weil die öffentliche Zugänglichmachung laut § 19a UrhG²³ und EuGH keinen tatsächlichen Zugriff einer Öffentlichkeit auf die verarbeiteten Werke bzw. Schutzgegenstände voraussetzt. Es genügt die entsprechende Möglichkeit.²⁴ § 44b UrhG greift hier nicht. Die öffentliche Zugänglichmachung ist nur für Zwecke wissenschaftlicher Forschung (teilweise) durch § 60d Abs. 4 UrhG gedeckt.

2. Training

Beim Training stellen sich gegenüber den unter II. 1. erörterten Gesichtspunkten keine wesentlich anders gelagerten Fragen.

a) Text und Data Mining

Angesichts der Definition des Text und Data Mining in § 44b Abs. 1 UrhG als Verfahren der Informationsgewinnung kann § 44b Abs. 1 UrhG derzeit nicht sicher auch auf das Training der KI-Modelle angewendet werden. Gerichtlich ist diese Frage bislang nicht geklärt. In der Literatur werden beide Auffassungen

¹² Zum Text and Data Mining Reservation Protocol s. BeckOK Urheberrecht/Bomhard, 48. Ed. 2025, UrhG § 44b Rn. 35 f.

¹³ S. Dreier/Schulze, UrhG/Dreier, 8. Aufl., UrhG § 44b Rn. 15; Maamar ZUM 2023, 481 (483).

¹⁴ RL (EU) 2019/790 des Europäischen Parlaments und des Rates v. 17.4.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG, ABl. 2019 L 130, 92.

¹⁵ Die EuGH-Rspr. zur Erforderlichkeit eines Ausgleichs bei cloudbasierten Vervielfältigungen (EuGH MMR 2022, 647 – Austro-Mechana/Strato AG) zeigt, dass die Entschädigungslosigkeit für die restriktive Anwendung von § 44b UrhG spricht. Ggü. privilegierten Vervielfältigungen mit Entschädigung der Urheber, wie zB cloudbasierten Privatkopien, dürfte der 3-Stufen-Test entsprechend Art. 5 Abs. 5 InfoSoc-RL, Art. 7 Abs. 2 S. 1 DSM-RL bei § 44b UrhG eher anschlagen als zB bei § 53 Abs. 1 S. 1 UrhG; mit LG Hamburg MMR 2024, 973 Rn. 50–53 wird dies zwar bei der Vervielfältigung iRd Informationssammlung noch keine entscheidende Rolle spielen. Für das anschließende Training deutet jedoch auch das LG Hamburg MMR 2024, 973 Rn. 52 an, dass dies wohl anders zu bewerten ist.

¹⁶ Hierzu Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 44b Rn. 8; BeckOK Urheberrecht/Bomhard, 48. Ed. 2025, UrhG § 44b Rn. 17; Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Pesch, 5. Aufl. 2026, UrhG § 44b Rn. 28; Müller-ter Jung/Rexin CR 2022, 169 (173).

¹⁷ S. Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 87b Rn. 2 ff.; BeckOK Urheberrecht/Vohwinkel, 48. Ed. 2025, UrhG § 87b Rn. 5 ff.; Wandtke/Bullinger, Urheberrecht/Hermes, 6. Aufl. 2022, UrhG § 87b; Rn. 23 ff.; Loewenheim, HdB. des Urheberrechts/Leistner/Zurth, 3. Aufl. 2021, § 49 Rn. 72 ff.

¹⁸ Das Erfordernis schränkt das weite Begriffsverständnis der Weiterverwendung aus der Datenbank-RL wieder ein, und ist daher iRe unionsrechtskonformen Anwendung des § 87b Abs. 1 UrhG im konkreten Einzelfall zwingend zu beachten, s. EuGH MMR 2021, 789 – CV-Online Latvia.

¹⁹ RL 96/9/EG des Europäischen Parlaments und des Rates v. 11.3.1996 über den rechtlichen Schutz von Datenbanken, ABl. 1996 L 77, 20.

²⁰ Zur Einschränkung nur des Vervielfältigungsrechts über §§ 87c Abs. 1 Nr. 4, 44b UrhG Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 87c Rn. 18; sowie ebenfalls dazu, dass für das Text und Data Mining für Zwecke der wissenschaftlichen Forschung gem. §§ 87c Abs. 1 Nr. 5, 60d UrhG neben dem Vervielfältigungsrecht auch das Recht der öffentlichen Zugänglichmachung von der Schrankenregelung erfasst wird.

²¹ Zum Kriterium der Online-Nutzung s. BeckOK Urheberrecht/Graef, 48. Ed. 2025, UrhG § 87g Rn. 2.

²² Zu den Einschränkungen Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 87i Rn. 2.; BeckOK Urheberrecht/Graef, 48. Ed. 2025, UrhG § 87i Rn. 2; Wandtke/Bullinger, Urheberrecht/Jani, 6. Aufl. 2022, UrhG § 87i Rn. 2 f.; Spindler/Schuster/Kaesling, Das Recht der elektronischen Medien/Wiedemann, 5. Aufl. 2026, UrhG § 87i Rn. 2 ff.

²³ S. Wandtke/Bullinger, Urheberrecht/Bullinger, 6. Aufl. 2022, UrhG § 19a Rn. 10.

²⁴ EuGH MMR 2014, 260 – Svensson; EuGH MMR 2017, 518 – Stichting Brein/Ziggo.

vertreten.²⁵ Näher am Sinn und Zweck von § 44b UrhG liegt die Auffassung, die nur die Datensammlung erfasst sieht. Hierfür sprechen auch die unionsrechtlichen Vorgaben zu § 44b UrhG, dh insbesondere Art. 4 DSM-RL sowie Erwägungsgrund 18 DSM-RL.²⁶ Ferner könnte die Anwendung von § 44b UrhG auf das Training § 44b Abs. 2 S. 2 UrhG zuwiderlaufen: Danach sind Vervielfältigungen zu löschen, wenn sie für das Text und Data Mining nicht mehr erforderlich sind. Diese Regelung liefe leer, wenn das Training der KI-Modelle als Teil der Informationsbeschaffung iSv § 44b Abs. 1 UrhG betrachtet würde, da KI-Modelle nie „zu Ende trainiert“ sind, dh eine dauerhafte Speicherung ermöglicht würde. Das widerspräche der Intention des Gesetzgebers²⁷ und wäre mit dem 3-Stufen-Test schwer vereinbar.²⁸

Teilweise wird auf Art. 53 Abs. 1 lit. d KI-VO verwiesen.²⁹ Danach müssen Anbieter von KI-Systemen mit allgemeinem Verwendungszweck die Trainingsinhalte offenlegen. Dass der Unionsgesetzgeber deswegen auch bei Art. 4 DSM-RL eine Schrankenregelung für das Training von KI-Modellen schaffen wollte, erscheint aber wegen der Definition des Text und Data Mining in Art. 2 Nr. 2 DSM-RL und des zeitlichen Ablaufs³⁰ fraglich. Eine erste Klärung könnte iRd Rs. C-250/25 – Like Company/Google erfolgen. Das Bezirksgericht Budapest hat dem EuGH am 3.4.2025 gem. Art. 267 AEUV die Frage vorgelegt, ob die Verwertung von Presseartikeln bei Gemini unter die Ausnahme des Text- und Data-Mining gem. Art. 4 DSM-RL fällt – sofern

das Training des KI-Modells eine Vervielfältigung iSv Art. 15 DSM-RL bzw. Art. 2 InfoSoc-RL³¹ ist.³²

b) Bearbeitungsrecht

Wenn die bei der Datensammlung abgegriffenen Werke beim Training verändert werden, kann das Bearbeitungsrecht gem. § 23 UrhG greifen, u.a. bei Datenbankwerken (§ 23 Abs. 2 Nr. 4 UrhG). Zwar können Änderungen beim Text und Data Mining gem. § 44b Abs. 2 UrhG der Ausnahmeregelung gem. § 23 Abs. 3 unterfallen. Voraussetzung ist jedoch, dass die Änderungen allein technisch bedingt sind – sonstige Änderungen sind unzulässig.³³

3. Ausgabe der Arbeitsergebnisse

Auch die Ausgabe der Arbeitsergebnisse kann den unter II. 1. erörterten Urheber- und Leistungsschutzrechten unterfallen.³⁴ Für die Rechteinhaber ist dabei insbesondere § 19a UrhG zielführend, weil dort die intendierte Verfügbarkeit der Arbeitsergebnisse in Deutschland genügt:³⁵ Richtet sich das Angebot an Nutzer in Deutschland, ist § 19a UrhG anwendbar. Ob, wo und durch wen zugrunde liegende Vervielfältigungen erfolgen, ist dann grundsätzlich nicht mehr relevant, denn § 19a UrhG ist auf das Werk bezogen, nicht auf das Vervielfältigungsstück.³⁶

Bei der Ausgabe der Arbeitsergebnisse kann es zu „Doppelschöpfungen“ kommen. Generiert das KI-Modell einen Text, der einem bestehenden Werk entspricht oder schutzfähige Elemente daraus enthält, kann eine zufällige Doppelschöpfung vorliegen.³⁷ Allerdings begründet die Übereinstimmung zweier Gestaltungen einen Anscheinsbeweis, dass das bestehende Werk – zustimmungspflichtig – genutzt wurde.³⁸ Mit dem Urteil des LG München I v. 11.11.2025³⁹ dürfte dieser Anscheinsbeweis schwer zu entkräften sein, vor allem wenn die Einbindung des vorbestehenden Werks in die Datensammlung nachweisbar bzw. unstrittig ist.

4. KI-VO als „Hebel“ für das Urheberrecht?

Diskutiert wird, ob die KI-VO zu Weiterungen führt, zB bei der territorialen Anwendbarkeit der Urheber- und Leistungsschutzrechte. Dies soll vor allem aus Art. 53 Abs. 1 lit. c KI-VO folgen, der von Anbietern allgemeiner KI-Modelle eine Strategie zur Einhaltung des Unionsurheberrechts fordert. Auch Erwägungsgrund 106 KI-VO erlaubt den Schluss, dass die Einhaltung der Vorgaben aus dem Unions-Urheberrecht mit zu den Zielen der KI-VO gehört.⁴⁰

Ob daraus durchsetzbare Ansprüche der Rechteinhaber folgen, ist offen. Aus der KI-VO selbst folgen im Hinblick auf Art. 53 Abs. 1 KI-VO keine Ansprüche. Solche Ansprüche sind daher gem. §§ 823 Abs. 2, 1004 BGB denkbar sowie ggf. – wenn Vorschriften der KI-VO als Marktverhaltensregelung iSv § 3a UWG einordnet werden – gem. § 8 UWG. Für die Anwendung von § 823 Abs. 2 BGB müsste die jeweils einschlägige Norm der KI-VO im Hinblick auf die Urheber- und Leistungsschutzrechte als Schutzgesetz einzuordnen sein.⁴¹

Ob die deutschen Gerichte eine solche Qualifikation einzelner Bestimmungen der KI-VO vornehmen werden und wie ggf. der EuGH sich hierzu positionieren würde, ist derzeit offen. Die Eigenschaft von Urheber- und Leistungsschutzrechten als Schutzgesetze wird angesichts der eigenständigen Regelung von urheberrechtlichen Schadensersatzansprüchen in § 97 Abs. 2 UrhG regelmäßig nicht diskutiert.⁴² Angesichts dessen ist es fraglich, über die KI-VO einen neuen Haftungstatbestand zu begründen, der das allgemeine Deliktsrecht erweitert.⁴³

5. Wettbewerbsrecht

Auch ohne (nachweisbare) urheberrechtliche Nutzungshandlungen kann ein ergänzender wettbewerbsrechtlicher Leistungsschutz gem. §§ 3 Abs. 1, 4 Nr. 3 UWG bestehen. Marktordnungsrechtlich dürfte relevant sein, dass die KI-Modelle we-

25 S. Pukas GRUR 2023, 614; von Welser GRUR-Prax 2023, 516; Pech/Böhme GRUR 2023, 997; Dornis GRUR 2024, 1676; De la Durantaye ZUM 2023, 645; Maarmar ZUM 2023, 481; Kraetzig NJW 2024, 697.

26 Ebenso Policy Department for Justice, Civil Liberties and Institutional Affairs Directorate-General for Citizens' Rights, Justice and Institutional Affairs, PE 774.095 – July 2025, S. 10, 24, 29, 40 ff., 50 (abrufbar unter: [https://www.europarl.europa.eu/thinktank/en/document/IUST_STU\(2025\)774095](https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)774095)).

27 BT-Drs. 19/27426, 88; Erwägungsgrund 18 DSM-RL.

28 Zum Text and Data Mining Reservation Protocol des World Wide Web Consortium s. BeckOK Urheberrecht/Bomhard, 48. Ed. 2025, UrhG § 44b Rn. 35 f.; von Welser GRUR-Prax 2023, 516 (518); Baumann NJW 2023, 3673 (3675); Schack NJW 2024, 113 (117); Dornis GRUR 2024, 1676 (1685); Policy Department for Justice, Civil Liberties and Institutional Affairs Directorate-General for Citizens' Rights, Justice and Institutional Affairs, PE 774.095 – July 2025, S. 44 (abrufbar unter: [https://www.europarl.europa.eu/thinktank/en/document/IUST_STU\(2025\)774095](https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)774095)).

29 S. Stieper/Denga GRUR 2024, 1473.

30 von Welser GRUR-Prax 2023, 516 (517 f.) notiert, dass die DSM-RL aus 2019 deutlich vor allgemeinem Bekanntwerden der Möglichkeiten generativer KI im Jahr 2022 verabschiedet wurde.

31 RL 2001/29/EG des Europäischen Parlaments und des Rates v. 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. L 167 v. 22.6.2001, 10.

32 Zu den Vorlagefragen BeckEuRS 2025, 771662.

33 Hierzu Dreier/Schulze, UrhG/Raue, 8. Aufl. 2025, UrhG § 23 Rn. 144; BeckOK Urheberrecht/Lauber-Rönsberg, 48. Ed. 2025, UrhG § 23 Rn. 24; Wandtke/Bullinger, Urheberrecht/Bullinger, 6. Aufl. 2022, UrhG § 23 Rn. 46.

34 Auch zur Ausgabe von Arbeitsergebnissen wurde dem EuGH in der Rs. C-250/25 (Like Company/Google) die Frage vorgelegt, ob die Anzeige eines Texts in der Antwort eines Chatbots, der teilweise mit einem geschützten Presseinhalt identisch ist, eine öffentliche Wiedergabe gem. Art. 3 InfoSoc-RL ist.

35 Zur Anwendung von § 19a UrhG auf Dienste, die nicht von Deutschland aus angeboten werden, Beurskens RD 2025, 1.

36 Hierzu Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 19a Rn. 1.

37 S. Hofmann WRP 2024, 11 (17); Steinrötter/Borchert CR 2024, 558 (562); Lejeune ITRB 2025, 99 (103); Dreier/Schulze, UrhG/Raue 8. Aufl. 2025, UrhG § 23 Rn. 37.

38 BGH GRUR 1988, 812 (813 f.) – Ein bisschen Frieden; OLG Köln GRUR 2000, 43 (44 ff.) – Klammerpose; KG GRUR-RR 2001, 292 (293) – Bachforelle.

39 LG München I MMR 2026, 74 mAnm Gierschmann.

40 S. Nordemann/Rasouli ZUM 2024, 780.

41 Für die Einordnung von Art. 53 Abs. 1 lit. c KI-VO als Schutzgesetz, Nordemann/Rasouli ZUM 2024, 780 (782 ff.).

42 S. Grüneberg, BGB/Sprau, 85. Aufl. 2026, BGB § 823 Rn. 72 mit Verweis auf ein Urteil aus der Zeit vor dem Inkrafttreten des UrhG.

43 Zu den Anforderungen an die Feststellung eines Schutzgesetzes BGH BeckRS 2008, 07112 (Rn. 20); BGH NJW 1976, 1740 (1740 f.); BeckOK BGB/Förster, 1.2. 2025, § 823, Rn. 267; Jauernig, BGB/Kern, 19. Aufl. 2023, BGB § 823 Rn. 40; Sebastian ZBB 2014, 382 (383).

sentlich auf Inhalten und Leistungen Dritter beruhen. Dies gilt insbesondere, soweit die Verwendung dieser Inhalte – beim Training oder Betrieb der KI-Modelle – die Refinanzierung der Inhalte-Angebote beeinträchtigen und damit zu einer relevanten⁴⁴ Marktbeeinträchtigung führen kann.

Die diskutierte Einführung einer Digitalsteuer⁴⁵ ändert daran nichts. Die entsprechende Planung auf Ministeriumsebene begründet keinen gesetzgeberischen Willen, der wettbewerbsrechtliche Ansprüche ausschließt. Zusätzlich können Ansprüche auch aus dem GWB, ggf. iVm Art. 6 DMA folgen, wie das Urteil des LG Frankfurt/M. v. 10.9.2025 zeigt.⁴⁶ Ebenfalls ordnungsrechtlich ist darüber hinaus ein Vorgehen der Medienanstalten gem. MStV bzw. DSA gegen die Anbieter von KI-Modellen denkbar.⁴⁷

III. Prozessuale Durchsetzung

1. Urheber und andere Rechteinhaber

Bei der Geltendmachung von Ansprüchen durch Urheber und Inhaber von Leistungsschutzrechten bestehen grundsätzlich keine prozessualen Besonderheiten. Insbesondere wurde der parallel zu den Entwürfen der KI-VO vorbereitete Vorschlag für eine Richtlinie zur KI-Haftung,⁴⁸ mit Beweiserleichterungen für Klagen gegen Anbieter von KI-Modellen, zurückgezogen.⁴⁹

Angeichts der Ausgestaltung der KI-Systeme als Black Box wird, soweit Informationen nicht aufgrund der Publizitätspflichten aus der KI-VO⁵⁰ vorliegen, eine gestufte Darlegungs- und Beweislast greifen, sodass dem Anbieter des KI-Systems eine entsprechende Darlegungslast obliegt. Zusätzlich kommen urheberrechtliche (§ 101 UrhG) und allgemeine (§ 242 BGB) Auskunftsansprüche sowie Vorlage- und Besichtigungsansprüche gem. §§ 101a f. UrhG in Betracht, die isoliert voneinander durchsetzbar sind. Die Auffassung, der Vorlage- und Besichtigungsanspruch gem. § 101a UrhG sei entbehrlich, sobald Auskunftsansprüche gem. § 101 UrhG die erforderlichen Informationen liefern,⁵¹ ist abzulehnen. Dagegen spricht insbesondere, dass beide Ansprüche unterschiedliche Anforderungen an die Wahrscheinlichkeit bzw. das Feststehen einer Rechtsverletzung stellen.⁵²

2. Verwertungsgesellschaften, -einrichtungen und Urhebervereinigungen

a) Verwertungsgesellschaften

Bei der Geltendmachung von Ansprüchen durch Verwertungsgesellschaften ist prozessual insbesondere § 128 VGG zu berücksichtigen, wonach die gerichtliche Geltendmachung von Ansprüchen erst nach Befassung der Schiedsstelle gem. § 92 Abs. 1 Nr. 1 VGG zulässig ist. Laut BGH gilt dies auch für Schadensersatzansprüche, soweit der Vermögensschaden anhand der üblichen tariflichen Lizenzgebühr berechnet werden soll.⁵³ In dem vom LG München I entschiedenen Fall spielte der Schiedsstellenvorbehalt wohl deswegen keine Rolle, weil die GEMA nicht aus eigenem Recht vorging, sondern in Prozessstandschaft für einzelne Urheber,⁵⁴ sodass keine Tarifrelevanz iSv §§ 128 Abs. 1, Abs. 2 S. 1 VGG bestand.

b) Abhängige und unabhängige Verwertungseinrichtungen

Für abhängige Verwertungseinrichtungen iSv § 3 VGG gelten die Ausführungen unter III.2.a) gem. § 3 Abs. 2 S. 1 VGG entsprechend. Für unabhängige Verwertungseinrichtungen, dh Einrichtungen der kollektiven Rechtswahrnehmung mit Gewinnerzielungsabsicht, gelten die o.g. Einschränkungen nicht.

c) Urhebervereinigungen

Auch Urhebervereinigungen können Anspruchsteller sein, zB mit Unterlassungsansprüchen gem. § 36b UrhG. Handelt eine

Verwertungsgesellschaft als Urhebervereinigung, können die Einschränkungen gem. § 128 VGG greifen, wie oben (III.2.a)) dargestellt. Dass Verwertungsgesellschaften trotz Repräsentativität und Ermächtigung keine Urhebervereinigungen sein können, weil sie nicht unabhängig bzw. gegnerfrei sind,⁵⁵ ist angesichts der Vorgaben der DSM-RL mittlerweile nicht mehr haltbar: Die DSM-RL stellt auf Vertreter der Urheber ab. Vertreter kann gem. Erwägungsgrund 78 DSM-RL jede Person sein, die nach nationalem und Unionsrecht wirksam bestellt wurde. Eine Unabhängigkeit bzw. Gegnerfreiheit ist laut DSM-RL keine Voraussetzung für diese Vertretereigenschaft. Daher ist § 36 Abs. 2 UrhG jedenfalls unionsrechtskonform dahingehend auszulegen, dass auch eine Verwertungsgesellschaft eine Urhebervereinigung sein kann.

Dies entspricht auch dem Zweck der DSM-RL. Laut Erwägungsgrund 3 DSM-RL soll die Stellung der Urheber gestärkt und eine effektivere Rechtsdurchsetzung sichergestellt werden.⁵⁶ Dem widerspräche es, wenn die Rechtsdurchsetzung einer – in der DSM-RL nicht vorgesehenen – unabhängigen bzw. gegnerfreien Vereinigung vorbehalten wäre. Die deutsche Gesetzesbegründung zu § 36 UrhG steht dem nicht entgegen, da diese aus einer Zeit deutlich vor Inkrafttreten der DSM-RL stammt.⁵⁷ Auch das zum 7.6.2021 in Kraft getretene Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarkts war vom Bestreben des deutschen Gesetzgebers getragen, die unionsrechtlichen Vorgaben umzusetzen.⁵⁸ Daher entspricht die unionsrechtskonforme Auslegung von § 36 UrhG auch dem gesetzgeberischen Willen.⁵⁹

3. Passivlegitimation

a) Anbieter des KI-Modells

■ **Einzelanbieter:** Beim Vorgehen gegen Einzelanbieter bestehen prinzipiell keine prozessualen Besonderheiten. Häufig wird es sich bei den Anbietern um Unternehmen mit Sitz außerhalb Deutschlands handeln, dh mit internationaler Zustellung.

■ **Anbieter im Konzernverbund:** Treten mehrere Personen als Anbieter des KI-Modells auf bzw. ist Anbieter in Deutschland eine Konzerngesellschaft, kann es für den Rechteinhaber zielführend sein, sogleich (auch) gegen eine oder mehrere Konzerngesellschaften vorzugehen, zumal wenn die AGB des Anbieters

⁴⁴ Zur wohlfahrtsökonomischen Betrachtung Harte-Bavendamm/Henning-Bode-wig, UWG/Sambuc, 5. Aufl. 2021, UWG § 4 Rn. 110.

⁴⁵ <https://rsw.beck.de/aktuell/daily/meldung/detail/digitalabgabe-google-meta-kulturminister-weimer-plattform-soli-digitalsteuer>.

⁴⁶ LG Frankfurt/M. MMR 2026, 442 mAnM Mendelsohn.

⁴⁷ <https://www.heise.de/news/KI-Uebersichten-Medienwaechter-nehmen-Goog-le-und-Perplexity-ins-Visier-11165485.html>.

⁴⁸ <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0496>.

⁴⁹ ZB gem. Art. 53 Abs. 1 lit. d KI-VO.

⁵⁰ Zu den Publizitätspflichten der KI-VO s. Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 2 ff.; Roos/Voget RdI 2024, 478 (490).

⁵¹ Wandtke/Bullinger, Urheberrecht/Ohst, 6. Aufl. 2022, UrhG § 101a Rn. 16.

⁵² LG Hamburg Urt. v. 22.6.2018 – 308 O 343/16; Dreier/Schulze, UrhG/Dreier, 8. Aufl. 2025, UrhG § 101a Rn. 4.

⁵³ BGH GRUR 2000, 872 (874) – Schiedsstellenanrufung.

⁵⁴ S. LG München I MMR 2026, 74 Rn. 6 ff. und Rn. 141 ff. mAnM Gierschmann.

⁵⁵ S. Dreier/Schulze, UrhG/Mantz, 8. Aufl. 2025, UrhG § 36 Rn. 21.

⁵⁶ Hierzu auch Dreier/Schulze, UrhG/Mantz, 8. Aufl. 2025, UrhG § 36 Rn. 3; Pfeifer ZUM 2019, 648, Frosio IIC 2020, 709.

⁵⁷ BT-Drs. 14/6433, 17 mit der Begründung des § 36 UrhG zum 1.1.2002; die DSM-RL v. 17.4.2019 wurde am 17.5.2019 im Amtsblatt der EU veröffentlicht und war bis zum 7.6.2021 umzusetzen.

⁵⁸ Der Gesetzentwurf (BT-Drs. 19/27426) erwähnt die unionsrechtlichen Vorgaben und § 36 UrhG, enthält jedoch keine Anhaltspunkte, dass der Gesetzgeber sich über das Unionsrecht hinwegsetzen wollte.

⁵⁹ Zu dieser Auslegungsgrenze BGH NJW 2009, 427 Rn. 21 (= MMR 2009, 214 (Ls.)) – Quelle; der erkennbare Willens des deutschen Gesetzgebers, eine unionsrechtskonforme Regelung zu gestalten (zum Kriterium BGH NJW 2009, 427 Rn. 25), gibt hinreichende Anhaltspunkte für die unionsrechtskonforme Auslegung von § 36 Abs. 2 UrhG.

eine konzernweite Nutzung vorsehen. Ein entsprechendes Vorgehen kommt in Betracht, wenn eine Konzern-Gesellschaft Nutzungshandlungen vornimmt oder unterstützt, sowie – in eng begrenzten Ausnahmefällen – wenn (gesellschaftsrechtliche) Durchgriffskonstellationen eine Haftung der Obergesellschaft rechtfertigen.⁶⁰

b) (Vertriebs-)Partner des Anbieters

Je nach Einbindung in das Angebot können auch andere Personen als der Anbieter des KI-Modells in Anspruch genommen werden, zB Anbieter spezialisierter KI-Dienste, die auf einer Nutzung allgemeiner KI-Modelle beruhen. Inhalt und Umfang der Verantwortlichkeit hängt dann vom konkreten „Tatbeitrag“ des Dritten ab. Dieser ist jeweils möglichst konkret darzulegen, auch um die sekundäre Darlegungslast auszulösen.

c) Nutzer

Auch eine Verantwortlichkeit der Nutzer kommt in Betracht. Dies wird insbesondere nicht durch das Urteil des LG München I v. 11.11.2025 ausgeschlossen. Das LG München I hat nur entschieden, dass OpenAI sich nicht auf ein (alleiniges) Handeln der Nutzer durch Eingabe der Prompts berufen und damit die eigene Verantwortlichkeit ausschließen kann. Ein (nachweisbares) rechtsverletzendes Nutzerverhalten kann wiederum Ansprüche gegen den Anbieter des KI-Systems auslösen, zB bei der Förderung eines rechtswidrigen Nutzerverhaltens als Teilnehmer.⁶¹

IV. Nutzerperspektive

Auch aus Nutzersicht sind urheberrechtliche Aspekte zu berücksichtigen.

1. Lizenzierung eigener Rechte

Die Eingabe von Daten unterfällt regelmäßig den AGB des Anbieters (soweit wirksam vereinbart, was nicht notwendig nach deutschem Recht zu bewerten ist⁶²). Die AGB enthalten häufig, gerade in den Grund- bzw. Basis-Modellen Nutzungsrechte zugunsten des Anbieters, zumindest für die umfassende Nutzung iRd KI-Modells. Insoweit verliert der Rechteinhaber die Kontrolle über die Verwendung der betreffenden Schutzgüter. Soweit Rechteinhaber und Nutzer nicht personenidentisch sind und der Nutzer nicht berechtigt ist, Lizenzen zu erteilen, ist das Nutzungsrecht zwar nach deutschen UrhG unwirksam, da es keinen gutgläubigen Erwerb von Nutzungsrechten gibt.⁶³ Die Durchsetzung etwaiger Unterlassungs- und Schadensersatzansprüche gegen den Anbieter dürfte jedoch – unabhängig von einer etwaigen Duldung bzw. einem etwaigen Mitverschulden des Rechteinhabers im Hinblick auf das Nutzerhandeln – mit erheblichen (u.a. Nachweis-)Schwierigkeiten verbunden sein. Auch

deswegen ist eine unternehmensinterne Richtlinie, die den Einsatz von KI-Modellen regelt, zu empfehlen.

2. Werkcharakter

Werke entstehen nur durch menschliche Gestaltung als persönliche geistige Schöpfungen, § 2 Abs. 2 UrhG. Werkschöpfungen durch KI-Systeme als Urheber sind daher ausgeschlossen.⁶⁴ Aus dem Schwarz-Weiß zwischen maschineller und menschlicher Erzeugung kann beim Einsatz von KI-Systemen im kreativen Prozess ein unübersichtliches Grau werden. Wird ein Text zB nach seiner Erstellung durch den Autor mittels KI auf seine Konsistenz geprüft, behält der betreffende Text regelmäßig auch bei Übernahme der Verbesserungsvorschläge seinen Werkcharakter, weil die Änderungen im Wesentlichen technischer Natur sind. Auch die – algorithmusbasierte – Rechtschreibkorrektur und Grammatikkontrolle sowie Anmerkungen zur besseren Verständlichkeit von Texten in Textverarbeitungsprogrammen führt üblicherweise nicht dazu, dass der betreffende Text seinen Werkcharakter verliert.

Ist ein Text jedoch KI-generiert und hat der Autor nur geringfügige Änderungen vorgenommen, fehlt der Werkcharakter gem. § 2 Abs. 2 UrhG. Und bei Texten, bei denen sich wesentliche Autorenbeiträge und wesentliche KI-Beiträge nicht trennen lassen, wird eine – auch wertende – Betrachtung erforderlich sein, um festzustellen, ob der Text Werkcharakter hat. Prinzipiell ist der Werkcharakter, sofern streitig, im gerichtlichen Verfahren objektiv zu bestimmen.⁶⁵ Dies gilt gleichermaßen für die weiteren Werkarten gem. § 2 Abs. 1 UrhG.

Aus Nutzersicht sollte die Erfüllung von § 2 Abs. 2 UrhG angemessen dokumentiert werden, um den Werkcharakter ggf. nachweisen zu können, zB mit Speicherung von Entwürfen, Dokumentation von Konzepten, zumal es keine „Werkvermutung“ zugunsten der Urheber gibt – § 10 UrhG betrifft nur die Urheber- oder Rechtsinhaberschaft.⁶⁶

Schnell gelesen ...

- Anbieter und Nutzer der KI-Modelle benötigen die Zustimmung der Rechteinhaber, soweit sie Nutzungshandlungen (zB Vervielfältigungen) vornehmen, ohne sich auf gesetzliche Schranken berufen zu können.
- Das Territorialitätsprinzip führt nicht notwendig dazu, dass das deutsche UrhG unanwendbar ist; bei der öffentlichen Zugänglichmachung von Arbeitsergebnissen auch in Deutschland liegt dies auf der Hand (§ 19a UrhG).
- Bei der gerichtlichen Durchsetzung etwaiger Ansprüche kommt der sekundären Darlegungslast der Anbieter von KI-Modellen eine besondere Rolle zu, da die KI-Modelle bewusst und gewollt als „Black Box“ ausgestaltet sind.
- Auch für die Nutzer bestehen erhebliche Risiken. So droht ein Rechtsverlust an den Anbieter des KI-Modells und kann der Einsatz von KI-Modellen im Schaffensprozess dazu führen, dass es ganz oder teilweise an der persönlichen geistigen Schöpfung fehlt, also statt einem schutzfähigen Werk urheberrechtliches Allgemeingut vorliegt.

⁶⁰ Emmerich/Habersack, Konzernrecht/Lüdeking, 12. Aufl. 2023, § 20 Rn. 25 f.; zur (entsprechenden) Durchgriffshaftung s. Eilers/Gleske, Handbuch Unternehmensfinanzierung/Hasselbach/Alles, 2024, Kap. 9 Rn. 17 und Kindler/Nachmann/Bitzer, Hdb Insolvenzrecht in Europa/Schilling, 13. Aufl. 2023, Kap. 9 Rn. 412 ff.

⁶¹ Eine allg. Kenntnis möglicher Urheberrechtsverletzungen durch Nutzer genügt zur Begründung des Vorsatzes regelmäßig nicht, s. OLG München BeckRS 2017, 108792; auch ohne Vorsatz kommt dann ggf. eine Störerhaftung in Betracht (hierzu Dreier/Schulze, UrhG/Specht/Riemenschneider, 8. Aufl. 2025, UrhG § 97 Rn. 28 f., auch zum möglichen Ausschluss einer Störerhaftung laut EuGH MMR 2021, 705 – YouTube).

⁶² S. zu Verbraucher-Verträgen Art. 6 der Rom I-VO.

⁶³ BGH GRUR 1959, 200 (203) – Der Heiligenhof.

⁶⁴ S. Hofmann WRP 2024, 11 (15); Dreier/Schulze, UrhG/Raue, 8. Aufl. 2025, UrhG § 2 Rn. 21, 25.

⁶⁵ BGH GRUR 1988, 812 (814); lt. Dreier/Schulze, UrhG/Raue, 8. Aufl. 2025, UrhG § 2 Rn. 46, also „von Amts wegen zu prüfen“. Aktuell dazu: AG München MMR 2026, 348 mAnm Howe/Bald.

⁶⁶ Hierzu Dreier/Schulze, UrhG/Mantz, 8. Aufl. 2025, UrhG § 2 Rn. 6; Schricker/Loewenheim, Urheberrecht/Loewenheim/Leistner, 6. Aufl. 2020, § 2 Rn. 32 ff.; EuGH GRUR 2019, 73 Rn. 35–37 – Levola Hengelo; zum Nachweis: LG Frankfurt/M. UrT. v. 17.2.2025 – 2-06 401/25.



Dr. Wolfgang Frhr. Raitz von Frentz
ist Rechtsanwalt und Partner bei McDermott Will & Schulte Rechtsanwälte Steuerberater LLP in München.



Dr. Christian L. Masch
ist Rechtsanwalt und Partner bei McDermott Will & Schulte Rechtsanwälte Steuerberater LLP in München.

Vom Bestellbutton über den Kündigungsbutton zum Widerrufsbutton

Die Widerrufsfunktion für Fernabsatzverträge

Verbraucherschutz

Neben einem Bestell- und Kündigungsbutton ist ab dem 19.6.2026 für über eine Online-Benutzeroberfläche geschlossene Fernabsatzverträge ein Widerrufsbutton in Form einer Widerrufsfunktion vorzuhalten, um Verbrauchern die Ausübung ihres Widerrufsrechts zu erleichtern. Der Beitrag erläutert die aus

der Neuregelung resultierenden Gestaltungsanforderungen sowie die möglichen Rechtsfolgen bei Verstößen und untersucht, inwieweit sich die für den Bestellbutton und den Kündigungsbutton entwickelten Maßstäbe auf die Widerrufsfunktion übertragen lassen.

Lesedauer: 22 Minuten

I. Einleitung

1. Hintergrund der Regelung

Die durch die Fernabsatz-Finanzdienstleistungs-RL¹ neu eingefügte Regelung des Art. 11a Verbraucherrechte-RL (VRRL) verlangt für über eine Online-Benutzeroberfläche geschlossene Fernabsatzverträge, dass der Verbraucher den Vertrag auch über eine Widerrufsfunktion widerrufen können muss. Mit diesem Widerrufsbutton soll der Widerruf eines Vertrags genauso einfach möglich sein wie der Abschluss, indem das Bewusstsein der Verbraucher für ihr Widerrufsrecht gestärkt und dessen Ausübung vereinfacht wird.² Die deutsche Umsetzung in § 356a BGB³ erfolgte in enger Orientierung an der Richtlinienvorgabe.

Neu eingefügt wurde zudem die Pflicht des Unternehmers, den Verbraucher über das Bestehen und die Platzierung der Widerrufsfunktion zu belehren (Art. 6 Abs. 1 lit. h VRRL, umgesetzt in Art. 246a § 1 Abs. 2 S. 1 Nr. 1 EGBGB), sowie ein Hinweis auf die Widerrufsfunktion in Gestaltungshinweis 3 der Muster-Widerrufsbelehrung (Anhang I VRRL, umgesetzt in Anlage 1 zu Art. 246a § 1 Abs. 2 S. 2 EGBGB). Die neuen Regelungen sind nach Art. 2 Abs. 1 UAbs. 2 Fernabsatz-Finanzdienstleistungs-RL ab dem 19.6.2026 anzuwenden.

2. Verwandte Vorschriften

Nach § 312j Abs. 3 iVm Abs. 2 BGB hat der Unternehmer die Bestellsituation bei einem Verbrauchervertrag im elektronischen Geschäftsverkehr, der den Verbraucher zur Zahlung verpflichtet, so zu gestalten, dass der Verbraucher mit seiner Bestellung ausdrücklich bestätigt, sich zu einer Zahlung zu verpflichten. Diese bereits seit 1.8.2012 geltende Regelung zum Bestellbutton geht auf Art. 8 Abs. 2 UAbs. 2 VRRL zurück und soll dem Verbraucher bewusst machen, dass die Abgabe der Bestellung eine Zahlungspflicht zur Folge hat und ab welchem Zeitpunkt dies der Fall ist.⁴

Seit 1.7.2022 sieht § 312k BGB für entgeltliche Dauerschuldverhältnisse, die im elektronischen Geschäftsverkehr über eine Webseite abgeschlossen werden können, die Möglichkeit zur Kündigung über eine Kündigungsschaltfläche vor. Mit diesem Kündigungsbutton will der Gesetzgeber erreichen, dass die Kündigung eines online geschlossenen Vertrags genauso leicht möglich ist wie dessen Abschluss.⁵ Anders als der Bestellbutton und die Widerrufsfunktion beruht der Kündigungsbutton nicht auf einer unionsrechtlichen Vorgabe, sondern ist eine rein nationale Regelung.⁶ Die für den Bestellbutton geltenden Grundsätze können teilweise auf die Widerrufsfunktion übertragen werden. Aufgrund ähnlicher Zielsetzung und Struktur lassen sich aber auch die zum Kündigungsbutton entwickelten Maßstäbe

heranziehen, sofern die Richtlinienvorgaben oder die Besonderheiten des Widerrufsrechts dem nicht entgegenstehen.⁷ Ein solcher Gleichlauf erleichtert zudem den betroffenen Unternehmen die Umsetzung der Gestaltungsvorgaben und den Verbrauchern die Ausübung ihrer Rechte.⁸ Da die in Art. 11a VRRL verwendeten Begriffe unionsautonom auszulegen sind, entscheidet über die Auslegung der Widerrufsfunktion jedoch letztendlich der EuGH.

II. Anwendungsbereich

1. Fernabsatzvertrag

Die Pflicht zur Bereitstellung der Widerrufsfunktion war in einer früheren Fassung der Fernabsatz-Finanzdienstleistungs-RL nur für Fernabsatzverträge über Finanzdienstleistungen vorgesehen,⁹ gilt nun aber für alle Fernabsatzverträge iSd § 312c Abs. 1 BGB, für die ein gesetzliches Widerrufsrecht vorgesehen ist.¹⁰ Wie beim Kündigungsbutton¹¹ ist der Unternehmer daher nur dann von der Pflicht zur Bereitstellung einer Widerrufsfunktion befreit, wenn für die von ihm angebotenen Verträge überhaupt kein Widerrufsrecht besteht.

2. Vertragsschluss über Online-Benutzeroberfläche

Der ebenfalls durch die Fernabsatz-Finanzdienstleistungs-RL neu eingefügte Art. 16e VRRL verweist für den Begriff der Online-Benutzeroberfläche auf Art. 3 lit. m DSA,¹² der diese als Software, darunter auch Webseiten oder Teile davon sowie Anwendungen, einschließlich Mobil-Apps, definiert. Erwägungsgrund 15 S. 2 Fernabsatz-Finanzdienstleistungs-RL ergänzt die möglichen Erscheinungsformen um Chatbots, Robo-Advice, interaktive Tools oder ähnliche Mittel. Der Begriff Online-Benut-

¹ RL (EU) 2023/2673.

² Erwägungsgrund 37 S. 2 und 13 Fernabsatz-Finanzdienstleistungs-RL.

³ BGBl. 2026 I 28.

⁴ Erwägungsgrund 39 S. 3 und S. 4 VRRL.

⁵ MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 1; BT-Drs. 19/30840, 15.

⁶ MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 2.

⁷ Ähnl. Wiebe/Sengül WRP 2025, 574 Rn. 4; Billing/Vetter K&R 2024, 387 (389); krit. Rätze WRP 2025, 1398 Rn. 67; Becker/Rätze WRP 2024, 280 Rn. 80.

⁸ Buchmann/Panfilii K&R 2023, 24 (29).

⁹ Zur Entstehungsgeschichte s. Föhlisch/Löwer CR 2024, 116 Rn. 1 ff.

¹⁰ Erwägungsgrund 37 S. 14 Fernabsatz-Finanzdienstleistungs-RL; BT-Drs. 21/1856, 37.

¹¹ MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 11.

¹² In Art. 3 lit. m DSA wird zwar der Begriff „Online-Schnittstelle“ verwendet, da aber etwa die engl. und franz. Sprachfassung in Art. 11a, 16e VRRL und Art. 3 lit. m DSA einheitlich von „online interface“ und „interface en ligne“ sprechen, ist von einem Redaktionsversehen in der deutschen Fassung auszugehen (Wiebe/Sengül WRP 2025, 574 Rn. 5; Becker/Rätze WRP 2024, 280 Rn. 82 f.).

zeroberfläche ist damit zwar weit auszulegen,¹³ umfasst jedoch ähnlich wie bei Bestellbutton¹⁴ und Kündigungsbutton¹⁵ keine individuelle Kommunikation zwischen Verbraucher und Unternehmer, selbst wenn diese wie bei E-Mails und Chat-Nachrichten softwaregestützt erfolgt.¹⁶ Dies ergibt sich daraus, dass die Regelung zur Widerrufsfunktion Massengeschäfte im Blick hat, bei denen der Vertragsschluss weitestgehend automatisiert abläuft.

Für die Anwendbarkeit des neuen § 356a BGB ist nicht erforderlich, dass der Unternehmer Verträge ausschließlich über eine Online-Benutzeroberfläche im Fernabsatz schließt, sodass eine Widerrufsfunktion auch dann bereitzustellen ist, wenn Verträge noch auf anderem Wege geschlossen werden, etwa telefonisch oder im Ladengeschäft. Da die Erklärung des Widerrufs formlos möglich ist,¹⁷ kann die Widerrufsfunktion von dem Verbraucher auch für den Widerruf dieser Verträge genutzt werden.

III. Gestaltungsvorgaben

Wie der Kündigungsbutton sieht auch § 356a BGB einen mehrstufigen Prozess vor: Über eine Widerrufsfunktion (dazu 1.) gelangt der Verbraucher zu einer Widerrufserklärung, die er über eine Bestätigungsfunktion an den Unternehmer senden kann (dazu 2.), und deren Eingang ihm der Unternehmer bestätigt (dazu 3.).

1. Widerrufsfunktion

Der Begriff „Funktion“ ist weder in der Richtlinienvorgabe noch in § 356a BGB definiert. In Anlehnung an den bei Bestellbutton¹⁸ und Kündigungsbutton¹⁹ verwendeten und weit auszulegenden Begriff „Schaltfläche“ können darunter alle Bedienelemente verstanden werden, mit denen der Verbraucher eine Ak-

tion in Gang setzen oder eine Rückmeldung geben kann, wie insbesondere anklickbare Links oder Buttons auf einer Internetseite.

a) Erreichbarkeit

Nach § 356a Abs. 1 S. 3 BGB nF muss die Widerrufsfunktion während des Laufs der Widerrufsfrist auf der Online-Benutzeroberfläche ständig verfügbar, hervorgehoben platziert und für den Verbraucher leicht zugänglich sein.

■ Ständige Verfügbarkeit

Wie die den Kündigungsprozess einleitende Kündigungsschaltfläche des Kündigungsbuttons²⁰ ist auch die Widerrufsfunktion für den Verbraucher dauerhaft zugänglich zu halten, wobei eine kurzzeitige Unerreichbarkeit aufgrund von Wartungsarbeiten oder technischen Störungen nicht schadet.²¹ Das Erfordernis der ständigen Verfügbarkeit während der Widerrufsfrist ist dahingehend zu verstehen, dass die Funktion mindestens während der laufenden Widerrufsfrist erreichbar sein muss, es aber unschädlich ist, wenn sie dauerhaft angezeigt wird.²² Ähnlich wie bei dem Kündigungsbutton²³ ist nicht erforderlich, dass der Unternehmer das Bestehen des Widerrufsrechts für jeden Vertragspartner individuell bestimmt und danach die Sichtbarkeit der Widerrufsfunktion ausrichtet. Aufgrund der verschiedenen maßgeblichen Faktoren (zB Vorliegen der Verbrauchereigenschaft, Zeitpunkt des Warenerhalts, ordnungsgemäße Widerrufsbelehrung) wird eine solche personalisierte Anzeige nicht nur bei einer Gastbestellung ohne Registrierung,²⁴ sondern auch nach einer Anmeldung im Benutzerkonto nicht immer möglich sein.²⁵ Dabei ist auch zu berücksichtigen, dass die VRRl zwar nach Erwägungsgrund 4 S. 2 VRRl ein hohes Verbraucherschutzniveau sicherstellen, gleichzeitig aber auch die Wettbewerbsfähigkeit der Unternehmen fördern soll und diese daher nicht unverhältnismäßig belasten darf.

Eine dauerhafte Verfügbarkeit der Widerrufsfunktion ist auch nicht irreführend, da der durchschnittliche Verbraucher aus dem alleinigen Vorhandensein der Funktion nicht das Bestehen eines Widerrufsrechts in seinem konkreten Fall ableiten wird.²⁶

■ Hervorgehobene Platzierung und leichte Zugänglichkeit

Nach Erwägungsgrund 37 S. 4 Fernabsatz-Finanzdienstleistungs-RL muss die Widerrufsfunktion für den Verbraucher einfach und leicht auffindbar und zugänglich sein. Die Ausübung des Widerrufsrechts ist dem Verbraucher damit so einfach wie möglich zu gestalten, wobei wie iRd Kündigungsbuttons²⁷ auf den durchschnittlichen Verbraucher abzustellen ist. Nach Erwägungsgrund 37 S. 6 Fernabsatz-Finanzdienstleistungs-RL kann der Unternehmer zur Vereinfachung des Verfahrens Hyperlinks bereitstellen, über die der Verbraucher zur Widerrufsfunktion gelangt. Die Verwendung des Plurals („Hyperlinks“) scheint für die Zulässigkeit auch mehrerer Klicks zu sprechen. In diesem Fall wäre die Widerrufsfunktion aber nicht mehr einfach und leicht zugänglich, sodass zu ihrem Aufruf höchstens ein vorausgehender Klick zulässig ist.²⁸ Wie beim Kündigungsbutton²⁹ muss der zu der Widerrufsfunktion führende Link eindeutig beschriftet sein (zB „Widerrufsrecht“)³⁰ und darf nicht in einer Vielzahl anderer Links untergehen.

Für den Kündigungsbutton ist die genaue Platzierung der den Kündigungsprozess einleitenden Kündigungsschaltfläche umstritten. Nach einer Ansicht muss diese sowohl von der Hauptseite als auch jeder Unterseite aus erreichbar sein, da nur dann die Schaltfläche für den durchschnittlichen Verbraucher leicht auffindbar ist.³¹ Eine andere Ansicht lässt die Zugänglichkeit von der Unterseite ausreichen, auf der Bestellprozess beginnt, da der Verbraucher zuerst dort nach einer Kündigungsmöglichkeit suchen wird.³² Bei komplexeren Benutzeroberflächen wird die

13 Wiebe/Sengül WRP 2025, 574 Rn. 5; Rätze WRP 2025, 1398 Rn. 10.

14 § 312j Abs. 5 S. 1 BGB.

15 Spindler/Schuster/Kaesling/Schirmbacher, 5. Aufl. 2026, BGB § 312k Rn. 19.

16 Seiwerth NJW 2026, 945 Rn. 7; Wiebe/Sengül WRP 2025, 574 Rn. 5; Rätze WRP 2025, 1398 Rn. 10. AA Becker/Rätze WRP 2024, 280 Rn. 85.

17 MüKoBGB/Fritsche, 10. Aufl. 2025, BGB § 355 Rn. 48.

18 MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312j Rn. 26; BT-Drs. 17/7745, 12.

19 KG MMR 2026, 529 Rn. 33 – in diesem Heft; KG MMR 2026, 532 Rn. 29 – in diesem Heft; KG MMR 2025, 538 Rn. 28; LG Hamburg MMR 2024, 892 Rn. 17.

20 KG MMR 2026, 532 Rn. 33 – in diesem Heft; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 15; BT-Drs. 19/30840, 18.

21 Föhlisch/Löwer CR 2024, 116 Rn. 7.

22 Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirmbacher, 5. Aufl. 2026, BGB § 356 Rn. 20; Wiebe/Sengül WRP 2025, 574 Rn. 28, 57; Rätze WRP 2025, 1398 Rn. 22, 24; Billing/Vetter K&R 2024, 387 (390); Becker/Rätze WRP 2024, 280 Rn. 93, 96; BT-Drs. 21/1856, 38.

23 MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 11; BT-Drs. 19/30840, 17.

24 Zu der Frage, ob solche Gastbestellungen im Fernabsatz aus datenschutzrechtlichen Gründen ermöglicht werden müssen, s. Britz/Indenhuck ZD 2023, 13 ff.

25 Seiwerth NJW 2026, 945 Rn. 11; Wiebe/Sengül WRP 2025, 574 Rn. 22 ff.; Rätze WRP 2025, 1398 Rn. 20 f.; Billing/Vetter K&R 2024, 387 (390); Becker/Rätze WRP 2024, 280 Rn. 93; Föhlisch/Löwer CR 2024, 116 Rn. 8 ff.; Leischel/Buchmann K&R Beil. 2023, 11 (14 f.).

26 Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirmbacher, 5. Aufl. 2026, BGB § 356 Rn. 20; Seiwerth NJW 2026, 945 Rn. 11; Wiebe/Sengül WRP 2025, 574 Rn. 30; Rätze WRP 2025, 1398 Rn. 23 f.; BT-Drs. 21/1856, 38; aA wohl Billing/Vetter K&R 2024, 387 (390); Becker/Rätze WRP 2024, 280 Rn. 94; Föhlisch/Löwer CR 2024, 116 Rn. 13.

27 KG MMR 2025, 538 Rn. 34 f.; OLG Koblenz MMR 2025, 145 Rn. 14; OLG München MMR 2025, 639 Rn. 28 ff.; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 15.

28 AA Rätze WRP 2025, 1398 Rn. 27 (direkte Erreichbarkeit); Föhlisch/Löwer CR 2024, 116 Rn. 17 (Verlinkung über mehrere Seiten).

29 OLG München MMR 2025, 639 Rn. 28 ff.

30 Wiebe/Sengül WRP 2025, 574 Rn. 11; Föhlisch/Löwer CR 2024, 116 Rn. 17; Leischel/Buchmann K&R Beil. 2023, 11 (15); Buchmann/Panfili K&R 2023, 24 (30).

31 KG MMR 2025, 538 Rn. 34 ff.

32 OLG Celle GRUR-RR 2024, 506 Rn. 15; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 18.

konkrete Bestellseite für den durchschnittlichen Verbraucher jedoch oftmals nicht ohne Weiteres auffindbar sein. Die Widerrufsfunktion muss daher von jeder Unterseite erreichbar sein, damit der Verbraucher sein Widerrufsrecht möglichst einfach ausüben kann.³³

Es bietet sich an, die Widerrufsfunktion selbst oder einen zu dieser führenden, eindeutig beschrifteten Link im Footer der Webseite neben Impressum und Datenschutzhinweisen zu platzieren, wobei darauf zu achten ist, dass die Angaben nicht durch ein Cookie-Banner verdeckt werden. Da der Widerrufsfunktion keine höhere Bedeutung als den übrigen Pflichtangaben zukommt, bedarf es gegenüber diesen keiner gesonderten grafischen Hervorhebung,³⁴ solange die Widerrufsfunktion für den durchschnittlichen Verbraucher nicht zwischen den anderen Angaben untergeht. Dies gilt auch dann, wenn neben der Widerrufsfunktion zusätzlich ein Kündigungsbutton bereitzustellen ist.³⁵

b) Kennzeichnung

Nach § 356a Abs. 1 S. 2 BGB ist die Widerrufsfunktion gut lesbar mit den Worten „Vertrag widerrufen“ oder einer entsprechenden eindeutigen Formulierung zu kennzeichnen. Für die Lesbarkeit kommt es wie iRd Bestellbuttons³⁶ und des Kündigungsbuttons³⁷ darauf an, dass die Beschriftung durch Schriftgröße und Kontrast gut erkennbar ist und von ihr nicht durch grafische Elemente abgelenkt wird.³⁸ Für die Bestimmung der Eindeutigkeit ist entsprechend den Grundsätzen zum Bestellbutton³⁹ auf das Verständnis eines Durchschnittsverbrauchers abzustellen, wobei allein die Beschriftung der Widerrufsfunktion maßgeblich ist. Wie beim Kündigungsbutton⁴⁰ muss für den Verbraucher erkennbar sein, dass über die Widerrufsfunktion der Widerrufsprozess begonnen werden kann, er darf aber nicht davon ausgehen, dass durch das Aktivieren der Funktion bereits der Widerruf erklärt wird.⁴¹ Neben der in § 356a Abs. 1 S. 2 BGB vorgesehenen (und damit sichersten⁴²) Kennzeichnung „Vertrag widerrufen“ dürften bei der Widerrufsfunktion auch Bezeichnungen mit „Widerruf“⁴³, „Weiter zum Widerruf“⁴⁴, „Hier widerrufen“⁴⁵, „Widerruf durchführen“⁴⁶, „Widerrufsprozess beginnen“⁴⁷ oder „Widerruf starten“⁴⁸ eindeutig sein.

2. Widerrufserklärung mit Bestätigungsfunktion

a) Erreichbarkeit

Nach § 356a Abs. 2 S. 2 BGB muss der Verbraucher die für den Widerruf erforderlichen Angaben in oder mit der Widerrufserklärung ohne Weiteres machen oder bestätigen können. In Anlehnung an die Anforderungen für die Bestätigungsseite des Kündigungsbuttons⁴⁹ dürfen keine Zwischenschritte enthalten sein, die den Verbraucher von der Ausübung des Widerrufsrechts abhalten könnten.⁵⁰ Wie beim Kündigungsbutton⁵¹ ist jedoch die Unterbreitung eines Bleibangebots mit verbesserten Konditionen zulässig, sofern der Verbraucher hierdurch nicht unter Druck gesetzt oder vom Widerrufsprozess abgelenkt wird.⁵²

b) Angaben zu Widerruf

§ 356a Abs. 2 S. 3 BGB nennt als Informationen für die Widerrufserklärung den Namen des Verbrauchers, Angaben zur Identifizierung des zu widerrufenden Vertrags oder Vertragsteils sowie ein elektronisches Kommunikationsmittel zur Übermittlung einer Eingangsbestätigung an den Verbraucher.

Als Name des Verbrauchers kommt neben dem bürgerlichen Namen auch ein Benutzername in Betracht, wenn dieser eine eindeutige Identifizierung ermöglicht. Der Vertrag kann über die Bestell-, Rechnungs- oder Vertragsnummer identifiziert werden.⁵³ Nach Erwägungsgrund 37 S. 10 Fernabsatz-Finanzdienstleistungs-RL kann der Unternehmer dem Verbraucher

auch die Möglichkeit eines Teilwiderrufs einräumen, wenn der abgeschlossene Vertrag mehrere Waren oder Dienstleistungen umfasst. § 356a Abs. 2 Nr. 2 BGB sieht daher, anders als die Richtlinienvorgabe, ausdrücklich die mögliche Angabe des zu widerrufenden Vertragsteils vor. Eine elektronische Übermittlung der Eingangsbestätigung kann insbesondere an die E-Mail-Adresse des Verbrauchers oder seine Mobilfunknummer (zB per SMS) erfolgen. Wie beim Kündigungsbutton⁵⁴ dürfen vom Unternehmer keine über den Katalog des § 356a Abs. 2 S. 3 BGB hinausgehenden Angaben abgefragt werden,⁵⁵ um dem Verbraucher einen möglichst unkomplizierten Widerruf zu ermöglichen und dem Grundsatz der Datensparsamkeit aus Art. 5 Abs. 1 lit. c DS-GVO Rechnung zu tragen.

§ 356a Abs. 2 BGB sieht neben der Bereitstellung auch die Möglichkeit zur Bestätigung der für den Widerruf erforderlichen Informationen vor. Nach Erwägungsgrund 37 S. 8 Fernabsatz-Finanzdienstleistungs-RL soll ein Verbraucher, der sich bereits identifiziert hat (zB durch Einloggen), den Vertrag widerrufen können, ohne sich oder den zu widerrufenden Vertrag erneut identifizieren zu müssen. Teilweise wird daraus gefolgert, dass bei einem im Kundenkonto angemeldeten Verbraucher die dort gespeicherten Angaben automatisch in die Widerrufserklärung übernommen werden müssen.⁵⁶ Dies würde jedoch für den Unternehmer nicht nur zusätzlichen technischen Aufwand bedeuten,⁵⁷ sondern könnte auch in den Fällen zu Problemen führen, in denen der Verbraucher mit dem Unternehmer mehrere Verträge geschlossen hat.⁵⁸ Zu berücksichtigen ist auch, dass die

33 So auch Wiebe/Sengül WRP 2025, 574 Rn. 10; Rätze WRP 2025, 1398 Rn. 28; Billing/Vetter K&R 2024, 387 (389); Leischel/Buchmann K&R Beil. 2023, 11 (15); Buchmann/Panfilii K&R 2023, 24 (28, 30); BT-Drs. 21/1856, 37.

34 Wohl auch Buchmann/Panfilii K&R 2023, 24 (28); aA Seiwert NJW 2026, 945 Rn. 8; Wiebe/Sengül WRP 2025, 574 Rn. 11; Rätze WRP 2025, 1398 Rn. 26; BT-Drs. 21/1856, 37.

35 AA Wiebe/Sengül WRP 2025, 574 Rn. 52; wohl auch Becker/Rätze WRP 2024, 280 Rn. 92.

36 LG Leipzig BeckRS 2013, 13273; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312j Rn. 27; BT-Drs. 17/7745, 12.

37 OLG München MMR 2025, 639 Rn. 22 f.; KG MMR 2025, 538 Rn. 35.

38 Wiebe/Sengül WRP 2025, 574 Rn. 11; Rätze WRP 2025, 1398 Rn. 14; BT-Drs. 21/1856, 37.

39 EuGH MMR 2022, 550 Rn. 28 ff. – Fuhrmann-2/B.

40 MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 17; BT-Drs. 19/30840, 17.

41 Leischel/Buchmann K&R Beil. 2023, 11 (15); Buchmann/Panfilii K&R 2023, 24 (30).

42 Wiebe/Sengül WRP 2025, 574 Rn. 7; Rätze WRP 2025, 1398 Rn. 16.

43 Vgl. LG Hamburg MMR 2024, 892 Rn. 16.

44 Vgl. MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 17.

45 Vgl. MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 17.

46 Vgl. Spindler/Schuster/Kaesling/Schirnbacher, 5. Aufl. 2026, BGB § 312k Rn. 24.

47 Vgl. Stiegler VuR 2021, 443 (447).

48 Wiebe/Sengül WRP 2025, 574 Rn. 7; Rätze WRP 2025, 1398 Rn. 16; Leischel/Buchmann K&R Beil. 2023, 11 (15); Buchmann/Panfilii K&R 2023, 24 (30).

49 LG Hamburg MMR 2024, 892 Rn. 19.

50 Wiebe/Sengül WRP 2025, 574 Rn. 33 f.; wohl auch Stiegler NJW 2024, 2769.

51 Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirnbacher, 5. Aufl. 2026, BGB § 312k Rn. 32, 55. Krit. MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 25.

52 Wiebe/Sengül WRP 2025, 574 Rn. 33. Offengelassen von Föhlisch/Löwer CR 2024, 116 Rn. 23.

53 Rätze WRP 2025, 1398 Rn. 34; Billing/Vetter K&R 2024, 387 (390); Föhlisch/Löwer CR 2024, 116 Rn. 21; Buchmann/Panfilii K&R 2023, 24 (30).

54 MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 19; BT-Drs. 19/30840, 18; weitergehend Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirnbacher, 5. Aufl. 2026, BGB § 312k Rn. 35 (weitere freiwillige Angaben zulässig).

55 Wiebe/Sengül WRP 2025, 574 Rn. 14, 40; Rätze WRP 2025, 1398 Rn. 31; Billing/Vetter K&R 2024, 387 (390).

56 Rätze WRP 2025, 1398 Rn. 43; Föhlisch/Löwer CR 2024, 116 Rn. 22. Davon zu trennen ist die unter IV.2. behandelte Frage, ob für den Zugang zur Widerrufsfunktion ein verpflichtendes Anmeldeerfordernis vorgesehen werden darf.

57 Rätze WRP 2025, 1398 Rn. 43.

58 Föhlisch/Löwer CR 2024, 116 Rn. 22.

VRRL zwar nach Erwägungsgrund 4 S. 2 VRRL ein hohes Verbraucherschutzniveau sicherstellen, gleichzeitig aber auch die Wettbewerbsfähigkeit der Unternehmen fördern soll. Eine automatische Übernahme der Angaben aus dem Benutzerkonto in die Widerrufserklärung sollte daher nicht zwingend erforderlich, sondern lediglich optional sein.⁵⁹

Das Gesetz schreibt für die Widerrufserklärung keine bestimmten Angaben vor. Um die über die Widerrufsfunktion abgegebene Erklärungen jedoch eindeutig zuordnen und dem Verbraucher den Eingang der Widerrufserklärung nach § 356a Abs. 4 BGB bestätigen zu können, darf der Unternehmer, ähnlich wie iRd Kündigungsbuttons⁶⁰, die in § 356a Abs. 2 S. 3 BGB genannten Informationen als Pflichtangaben ausgestalten. Dafür spricht auch der Wortlaut des § 356a Abs. 3 BGB nF, wonach der Unternehmer dem Verbraucher die Übermittlung der Widerrufserklärung und der Informationen ermöglicht, sobald der Verbraucher diese gem. § 356a Abs. 2 BGB bereitgestellt oder bestätigt hat.

c) Bestätigungsfunktion

Der Unternehmer hat dem Verbraucher nach § 356a Abs. 3 S. 1 BGB nF zu ermöglichen, seine Widerrufserklärung und die Informationen dem Unternehmer mittels einer Bestätigungsfunktion⁶¹ zu übermitteln. Diese muss nach § 356a Abs. 3 S. 2 BGB gut lesbar⁶² und mit „Widerruf bestätigen“ oder einer anderen gleichbedeutenden eindeutigen Formulierung beschriftet sein.

Ähnlich wie beim Kündigungsbutton⁶³ muss für den durchschnittlichen Verbraucher erkennbar sein, dass er mit Betätigen der Bestätigungsfunktion den Widerruf erklärt.⁶⁴ Die in § 356a Abs. 3 S. 2 BGB vorgesehene Beschriftung „Widerruf bestätigen“ ist jedoch weniger eindeutig⁶⁵ als das Pendant „Jetzt kündigen“ in § 312k Abs. 2 S. 3 Nr. 2 BGB oder die ebenfalls für den Kündigungsbutton als ausreichend erachtete Formulierung „Kündigung abschicken“⁶⁶, die in entsprechend angepasster Form („Jetzt widerrufen“⁶⁷, „Widerruf abschicken“) auch als Beschriftung der Widerrufsfunktion möglich sein dürften.⁶⁸

3. Eingangsbestätigung

Nach § 356a Abs. 4 BGB hat der Unternehmer dem Verbraucher nach Aktivierung der Bestätigungsfunktion unverzüglich eine Eingangsbestätigung auf einem dauerhaften Datenträger iSd § 126b S. 2 BGB zu übermitteln, die zumindest den Inhalt der Widerrufserklärung nach § 356a Abs. 2 BGB sowie das Datum und die Uhrzeit ihres Eingangs enthält. Hierfür bietet sich insbesondere eine automatisiert versandte E-Mail an.⁶⁹

Nach § 356a Abs. 5 BGB gilt die Widerrufserklärung des Verbrauchers dem Unternehmer innerhalb der Widerrufsfrist zugegangen, wenn er die Widerrufserklärung vor Fristablauf über die Widerrufsfunktion versandt hat. Wie beim Kündigungsbutton⁷⁰ bezieht sich diese (widerlegbare) Vermutung nur auf den Zugang der Erklärung, nicht aber auf das Bestehen des Widerrufsrechts.⁷¹ Entsprechend sollte der Unternehmer bei der Formulierung darauf achten, nur den Eingang der Erklärung, nicht aber zugleich einen erfolgten Widerruf zu bestätigen.⁷²

IV. Sonderfragen

1. Vertragsschluss über fremde Online-Benutzeroberfläche

Wie beim Kündigungsbutton⁷³ muss die für den Vertragsschluss genutzte Online-Benutzeroberfläche nicht zwingend durch den Unternehmer selbst betrieben werden, sodass die Pflicht zur Bereitstellung einer Widerrufsfunktion auch bei von Dritten angebotenen Verkaufs- und Vermittlungsplattformen besteht.⁷⁴ Vergleichbar mit der Situation beim Kündigungsbutton⁷⁵ ist in einem solchen Fall auch die Widerrufsfunktion auf der Online-Benutzeroberfläche des Dritten vorzuhalten, sodass eine Platzierung nur auf der eigenen Internetseite des Unternehmers nicht ausreicht.⁷⁶ Dafür spricht auch der Wortlaut des § 356a Abs. 1 S. 1 BGB, wonach der Verbraucher auf „der“ Online-Benutzeroberfläche eine Widerrufserklärung über die Widerrufsfunktion abgeben können muss.

Um die Widerrufserklärung in diesen Fällen dem jeweiligen Unternehmer zuordnen zu können, wird vorgeschlagen, den Verbraucher nach Aufruf der Widerrufsfunktion auf der von dem Dritten betriebenen Online-Benutzeroberfläche zunächst seinen Vertragspartner angeben oder auswählen zu lassen.⁷⁷ Problematisch daran ist, dass dies einen nicht in § 356a BGB nF vorgesehen Zwischenschritt bei der Übermittlung der für den Widerruf erforderlichen Informationen an den Unternehmer darstellen könnte.⁷⁸ Da die VRRL nach Erwägungsgrund 4 S. 2 VRRL ein hohes Verbraucherschutzniveau sicherstellen, gleichzeitig aber auch die Wettbewerbsfähigkeit der Unternehmen fördern soll, dürfen die Anforderungen jedoch nicht zu hoch angesetzt werden. Dennoch bleibt der Unternehmer in Bezug auf die ordnungsgemäße Ausgestaltung der Widerrufsfunktion auf die Kooperation mit dem Betreiber der Online-Benutzeroberfläche angewiesen.⁷⁹

2. Verpflichtende Anmeldung in Benutzerkonto

Für den Kündigungsbutton ist umstritten, ob im Prozess zur Abgabe der Kündigungserklärung eine verpflichtende Anmeldung in einem bereits vorhandenen Benutzerkonto vorgesehen werden darf. Eine Ansicht verneint dies, da ein Login-Erfordernis den Verbraucher von der Kündigung abhalten könne, wenn ihm die Zugangsdaten nicht mehr vorliegen.⁸⁰ Eine andere Ansicht erlaubt eine verpflichtende Anmeldung zumindest dann, wenn die vertraglich geschuldete Leistung des Unternehmers nur nach Login im Benutzerkonto erbracht werden kann, da hier davon auszugehen sei, dass der Verbraucher die Anmeldedaten parat habe oder zumindest über die „Passwort vergessen“-Funktion auf einfachem Wege erlangen könne.⁸¹ Weiterhin könnten nach einer Anmeldung im Benutzerkonto die erforder-

⁵⁹ So wohl auch Wiebe/Sengül WRP 2025, 574 Rn. 15.

⁶⁰ MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 24; Stiegler VuR 2021, 443 (448); Sümmernann/Ewald MMR 2022, 713 (716).

⁶¹ Zum Begriff „Funktion“ s. unter 1.

⁶² S. dazu unter 1. b.

⁶³ OLG Köln GRUR-RR 2025, 121 Rn. 31; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 25.

⁶⁴ BT-Drs. 21/1856, 38.

⁶⁵ Krit. auch Rätze WRP 2025, 1398 Rn. 45.

⁶⁶ Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirnbacher, 5. Aufl. 2026, BGB § 312k Rn. 52.

⁶⁷ Buchmann/Panfili K&R 2023, 24 (30).

⁶⁸ AA wohl Leischel/Buchmann K&R Beil. 2023, 11 (16).

⁶⁹ Wiebe/Sengül WRP 2025, 574 Rn. 20; Föhlisch/Löwer CR 2024, 116 Rn. 25.

⁷⁰ Spindler/Schuster/Kaesling, Recht der elektronischen Medien/Schirnbacher, 5. Aufl. 2026, BGB § 312k Rn. 61.

⁷¹ Wiebe/Sengül WRP 2025, 574 Rn. 19.

⁷² Wiebe/Sengül WRP 2025, 574 Rn. 20; Rätze WRP 2025, 1398 Rn. 49; Föhlisch/Löwer CR 2024, 116 Rn. 25; BT-Drs. 21/1856, 38.

⁷³ OLG Hamburg MMR 2025, 543 Rn. 23; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 7; BT-Drs. 19/30840, 16.

⁷⁴ Seiwert NJW 2026, 945 Rn. 3; Rätze WRP 2025, 1398 Rn. 62 f.; Becker/Rätze WRP 2024, 280 Rn. 86; BT-Drs. 21/1856, 38.

⁷⁵ OLG Hamburg MMR 2025, 543 Rn. 24.

⁷⁶ Wiebe/Sengül WRP 2025, 574 Rn. 46; Rätze WRP 2025, 1398 Rn. 64.

⁷⁷ Wiebe/Sengül WRP 2025, 574 Rn. 49; Leischel/Buchmann K&R Beil. 2023, 11 (16).

⁷⁸ Wiebe/Sengül WRP 2025, 574 Rn. 48; Rätze WRP 2025, 1398 Rn. 68.

⁷⁹ Rätze WRP 2025, 1398 Rn. 70; Wiebe/Sengül WRP 2025, 574 Rn. 49.

⁸⁰ KG MMR 2026, 529 Rn. 38 – in diesem Heft; MMR 2026, 532 Rn. 34 – in diesem Heft; OLG Frankfurt/M. NJW-RR 2025, 815 Rn. 24; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 15; BT-Drs. 19/30840, 18.

⁸¹ OLG Nürnberg MMR 2025, 298 Rn. 28.

lichen Angaben vorausgefüllt werden, die ansonsten erst mühsam herausgesucht werden müssten.⁸²

Die Gesetzesbegründung zu § 356a BGB geht davon aus, dass die Widerrufsfunktion grundsätzlich ohne Login erreichbar sein muss, lässt die alleinige Bereitstellung der Widerrufsfunktion im Login-Bereich jedoch ausreichen, wenn und soweit der Vertrag ausschließlich mit der Einrichtung eines Kundenkontos geschlossen werden kann.⁸³

Nach § 356a Abs. 1 S. 3 BGB hat die Widerrufsfunktion ständig verfügbar, hervorgehoben platziert und leicht zugänglich zu sein und muss nach § 356a Abs. 2 BGB dem Verbraucher ermöglichen, ohne Weiteres die für den Widerruf erforderlichen Angaben bereitzustellen oder zu bestätigen. Erwägungsgrund 37 S. 5 Fernabsatz-Finanzdienstleistungs-RL konkretisiert dies dahingehend, dass der Verbraucher nicht erst ein Verfahren durchführen müssen soll, um die Widerrufsfunktion zu finden oder darauf zuzugreifen, wie zB das Herunterladen einer Anwendung, wenn der Vertrag nicht darüber geschlossen wurde. Aber auch eine verpflichtende Anmeldung in einem Benutzerkonto erschwert dem Verbraucher die Ausübung des Widerrufsrechts insbesondere dann, wenn ihm Benutzername und/oder Passwort nicht mehr bekannt sind, sodass die Widerrufsfunktion stets auch ohne Login zugänglich sein muss.⁸⁴ Wie beim Kündigungsbutton⁸⁵ bleibt es dem Unternehmer jedoch unbenommen, zusätzlich zu einer frei zugänglichen Widerrufsfunktion auch eine entsprechende Funktion mit vorausgefüllten Informationen nach Anmeldung im Benutzerkonto vorzusehen.⁸⁶

V. Rechtsfolgen bei Verstößen

Anders als die Regelungen zu Bestellbutton (§ 312j Abs. 4 BGB) und Kündigungsbutton (§ 312k Abs. 6 BGB) enthalten weder Art. 11a VRRl noch § 356a BGB eine Sanktion bei fehlender oder unzureichend umgesetzter Widerrufsfunktion. Dies bedeutet jedoch nicht, dass ein Verstoß ohne rechtliche Konsequenzen bleibt.

1. Verlängerung der Widerrufsfrist

Nach § 356 Abs. 3 S. 1 BGB nF iVm Art. 246a § 1 Abs. 2 S. 1 Nr. 1 EGBGB ist die Unterrichtung des Verbrauchers über das Bestehen und die Platzierung der Widerrufsfunktion Voraussetzung dafür, dass die Widerrufsfrist zu laufen beginnt. Wird eine Widerrufsfunktion gar nicht angeboten, kann der Unternehmer auch nicht ordnungsgemäß über deren Bestehen und Platzierung informieren, sodass sich die Widerrufsfrist nach § 356 Abs. 4 S. 1 BGB auf 12 Monate und 14 Tage verlängert.⁸⁷ Die lediglich fehlerhafte Umsetzung der Widerrufsfunktion führt nach dem Wortlaut von Art. 246a § 1 Abs. 2 S. 1 Nr. 1 EGBGB jedoch nicht zu einer längeren Widerrufsfrist, solange der Unternehmer ordnungsgemäß über Bestehen und Platzierung belehrt.⁸⁸

2. Schadensersatz

Wie beim Kündigungsbutton⁸⁹ kann ein Verstoß gegen § 356a BGB einen Schadensersatzanspruch wegen Verletzung einer vertraglichen Nebenpflicht (§§ 280 Abs. 1, 241 Abs. 2 BGB) begründen, wenn der Verbraucher dadurch von der rechtzeitigen Ausübung seines Widerrufsrechts abgehalten wird.⁹⁰

3. UKlaG

Bei § 356a BGB handelt es sich um ein Verbraucherschutzgesetz für Verträge im Fernabsatz iSd § 2 Abs. 2 Nr. 1 lit. b UKlaG,⁹¹ sodass die in § 3 UKlaG genannten Organisationen (zB Verbraucherverbände) Unterlassungs- und Beseitigungsansprüche nach § 2 Abs. 1 UKlaG geltend machen können.

4. Lauterkeitsrecht

§ 356a BGB stellt wie die Regelungen zu Bestellbutton (§ 312j Abs. 3 BGB)⁹² und Kündigungsbutton (§ 312k BGB)⁹³ eine gesetzliche Vorschrift iSd § 3a UWG dar, die im Interesse der Marktteilnehmer das Marktverhalten regeln soll,⁹⁴ sodass insbesondere auch Mitbewerber Unterlassungs- und Beseitigungsansprüche nach § 8 UWG zustehen können.

Eine Unlauterkeit kann sich auch daraus ergeben, dass der Unternehmer den Verbraucher bei fehlender Widerrufsfunktion nicht ordnungsgemäß nach Art. 246a § 1 Abs. 2 S. 1 Nr. 1 EGBGB über deren Bestehen und Platzierung unterrichtet,⁹⁵ wobei hier aber noch nicht abschließend geklärt ist, ob sich die Ansprüche aus dem Rechtsbruchtatbestand (§ 3a UWG) oder einer Irreführung durch Unterlassen (§ 5a UWG) ergeben.⁹⁶

5. Ordnungswidrigkeit

Eine nicht vorhandene oder nicht nach Maßgabe des § 356a Abs. 1–3 BGB nF umgesetzte Widerrufsfunktion sowie eine nicht nach Maßgabe des § 356a Abs. 4 BGB erfolgte Übermittlung der Eingangsbestätigung kann aufgrund des neu eingefügten Art. 246e § 1 Abs. 2 Nr. 14a EGBGB eine Ordnungswidrigkeit darstellen, wenn es sich um einen weitverbreiteten Verstoß handelt.

VI. Fazit

Der hinter der Widerrufsfunktion stehende Gedanke, Verbrauchern die Ausübung ihres Widerrufsrechts zu erleichtern, verdient grundsätzlich Zustimmung. Doch gut gemeint ist auch in diesem Fall nicht zwangsläufig gut gemacht.

Die Widerrufsfunktion wird teilweise wegen des damit für den Unternehmer verbundenen großen technischen und organisatorischen Aufwands kritisiert,⁹⁷ zudem wird eine Zunahme fehlerhafter oder unberechtigter Widerrufserklärungen erwartet.⁹⁸ Tatsächlich dürften sich die erforderlichen technischen Anpassungen jedoch in Grenzen halten, da eine im Footer verlinkte Unterseite mit einem erweiterten Kontaktformular und automatischer Eingangsbestätigung ausreichen sollte, um die Vorgaben an die Widerrufsfunktion zu erfüllen. Aus organisatorischer Sicht könnte die Widerrufsfunktion sogar zu einer Erleichterung führen, da der Unternehmer darüber strukturierte Widerrufser-

⁸² Spindler/Schuster/Kaesling/Schirmbacher, 5. Aufl. 2026, BGB § 312b Rn. 34, 47.

⁸³ BT-Drs. 21/1856, 38.

⁸⁴ So auch Seiwerth NJW 2026, 945 Rn. 9; Wiebe/Sengül WRP 2025, 574 Rn. 25, 43; Rätze WRP 2025, 1398 Rn. 27, 41 f.; Billing/Vetter K&R 2024, 387 (389 f.); Föhlisch/Löwer CR 2024, 116 Rn. 12.

⁸⁵ OLG Koblenz MMR 2025, 145 Rn. 17; LG München I MMR 2024, 813 Rn. 28; LG Frankfurt/M. CR 2024, 274; LG Köln MMR 2023, 381 Rn. 7; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 16.

⁸⁶ Seiwerth NJW 2026, 945 Rn. 9; Leischel/Buchmann K&R Beil. 2023, 11 (15); Buchmann/Panfilii K&R 2023, 24 (30); Billing/Vetter K&R 2024, 387 (392).

⁸⁷ Seiwerth NJW 2026, 945 Rn. 4; Rätze WRP 2025, 1398 Rn. 80; Wiebe/Sengül WRP 2025, 574 Rn. 36; Billing/Vetter K&R 2024, 387 (388).

⁸⁸ AA Seiwerth NJW 2026, 945 Rn. 4; Wiebe/Sengül WRP 2025, 574 Rn. 36; Billing/Vetter K&R 2024, 387 (389).

⁸⁹ MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 38.

⁹⁰ Billing/Vetter K&R 2024, 387 (389).

⁹¹ Wiebe/Sengül WRP 2025, 574 Rn. 37; Billing/Vetter K&R 2024, 387 (389); Föhlisch/Löwer CR 2024, 116 Rn. 29.

⁹² KG MMR 2020, 480 Rn. 15 f.; OLG München MMR 2019, 249 Rn. 18; OLG Köln MMR 2017, 552 Rn. 12; OLG Hamm MMR 2014, 534 (535).

⁹³ KG MMR 2026, 532 Rn. 22 ff. – in diesem Heft.

⁹⁴ Wiebe/Sengül WRP 2025, 574 Rn. 37; Billing/Vetter K&R 2024, 387 (389); Föhlisch/Löwer CR 2024, 116 Rn. 29.

⁹⁵ Wiebe/Sengül WRP 2025, 574 Rn. 37; Rätze WRP 2025, 1398 Rn. 81; Billing/Vetter K&R 2024, 387 (389); Föhlisch/Löwer CR 2024, 116 Rn. 29.

⁹⁶ Köhler/Feddersen/Köhler/Odörfer, 44. Aufl. 2026, UWG § 3a Rn. 1.19.

⁹⁷ Rätze WRP 2025, 1398, 92 ff.; Föhlisch/Löwer CR 2024, 116 Rn. 32; Billing/Vetter K&R 2024, 387 (391).

⁹⁸ Billing/Vetter K&R 2024, 387 (392).

klärungen mit allen erforderlichen Informationen erhält, die eine schnellere Abwicklung ermöglichen.⁹⁹ Eine Zunahme fehlerhafter Widerrufserklärungen ist daher weniger zu erwarten, die Zahl unberechtigter Widerrufserklärungen könnte jedoch tatsächlich steigen.

Problematisch ist zudem, dass durch das Offenlassen von Fragen, die bereits für den Kündigungsbutton diskutiert wurden (zB Log-in-Erfordernis, Vertragsschluss über von Dritten betriebene Online-Benutzeroberfläche) Rechtsunsicherheit entsteht.¹⁰⁰

Teilweise wird auch ein Mehrwert der Widerrufsfunktion für den Verbraucher in Frage gestellt, da die Identifizierung des Vertrags idR die Durchsicht des E-Mail-Postfachs erfordere und der Widerruf bei dieser Gelegenheit auch per E-Mail erklärt werden könne.¹⁰¹ Wie für den Kündigungsbutton¹⁰² könnte daher anstelle eines mehrstufigen Verfahrens auch die Pflicht zur Angabe einer zentralen E-Mail-Adresse mit verpflichtender Eingangsbestätigung ausreichen. Dem ist entgegenzuhalten, dass die Möglichkeit zur Abgabe der Widerrufserklärung direkt über die Benutzeroberfläche und die mit der Widerrufsfunktion verbundene Vereinheitlichung des Widerrufsprozesses die Ausübung des Widerrufsrechts für den Verbraucher erleichtert.¹⁰³ Zudem stärkt die geforderte hervorgehobene Platzierung der Widerrufsfunktion auch das Verbraucherbewusstsein für das mögliche Bestehen eines Widerrufsrechts.

Ungeachtet der in Teilbereichen berechtigten Kritik an der Neuregelung sind Unternehmer gut beraten, die Widerrufsfunktion

rechtzeitig bis zum 19.6.2026 umzusetzen. Die zahlreichen gerichtlichen Auseinandersetzungen um den Kündigungsbutton, bei denen bereits im Monat des Inkrafttretens erste einstweilige Verfügungen ergingen,¹⁰⁴ lassen eine vergleichbare Entwicklung auch für die Widerrufsfunktion erwarten.

Schnell gelesen ...

- Die für Bestellbutton und Kündigungsbutton entwickelten Grundsätze können teilweise auf die Widerrufsfunktion übertragen werden.
- Die Pflicht zur Vorhaltung einer Widerrufsfunktion erfasst sämtliche über eine Online-Benutzeroberfläche geschlossenen Fernabsatzverträge mit Widerrufsrecht, unabhängig davon, wer die Benutzeroberfläche betreibt.
- Die mit „Vertrag widerrufen“ oder einer ähnlich eindeutigen Beschriftung gekennzeichnete Widerrufsfunktion muss für den durchschnittlichen Verbraucher ständig verfügbar, hervorgehoben platziert und leicht zugänglich sein, ohne dass eine Anpassung an die individuelle Widerrufssituation des Verbrauchers erforderlich ist.
- Nach Betätigung der Widerrufsfunktion muss der Verbraucher eine Widerrufserklärung ohne Anmeldung im Benutzerkonto oder andere Zwischenschritte an den Unternehmer übermitteln können.
- Verstöße gegen die Vorgaben zur Widerrufsfunktion können die Widerrufsfrist verlängern, Schadensersatzansprüche sowie Ansprüche nach UKlaG und UWG auslösen und eine Ordnungswidrigkeit darstellen.

⁹⁹ So auch Seiwerth NJW 2026, 945 Rn. 16.

¹⁰⁰ So auch Wiebe/Sengül WRP 2025, 574 Rn. 55; Rätze WRP 2025, 1398, Rn. 94; Föhlich/Löwer CR 2024, 116 Rn. 32.

¹⁰¹ Rätze WRP 2025, 1398 Rn. 89, 92; Billing/Vetter K&R 2024, 387 (390 f.).

¹⁰² Güster/Booke MMR 2022, 450 (451 f.).

¹⁰³ So auch Seiwerth NJW 2026, 945 Rn. 20; Wiebe/Sengül WRP 2025, 574 Rn. 55 f.

¹⁰⁴ ZB LG Köln MMR 2023, 381.



Dr. Sebastian Pech, LL.M. (Duke),
ist Rechtsanwalt im Bereich IP- und IT-Recht.

MORITZ GRIESEL / HANS BRORSEN

Kennzeichnungspflichten für synthetische Medieninhalte

Rechtliche Anforderungen und technische Realität

Transparenz

Der Beitrag untersucht die Regulierung synthetischer Medieninhalte im europäischen Recht mit einem besonderen Fokus auf die in Art. 50 Abs. 2 KI-VO vorgesehene Kennzeichnungspflicht. Ausgangspunkt ist die rasante Verbreitung KI-generierter Medieninhalte, deren schnelle Produktion und Reichweite über digitale Plattformen erhebliche Risiken für individuelle Rechtsgüter und die Funktionsfähigkeit des öffentlichen Dis-

kurses bergen. Vor diesem Hintergrund werden in diesem Beitrag die einschlägigen Regelungen der KI-VO und nachgelagertem Soft law analysiert. Anhand ausgewählter Kennzeichnungsmethoden wird die praktische Umsetzung der Kennzeichnungspflichten exemplarisch beleuchtet und eingeordnet.

Lesedauer: 24 Minuten

I. Einführung

Die Nutzung generativer KI-Systeme und die damit verbundene Verbreitung synthetischer Medieninhalte hat in den vergangenen Jahren erheblich an Bedeutung gewonnen. Immer deut-

licher zeigt sich, dass diese Systeme nicht nur nützliche, sondern ebenso missbräuchliche oder schädliche Inhalte hervorbringen können. Ihr Spektrum erstreckt sich über sämtliche Medienformate hinweg und findet seine Grenzen vor allem in der Kreativität und technischen Kompetenz der Nutzerinnen und Nutzer. Eine Unterscheidung zwischen authentischen und synthetischen Medien ist nicht nur allgemein für menschliche Rezipientinnen und Rezipienten inzwischen vielfach kaum noch möglich¹,

¹ Auch für geschultes Personal von Rundfunkanstalten fällt der Unterscheidung zunehmend schwer, vgl. <https://presseportal.zdf.de/pressemitteilung/zdf-entschuldigt-sich-fuer-fehler-im-heute-journal>.

sondern wird auch von 91% der Deutschen als schwierig eingeschätzt.² Die Verbreitung synthetischer Medien ist damit längst kein randständiges Phänomen mehr, sondern hat sich zu einem dynamisch wachsenden Bestandteil moderner Informations-ökosysteme entwickelt. Neben den sich dadurch abzeichnenden, erheblichen Herausforderungen für Individuen und die Gesellschaft, dürften auch materielle Schäden bei den Betreibern bzw. Anbietern von KI-Systemen zu erwarten sein – das (versehentliche) Einspeisen synthetischer Inhalte in Trainingsdaten kann deren Funktionsweise bis hin zur Unbrauchbarkeit beeinträchtigen.³ Vor diesem Hintergrund sollten alle Akteure daran interessiert sein, belastbare rechtliche und technische Lösungen zur Kennzeichnung synthetischer Inhalte zu entwickeln.

Dieser Beitrag⁴ nimmt die Kennzeichnungspflicht aus Art. 50 Abs. 2 KI-VO⁵ zum Anlass, die einschlägigen ergebnisbezogenen Modalitäten und deren beabsichtigte Umsetzung im Praxisleitfaden über die Transparenz KI-generierter Inhalte⁶ (CoP-E) herauszuarbeiten sowie einer ersten (praktischen) Bewertung zuzuführen.

II. Kennzeichnungspflichten in der KI-VO

Die Regulierung der Nutzung generativer KI-Systeme wird in unterschiedlichen Rechtsgebieten⁷ nachvollzogen. Auf unionsrechtlicher Ebene stellen die im öffentlichen Produktsicherheits-, Medien- und Plattformrecht zu verortenden Transparenzpflichten für unterschiedliche Ausgaben von KI-Systemen einen nicht nur mitgliedstaats-, sondern auch system- und inhaltsübergreifenden Ansatz dar.⁸ Die Regelungen in Art. 50 KI-VO dienen dabei als rechtsaktübergreifender Ausgangspunkt. Sie beinhalten zunächst eine Pflicht des KI-Anbieters zur Kennzeichnung von synthetischen Inhalten, die sein KI-System ausgibt (Art. 50 Abs. 2 KI-VO). Daneben sind KI-System-Betreiber zur Offenlegungen des synthetischen Ursprungs eines Medieninhalts verpflichtet (Art. 50 Abs. 4 KI-VO).⁹

1. Kennzeichnungspflichten für Anbieter von KI-Systemen

Nach Art. 50 Abs. 2 KI-VO¹⁰ müssen Anbieter von KI-Systemen¹¹, die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen¹², sicherstellen, dass die Ausgaben des KI-Systems in einem maschinenlesbaren¹³ Format¹⁴ gekennzeichnet und als künstlich erzeugt oder manipuliert erkennbar sind.¹⁵ Das in Art. 1 KI-VO definierte Leitbild einer auf den Menschen ausgerichteten und vertrauenswürdigen KI dient dabei als normativer Hintergrund für den auslegungsbedürftigen Wortlaut der Vorschrift.

a) Modalitäten der Kennzeichnung

Die KI-VO gibt keine konkreten Kennzeichnungsmethoden vor, sondern stellt die Auswahl in das Ermessen des Anbieters. Die technischen Lösungen sollen jedoch wirksam, interoperabel, belastbar und zuverlässig sein, wobei verfügbare Techniken wie Wasserzeichen, Metadaten-Identifizierungen, kryptografische Methoden zum Nachweis der Herkunft und Authentizität des Inhalts, Protokollierungsmethoden, Fingerabdrücke oder andere Techniken einzeln oder in Kombination verwendet werden können.¹⁶ Kennzeichnungslösungen können damit sowohl auf KI-System- als auch auf KI-Modell-Ebene angesiedelt werden – wenngleich Art. 50 Abs. 2 KI-VO „nur“ die Anbieter eines KI-Systems als Verpflichtungsadressaten benennt. Insgesamt unterliegen Auswahl und Anwendung der Kennzeichnungsmethoden daher dem Verhältnismäßigkeitsprinzip.¹⁷

b) Stand der Technik

Bei der Identifikation geeigneter Lösungen hat der Anbieter die Besonderheiten und Beschränkungen verschiedener Medienfor-

mate¹⁸, die Kosten der Implementierung und den allgemein anerkannten Stand der Technik zu berücksichtigen. Zur Bestimmung der technikbezogenen Anforderungen ist mit dem „Stand der Technik“ somit ein Begriff maßgeblich, der zwar nicht in der KI-VO definiert ist, im deutschen Recht allerdings einer umfänglichen Kasuistik – der Drei-Stufen-Theorie¹⁹ – unterworfen wurde.²⁰ Trotz eines zunächst unionsrechtsautonom zu bestimmenden Begriffsverständnisses, spricht der bisherige Umgang mit dem „Stand der Technik“ in der DS-GVO, der DS-RL²¹ und weiterem EU-Recht²² für einen weitgehenden Gleichlauf mit dem zum deutschen Umwelt-, Technik- und Produktsicherheitsrecht²³ entwickelten Begriffsverständnis.²⁴

Im drei-stufigen Anforderungskatalog des öffentlichen Sicherheitsrechts²⁵ ist der „Stand der Technik“ unterhalb des Begriffs „Stand von Wissenschaft und Technik“ anzusiedeln, der aus dem AtomG²⁶ sowie in ähnlicher Fassung auch aus dem GenTG²⁷ bekannt ist. Diesem höchsten Standard wird entsprochen, wenn Schadensvorsorge in demjenigen Umfang getroffen wird, der „nach den neuesten wissenschaftlichen Erkennt-

² <https://www.tuev-verband.de/studien/chatgpt-studie-2025-generative-ki-wird-zum-massenphänomen-aber-sicherheit-und-orientierung-fehlen>.

³ Xing et al., When AI Eats Itself: On the Caveats of AI Autophagy, *Nature Machine Intelligence*, 2025.

⁴ Der Beitrag entwickelt wesentliche Gedanken weiter, die die Verf. an anderer Stelle formuliert haben, vgl. Griesel/Brorsen, Tagungsbeitrag Plattform Privatheit 2025 (im Erscheinen).

⁵ VO (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. 2024 144/1.

⁶ Second Draft Code of Practice on Transparency of AI-Generated Content v. 3.3. 2026, abrufbar unter: <https://ec.europa.eu/newsroom/dae/redirection/document/125388>.

⁷ Zum Produktsicherheitsrecht: Kumkar/Griesel KIR 2024, 117; Molavi Vasse'i RDi 2024, 406; zum Strafrecht: Pfeiffer MMR 2025, 934; Blocher KIR 2025, 225; zum Deliktsrecht: Kumkar/Rapp ZfDR 2022, 199 (204 ff.); Lantwinn MMR 2019, 574.

⁸ Transparenzpflichten finden sich in folgenden Vorschriften: Art. 50 Abs. 2, Abs. 4 KI-VO; Art. 35 Abs. 1 S. 2 lit. k DSA; Art. 18 Abs. 1 lit. e EMFA.

⁹ Art. 50 Abs. 4 KI-VO ist nicht Gegenstand dieses Beitrags; s. dazu Kumkar/Griesel KIR 2024, 117 (119 ff.).

¹⁰ Einzelheiten zur Transparenzpflicht finden sich in Kumkar/Griesel KIR 2024, 117; Molavi Vasse'i RDi 2024, 406; Becker CR 2024, 355; zu Textinhalten Schwarz MMR 2025, 786.

¹¹ Art. 3 Nr. 3 KI-VO.

¹² Dem Wortlaut nach sind manipulierte Medieninhalte nicht erfasst; mit Blick auf Erwägungsgrund 133 S. 1 KI-VO dürfte es sich dabei allerdings um ein redaktionelles Versehen gehandelt haben, so bereits Kumkar/Griesel KIR 2024, 117 (123).

¹³ Zum Begriff Brorsen/Falk MMR 2025, 7 ff.

¹⁴ Zur Frage ob auch ein menschenlesbares Format erforderlich ist Kumkar/Griesel KIR 2024, 117 (124).

¹⁵ Kumkar/Griesel KIR 2024, 117 (122 ff.).

¹⁶ Erwägungsgrund 133 S. 3, 135 KI-VO.

¹⁷ Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 77.

¹⁸ Nicht gemeint sind Unterscheidungen in Bezug auf die im Inhalt transportierten Informationen, die z.B. journalistischer, satirischer, künstlerischer, meinungsbildungsrelevanter oder sonstiger Natur sein können.

¹⁹ Breuer AöR 101 (1976), 46 (67 f.); übernommen durch BVerfG Beschl. v. 8.8.1978 – 2 BvL 8/77 = NJW 1979, 359 (362) – Kalkar.

²⁰ Vgl. BVerfG Beschl. v. 8.8.1978 – 2 BvL 8/77 – Kalkar; BGH Urt. v. 05.02.2013 – VI ZR 1/12 Rn. 13; BGH Urt. v. 16.6.2009 – VI ZR 107/08 Rn. 15 ff. mwN; MüKoBGB/Wagner, 9. Aufl. 2024, ProdHaftG § 1 Rn. 56; Klindt/Handorn NJW 2010, 1105; Marburger, Die Regeln der Technik im Recht, 1979, S. 429 ff.

²¹ Erwägungsgrund 46 RL 95/46/EG, Art. 17 Abs. 1 RL 95/46/EG.

²² Vgl. zB Art. 14 RL (EU) 2016/1148 (NIS-RL); Art. 21 Abs. 1 UAbs. 2 RL (EU) 2022/2555 (NIS-2-RL).

²³ Beispiele finden sich bei Seibel NJW 2013, 3000 (3002).

²⁴ Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 79; Sydow/Marsch, DS-GVO/BDSG/Johannes/Weinhold, 3. Aufl. 2022, BDSG § 64 Rn. 33.

²⁵ MüKoBGB/Wagner, 9. Aufl. 2024, ProdHaftG § 1 Rn. 56; Seibel NJW 2013, 3000.

²⁶ §§ 6 Abs. 2 Nr. 2, 7 Abs. 2 Nr. 3, 9 Abs. 2 Nr. 3 AtG.

²⁷ § 6 Abs. 1 S. 1 Nr. 2 GenTG.

nissen für erforderlich gehalten wird“.²⁸ Dabei handelt es sich um den höchstmöglichen Stand, wie er zum Zeitpunkt des Inverkehrbringens des betreffenden Produkts existierte.²⁹

Unterhalb des Begriffs „Stand der Technik“ sind zudem die „allgemein anerkannten Regeln der Technik“ zu verorten. Maßgeblich ist derjenige Technikstand, der der hA unter den technischen Praktikern entspricht. Folglich können die anerkannten Regeln der Technik auch hinter einer weiterstrebenden technischen Entwicklung (zB in der Wissenschaft) zurückbleiben.³⁰

Für den „Stand der Technik“ ist schließlich über die allgemeine Anerkennung und die praktische Bewährung einer Technik oder Methode³¹ hinausgehend auch auf die Meinungsstreitigkeiten der Techniker einzugehen ist, um fortlaufend zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist.³² Für die Anbieter von KI-Systemen bedeutet das, dass sie ihre Kennzeichnungsmethoden und -techniken iRe kontinuierlichen iterativen Prozesses regelmäßigen systematischen Überprüfung und Aktualisierung unterwerfen müssen, um dem dynamisch zu bestimmenden Anforderungsniveau von Art. 50 Abs. 2 KI-VO zu entsprechen.³³

c) Interoperabilität

Die technischen Lösungen der Anbieter sollen nicht nur die Kennzeichnung in einem maschinenlesbaren Format³⁴ gewährleisten, sondern auch die Feststellung ermöglichen, dass die Ausgabe von einem KI-System und nicht von einem Menschen erzeugt oder manipuliert wurde – mit anderen Worten: sie müssen einen spezifischen inhaltlichen Aussagegehalt aufweisen.³⁵ Die Interoperabilitätsvorgabe bezieht sich auf beide Aspekte gleichermaßen. Die Transparenzkennzeichnung muss daher in fremden Systeminfrastrukturen auslesbar sein (syntaktische Interoperabilität) und zudem von diesen Systeminfrastrukturen auch verstanden werden können (semantische Interoperabilität).³⁶

Es ist anzunehmen, dass der Ordnungsgeber hier wohl ein Zusammenspiel der verschiedenen Rechtsakte der Europäischen Digitalrechtsordnung vor Augen hatte: Bereits KI-systemseitig soll eine maschinenlesbare Kennzeichnung nach Art. 50 Abs. 2 KI-VO erfolgen, die bei möglichen Erst- und Anschluss-

verwendungen des gekennzeichneten Medieninhalts in fremden Systeminfrastrukturen wie sozialen Plattformen ausgelesen werden kann. Die Anbieter dieser Plattformen können die maschinenlesbare Kennzeichnung schließlich nutzen, um auf ihren Plattformen eine verlässliche – menschenlesbare – Kennzeichnung zu ermöglichen – sei es aus intrinsischer Motivation, aufgrund einer Selbstverpflichtung³⁷ oder weil sie als sehr große Online-Plattform (VLOP) und sehr große Online-Suchmaschine (VLOSE) bei sich ein systemisches Risiko iSv Art. 34 DSA identifiziert haben und damit der Pflicht nach Art. 35 Abs. 1 S. 2 lit. k DSA unterfallen. Bereits die maschinenlesbare Kennzeichnung verfolgt damit den Zweck, Rezipientinnen und Rezipienten eines Medieninhalts auf dessen synthetischen Ursprung hinzuweisen, um Fiktion und Wirklichkeit wirksam voneinander unterscheiden zu können. Die Vorgabe kommt damit letztlich der Integrität des Informationsökosystems zugute.³⁸

d) Belastbarkeit und Zuverlässigkeit

Weiterhin müssen die Kennzeichnungen belastbar und zuverlässig sein³⁹, wobei die KI-VO insoweit keine Legaldefinitionen enthält. Im allgemeinen Sprachgebrauch weisen die Begriffe eine gewisse inhaltliche Überlappung auf: Der Duden definiert „belastbar“ als „zuverlässig, überprüfbar; belegbar“⁴⁰ und „zuverlässig“ als „mit großer Sicherheit zutreffend; richtig“⁴¹. Bei den Adjektiven ist damit gemein, dass sie sich auf die Qualität der Authentifikation einer bestimmten Tatsache oder Information beziehen. Hier besteht diese Information in der des synthetischen Ursprungs eines Medieninhalts.⁴² Relevante Parameter können daher sein, ob die Kennzeichnung dauerhaft mit dem Medieninhalt verbunden, mit einfachen (technischen) Mitteln zu trennen, oder mit (technischen) Mitteln inhaltlich veränderbar ist.⁴³

e) Wirksamkeit

Die Kennzeichnung muss zudem auch wirksam sein, wobei die KI-VO erneut keine Legaldefinition enthält. Der Begriff „wirksam“ wird im Duden als „eine beabsichtigte Wirkung erzielend; mit Erfolg wirkend“⁴⁴ definiert. Anders als die zuvor genannten Tatbestandsmerkmale scheint sich der Begriff „Wirksamkeit“ nicht nur auf die technische Funktionalität der Kennzeichnungsmethoden zu beziehen. Es bräuchte nämlich keiner gesetzlichen Vorgabe einer Kennzeichnungspflicht, wenn die technischen Lösungen nicht auch wirksam iSv funktionsfähig wären. Welcher Grad an Funktionsfähigkeit erreicht werden muss, ergibt sich ohnehin bereits aus dem aktuellen Stand der Technik und den korrespondierenden Anforderungen an Belastbarkeit und Zuverlässigkeit.⁴⁵

Ob eine Kennzeichnung wirksam ist, ist also über die technikbezogene Funktionalität hinaus in Abhängigkeit der vom Unionsgesetzgeber verfolgten Ziele zu beurteilen.⁴⁶ Entsprechende Transparenzmechanismen versprechen zwar grundsätzlich einen von der individuellen technischen Kompetenz unabhängigen Einfluss auf die Glaubwürdigkeit und Genauigkeit von Inhalten.⁴⁷ Dabei ergeben sich jedoch Unterschiede je nach gewähltem Transparenzansatz:⁴⁸ Kennzeichnungen⁴⁹ von Medieninhalten könnten zunächst an deren Entstehungsprozess anknüpfen und damit das Ziel verfolgen, sämtliche KI-generierte Ausgaben als solche – also unter Nutzung einer bestimmten Technologie erstellten Inhalte – zu deklarieren. Die Kennzeichnung steht damit unabhängig vom konkreten Inhalt oder den mit dessen Generierung und Verbreitung beabsichtigten Wirkungen.

Anlass für das regulatorische Tätigwerden war allerdings weniger die bloße Tatsache maschineller Generierung von Inhalten als vielmehr das Risiko, dass bestimmte Inhalte geeignet sind, Rezipientinnen und Rezipienten in die Irre zu führen und da-

²⁸ BVerfG NJW 1979, 359 (362) – Kalkar.

²⁹ EuGH Urt. v. 29.5.1997 – C-300/95 Rn. 26.

³⁰ BVerfG NJW 1979, 359 (362) – Kalkar.

³¹ Hierbei handelt es sich „lediglich“ um die Definition des Begriffs „allgemein anerkannte Regeln der Technik“, der etwa in § 17 Abs. 2 Nr. 1 SprengG und in § 630a Abs. 2 BGB verwendet wird.

³² BVerfG NJW 1979, 359 (362) – Kalkar.

³³ Kumkar/Griesel KIR 2024, 117 (123); Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 79.

³⁴ S.a. Erwägungsgrund 12, 133 S. 3 Hs. 1 KI-VO.

³⁵ Erwägungsgrund 133 S. 3 Hs. 2 KI-VO.

³⁶ Allg. iSe Fähigkeit eines Systems zur Zusammenarbeit s. Bomhard/Pieper/Wende, KI-VO/Merkle, 1. Aufl. 2025, KI-VO Art. 50 Rn. 80.

³⁷ Vgl. Code of Practice on Disinformation 2022, Commitment 21 und 23.

³⁸ S. dazu unter II.1.e); Erwägungsgrund 133 S. 2 KI-VO.

³⁹ Art. 50 Abs. 2 S. 2 KI-VO.

⁴⁰ Duden, <https://www.duden.de/rechtschreibung/belastbar>.

⁴¹ Duden, <https://www.duden.de/suchen/dudenonline/zuverl%C3%A4ssig>.

⁴² Molavi Vasse'i RD 2024, 406 Rn. 29 f.

⁴³ Bomhard/Pieper/Wende, KI-VO/Merkle, 2025, KI-VO Art. 50 Rn. 80 unter Verweis auf EUIPO, Automated Content Recognition: Discussion Paper – Phase 1 Existing technologies and their impact on IP, 2020, S. 6.

⁴⁴ Duden, <https://www.duden.de/rechtschreibung/wirksam>.

⁴⁵ Molavi Vasse'i RD 2024, 406 Rn. 31.

⁴⁶ Molavi Vasse'i RD 2024, 406 Rn. 31.

⁴⁷ Kleine, Perception of Deepfake Technology, 2022.

⁴⁸ Epstein/Fang/Arechar/Rand, What label should be applied to content produced by generative AI?, 2023, 2.

⁴⁹ S. bereits Griesel/Brorsen, Tagungsbeitrag Plattform Privatheit 2025 (im Erscheinen).

durch individuelle oder gesellschaftliche Schutzgüter zu beeinträchtigen. Entsprechenden Schutz vermitteln jedoch nur Kennzeichnungs- und Offenlegungspflichten, die stärker wirkungsbezogen ausgestaltet sind.⁵⁰ Hier tritt der Entstehungsprozess in den Hintergrund; entscheidend ist vielmehr Inhalte zu identifizieren, die ein besonderes Täuschungs- oder Manipulationspotenzial aufweisen. Das Problem KI-generierter Inhalte ist damit besser im Kontext bekannter Erscheinungsformen missbräuchlicher Inhalte wie Fehl-, Miss- und Desinformation zu verorten, das durch den hohen Grad an vermeintlicher Authentizität synthetischer Medieninhalte nur verstärkt wird.⁵¹ Wirkungsbezogene Transparenzpflichten zielen damit primär auf den Schutz übergeordneter öffentlicher Interessen wie Authentizität, Richtigkeit und Verlässlichkeit von Medieninhalten. Die Vertrauenswürdigkeit einer Information soll dabei von ihrer nachvollziehbaren Erstellung bis zu ihrer Zirkulation, Nutzung und Bearbeitung über Plattform- und andere Systeminfrastrukturgrenzen hinweg gewährleistet sein. Methoden und Wirkmechanismen dieser Interventionsstrategie gegen den Verlust des Vertrauens in das Informationsökosystem wurden schließlich auch vielfach empirisch untersucht und stützen dieses Verständnis.⁵²

Vorliegend soll die Brücke zwischen diesen beiden Transparenzverständnissen geschlagen werden: Die Wirksamkeit ist daher anzunehmen, wenn die Kennzeichnung einen relevanten Beitrag im arbeitsteiligen Zusammenwirken unter Berücksichtigung nachgelagerter Detektions- und Offenlegungsmechanismen leistet und dadurch die entsprechenden negativen Auswirkungen zumindest reduziert werden.⁵³ Unwirksam wäre die Kennzeichnung eines synthetischen Inhalts zB dann, wenn diese in praktischer Hinsicht nicht hinreichend zwischen menschlich- und synthetisch-erzeugten Inhalten unterscheiden oder lediglich vom KI-Anbieter selbst ausgelesen werden kann.

2. Praxisleitfaden über die Transparenz KI-generierter Inhalte

Die o.g. Pflichten sollen zukünftig zur Erleichterung der wirksamen Umsetzung von Art. 50 KI-VO Gegenstand eines Praxisleitfadens (CoP-E) iSd Art. 50 Abs. 7 KI-VO sein, der Mitte 2026 verabschiedet werden soll. Praxisleitfäden gehören in der KI-VO zu einer Reihe von Konkretisierungsinstrumenten zur praxisgerechten Umsetzung der verordnungsrechtlichen Vorgaben. Dazu zählen harmonisierte (technische) Normen iSv Art. 40 ff. KI-VO, Verhaltenskodizes iSv Art. 95 KI-VO und Leitlinien der EU-Kommission iSv Art. 96 KI-VO.⁵⁴

Der Praxisleitfaden ist als Soft-Law-Instrument einzuordnen, das zunächst auf freiwilligen Selbstverpflichtungen der beteiligten Anbieter und Betreiber von KI-Systemen beruht. Er konkretisiert die abstrakt gehaltenen Transparenzpflichten der KI-VO, ohne rechtliche Verbindlichkeit jenseits des Unterzeichnerkreises zu begründen oder eine Konformitätsvermutung wie harmonisierte Normen⁵⁵ auszulösen. Vergleichbare Kodizes in anderen Bereichen des europäischen Digitalrechts konnten in der Praxis bisher häufig nur begrenzten Erfolg verzeichnen.⁵⁶ Die Erarbeitung erfolgt dabei nicht durch ein demokratisch legitimes Legislativorgan, sondern durch Beteiligungsformate von Stakeholdern unter Leitung einer Art „Expertengruppe“. Die Beteiligten müssen keine konkreten Auswahlkriterien erfüllen⁵⁷, sondern können sich etwa aufgrund eines beruflichen, wissenschaftlichen, gesellschaftspolitischen oder sonstigen Interesses am Regelungsgegenstand bewerben.⁵⁸

Während diese initiale Erarbeitung des Praxisleitfadens keinem formellen Verfahren⁵⁹ folgt, sondern nur durch das Büro für künstliche Intelligenz⁶⁰ erleichtert und gefördert werden soll⁶¹,

kann die EU-Kommission die Genehmigung in Form eines Durchführungsrechtsakts aussprechen und den Praxisleitfaden damit unionsweit als Referenzrahmen für die Konkretisierung der Transparenzpflichten anerkennen.⁶² Im Prüfverfahren ist die EU-Kommission an die Empfehlung eines aus Vertretern der Mitgliedstaaten zusammengesetzten Ausschusses gebunden.⁶³ Mit der Genehmigungsentscheidung wird der individuell zu erbringende Nachweis der Rechtskonformität der unterzeichnenden Anbieter und Betreiber von KI-Systemen mit den Transparenzvorschriften in Art. 50 Abs. 2, Abs. 4, Abs. 5 KI-VO erleichtert.⁶⁴ Daneben dürfte ihm auch eine über den Unterzeichnerkreis hinausgehende praxisrelevante Steuerungswirkung zukommen, deren Beeinflussung wohl auch Anreiz für die initiale Mitarbeit der Anbieter und Betreiber von KI-Systemen ist. Umgekehrt signalisiert die Versagung der Genehmigung, dass der Praxisleitfaden die Anforderungen der KI-VO nicht hinreichend operationalisiert und kann damit gegenüber allen Akteuren ebenfalls richtungsweisend sein.⁶⁵

Doch auch nach Verabschiedung und Genehmigung des Praxisleitfadens ist es Anbietern und Betreibern von KI-Systemen zukünftig möglich, die Einhaltung der Transparenzpflichten in

50 S. bereits Griesel/Brorsen, Tagungsbeitrag Plattform Privatheit 2025 (im Erscheinen).

51 Zu den Schutzgütern der im DSA vorgegebenen Anti-Desinformationsmaßnahmen s. Peukert JZ 2023, 278 (281) mwN; Gerdemann/Spindler GRUR 2023, 115 (123); Brorsen/Falk MMR 2024, 32; Becker CR 2024, 353 Rn. 60; Becker GRUR 2024, 505 (507).

52 Zur Terminologie von KI-Labels s. Epstein/Fang/Arechar/Rand, What label should be applied to content produced by generative AI?, 2023; Rauchfleisch et al., Deepfakes or Synthetic Media? The Effect of Euphemisms for Labeling Technology on Risk and Benefit Perceptions, 2025; Altay/Gilardi, People are skeptical of headlines labeled as AI-generated, even if true or human-made, because they assume full AI automation, 2024; zu KI-Labels in einzelnen Branchen s. Toff/Simons The International Journal of Press/Politics 2025, p. 881-903; Li/Yang, Impact of Artificial Intelligence-Generated Content Labels On Perceived Accuracy, Message Credibility, and Sharing Intentions for Misinformation, 2024; Wittenberg et al., Labeling AI-generated media online, 2025; Gamage et al., Labeling Synthetic Content: User Perceptions of Warning Label Designs for AI-generated Content on Social Media, 2025; Lockhart/Tessono, Human or AI? Evaluating Labels on AI-Generated Social Media Content, 2025; zur Wirkung von ampelfarbenbasierten Warnhinweisen s. Dobber et al., The effect of traffic light veracity labels on perceptions of political advertising source and message credibility on social media, 2025.

53 Ähnl. Bomhard/Pieper/Wende, KI-VO/Merkle, 2025, KI-VO Art. 50 Rn. 79, die in der Wirksamkeit jedoch eine „inhaltsleere“ Voraussetzung sieht.

54 S. dazu EU-Kommission, Draft Guidelines on the implementation of the transparency obligations for certain AI systems under Article 50 of Regulation (EU) 2024/1689 (the 'AI Act'), abrufbar unter: <https://ec.europa.eu/newsroom/dae/redirection/document/128275>.

55 Art. 40 KI-VO.

56 Konstruktiv mit dem Vorschlag einer „Selbstregulierung mit Zähnen“ Martini JZ 2017, 1017 (1023); allgemeiner Bomhard/Pieper/Wende, KI-VO/Beurskens, 2025, KI-VO Art. 56 Rn. 1.

57 Auch der Sitz innerhalb der EU ist hier kein Kriterium; so wurde die Leitung des Entwurfsprozesses teilweise an akademische Institutionen aus Nicht-EU-Ländern delegiert, ebenso sind mehrere politische Organisationen mit Sitz außerhalb der EU Teil des Entwurfsprozesses (vgl. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>); s.a. Peukert, Research Paper of the Faculty of Law of Goethe University Frankfurt/M. No. 3/2025 Rn. 30, abrufbar unter: https://publikationen.ub.uni-frankfurt.de/opus4/frontdoor/deliver/index/docId/77658/file/25-03_RPS.pdf.

58 Chibanguza/Kuß/Steeger, Künstliche Intelligenz/Lohse/Köbl, 2. Aufl. 2026, 1. Teil: § 2 B. Rn. 53 sprechen insoweit von einem „Wissensvorsprung“ der Beteiligten ggü. dem Gesetzgeber.

59 Demgegenüber sollen bei der Erarbeitung der Praxisleitfäden für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck etwa auch internationale Ansätze und der Stand der Technik berücksichtigt werden, vgl. Erwägungsgrund 116, 117 KI-VO.

60 Art. 3 Nr. 47 KI-VO.

61 Art. 56 Abs. 1 KI-VO.

62 Art. 56 Abs. 6 KI-VO.

63 Art. 50 Abs. 7, 56 Abs. 6 UAbs. 2 S. 2, 98 Abs. 2 KI-VO iVm Art. 5 Abs. 1, 2 VO (EU) 182/2011 iVm Art. 3 Abs. 2 VO (EU) 182/2011, Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 166.

64 Bomhard/Pieper/Wende, KI-VO/Beurskens, 2025, KI-VO Art. 56 Rn. 3.

65 Bomhard/Pieper/Wende, KI-VO/Beurskens, 2025, KI-VO Art. 56 Rn. 3.

Art. 50 KI-VO mithilfe „geeigneter alternativer Verfahren“⁶⁶ darzulegen. Diese alternativen Ansätze dürften schließlich nur den allgemeinen Durchsetzungsregelungen der KI-VO unterliegen.⁶⁷

Anders als die Praxisleitfäden für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck⁶⁸ wird der Praxisleitfaden nach Art. 50 Abs. 7 KI-VO nicht durch die Veröffentlichung harmonisierter Normen⁶⁹ abgelöst.⁷⁰ Konzeptionell ist er damit nicht als „Interimsinstrument“⁷¹ angelegt, sondern eher an bekannten Verhaltenskodizes⁷² wie dem Code of Conduct on Disinformation⁷³ zur Bekämpfung verschiedener Arten rechtswidriger Inhalte und systemischer Risiken im Internet angelehnt.⁷⁴ Aufgrund der fehlenden technischen Normen und entsprechender Normsetzungsinitiativen wird dem Praxisleitfaden daher zukünftig erhebliche Bedeutung bei der praktischen Auslegung der Transparenzpflichten zukommen.⁷⁵

3. Kennzeichnungsverfahren

In praktischer Hinsicht kann bei der Kennzeichnung von KI-generierten Ausgaben zwischen zwei grundsätzlich unterschiedlichen Verfahren unterschieden werden: Der Kennzeichnung des Inhalts der Ausgabe (sog. soft-binding) und der Kennzeichnung des Datenträgers der Ausgabe (sog. hard-binding).

Die Kennzeichnung des Inhalts der Ausgabe erfolgt zB durch die Einfügung von sog. Wasserzeichen. Dabei handelt es sich um für das menschliche Auge nicht erkennbare – aber dennoch für Maschinen auslesbare – technische Muster im jeweiligen Inhalt. Ein Beispiel für ein solches Verfahren ist Googles SynthID, bei dem digitale Spuren in synthetisch hergestellte Bilder eingefügt werden, die wiederum mit der passenden Software zwecks Verifikation ausgelesen werden können.⁷⁶ Eine andere Methode ist die Speicherung von sog. digitalen Fingerabdrücken. Bei diesem Verfahren wird eine Abstraktion des synthetischen Inhalts (zB ein Vektor oder ein Hash-Digest) hergestellt und in einer Daten-

bank samt entsprechender Metadaten gespeichert. Bei zu verifizierenden Inhalten wird ebenfalls ein digitaler Fingerabdruck entnommen und mit dem Datenbestand an Fingerabdrücken verglichen. Ergibt der Vergleich einen Treffer, können die passenden Metadaten über den Inhalt offengelegt werden (Beispiel: „dieses Bild ist synthetisch“). Die Vorteile dieses Verfahrens sind die Schnelligkeit und die Robustheit gegenüber Veränderungen bei gekennzeichneten Inhalten sowie die Möglichkeit, sehr viele Informationen zum jeweiligen „fingerprinted“ Inhalt vorzuhalten.⁷⁷

Eine Methode zur Kennzeichnung des Datenträgers des Mediums ist das Verfahren nach dem Industriestandard der C2PA.⁷⁸ Dabei werden Medien-Metadaten mittels eines kryptografischen Verfahrens mit den Mediendatenträgern verbunden.⁷⁹ Um das Verfahren der Kennzeichnung im C2PA-Standard möglichst sicher zu gestalten, gibt es ein Zertifizierungsverfahren für Unternehmen, die kryptografischen Kennzeichnungen anbieten.⁸⁰ Auch diese dem Mediendatenträger eingefügten, standardisierten Metadaten können mittels Software ausgelesen werden. Vereinzelt soziale Medien lesen bereits die C2PA-Medien-Metadaten aus und legen diese ihren Nutzerinnen und Nutzern in Form von sog. Content Credentials offen.⁸¹

4. Einordnung

Die Anwendung des C2PA-Standards zur Kennzeichnung synthetischer Inhalte ist derzeit weitestgehend eine technische Lösung, die den Anforderungen gem. Art. 50 Abs. 2 KI-VO entspricht. Die entsprechenden Kennzeichnungen erfolgen in maschinenlesbarer Form und enthalten Informationen, anhand derer (in unterschiedlichen Systeminfrastrukturen) erkennbar ist, dass der vom Datenträger getragene Inhalt synthetisch ist⁸². Sie erfüllen mithin das Erfordernis der Interoperabilität. Der C2PA-Standard ist Open Source, kann im Grundsatz von jedem KI-System-Anbieter zur Kennzeichnung und von jedem Dritten zur Erkennung angewendet werden. Dementsprechend ist eine solche Kennzeichnung auch wirksam. Ferner wird der Standard stetig von Experten aus Industrie und Wissenschaft weiterentwickelt und entspricht damit dem Stand der Technik. Einzig bei dem Erfordernis der Belastbarkeit/Zuverlässigkeit ist zu differenzieren. Wie bereits erläutert, sieht der C2PA-Standard grundsätzlich vor, dass die Kennzeichnung dem Datenträger des Inhalts beigelegt wird. Sobald der Datenträger verändert wird – etwa durch ein Versenden des Datenträgers –, besteht die Möglichkeit, dass die Kennzeichnung zerstört und damit nicht mehr auslesbar wird. Allerdings sieht der Industriestandard in seiner Erweiterung vor, dass die o.g. Methoden des sog. soft-bindings zusätzlich zum Einsatz kommen können.⁸³ In einem solchen Fall könnte die Kennzeichnung auch unabhängig von der Unversehrtheit des Datenträgers und anhand des Inhalts selbst abgerufen werden. Eine Kennzeichnung mit einem solchen „Multilayer“-Ansatz ist jedenfalls belastbar(er) und zuverlässig(er).

Darüber hinaus sieht der C2PA-Standard vor, dass die entsprechenden Kennzeichnungen in einem menschenlesbaren Format offengelegt werden können (sog. Content Credentials). Von dieser Offenlegung sind der Ursprung und die Authentizität des Medieninhalts und ggf. ein Hinweis auf die synthetische Erstellung oder Manipulation des Inhalts umfasst. Im gleichen Sinne könnten auch VLOPs oder VLOSEs ihren Risikominderungspflichten gem. Art. 35 Abs. 1 S. 2 lit. k DSA nachkommen, wenn sie die maschinenlesbaren C2PA-Kennzeichnungen auslesen und ihre Nutzerinnen und Nutzer auf den synthetischen Ursprung von ausgespielten Medien hinweisen.⁸⁴ Dieses Ineinandergreifen von Art. 50 Abs. 2 KI-VO und Art. 35 Abs. 1 S. 2 lit. k DSA würde schließlich nach hier vertretener Auffassung

⁶⁶ Art. 53 Abs. 4 S. 3, 55 Abs. 2 S. 3 KI-VO.

⁶⁷ ZB den in Art. 99 Abs. 4 lit. g KI-VO vorgesehenen Sanktionen; s. dazu Kumkar/Griesel KIR 2024, 117 (125); Bronner DSRITB 2024, 477.

⁶⁸ Art. 53 Abs. 4 KI-VO, Art. 55 Abs. 2 KI-VO.

⁶⁹ Gegenwärtig ist kein Normierungsauftrag für die Erarbeitung von Transparenznormen bekannt.

⁷⁰ Art. 50 KI-VO enthält folgerichtig keine der Art. 53 Abs. 4 KI-VO oder Art. 55 Abs. 2 KI-VO vergleichbare Regelung.

⁷¹ Zum Begriff im Kontext der Praxisleitfäden nach Art. 53 Abs. 4 KI-VO und Art. 55 Abs. 2 KI-VO Martini/Wendehorst, KI-VO/Martini, 2. Aufl. 2026, KI-VO Art. 50 Rn. 165.

⁷² Die Begrifflichkeiten in KI-VO und DSA zur Bestimmung einzelner Selbstregulierungsmechanismen sind – trotz weitgehender inhaltlicher Überschneidung – nicht zwingend identisch. Der Verhaltenskodex-Begriff des DSA scheint eher dem Praxisleitfaden-Begriff der KI-VO zu entsprechen.

⁷³ S. Code of Conduct on Disinformation 2022.

⁷⁴ Art. 45 Abs. 1 DSA; dazu Brorsen/Falk MMR 2024, 32.

⁷⁵ So kann das Büro für Künstliche Intelligenz Anbieter von KI-Systemen dazu er-suchen, die Praxisleitfäden zu befolgen, Art. 56 Abs. 7 KI-VO.

⁷⁶ <https://deepmind.google/models/synthid/>.

⁷⁷ ZB nutzt die Applikation Lumid Fingerprinting-Technologien, um maschinen- und menschenlesbare Informationen zur Herkunft, zum Erstellungsdatum sowie zu urheberrechtlich relevanten Metadaten eines Medieninhalts bereitzustellen.

⁷⁸ Vgl. <https://c2pa.org/>.

⁷⁹ S. https://spec.c2pa.org/specifications/specifications/2.2/specs/C2PA_Specification.html, Ziff. 9; <https://spec.c2pa.org/specifications/specifications/2.3/softbinding/Decoupled.html>.

⁸⁰ In Deutschland ist etwa die Valid Technologies GmbH dazu befugt.

⁸¹ So etwa LinkedIn, s. <https://www.linkedin.com/help/linkedin/answer/a6282984>.

⁸² S. https://spec.c2pa.org/specifications/specifications/1.3/explainer/Explainer.html#_use_of_artificial_intelligence_machine_learning_aiml.

⁸³ S. https://spec.c2pa.org/specifications/specifications/2.2/specs/C2PA_Specification.html, Ziff. 9.3.

⁸⁴ S.o. unter II.1.c.; Code of Conduct on Disinformation 2022, Commitment 20.

auch die – eigentlich Bertreiber-seitig zu erfüllende – Offenlegungspflicht nach Art. 50 Abs. 4 KI-VO funktional ersetzen.⁸⁵

III. Fazit und Ausblick

Kennzeichnungspflichten für synthetische Inhalte gesellschaftlich sind erforderlich und technisch möglich. Mit Art. 50 Abs. 2 KI-VO schafft der Unionsgesetzgeber eine auslegungsbedürftige rechtliche Grundlage, die den Rahmen für den zukünftigen Praxisleitfaden setzt, den es nun in Erwägung der vorstehenden ergebnisbezogenen Modalitäten zu erarbeiten gilt. Es existieren bereits technische Lösungen, die den Anforderungen der KI-VO entsprechen. Nun liegt es zunächst an den KI-Anbietern fristgerecht diese technischen Lösungen zu implementieren und dann an den zuständigen Behörden mit rechtlicher und technischer Expertise diese Kennzeichnungspflichten durchzusetzen.

Schnell gelesen ...

- Art. 50 Abs. 2 KI-VO etabliert eine zentrale, systemübergreifende Kennzeichnungspflicht für synthetische Medieninhalte als Grundpfeiler unionsrechtlicher Transparenzvorgaben.
- Die Anforderungen „wirksam, interoperabel, belastbar und zuverlässig“ konkretisieren sich an einem dynamischen Stand der Technik und verlangen kontinuierliche Anpassung der Kennzeichnungsmethoden durch die Anbieter.

■ Wirksame Kennzeichnung erschöpft sich nicht im Technikbezug, sondern muss im Zusammenspiel mit nachgelagerten Detektions- und Offenlegungsmechanismen zur Eindämmung von Täuschungs- und Manipulationsrisiken beitragen.

■ Der geplante Praxisleitfaden zur Transparenz KI-generierter Inhalte wird als Soft-Law-Instrument eine zentrale Rolle für die praktische Auslegung von Art. 50 KI-VO einnehmen, ohne die gesetzlichen Pflichten zu ersetzen.



Dipl.-Jur. Moritz Griesel

ist Wissenschaftlicher Mitarbeiter an der Georg-August-Universität in Göttingen.



Hans Brorsen, LL.M. (London),

ist Rechtsanwalt und Mitgründer der Valid Technologies GmbH in Berlin.

⁸⁵ So wohl auch Bomhard/Pieper/Wende, KI-VO/Merkle, 2025, Art. 50 Rn. 150; allg. zum Verhältnis der Transparenzpflichten aus KI-VO und DSA s. Erwägungsgrund 136 KI-VO; Kumkar/Griesel KIR 2024, 117 (125); Becker CR 2024, 353 Rn. 94.

ANKE DIECKHOFF / FELIX HEMPEL

Die Reform der Datenschutzaufsicht

Wer beaufsichtigt die neuen EU-Digitalrechtsakte?

Digitalrechtsakte

Die Bundesregierung hat die Reform der Datenschutzaufsicht zur Chefsache erklärt. Bis spätestens Ende 2027 soll die Aufsicht über die Wirtschaft neu justiert werden. Die Pläne stoßen vor allem bei Unternehmen auf offene Ohren. Wie ernst es die Bundesregierung damit meint, zeigt sich derzeit bei der Umsetzung zweier EU-Digitalrechtsakte: dem Data Act und der Verordnung über die Transparenz und das Targeting politischer Werbung. Bei beiden Gesetzen muss der Gesetzgeber unter Federführung des neuen Digitalministers heikle Fragen zur Zuständigkeit für datenschutzrechtliche Themen regeln. Dieser

Beitrag bewertet die jeweils geplante Umsetzung und macht Vorschläge, worauf die Bundesregierung bei ähnlich gelagerten Gesetzgebungsverfahren künftig achten sollte. Aus Unternehmenssicht verschlechtert sich der Status quo: Statt einer Vereinheitlichung der Datenschutzaufsicht drohen (erneut) unklare Zuständigkeiten und damit eine (weitere) Zersplitterung der Datenschutzaufsicht. Um dies zu verhindern, sollte der Gesetzgeber die Regulierung der Aufsicht nach DS-GVO und den verschiedenen Digitalrechtsakten aus einem Guss denken.

Lesedauer: 20 Minuten

I. Einleitung

Die Reform der Datenschutzaufsicht hat in letzter Zeit für viel Gesprächsstoff gesorgt. Nachdem die geplante Umstrukturierung der Zuständigkeiten schon in den Wahlprogrammen der Parteien zum aktuellen Bundestag prominent vorkam,¹ strebt nun auch die Bundesregierung eine Vereinfachung und Entbürokratisierung des Datenschutzes an. Teil davon soll eine Reform der Datenschutzaufsicht sein. Viele der derzeit auf 17 Landes- und eine Bundesdatenschutzbehörde verteilten Zuständigkeiten sollen in Zukunft bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gebündelt werden.² Der Bund will gar die Pflicht zur Bestellung von Landesdatenschutzbeauftragten gänzlich auf den Prüfstand stellen.³

Diese Diskussion ist nicht neu. Vor allem Unternehmen fordern seit Langem eine Überarbeitung des Status quo.⁴ Die Reformab-

sichten hatten schon unter der Ampelkoalition erheblichen Aufschwung erhalten.⁵ Anders als zuvor hat sich die Bundesregierung nun gemeinsam mit den Ländern eine Frist gesetzt: Die

¹ Hempel/Willecke PinG 2025, 79 (85).

² CDU/CSU/SPD, Verantwortung für Deutschland – Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode, 2025 (Koalitionsvertrag), Zeilen 2106-2108, abrufbar unter: https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf.

³ Beschluss der Besprechung des Bundeskanzlers mit den Regierungschefinnen und -chefs der Länder am 4.12.2025, TOP 2.2 AG Staatsmodernisierung, Rn. 158, abrufbar unter: https://www.rlp.de/fileadmin/02/MPK_Vorsitz/Beschluesse_MPK_4_Dezember_2025_Berlin/TOP_2.2_AG_Staatsmodernisierung.pdf.

⁴ S. schon Martini/Botta DÖV 2022, 605 und Dieckhoff/Hempel MMR 2025, 494 mwN.

⁵ Vgl. Gesetzentwurf der Bundesregierung zur Änderung des BDSG, BT-Drs. 20/10859, 13.

Neuordnung der Datenschutzaufsicht im nicht-öffentlichen Bereich soll bis Ende 2027 erfolgen.⁶ Damit ist die angestrebte Reform nicht mehr nur ein loser Gedanke, sondern mit einem Termin und damit auch politischem Druck verbunden. Während die Bundesregierung dadurch eine einheitlichere Auslegung der Datenschutzvorschriften und eine Entlastung von Unternehmen erwartet,⁷ warnen die Landesdatenschutzbeauftragten vor dem Verlust regionaler Nähe und jahrzehntelanger Kompetenz.⁸ Konkrete Umsetzungspläne liegen bislang nur punktuell vor. Neben verfassungsrechtlichen Fragen⁹ stellen sich vor allem europä- und rechtspolitische Probleme. Wie lassen sich neue EU-Verordnungen mit datenschutzrechtlichem Einschlag umsetzen, ohne die Datenschutzaufsicht (weiter) zu zersplittern? Damit musste sich zuletzt vor allem das neu gegründete Bundesministerium für Digitales und Staatsmodernisierung (BMDS) befassen. Sowohl bei der Umsetzung des Data Act als auch der EU-Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) muss der Gesetzgeber unter Federführung des BMDS die Aufsicht über die datenschutzrechtlichen Aspekte der Verordnungen regeln. Hierzu hat der Bundestag kürzlich das Data-Act-Durchführungsgesetz (DA-DG)¹⁰ verabschiedet; zudem hat die Bundesregierung einen Regierungsentwurf für ein Politische-Werbung-Transparenz-Gesetz (PWTG)¹¹ vorgelegt.

Vor diesem Hintergrund bewertet dieser Beitrag die in diesen Gesetzgebungsvorhaben vorgesehenen Zuständigkeiten und entwickelt Verbesserungsvorschläge, um das erklärte Ziel des Gesetzgebers – die Harmonisierung und Verbesserung der Kohärenz iRd Datenschutzaufsicht – zu erreichen. Die Messlatte liegt hoch: Das federführende BMDS hat das „Mission Statement“ verlaublich, Bürokratie und komplizierte Verwaltungswege zu verringern.¹²

6 Beschluss der Besprechung des Bundeskanzlers mit den Regierungschefinnen und -chefs der Länder am 4.12.2025, TOP 2.2 AG Staatsmodernisierung, Rn. 158.

7 Koalitionsvertrag, Zeilen 2102-2103. S. zuletzt auch die Prinzipien und Handlungsempfehlungen der Expertenkommission „Wettbewerb & Künstliche Intelligenz“, eingesetzt vom Bundesministerium für Wirtschaft und Energie v. 28.4.2026 in Ziffer 9: „Die Kommission empfiehlt, die Regelungen zum Datenschutz erheblich zu vereinfachen und die Aufsichtsstrukturen zu zentralisieren“, abrufbar unter <https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/Ministerium/handlungsempfehlungen-der-expertenkommission-wettbewerb-und-kuenstliche-intelligenz.html>.

8 So zB Kugelman, Ausschuss-Drs. 21(23) 42, 6. Gleichwohl unterstützen einige Landesregierungen die Pläne des Bundes, s. zuletzt in Baden-Württemberg: Bündnis 90/Die Grünen/CDU, Aus Verantwortung fürs Land – Entwurf des Koalitionsvertrags für 2026–2031, S. 141, abrufbar unter https://www.gruene-bw.de/wp-content/uploads/2026/05/2026–2031_Koalitionsvertrag_GrueneBW_CDUBW.pdf.

9 Martini/Botta DÖV 2022, 605 ff. und Hempel/Willecke PinG 2025, 79 mwN.

10 Das Gesetz wurde am 29.5.2026 im Bundesgesetzblatt verkündet und trat am 30.5.2026 in Kraft, vgl. BGBl. 2026 I Nr. 157, Art. 3.

11 Entwurf eines Gesetzes zur Durchführung der VO (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung, BR-Drs. 21/4089.

12 Die Datenschutzaufsicht ist auch iRd KI-VO relevant, s. Roth-Isigkeit KIR 2025, 356.

13 Art. 37 Abs. 1 Data Act.

14 Ausf. Dieckhoff/Hempel MMR 2025, 494.

15 Für eine Zuständigkeit der „Datenschutzbehörden“: Hollas, Ausschuss-Drs. 21(23) 41, 2.

16 Kugelman, Ausschuss-Drs. 21(23) 42, 5.

17 Vgl. DA-DG-RefE v. 5.2.2025, 26 und zu § 3 Abs. 1; Dieckhoff/Hempel, MMR 2025, 494.

18 So zB DSK, Stellungnahme v. 13.3.2025 zum Data-Act-Durchführungsgesetz, S. 2 f.; Schmidt/Rätze WRP 2025, I.

19 AA zB Bundesrat, Stellungnahme zu BR-Drs. 636/25, 2; Glatzner, Ausschuss-Drs. 21(23) 40, 7.

20 Ausf. Dieckhoff/Hempel MMR 2025, 494.

21 Dieckhoff/Hempel MMR 2025, 494 (497).

22 Dieckhoff/Hempel MMR 2025, 494 (497).

23 DA-DG-RefE v. 5.2.2025, 27 zu § 3 Abs. 5.

24 Dieckhoff/Hempel MMR 2025, 494 (498).

25 BT-Drs. 21/2998.

26 BT-Drs. 21/4089.

II. Datenschutzaufsicht im Data Act

Nach dem gescheiterten Referentenentwurf Anfang 2025 hat der Bundestag den zweiten Anlauf des Gesetzgebers zur nationalen Umsetzung des Data Act nunmehr verabschiedet. Als Verordnung gilt der Data Act zwar unmittelbar in allen Mitgliedstaaten, er verpflichtet sie jedoch zu regeln, welche Behörde die Anwendung des Data Act überwacht.¹³

1. Was bisher geschah – der Referentenentwurf der Ampel und seine Schwächen

Anfang 2025 veröffentlichte das Bundesministerium für Wirtschaft und Klimaschutz einen Referentenentwurf für ein Data-Act-Durchführungsgesetz (DA-DG-RefE),¹⁴ der die behördliche Zuständigkeit zur Überwachung des Data Act regelte. Demnach sollte die Bundesnetzagentur (BNetzA) grundsätzlich zuständig sein (§ 2 Abs. 1 DA-DG-RefE).¹⁵ Daneben begründete der Entwurf eine Sonderzuständigkeit der BfDI für die Überwachung der Einhaltung des Datenschutzrechts iRd Data Act (§ 3 Abs. 1 DA-DG-RefE). Nach außen hin sollte zwar allein die BNetzA auftreten, die datenschutzrechtliche Bewertung der BfDI aber Teil dieser Entscheidung sein (§ 3 Abs. 6 S. 1 DA-DG-RefE). Diese Letztentscheidungskompetenz der BNetzA wird zT als bedenkliches Ungleichgewicht zwischen einer gleichrangigen Behördentätigkeit kritisiert.¹⁶

Damit verfolgte der Gesetzgeber drei Ziele: Die datenschutzrechtliche Expertise der BfDI sollte in die Entscheidungen der BNetzA einfließen, es sollte kein Abstimmungsaufwand zwischen zahlreichen Landesdatenschutzbeauftragten und der BNetzA entstehen und Unternehmen sollten nur einer zuständigen Datenschutzbehörde gegenüberstehen.¹⁷ Die geplante Sonderzuständigkeit der BfDI entfachte Diskussionen über ihre Vereinbarkeit mit den Zuständigkeitsregelungen in Art. 37 Abs. 3 Data Act und § 40 Abs. 1 BDSG sowie den Gesetzgebungskompetenzregelungen im GG.¹⁸ Im Ergebnis ist eine solche Sonderzuständigkeit mit diesen Vorschriften vereinbar,¹⁹ der DA-DG-RefE wies bei ihrer Umsetzung jedoch Schwächen auf.²⁰ Dazu gehörten vor allem:

■ Der DA-DG-RefE regelte nicht, ob die BNetzA die BfDI im Rahmen ihrer Letztentscheidungskompetenz überstimmen kann.²¹ Eine Auslegung von § 3 Abs. 6 DA-DG-RefE legte nahe, dass dies nicht möglich ist. Der Wortlaut schützte die Unabhängigkeit der BfDI jedoch nicht ausdrücklich.

■ Unklar blieb, zu welchem Zeitpunkt die BNetzA die BfDI in ihre Entscheidung einbeziehen muss, dh ob bereits bei der Frage des Personenbezugs oder erst danach.²² Nach dem Wortlaut von § 3 Abs. 5 DA-DG-RefE prüft die BNetzA zunächst selbst, ob personenbezogene Daten betroffen sind, und bezieht die BfDI erst anschließend ein. Die Gesetzesbegründung hingegen sah eine Einbindung der BfDI bereits bei der Frage des Personenbezugs vor.²³

■ Der DA-DG-RefE grenzte die Zuständigkeiten der Datenschutzbehörden untereinander nicht ab.²⁴ Für Unternehmen drohte eine Doppelzuständigkeit von BfDI (Data Act) und Landesdatenschutzbeauftragten (DS-GVO).

Der DA-DG-RefE verfehlte damit seine eigenen Ziele. Das Ende der Ampelkoalition und die sachliche Diskontinuität des Gesetzgebungsprozesses eröffneten dem Gesetzgeber die Möglichkeit, diese Schwächen zu beheben.

2. Bringt das neue Data-Act-Durchführungsgesetz Verbesserungen?

Ende 2025 legte die Bundesregierung den neuen Regierungsentwurf für ein Data-Act-Durchführungsgesetz vor,²⁵ den der Bundestag nunmehr in leicht abgewandelter Form²⁶ verabschiedet hat. Das Data-Act-Durchführungsgesetz hält an der grund-

sätzlichen Zuständigkeit der BNetzA und der Sonderzuständigkeit der BfDI fest.²⁷ Wohl aufgrund der Diskussionen um die Vereinbarkeit der Sonderzuständigkeit mit geltendem Recht, begründet der DA-DG nun aber ausführlicher, warum diese mit den bestehenden Vorschriften vereinbar ist.²⁸ Unter Verweis auf Art. 51 DS-GVO führt das Gesetz aus, dass die Benennung der zuständigen Aufsichtsbehörde den Mitgliedstaaten obliegt und der EU-Gesetzgeber dazu neutral bleibt.²⁹ Gleichwohl sieht der DA-DG punktuelle Anpassungen bei der Ausgestaltung der Aufsicht vor. Diese adressieren die Schwächen des DA-DG-RefE aber nur teilweise.

§ 3 Abs. 2 DA-DG regelt weiterhin die kooperative und vertrauensvolle Zusammenarbeit zwischen BfDI und BNetzA sowie die zuvor in Absatz 4 enthaltene Unterstützung durch die BfDI bei allen Fragen hinsichtlich des Schutzes personenbezogener Daten. Die Gesetzesbegründung sieht nun außerdem vor, dass die Behörden Leitlinien zu Grundsatzfragen ausarbeiten, um den Abstimmungsaufwand zu reduzieren.³⁰ Konkrete Verfahren, um die Komplexität der Abstimmung zu verringern, enthält der DA-DG hingegen nicht.³¹

Neu ist die Pflicht der BfDI in § 3 Abs. 3 DA-DG, ihrerseits die BNetzA zu beteiligen, wenn sie Bezüge zum Data Act feststellt. Diese Pflicht fördert eine kooperative Zusammenarbeit. Offen bleibt jedoch, wie die Landesdatenschutzbeauftragten mit einem möglichen Bezug zum Data Act umgehen müssen. Wie bereits der DA-DG-RefE regelt auch der DA-DG, dass die BNetzA die BfDI beteiligt, wenn ihre Entscheidung die „Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten“ erfordert (§ 3 Abs. 4 DA-DG). Der Wortlaut schreibt also weiterhin nicht vor, dass die BNetzA die BfDI bereits bei der Frage des Personenbezugs einbindet. Die Gesetzesbegründung sieht zwar eine Einbindung der BfDI schon bei der „initialen Prüfung“ vor, ob eine Verarbeitung personenbezogener Daten vorliegt. Der Widerspruch zwischen Gesetzeswortlaut und -begründung bleibt aber bestehen.³² Die Entscheidung der BfDI bleibt nach § 3 Abs. 5 DA-DG Bestandteil der Entscheidung der BNetzA und ist nicht separat anfechtbar.³³ Der neue Wortlaut stellt nun aber ausdrücklich klar, dass die BNetzA an die Entscheidung der BfDI gebunden ist.

Diese Klarstellung ist erfreulich, da sie die Unabhängigkeit der BfDI klarer berücksichtigt und eine Auslegung der Vorschrift entbehrlich macht. Die Gefahr der Doppelzuständigkeit von BfDI und Landesdatenschutzbeauftragten adressiert der DA-DG weiterhin nicht.³⁴ Die Gesetzesbegründung betont sogar, dass eine Regelung zur Zusammenarbeit der BNetzA mit den Landesdatenschutzbeauftragten nicht erforderlich sei.³⁵ Die BfDI sei für die „Überwachung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten“ zuständig, für Fragen über den Anwendungsbereich des Data Act hinaus bestehe kein Regelungsbedarf.³⁶ Dies ist allerdings kritisch zu bewerten.³⁷

Denn die Begründung wirft eher weitere Fragen auf, statt Klarheit zu schaffen. Der DA-DG lässt nicht nur offen, wie die Zusammenarbeit mit den Landesdatenschutzbeauftragten erfolgen soll. Es formuliert jetzt auch uneinheitlich, wofür die BfDI zuständig sein soll, sodass weitere Abgrenzungsschwierigkeiten drohen. Während § 3 Abs. 1 und Abs. 2 DA-DG die Zuständigkeit der BfDI für Fragen des „Schutzes personenbezogener Daten“ vorsehen, dh die DS-GVO insgesamt, sprechen die nachstehenden Normen von einer Zuständigkeit für die Prüfung der „Rechtmäßigkeit“ der Verarbeitung. Unter der DS-GVO betrifft der Grundsatz der Rechtmäßigkeit der Verarbeitung jedoch die Frage, ob die Verarbeitung von einer Rechtsgrundlage gedeckt ist und nicht, ob sie den datenschutzrechtlichen Anforderungen insgesamt genügt.³⁸

Auch die Gesetzesbegründung des DA-DG bleibt diesbezüglich unklar. Als Beispiele dafür, was über den Anwendungsbereich des Data Act hinausgeht und damit der Zuständigkeit der Landesdatenschutzbeauftragten unterliegt, nennt der Gesetzgeber das Recht auf Auskunft in Art. 15 DS-GVO und das Recht auf Datenübertragbarkeit in Art. 20 DS-GVO.³⁹ Als Beispiel für die Zuständigkeit der BfDI nennt er Fälle, in denen ein Herausgabeverlangen von Daten die Prüfung erfordert, ob dafür eine Rechtsgrundlage nach Art. 6 DS-GVO besteht.⁴⁰ Vieles spricht jedoch dafür, dass der DA-DG keine Beschränkung der Sonderzuständigkeit vorsieht. Nicht nur § 3 Abs. 1 und Abs. 2 DA-DG normieren eine umfassende Zuständigkeit der BfDI. Auch bei der Bewertung des Erfüllungsaufwands des Bundes geht der DA-DG von einer weitreichenden Zuständigkeit der BfDI aus, Sachverhalte mit datenschutzrechtlichem Bezug zu bewerten.⁴¹ Die Bundesregierung ging im Nachgang zum Regierungsentwurf für das Data-Act-Durchführungsgesetz ebenfalls davon aus, dass die BfDI für die Aufsicht über „die Verarbeitung personenbezogener Daten“ zuständig ist.⁴² Die BfDI selbst geht in ihrer Stellungnahme auch von einer „datenschutzrechtlichen Zuständigkeit“ aus.⁴³ Dafür spricht auch der Sinn und Zweck der Sonderzuständigkeit: Sie soll den Abstimmungsbedarf für Unternehmen reduzieren. Andernfalls wäre stets auch eine/r der Landesdatenschutzbeauftragten zuständig, etwa für die Frage, ob die betroffene Person nach Art. 13 DS-GVO oder Art. 14 DS-GVO informiert wurde. Besonders deutlich zeigt sich dies beim Recht auf Löschung: Es ist zwar ein Betroffenenrecht, erfordert aber zugleich die Prüfung, ob eine Rechtsgrundlage für die Datenverarbeitung besteht. Diese miteinander verwobenen Fragen unterschiedlichen Aufsichtsbehörden zuzuweisen, kann weder gemeint noch gewollt sein.

Im Ergebnis wird der DA-DG dem gesetzgeberischen Ziel einer einheitlichen Datenschutzaufsicht nicht gerecht. Das Risiko einer Doppelzuständigkeit mit widersprüchlichen Bewertungen und einer (weiteren) Zersplitterung der Datenschutzaufsicht besteht fort.⁴⁴ Unternehmen sehen sich damit genau den Herausforderungen gegenüber, die der DA-DG eigentlich beseitigen will.

27 Gegen eine Sonderzuständigkeit zB Kugelman, Ausschuss-Drs. 21(23) 42, 8; Glatzner, Ausschuss-Drs. 21(23) 40, 9 f.; für eine Sonderzuständigkeit zB: Dose, Ausschuss-Drs. 21(23) 38, 3; Schmidt-Kessel, Ausschuss-Drs. 21(23) 48, 7; Zech, Ausschuss-Drs. 21(23) 52, 1.

28 Der Bundesrat hält das für fraglich, s. Stellungnahme zu BR-Drs. 636/25, 2.

29 BT-Drs. 21/2998, 26; Dieckhoff/Hempel MMR 2025, 494 (495).

30 BT-Drs. 21/2998, 28.

31 Zur Kritik an fehlenden Fristen und abgestimmten Verfahren: Bitkom, Stellungnahme Data Act – Durchführungsgesetz Kabinettsentwurf Januar 2026, S. 2, abrufbar unter: <https://www.bitkom.org/sites/main/files/2026-01/bitkom-stellungnahme-data-act-durchfuehrungsgesetz-kabinettsentwurf.pdf>.

32 Ausf. Dieckhoff/Hempel MMR 2025, 494 (497).

33 Die Gesamtentscheidung der BNetzA erfährt weiterhin Kritik vom Bundesrat (Stellungnahme zu BR-Drs. 636/25, 4); dem hält die Bundesregierung entgegen, dass der nationale Gesetzgeber eine Anlaufstelle bestimmen muss, um nicht gegen EU-Recht zu verstoßen (Bundesregierung, Gegenäußerung zu BR-Drs. 636/25, 3); im Ergebnis beeinträchtigt die Letztentscheidungsbefugnis der BNetzA die Unabhängigkeit der BfDI nicht, s. Dieckhoff/Hempel MMR 2025, 494 (499).

34 Auch der Bundesrat sieht die Gefahr der Doppelzuständigkeit und die Notwendigkeit, die Zusammenarbeit mit den Landesdatenschutzbeauftragten zu regeln (Stellungnahme zu BR-Drs. 636/25, 2).

35 BT-Drs. 21/2998, 28.

36 BT-Drs. 21/2998, 28.

37 Im Ergebnis: Kugelman, Ausschuss-Drs. 21(23)42, 4; Dose, Ausschuss-Drs. 21(23)38, 3; Süme, Ausschuss-Drs. 21(23)46, 3.

38 Gola/Heckmann, DS-GVO BDSG/Pöters, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 7; BeckOK Datenschutzrecht/Schantz, 54. Ed., DS-GVO Art. 5 Rn. 5.

39 BT-Drs. 21/2998, 28.

40 BT-Drs. 21/2998, 29.

41 BT-Drs. 21/2998, 23.

42 Bundesregierung, Gegenäußerung zu BR-Drs. 636/25, 2.

43 BfDI, Ausschuss-Drs. 21(23) 50, 3.

44 Im Ergebnis auch: Kugelman, Ausschuss-Drs. 21(23) 42, 8; Glatzner, Ausschuss-Drs. 21(23) 40, 7 f.; Zech, Ausschuss-Drs. 21(23) 52, 2.

III. Datenschutzaufsicht bei politischer Werbung

Auch bei der TTPW-VO⁴⁵ muss der Gesetzgeber festlegen, wie die Aufsicht über die datenschutzrechtlichen Aspekte der Verordnung ausgestaltet werden soll.⁴⁶ Die Verordnung ist am 18.10.2025 in Kraft getreten und hat spürbare Reaktionen ausgelöst: Mehrere große Plattformen – darunter Google, ByteDance, X und Meta – haben das Ausspielen politischer Werbung in der EU eingestellt. Meta begründete diesen Schritt ausdrücklich mit der TTPW-VO.⁴⁷ Gleichwohl haben weder der Referenten- noch Regierungsentwurf des deutschen Umsetzungsgesetzes in der Debatte um die Neuordnung der Datenschutzaufsicht bislang eine zentrale Rolle gespielt. Die vorhandene Literatur beschränkt sich weitgehend auf inhaltliche Übersichten,⁴⁸ und behandelt die Aufsichtsstruktur nur am Rande. Gleiches gilt für die Rückmeldungen zum Referentenentwurf.⁴⁹

Diese Zurückhaltung überrascht. Die TTPW-VO verschiebt die datenschutzrechtlichen Leitplanken für politische Werbung grundlegend. Sie regelt insbesondere, unter welchen Voraussetzungen personenbezogene Daten für das „Targeting und die Anzeigenschaltung“ (im Folgenden: Targeting) von politischer Werbung im Internet verwendet werden dürfen. Dies betrifft nicht nur politische Parteien, sondern auch, in verschiedenen Abstufungen, sämtliche Akteure im Umfeld „politischer Werbung“: Parteien, Plattformen, Werbe- und PR-Agenturen, Influencer sowie Datenanalyse- und Maklerunternehmen.⁵⁰ Für viele von ihnen schränkt die Verordnung datengetriebene Einflussmöglichkeiten auf politische Meinungsbildung erheblich ein. Ziel dieser neuen Regeln ist mehr Transparenz von politischer Werbung vor, während und zwischen Wahlen und ein gestärkter demokratischer Diskurs.

⁴⁵ VO (EU) 2024/900 des Europäischen Parlaments und des Rates v. 13.3.2024 über die Transparenz und das Targeting politischer Werbung.

⁴⁶ Art. 22 TTPW-VO.

⁴⁷ Meta, Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation, Juli 2025, abrufbar unter: <https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>.

⁴⁸ Vgl. zB di Fabio MMR 2024, 467; Gutjahr NVwZ 2025, 1307 und Panahi/Schindler K&R 2024, 621.

⁴⁹ Abrufbar unter: <https://bmds.bund.de/service/gesetzgebungsverfahren/politische-werbung-transparenz-gesetz-pwtg>.

⁵⁰ Vgl. Erwägungsgrund 1 TTPW-VO.

⁵¹ Vgl. Harker, Legal Studies 2020, 151; Caspar ZRP 2024, 90.

⁵² Umkehrschluss aus Art. 2 Abs. 3 TTPW-VO, s. zudem Erwägungsgrund 113 TTPW-VO.

⁵³ Vgl. Art. 2 und 3 TTPW-VO: „Politische Werbung“ meint die Ausarbeitung, Platzierung, Förderung, Veröffentlichung, Zustellung oder Verbreitung einer Botschaft mithilfe eines beliebigen Mittels, die in der Regel gegen Entgelt oder im Rahmen interner Tätigkeiten oder als Teil einer politischen Werbekampagne erfolgt, a) durch oder für einen politischen Akteur oder in seinem Namen, es sei denn, sie ist rein privater oder rein kommerzieller Natur; oder b) die geeignet und darauf ausgerichtet ist, das Ergebnis einer Wahl oder eines Referendums, ein Abstimmungsverhalten oder einen Rechtsetzungs- oder Regulierungsprozess auf Unionsebene oder auf nationaler, regionaler oder lokaler Ebene zu beeinflussen; nicht erfasst sind bestimmte amtliche und parteiinterne Kommunikationen, vgl. Gutjahr NVwZ 2025, 1307 (1310).

⁵⁴ Zum Inhalt vgl. Kalveram NJW 2024, 3702.

⁵⁵ S. Commission Staff Working Document, Impact Assessment Report accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising, 25.11.2021, SWD (2021) 355 final, Nr. 1, 3, 25.

⁵⁶ Vgl. Kruschinski/Haller Internet Policy Review 2017, 1.

⁵⁷ Vgl. Caspar ZRP 2024, 90 mit Verweis auf prominente Beispiele.

⁵⁸ Gutjahr NVwZ 2025, 1307 (1308).

⁵⁹ Harker Legal Studies 2020, 151 (152).

⁶⁰ Vgl. Gutjahr NVwZ 2025, 1307.

⁶¹ Gem. Art. 4 Nr. 7 DS-GVO.

⁶² S. Erwägungsgrund 77 TTPW-VO; zudem verbietet Art. 18 Abs. 2 TTPW-VO das Targeting, wenn der Verantwortliche mit hinreichender Sicherheit annehmen kann, dass die betroffene Person das nationale Wahlalter erst innerhalb des nächsten Jahres erreichen wird.

Bereits dies rechtfertigt einen breiten Diskurs über Auswirkungen der Verordnung auf politische Meinungsfreiheit sowie Chancengleichheit für politische Akteure.⁵¹ Hinzu kommt eine dogmatische „Besonderheit“: Die datenschutzrechtlichen Regelungen der TTPW-VO sind „lex specialis“ zur DS-GVO und lassen diese gerade nicht „unberührt“. ⁵² Darin unterscheidet sich die TTPW-VO sowohl vom Data Act als auch von anderen Digitalrechtsakten wie dem Digital Services Act (DSA), der KI-VO und dem Digital Markets Act (DMA). In diesem Potpourri digitalrechtlicher Interessen muss der deutsche Gesetzgeber entscheiden, welche Behörde(n) die datenschutzrechtlichen Aspekte der TTPW-VO beaufsichtigen sollen. Dabei stellt sich erneut die Frage nach der Kompetenzverteilung zwischen Bund und Ländern.

1. Datenschutzrechtliche Regelungen der TTPW-VO

Bislang existierte in der EU weder eine einheitliche Definition noch ein harmonisiertes Regelungsregime für „politische Werbung“. Die TTPW-VO ändert dies grundlegend. Sie führt eine weite Definition ein, die sowohl in „klassischen Medien“ als auch online ausgespielte Werbung umfasst,⁵³ und etabliert einheitliche Transparenz- und Sorgfaltspflichten für politische Werbung sowie damit verbundene Dienstleistungen.⁵⁴

Aus datenschutzaufsichtsrechtlicher Sicht relevant ist das neue Regelungsregime für Targeting. Hintergrund war der Wunsch der EU-Kommission nach klaren Leitplanken für politisches Microtargeting.⁵⁵ Dabei nutzen politische Akteure Profiling-Methoden, um Wählerinnen und Wähler gezielt anzusprechen, bestimmte Themen hervorzuheben oder individuelle Anfälligkeiten auszunutzen, um Wahlergebnisse zu beeinflussen.⁵⁶ Eine Partei kann somit verschiedene, teils gegenteilige Nachrichten an einzelne Wählerinnen und Wähler ausspielen, ohne dass dies öffentlich bekannt wird.⁵⁷ Je mehr Daten über eine Person erhoben und verarbeitet werden, desto treffsicherer ist das Targeting.⁵⁸ Dies kann die öffentliche Debatte vor und nach Wahlen erheblich beeinflussen.⁵⁹

Bislang richtete sich die Zulässigkeit dieser Art von Targeting vor allem nach der DS-GVO, insbesondere Art. 6 und 9 DS-GVO, eingerahmt durch die allgemeinen verfassungsrechtlichen Leitplanken.⁶⁰ Dies hat sich durch die TTPW-VO grundlegend geändert. Konkret regeln Art. 18, 19 und 20 TTPW-VO das Targeting bei politischer Werbung neu. Am brisantesten ist dabei Art. 18 Abs. 1 TTPW-VO. Adressaten dieser Vorschrift sind die datenschutzrechtlich Verantwortlichen.⁶¹ Targeting von Personen für politische Online-Werbung ist danach nur noch unter engen Voraussetzungen zulässig, die kumulativ vorliegen müssen:

■ Der Verantwortliche hat die personenbezogenen Daten, die er zum Targeting verwendet, bei der betroffenen Person selbst erhoben (lit. a).

■ Die betroffene Person hat ausdrücklich und gesondert in die Verarbeitung ihrer Daten zu diesem Zweck eingewilligt (lit. b mit Verweis auf Art. 9 Abs. 2 lit. h DS-GVO).

■ Das Targeting umfasst kein „Profiling“ iSv Art. 4 Nr. 4 DS-GVO unter Verwendung besonderer Kategorien personenbezogener Daten (lit. c).⁶²

Diese Änderung ist brisant. Damit ist Profiling mit Daten iSv Art. 9 DS-GVO für Zwecke des Targetings generell verboten. Zudem scheidet das berechtigte Interesse (Art. 6 Abs. 1 lit. f DS-GVO) als Rechtsgrundlage für Targeting selbst dann aus, wenn Verantwortliche ausschließlich „normale“ Daten verwenden, die eigentlich nicht unter dem besonderen Schutz von Art. 9 DS-GVO stehen. Verantwortliche benötigen nun eine ausdrückliche Einwilligung, was in der Praxis oft schwer rechtssicher umzusetzen ist. Auch der Einsatz von Datenhändlern für die Sammlung personenbezogener Daten zur Durchführung von

Targeting wird eingeschränkt.⁶³ Die datenschutzrechtliche Aufsicht über diese Vorgaben ist anspruchsvoll, da sie zahlreiche komplexe (Auslegungs-)Fragen aufwirft.

2. Zuständigkeit der BfDI – oder doch nicht?

Im Dezember 2025 veröffentlichte die Bundesregierung einen Entwurf für ein PWTG (PWTG-E)⁶⁴. Danach soll die BfDI grundsätzlich für die Überwachung der Anwendung von Art. 20 TTPW-VO zuständig sein. Art. 20 TTPW-VO regelt die Offenlegung von bestimmten Informationen im Zusammenhang mit Targeting von politischer Werbung an privilegierte Interessenten wie zB Journalisten oder Wahlbeobachter. Die Ausnahme von dieser Zuständigkeit folgt sogleich: Sie gilt nur, soweit die BfDI bereits nach dem BDSG für die Durchsetzung der DS-GVO zuständig ist (§ 2 Abs. 1 PWTG-E).

Damit schafft der PWTG-E – anders als der DA-DG – gerade keine Sonderzuständigkeit der BfDI. Auffällig ist: Der Gesetzgeber regelt auch nicht ausdrücklich, welche Behörde für die Überwachung der neuen – und im Vergleich zu Art. 20 TTPW-VO weitaus brisanteren – datenschutzrechtlichen Vorschriften zum Targeting politischer Werbung in Art. 18 und 19 TTPW-VO zuständig ist. Laut Gesetzgeber soll § 2 PWTG-E nichts an der grundsätzlich im BDSG geregelten Zuständigkeitsverteilung ändern.⁶⁵ Damit bleibt es bei der Zuständigkeitsverteilung nach § 9 Abs. 1 bzw. § 40 Abs. 1 BDSG.⁶⁶ Die Länder sind weiterhin für ihre jeweiligen Landesbehörden sowie, mit wenigen Ausnahmen, für alle nichtöffentlichen Stellen zuständig. Der Gesetzgeber begründet dieses Vorgehen mit Art. 22 Abs. 1 TTPW-VO. Danach sei dort die Zuständigkeit für die Überwachung der Anwendung der datenschutzrechtlichen Regelungen in der TTPW-VO selbst abschließend geregelt.⁶⁷ Die nach nationalem Recht zuständigen Datenschutzbehörden seien in ihrem originären Zuständigkeitsbereich auch für die Überwachung der datenschutzrechtlichen Vorschriften der TTPW-VO zuständig.⁶⁸ Eine gesonderte Zuständigkeitsregelung im PWTG-E „verbie“ sich daher.⁶⁹ Im Gegensatz dazu könne der Gesetzgeber die Zuständigkeit zur Überwachung von Art. 20 TTPW-VO festschreiben, da Art. 22 Abs. 4 TTPW-VO anders als Art. 22 Abs. 1 TTPW-VO dahingehend keine „Vorentscheidung“ trafe.⁷⁰

Die Begründung überzeugt nicht. Ein solches Verbot ergibt sich weder aus dem Wortlaut noch aus dem Sinn und Zweck von Art. 22 Abs. 1 TTPW-VO. Danach sind die Datenschutzbehörden iSv Art. 51 DS-GVO in ihrem jeweiligen Zuständigkeitsbereich auch für die Überwachung der datenschutzrechtlichen Vorschriften in der TTPW-VO verantwortlich. Der Verweis auf Art. 51 DS-GVO steht einer im nationalen Recht geregelten Sonderzuständigkeit aber nicht entgegen. Art. 51 DS-GVO regelt nicht abschließend, für welche sektoralen Bereiche die Datenschutzbehörden des Bundes und der Länder zuständig sind – die Norm verweist schlicht auf das nationale Recht. Art. 51 DS-GVO bedarf daher nationaler Ausgestaltung, wovon der Gesetzgeber bisher in §§ 9, 40 BDSG Gebrauch gemacht hat. Diese nationale Ausgestaltung kann der Gesetzgeber aber jederzeit ändern – ein Beispiel dafür ist der DA-DG.

Die TTPW-VO schreibt auch keine bestimmte innerstaatliche Aufsichtsstruktur vor. Sie stellt lediglich klar, dass die nationalen Datenschutzbehörden neben der DS-GVO auch die Vorschriften zum Targeting überwachen sollen. Dass der europäische Gesetzgeber damit die deutsche föderale Struktur auch für das Targeting politischer Werbung festschreiben wollte, liegt fern. Naheliegender ist vielmehr, dass der EU-Gesetzgeber den deutschen Sonderweg (18 Aufsichtsbehörden) nicht bedacht hat. Der Verweis auf Art. 51 DS-GVO hindert den deutschen Gesetzgeber jedenfalls nicht daran, seine nationale Aufsichtsstruktur anzupassen. Die Begründung des Gesetzgebers, eine Sonderzustän-

digkeit verbiete sich, scheint zudem mit Blick auf den Data Act konfus. Art. 37 Abs. 3 S. 1 DA enthält eine mit Art. 22 Abs. 1 TTPW-VO vergleichbare Zuständigkeitsregelung: Danach sollen die Datenschutzbehörden auch für die Überwachung aller Regelungen im Data Act zuständig sein, die den Schutz personenbezogener Daten betreffen. Obwohl einige Stimmen auch hier eine Sonderzuständigkeit der BfDI ablehnten,⁷¹ hat der Gesetzgeber bewusst einen anderen Weg gewählt (s. unter II.). Dieser stünde dem Gesetzgeber auch für die TTPW-VO offen.

In der Praxis heißt das: Die BfDI ist nur in wenigen Konstellationen originär für die Überwachung der Anwendung datenschutzrechtlicher Vorschriften in der TTPW-VO zuständig. Die Aufsicht über die typischen Stakeholder im Bereich politischer Werbung, also Parteien, Plattformen, Werbe- und PR-Agenturen sowie Influencer, verbleibt weitgehend bei den Ländern (§ 40 Abs. 1 BDSG).⁷² Die örtliche Zuständigkeit bestimmt sich dabei nach dem Sitz des Verantwortlichen.⁷³ Da nahezu alle Bundesparteien ihren Sitz in Berlin haben,⁷⁴ ist für diese Stakeholder vor allem die Berliner Landesbeauftragte für Datenschutz und Informationsfreiheit zuständig. Eine Zuständigkeit der BfDI käme regelmäßig nur bei Bundesbehörden in Betracht, die sich mit (dem Targeting von) politischer Werbung befassen.

3. Schritt in die richtige Richtung oder Schritt zur Seite?

Die Regelungen im DA-DG und im PWTG-E gehen konträr auseinander. Während der Gesetzgeber beim Data Act – entgegen aller Proteste – die Sonderzuständigkeit der BfDI mit mehr Kohärenz und weniger Ansprechpartnern für Unternehmen begründete, scheinen diese Erwägungen beim PWTG-E keine Rolle zu spielen.

Dies überrascht, da für beide Gesetzesentwürfe das BMDS zuständig war. Selten hatte ein Ministerium die Möglichkeit, die Struktur der Datenschutzaufsicht so unmittelbar zu prägen. Gleichwohl scheint dasselbe Ministerium dieselbe Rechtsfrage – „Wie ist der Verweis auf die nationalen Datenschutzbehörden zu verstehen?“ – je nach Gesetzesentwurf unterschiedlich zu bewerten. Dabei treffen die Argumente für eine Sonderzuständigkeit der BfDI im Data Act (weniger Ansprechpartner für Unternehmen, schnellere und kohärente Durchsetzung), gleichermaßen auf die TTPW-VO zu. Folglich drohen bei der Aufsicht über die TTPW-VO altbekannte Probleme: ein Thema, viele Behörden, viele Meinungen. Dabei werden Aufsichtsbehörden bei der Anwendung der TTPW-VO verschiedene Grundsatzfragen klären müssen: Wer ist (gemeinsam) Verantwortlicher für das Targeting politischer Werbung? Welche Daten sind Daten iSv Art. 9 DS-GVO? Was genau gilt in diesem Umfeld als „Profi-

⁶³ S. hierzu Kefford et al., Party Politics 2023, 448.

⁶⁴ Der Bundestag hat das PWTG nach vorheriger Befassung im Bundesrat zuletzt am 18.3.2026 als BT-Drs. 21/04089 im Digitalausschuss beraten.

⁶⁵ BT-Drs. 21/04089, 27.

⁶⁶ BT-Drs. 21/04089, 27: „Die Abgrenzung zwischen der Zuständigkeit [der BfDI] und der Zuständigkeit der [Landesdatenschutzbeauftragten] richtet sich nach dem BDSG“.

⁶⁷ BT-Drs. 21/04089, 27.

⁶⁸ BT-Drs. 21/04089, 27.

⁶⁹ BT-Drs. 21/04089, 44.

⁷⁰ BT-Drs. 21/04089, 44.

⁷¹ Vgl. Dieckhoff/Hempel MMR 2025, 494.

⁷² Der Bundesrat hatte gefordert, die Rolle der LfDI im Gesetzestext „angemessen abzubilden“. Der Bund solle insbesondere prüfen, ob die Fokussierung im PWTG-E auf die BfDI „sachlich gerechtfertigt“ sei oder ob zusätzlich auch Regelungen für den Zuständigkeitsbereich der LfDI getroffen werden sollten, vgl. BT-Drs. 21/04089, 38, 42. Die Bundesregierung hat diesen Vorschlag mit Verweis auf die oben dargestellten Argumente abgelehnt, vgl. BT-Drs. 21/04089, 44. Die BfDI hingegen hat sich dem Bundesrat angeschlossen: Die Rolle der Landesdatenschutzbeauftragten solle deutlicher abgebildet werden, um Auslegungsschwierigkeiten vorzubeugen, vgl. BfDI, Ausschuss-Drs. 21(23) 58, 3.

⁷³ § 40 Abs. 2 S. 3 VwVfG iVm § 3 Abs. 1 Nr. 3 VwVfG.

⁷⁴ Die CSU hat ihren Sitz in München.

ling“? Welche Behörde ist bei grenzüberschreitender Datenverarbeitung zuständig?⁷⁵ Die Antworten auf diese Fragen sind über das Feld der politischen Werbung hinaus relevant. Bei deren Beantwortung werden abermals bis zu 18 verschiedene Datenschutzbehörden mitmischen, mit allen Vor- und Nachteilen.

Nichtsdestotrotz ist das PWTG-E gewappnet für eine umfassendere Reform der Datenschutzaufsicht. Durch den Verweis auf die Zuständigkeitsregeln des BDSG ist das Wohl und Wehe der Aufsicht im Bereich politischer Werbung von jenen Vorschriften unmittelbar abhängig. Ändert sich die Zuständigkeit im BDSG, ändert sich auch die Zuständigkeit im PWTG-E.

IV. Zusammenfassung und Ausblick

Die neue Bundesregierung und insbesondere das BMDS haben sich den Abbau von Bürokratie und komplizierten Verwaltungswegen zum Ziel gesetzt. Bei der Umsetzung des Data Acts war seitens des BMDS gar von „innovationsfreundlich[er]“ Umsetzung europäischen Rechts „ohne Schnörkel“ die Rede.⁷⁶ Zwar mag dies auf einige der umgesetzten Vorschriften zutreffen.⁷⁷ Für die Datenschutzaufsicht in den neuen Digitalgesetzen hat der Gesetzgeber dieses Ziel aber (bisher) nur teilweise erreicht.

Für die TTPW-VO hat der Gesetzgeber keinen zentralen Ansprechpartner für datenschutzrechtliche Fragen geschaffen, obwohl Unternehmensvertreter dies hoffnungsvoll erwartet hatten.⁷⁸ Stattdessen konterkariert der Gesetzgeber iRd PWTG-E die Harmonisierung der Datenschutzaufsicht, die er an anderer Stelle anstrebt, durch einen Rückzug auf den eigens kritisierten Status quo. Im Data Act sieht der Gesetzgeber die BfDI zwar als zentrale Ansprechpartnerin für datenschutzrechtliche Fragen vor. Im Ergebnis wird das Konzept aber zu einer Doppelzuständigkeit führen, da der Gesetzgeber nicht regelt, wie mit Überschneidungen mit der DS-GVO zu verfahren ist.

⁷⁵ Für die DS-GVO s. Auernhammer, DSGVO BDSG/Hermerschmidt/Hempel, 8. Aufl. 2024, BDSG §§ 18, 19.

⁷⁶ BMDS, PM 22/2025, abrufbar unter: <https://bmds.bund.de/aktuelles/pressemitteilungen/detail/kabinett-beschliesst-data-act-durchfuehrungsgesetz>.

⁷⁷ Dose MMR 2025, 591.

⁷⁸ Der BVDW ging davon aus, dass die Zuständigkeit mit Benennung der BfDI „klar“ geregelt werde und hatte vermutlich den Verweis in das BDSG übersehen, Stellungnahme des BVDW vom 29.8.2025, abrufbar unter: https://bmds.bund.de/fileadmin/BMDS/Dokumente/Gesetzesvorhaben/250829_14.29_RefE_PWG_25.7._SN_BVDW_geschw%C3%A4rzt.pdf.

⁷⁹ Dieckhoff/Hempel MMR 2025, 494 (499).

Noch ist nicht aller Tage Abend. Der Gesetzgeber hat bis zu seinem selbstgesteckten Ziel Ende 2027 noch Zeit, die hier aufgezeigten Verbesserungsvorschläge aufzugreifen. Bereits laufende und künftige Gesetzgebungsvorhaben sollten die geplante Neuordnung der Datenschutzaufsicht mitdenken. Andernfalls verabschiedet der Gesetzgeber Rechtsakte, die dem von der Bundesregierung selbst gesteckten Ziel – Reform der Datenschutzaufsicht bis Ende 2027 – zuwiderlaufen.

Wie schon an anderer Stelle angeregt,⁷⁹ sollte der Gesetzgeber die Aufsicht nach DS-GVO und den verschiedenen Digitalrechtsgesetzen aus einem Guss denken. Andernfalls perpetuieren sich die oftmals kritisierten Irrungen und Wirrungen datenschutzrechtlicher Zuständigkeiten. Das dient weder Unternehmen noch Betroffenen und widerspricht auch dem Interesse der Behörden an einer klaren Aufgabenverteilung.

Schnell gelesen ...

- Das Data-Act-Durchführungsgesetz behebt die Schwächen des Referentenentwurfs nur teilweise und trägt nicht ausreichend zur Vereinheitlichung der Datenschutzaufsicht bei. Es droht weiterhin eine Doppelzuständigkeit.
- Für die EU-Verordnung zur politischen Werbung hat der Gesetzgeber keinen zentralen Ansprechpartner für datenschutzrechtliche Fragen geschaffen, sondern verteilt die Zuständigkeit auf alle 18 Datenschutzbehörden.
- Zur Verhinderung einer (weiteren) Zersplitterung der Datenschutzaufsicht sollte der Gesetzgeber die Aufsicht nach DS-GVO und den verschiedenen Digitalrechtsgesetzen aus einem Guss denken.



Dr. Anke Dieckhoff
ist Rechtsanwältin bei Bird & Bird LLP in Frankfurt/M.



Dr. Felix Hempel, LL.M.,
ist Rechtsanwalt bei Bird & Bird LLP in Frankfurt/M. sowie Honorary Research Fellow am Department of Law der Queen Mary University London.

ANNA LENA NOWICKI / LISA FLECKENSTEIN / LUCAS BLUM / DANIEL WERNER

Diensteanbieter im Fokus der e-Beweismittelsicherungs-Verordnung

Alles neu bei elektronischen Beweismitteln?

Strafverfolgung

Der Beitrag geht auf die rechtlichen Voraussetzungen für den Erlass Europäischer Sicherungs- und Herausgabeanordnungen nach der e-Beweismittelsicherungs-Verordnung, dem Gesetz zur Durchführung der Verordnung und der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL ein; außerdem befasst er sich mit den daraus resultierenden Pflichten und Mitwirkungsobliegenheiten von Diensteanbietern. Ausgehend von den vier Datenkategorien der e-Beweismittelsicherungs-Verordnung wird

abgeleitet, unter welchen formellen und materiellen Bedingungen Europäische Sicherungs- und Herausgabeanordnungen erlassen werden. Der Beitrag ist eine praxisorientierte Leitlinie, mit der Diensteanbieter Europäische Herausgabe- und Sicherungsanordnungen im Anwendungsbereich der e-Beweismittelsicherungs-Verordnung rechtssicher handhaben können.

Lesedauer: 26 Minuten

I. Einleitung

Mit der e-Beweismittelsicherungs-Verordnung (auch bezeichnet als sog. e-Evidence-VO)¹ hat die EU ein neues Instrument geschaffen, um Strafverfolgungsbehörden den grenzüberschreitenden Zugriff auf elektronische Beweismittel in Strafverfahren zu erleichtern. Flankiert wird die e-Beweismittelsicherungs-Verordnung durch die e-Beweismittel-Diensteanbieter-Rechtshilfe-RL.² Hintergrund ist die zunehmende Bedeutung digitaler Dienste für kriminelle Aktivitäten. Allerdings stehen Strafverfolgungsbehörden bei der Beweismittelbeschaffung aufgrund der grenzüberschreitenden Nutzung elektronischer Kommunikation und der Speicherung von relevanten Daten durch Diensteanbieter³ in verschiedenen Ländern vor erheblichen Herausforderungen. Aber auch Diensteanbieter finden in der EU bislang lediglich fragmentierte rechtliche Rahmenbedingungen vor, die es ihnen erschweren, Ersuchen von Strafverfolgungsbehörden nachzukommen.⁴

Hier knüpfen die Regelungen der e-Beweismittelsicherungs-Verordnung und der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL sowie die nationalen Durchführungs- und Umsetzungsgesetze an. Sie führen dazu, dass sich Behörden und Diensteanbieter mit dem neuen Rechtsregime vertraut machen und etablierte Prozesse überarbeiten und neu ausrichten müssen. Im Folgenden wird auf die Europäische Herausgabe-⁵ und Europäische Sicherungsanordnung⁶ nach der e-Beweismittelsicherungs-Verordnung und deren Voraussetzungen eingegangen. Daneben wird dargestellt, welche Pflichten Diensteanbieter unter der e-Beweismittelsicherungs-Verordnung, der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL und den nationalen Durchführungs- und Umsetzungsgesetzen – am Beispiel der Rechtslage in Deutschland – treffen und wie sie Herausgabe- und Sicherungsanordnungen bearbeiten müssen.

II. Hintergrund

1. e-Beweismittelsicherungs-Verordnung

Strafverfolgungsbehörden eines EU-Mitgliedstaats können auf der Grundlage der e-Beweismittelsicherungs-Verordnung künftig Herausgabeanordnungen (Art. 5 e-Beweismittelsicherungs-Verordnung) oder Sicherungsanordnungen (Art. 6 e-Beweismittelsicherungs-Verordnung) unmittelbar an Diensteanbieter in einem anderen EU-Mitgliedstaat richten, ohne den bisher rechtlich vorgeschriebenen Weg über Rechtshilfeersuchen oder Europäische Ermittlungsanordnungen gehen zu müssen.⁷ Während Herausgabeanordnungen auf die Herausgabe von elektronischen Beweismitteln gerichtet sind, verpflichten Sicherungsanordnungen den Diensteanbieter die elektronischen Beweismittel zu sichern, damit diese zu einem späteren Zeitpunkt für eine Herausgabeanordnung verfügbar sind.

Die e-Beweismittelsicherungs-Verordnung erfasst in ihrem Anwendungsbereich Kommunikationsdienste (Art. 3 Nr. 3 lit. a e-Beweismittelsicherungs-Verordnung) wie zB Messenger-Dienste, E-Mail-Dienste, soziale Netzwerke sowie Cloud-Computing-Dienste nach Art. 3 Nr. 3 lit. c sublit. ii e-Beweismittelsicherungs-Verordnung als „andere Dienste der Informationsgesellschaft“.⁸ Für die Eröffnung des Anwendungsbereichs ist darüber hinaus entscheidend, dass es sich bei dem Anordnungsgegenstand um einen grenzüberschreitenden Fall sowie um elektronische Beweismittel handelt, die zum Zeitpunkt des Eingangs der jeweiligen Anordnung bereits bei dem Diensteanbieter vorliegen (Art. 3 Nr. 8 e-Beweismittelsicherungs-Verordnung).⁹ Eine Echtzeitüberwachung (etwa durch Live-TKÜ) fällt daher nicht unter die e-Beweismittelsicherungs-Verordnung, genauso wenig wie die Vorratsdatenspeicherung.¹⁰

Für die Frage, ob ein grenzüberschreitender Fall¹¹ vorliegt und ausländische Behörden eine Anordnung überhaupt erlassen dürfen, ist weder der Ort entscheidend, an dem die der Anordnung zugrunde liegende Straftat begangen wurde bzw. die betroffene Person ansässig ist (vgl. Art. 8 Abs. 2 e-Beweismittelsicherungs-Verordnung) noch wo die fraglichen Daten verarbeitet werden, sondern allein der Sitz des für den jeweiligen Diensteanbieter handelnden Adressaten der Anordnung (Art. 1 Abs. 1 e-Beweismittelsicherungs-Verordnung).¹² Hervorzuheben ist, dass Diensteanbieter in der EU, die ihre Dienste nur außerhalb der EU anbieten, nicht in den Anwendungsbereich fallen (Art. 2 Abs. 1 und Abs. 3 sowie Erwägungsgrund 26 e-Beweismittelsicherungs-Verordnung).¹³ Das entscheidende Kriterium für den Geltungsbereich der e-Beweismittelsicherungs-Verordnung ist damit unter Anwendung des Marktortprinzips das Anbieten eines Dienstes in der EU.¹⁴

2. e-Beweismittel-Diensteanbieter-Rechtshilfe-RL

Mit der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL sollen einheitliche Vorschriften für die Vertretung bestimmter Diensteanbieter in der EU sichergestellt werden. Hierdurch soll gewährleistet werden, dass Beschlüsse der Strafverfolgungsbehörden entgegengenommen, befolgt und durchgesetzt werden können.¹⁵ Die EU-Mitgliedstaaten sollen eine oder mehrere zentrale Behörden benennen, um die kohärente Anwendung der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL sicherzustellen (Art. 6 Abs. 1 e-Beweismittel-Diensteanbieter-Rechtshilfe-RL). Die e-Beweismittel-Diensteanbieter-Rechtshilfe-RL verpflichtet die EU-Mitgliedstaaten bis spätestens zum 18.2.2026 die zur Umsetzung erforderlichen Rechts- und Verwaltungsvorschriften zu erlassen.

3. Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz

In Deutschland erfolgt die Umsetzung der e-Beweismittel-Diensteanbieter-Rechtshilfe-RL in einem neuen Stammgesetz – dem Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz (EBewMG) – in dem auch die Vorgaben zur Durchführung der e-Beweismittelsicherungs-Verordnung aufgenommen sind. Das EBewMG ist zum Großteil am 13.3.2026 in Kraft getreten; am 18.8.2026 treten einzelne weitere Vorschriften in Kraft.¹⁶

¹ VO (EU) 2023/1543 des Europäischen Parlaments und des Rates v. 12.7.2023 über Europäische Herausgabeanordnungen und Europäische Sicherungsanordnungen für elektronische Beweismittel in Strafverfahren und für die Vollstreckung von Freiheitsstrafen nach Strafverfahren, ABl. 2023 L 191, 118.

² RL (EU) 2023/1544 des Europäischen Parlaments und des Rates v. 12.7.2023 zur Festlegung einheitlicher Regeln für die Benennung von benannten Niederlassungen und die Bestellung von Vertretern zu Zwecken der Erhebung elektronischer Beweismittel in Strafverfahren, ABl. 2023 L 191, 181.

³ ISv Art. 3 Nr. 3 e-Beweismittelsicherungs-Verordnung.

⁴ Vgl. Erwägungsgrund 6 und 9 e-Beweismittelsicherungs-Verordnung.

⁵ ISv Art. 3 Nr. 1 e-Beweismittelsicherungs-Verordnung; im Folgenden: „Herausgabeanordnung“.

⁶ ISv Art. 3 Nr. 2 e-Beweismittelsicherungs-Verordnung; im Folgenden: „Sicherungsanordnung“.

⁷ S. Art. 1 Abs. 1 e-Beweismittelsicherungs-Verordnung sowie Erwägungsgrund 18 e-Beweismittelsicherungs-Verordnung; vgl. Hüttemann NZWiSt 2024, 81 (84).

⁸ Übersichtlich zum Begriff des „Diensteanbieters“ Weiß/Pradel CCZ 2024, 102 (105 ff.) sowie Rexin CR 2025, 133 (134).

⁹ Erwägungsgrund 19 e-Beweismittelsicherungs-Verordnung.

¹⁰ Von der Groeben/F. Meyer, 8. Aufl. 2025, AEUV Art. 82 Rn. 59; Babucke wistra 2024, 57 (61).

¹¹ Vgl. Erwägungsgrund 18 e-Beweismittelsicherungs-Verordnung.

¹² Hüttemann NZWiSt 2024, 81 (88); Babucke wistra 2024, 57 (59).

¹³ Babucke wistra 2024, 57 (61); Weiß/Brinkel RD 2023, 522 (523).

¹⁴ Hüttemann NZWiSt 2024, 81 (84); Ambos ZfStW 2025, 204 (208).

¹⁵ Vgl. Erwägungsgrund 5 e-Beweismittel-Diensteanbieter-Rechtshilfe-RL.

¹⁶ Art. 4 des Gesetzes zur Umsetzung der RL (EU) 2023/1544 und zur Durchführung der VO (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union, BGBl. 2026 I Nr. 64 v. 12.3.2026.

III. Voraussetzungen der Herausgabe- und Sicherungsanordnungen

1. Datenkategorien der e-Beweismittelsicherungs-Verordnung

Die e-Beweismittelsicherungs-Verordnung differenziert zwischen drei Hauptkategorien elektronischer Beweismittel:¹⁷ Teilnehmerdaten, Verkehrsdaten und Inhaltsdaten. Daneben werden die ausschließlich zum Zweck der Identifizierung des Nutzers angeforderten Daten¹⁸ als Unterkategorie der Verkehrsdaten eingeführt. Den Datenkategorien der e-Beweismittelsicherungs-Verordnung werden in § 8 EBewMG die im deutschen Recht verwendeten Datenkategorien zugeordnet. So gelten als Teilnehmerdaten iSv Art. 3 Nr. 9 e-Beweismittelsicherungs-Verordnung insbesondere sowohl Bestandsdaten nach § 3 Nr. 6 TKG und Daten nach § 172 TKG sowie Bestandsdaten gem. § 2 Abs. 2 Nr. 2 TDDDg. Als Verkehrsdaten iSv Art. 3 Nr. 11 e-Beweismittelsicherungs-Verordnung gelten insbesondere Verkehrsdaten nach § 3 Nr. 70 TKG und Nutzungsdaten nach § 2 Abs. 2 Nr. 3 lit. b und c TDDDg. Als Identifizierungsdaten iSv Art. 3 Nr. 10 e-Beweismittelsicherungs-Verordnung gelten insbesondere Nutzungsdaten gem. § 2 Abs. 2 Nr. 3 lit. a TDDDg. Für die Kategorie der Inhaltsdaten findet sich im deutschen Recht kein unmittelbares Pendant.¹⁹

Die Differenzierung zwischen den Datenkategorien ist von entscheidender Bedeutung, wie nachfolgende Ausführungen zu den formellen und materiellen Anforderungen der Herausgabe- und Sicherungsanordnung zeigen.

2. Formelle Voraussetzungen

Für Diensteanbieter wird die Handhabung der Anordnungen im Vergleich zu auf nationales Recht gestützten Beweismittelersuchen dadurch vereinfacht, dass die e-Beweismittelsicherungs-Verordnung für alle europäischen Justiz- und Ermittlungsbehörden ein im Ausgangspunkt formalisiertes und standardisiertes Verfahren vorsieht. Die Behörden müssen die Anordnungen insbesondere in der Form der in der e-Beweismittelsicherungs-Verordnung aufgenommenen Bescheinigungen erlassen und können keine davon abweichenden nationalen Formulare verwenden (Art. 9 Abs. 1 iVm Anhang I und Anhang II e-Beweismittelsicherungs-Verordnung, Bescheinigung über eine Europäische Herausgabeanordnung – EPOC – und Bescheinigung über eine Europäische Sicherungsanordnung – EPOC-PR).

Bei formell fehlerhaften Anordnungen können Diensteanbieter gem. Art. 10 Abs. 6 e-Beweismittelsicherungs-Verordnung bzw. Art. 11 Abs. 6 e-Beweismittelsicherungs-Verordnung unverzüglich eine Klarstellung von der Anordnungsbehörde verlangen, der diese umgehend, spätestens jedoch nach 5 Tagen, nachkommen muss. Nach Art. 10 Abs. 6 S. 3 e-Beweismittelsicherungs-Verordnung gelten die Verpflichtungen zur Herausgabe der angeforderten Daten erst, wenn diese Klarstellung oder Berichtigung durch eine der zuständigen Behörden erfolgt ist. Für die weniger eingriffsintensiven Sicherungsanordnungen ordnet Art. 11 Abs. 6 S. 2 e-Beweismittelsicherungs-Verordnung weitergehend an, dass der Diensteanbieter von seinen Sicherungsverpflichtungen

befreit ist, sofern die Anordnungsbehörde nicht innerhalb der Fünftagesfrist reagiert.²⁰ Nicht zuletzt wegen des in Art. 10, 11 Abs. 6 e-Beweismittelsicherungs-Verordnung vorgesehenen Schutzmechanismus sind die formellen Anforderungen der Anordnungen von entscheidender Bedeutung.

a) Zuständige Behörde

Die e-Beweismittelsicherungs-Verordnung verfolgt für die Bestimmung der zuständigen Behörde für die Letztentscheidung über die Anordnung einen gestuften Ansatz, je nach der Schwere der in Frage stehenden Maßnahmen. Hiernach gelten Herausgabeanordnungen zu Inhalts- und solchen Verkehrsdaten, die keine Identifizierungsdaten sind, als besonders eingriffsintensiv.²¹ Als weniger gravierend wird die Herausgabeanordnung eingestuft, wenn sie sich auf Teilnehmer- und Identifizierungsdaten bezieht. Vor diesem Hintergrund differenziert Art. 4 Abs. 1 und Abs. 2 e-Beweismittelsicherungs-Verordnung zwischen der Anordnung und der Validierung (der Bestätigung) einer Anordnung und sieht hierfür auch unterschiedliche Behörden vor: die Anordnungs- sowie die Validierungsbehörde.

Die Anordnungsbehörde ist aus der Sicht des Diensteanbieters die ausländische Behörde, die die Daten im Wege der Herausgabe- oder Sicherungsanordnung ersucht. Die Validierungsbehörde befindet sich im gleichen EU-Mitgliedstaat wie die Anordnungsbehörde. Sie ist eine der Anordnungsbehörde übergeordnete Justizbehörde, die solche Anordnungen überprüft, die sich auf sensible Datenkategorien wie Verkehrs- und Inhaltsdaten beziehen oder die von Nicht-Justizbehörden („andere Behörden“) angeordnet wurden.²²

Im Vollstreckungsverfahren (Art. 16 e-Beweismittelsicherungs-Verordnung) ist die Vollstreckungsbehörde für die Anerkennung und Durchsetzung einer Anordnung zuständig. Sie befindet sich im Staat des Sitzes des Diensteanbieters (bzw. seiner benannten Niederlassung/Vertretung) gem. Art. 3 Nr. 17 e-Beweismittelsicherungs-Verordnung.

■ Herausgabeanordnungen für Inhalts- und Verkehrsdaten

Herausgabeanordnungen für Verkehrs- und Inhaltsdaten müssen entweder durch einen Richter, ein Gericht oder einen für den betreffenden Fall zuständigen Ermittlungsrichter erlassen werden (Art. 4 Abs. 2 lit. a e-Beweismittelsicherungs-Verordnung). Werden Anordnungen auf die Herausgabe dieser Daten durch die Staatsanwaltschaft erlassen, müssen diese durch einen Richter, ein Gericht oder den Ermittlungsrichter validiert werden (Art. 4 Abs. 2 lit. b e-Beweismittelsicherungs-Verordnung).

Die konkrete Bestimmung der Anordnungsbefugnis bestimmt sich nach den Voraussetzungen des nationalen Rechts. Gem. § 7 EBewMG gelten die Vorschriften der StPO und des GVG ergänzend zu Art. 4 e-Beweismittelsicherungs-Verordnung.²³ Die sachliche und örtliche Zuständigkeit eines deutschen (Ermittlungs-)Richters, Gerichts oder Staatsanwalts richtet sich nach §§ 9, 10 EBewMG iVm §§ 94 ff. StPO. Die EU-Mitgliedstaaten können nach Art. 4 Abs. 2 lit. b e-Beweismittelsicherungs-Verordnung neben den Gerichten und Staatsanwaltschaften andere verfahrensführende Behörden bestimmen, die für den Erlass einer Anordnung über Verkehrs- und Inhaltsdaten zuständig sein können. Eine zusätzliche Validierung solcher Anordnungen anderer Behörden durch ein Gericht als Justizbehörde ist jedoch stets erforderlich.

■ Herausgabeanordnungen für Teilnehmer- und Identifizierungsdaten

Herausgabeanordnungen für Teilnehmer- sowie Identifizierungsdaten können nach den europäischen Vorgaben für sämtliche Straftaten (auch) durch die zuständige Staatsanwaltschaft,

¹⁷ Vgl. Art. 3 Nr. 8 e-Beweismittelsicherungs-Verordnung.

¹⁸ Vgl. Art. 3 Nr. 10 e-Beweismittelsicherungs-Verordnung; im Folgenden: „Identifizierungsdaten“.

¹⁹ In Bezug auf die Differenzierung zwischen den Datenkategorien wird auf den Beitrag von Blum/Werner ZD 2026, 77 ff. verwiesen.

²⁰ von der Groeben/F. Meyer, 8. Aufl. 2025, AEUV Art. 82 Rn. 59.

²¹ EBewMG, BT-Drs. 21/3192, 40.

²² Zu den Justizbehörden nach Erwägungsgrund 37 e-Beweismittelsicherungs-Verordnung zählen nach Art. 4 Abs. 1, Abs. 2, Abs. 3 lit. b Richter, Gerichte, Ermittlungsrichter oder die Staatsanwaltschaft im Anordnungsstaat.

²³ EBewMG, BT-Drs. 21/3192, 40.

ohne eine Validierung durch einen Richter, ein Gericht oder den zuständigen Ermittlungsrichter, angeordnet werden. Die EU-Mitgliedsstaaten können auch für Teilnehmer- und Identifizierungsdaten andere verfahrensführende Behörden bestimmen, die für den Erlass einer Anordnung zuständig sein können (Art. 4 Abs. 1 lit. b e-Beweismittelsicherungs-Verordnung). In Deutschland zählen hierzu nach § 9 Abs. 2 Nr. 1 EBewMG Polizeibeamte als Ermittlungspersonen der Staatsanwaltschaft. Zu den Ermittlungspersonen der Staatsanwaltschaft zählen ferner Finanz- und Zollbeamte, soweit sie gesetzlich hierzu ermächtigt sind (zB § 404 AO, § 14 SchwarzArbG, § 21 AWG). Darüber hinaus sind sie nach § 9 Abs. 2 Nr. 2 und 3 EBewMG zuständig, wenn sie kraft Gesetzes in die Stellung der Staatsanwaltschaft eintreten (zB §§ 399 Abs. 1, 386 Abs. 2 AO bei Steuerstraftaten oder nach §§ 14a, 14b SchwarzArbG). Sofern andere Behörden Anordnungen zu Teilnehmer- oder Identifizierungsdaten erlassen, bleibt eine Validierung durch eine Justizbehörde, mithin durch die Staatsanwaltschaft oder einen (Ermittlungs-)Richter bzw. ein Gericht, zwingend erforderlich.

■ Sicherungsanordnungen

Für den Erlass der weniger eingriffsintensiven Sicherungsanordnung unterscheidet die e-Beweismittelsicherungs-Verordnung nicht zwischen den Datenkategorien (Art. 4 Abs. 3 e-Beweismittelsicherungs-Verordnung). Sie kann somit für alle Datenarten und für jede Straftat durch ein Gericht oder durch die Staatsanwaltschaft erlassen werden (Art. 6 Abs. 3 e-Beweismittelsicherungs-Verordnung), wenn sie in einem vergleichbaren nationalen Fall unter denselben Voraussetzungen hätten erlassen werden können oder, wenn sie zur Vollstreckung einer mindestens viermonatigen Freiheitsstrafe oder freiheitsentziehenden Maßregel der Sicherung dient (Art. 6 Abs. 3 e-Beweismittelsicherungs-Verordnung). Bei Sicherungsanordnungen für Inhalts- und Verkehrsdaten ist nach Art. 4 Abs. 3 lit. b e-Beweismittelsicherungs-Verordnung eine Validierung einer Justizbehörde für Anordnungen von anderen verfahrensführenden Behörden vorgeschrieben.

■ Nachholung der Validierung bei Herausgabe- oder Sicherungsanordnungen

In begründeten Notfällen, etwa bei unmittelbarer Gefahr für Leib und Leben, gestattet die e-Beweismittelsicherungs-Verordnung den Erlass von Sicherungsanordnungen zu allen Datenkategorien sowie Herausgabeanordnungen zu Teilnehmer- und Identifizierungsdaten ohne eine ansonsten erforderliche Validierung vor der Übermittlung der Anordnung, wenn die Anordnung in einem vergleichbaren nationalen Fall ebenfalls ohne eine vorherige Überprüfung durch eine Justizbehörde erlassen werden könnte und die Validierung nicht rechtzeitig eingeholt werden kann (Art. 4 Abs. 5 e-Beweismittelsicherungs-Verordnung). Die Anordnungsbehörde muss jedoch unverzüglich, spätestens innerhalb von 48 Stunden, eine Ex-post-Validierung der betreffenden Anordnung anfordern (Art. 4 Abs. 5 e-Beweismittelsicherungs-Verordnung).

b) Adressat der Anordnung

Die Anordnung ist grundsätzlich an den Diensteanbieter zu richten, der als Verantwortlicher iSd DS-GVO handelt, vgl. Art. 5 Abs. 6 S. 1 e-Beweismittelsicherungs-Verordnung.²⁴ Nur in Ausnahmefällen soll die Anordnung direkt an den Diensteanbieter gerichtet werden können, der die Daten im Auftrag des Verantwortlichen als Auftragsverarbeiter iSd DS-GVO verarbeitet.²⁵ Nach der e-Beweismittelsicherungs-Verordnung liegt eine solche Ausnahme vor, wenn der Verantwortliche trotz angemessener Bemühungen nicht ermittelt werden kann, oder die Ermittlungen gefährdet werden könnten, wenn die Anordnung an den Verantwortlichen gerichtet werden würde, vgl. Art. 5 Abs. 6 S. 2 lit. a und lit. b e-Beweismittelsicherungs-Verordnung.

Dabei geht der erste Ausnahmefall, wie in Erwägungsgrund 42 e-Beweismittelsicherungs-Verordnung ausgeführt, darauf zurück, dass es für die Unterscheidung zwischen der Funktion des Verantwortlichen und der Funktion des Auftragsverarbeiters nicht nur spezieller Kenntnisse des Rechtsrahmens, sondern ggf. auch der Auslegung komplexer Vertragswerke bedarf. Wenn Daten von einem Diensteanbieter gespeichert oder anderweitig verarbeitet werden und es trotz „verhältnismäßiger Bemühungen“ bzw. „angemessener Bemühungen“ seitens der Strafverfolgungsbehörde nicht möglich ist, den Verantwortlichen zu bestimmen, soll es daher möglich sein, die Anordnung direkt an den Diensteanbieter zu richten. Offen bleibt, welche Anforderungen an die „angemessenen/verhältnismäßigen Bemühungen“ der Strafverfolgungsbehörden zu stellen sind.

Die zweite Ausnahme erfasst nicht nur den Fall, dass der Verantwortliche zB Verdächtiger, Angeklagter oder Verurteilter ist, sondern auch, dass der Verantwortliche möglicherweise im Interesse der Person handelt, gegen die ermittelt wird, vgl. Erwägungsgrund 42 e-Beweismittelsicherungs-Verordnung.

Relevant dürfte die Differenzierung insbesondere für Cloud-Service-Anbieter sein, die Daten im Auftrag ihrer Kunden – sowohl im Fall von Unternehmenskunden als auch Privatkunden – verarbeiten.²⁶ Ausgehend von dem in Art. 5 Abs. 6 e-Beweismittelsicherungs-Verordnung normierten Subsidiaritätsprinzip sind Strafverfolgungsbehörden grundsätzlich verpflichtet, zunächst auf den Kunden des Cloud-Service-Anbieters zuzugehen. Allerdings dürften in der Praxis eine Vielzahl von Herausgabe- bzw. Sicherungsanordnungen auf die Erlangung von elektronischen Beweismitteln in Ermittlungen gegen Kunden von Cloud-Service-Anbietern gerichtet sein. In der Praxis dürfte sich daher eine Umkehr des in Art. 5 Abs. 6 e-Beweismittelsicherungs-Verordnung aufgenommenen Regel-Ausnahme-Verhältnisses zeigen.²⁷

c) Weitere erforderliche Angaben der Anordnung

Die Anordnungsbehörde muss in der Bescheinigung u.a. die „anwendbaren Bestimmungen des Strafrechts des Anordnungsstaats“ angeben (Art. 5 Abs. 5 lit. f e-Beweismittelsicherungs-Verordnung für Herausgabeanordnungen, Art. 6 Abs. 4 lit. f e-Beweismittelsicherungs-Verordnung für Sicherungsanordnungen). Entsprechend sehen die Vorlagen der e-Beweismittelsicherungs-Verordnung für EPOC und EPOC-PR Felder hierfür vor. Die e-Beweismittelsicherungs-Verordnung präzisiert jedoch nicht weiter, welche Angaben konkret erforderlich sind. Die Formulierung „anwendbare Bestimmungen des Strafrechts des Anordnungsstaats“ lässt zwei Auslegungen zu: Sie kann sich allein auf die zugrunde liegende Straftat (materielles Recht) beziehen²⁸ oder – weiter verstanden – auch die verfahrensrechtlichen Grundlagen umfassen, die eine Datenerhebung im Ermittlungsverfahren ermöglichen.

Die Vorlagen für Herausgabeanordnungen im Anhang I Abschnitt G lit. b e-Beweismittelsicherungs-Verordnung und für Sicherungsanordnungen im Anhang II Abschnitt E lit. b e-Beweismittelsicherungs-Verordnung sprechen insoweit mehrdeutig von der „Art und rechtliche[n] Würdigung der Straftat(en), die dem EPOC [bzw. EPOC-PR] zugrunde liegen, und anwendbare Rechtsnorm“. Die Verknüpfung der beiden Satzteile durch die Konjunktion „und“ könnte darauf hindeuten, dass sich die Formulierung „anwendbare Rechtsnorm“ auf die Straftat selbst, al-

²⁴ S. Art. 4 Nr. 7 DS-GVO.

²⁵ S. Art. 4 Nr. 8 DS-GVO.

²⁶ Hierzu Weiß/Brinkel RD 2023, 522 (527).

²⁷ So Weiß/Brinkel RD 2023, 522 (527).

²⁸ In diese Richtung Rexin CR 2024, 64 (71).

so das materielle Recht, bezieht. Nichtsdestotrotz ist die Formulierung weit gefasst und schließt die verfahrensrechtlichen Grundlagen nicht aus. Die Behördenpraxis und hierzu ggf. erfolgende Rechtsprechung sind vor diesem Hintergrund zu beobachten.

3. Materielle Voraussetzungen

a) Strafverfahren wegen einer Straftat nach dem Recht des Anordnungsstaats

Eine Herausgabeanordnung setzt ein Strafverfahren wegen einer Straftat nach dem Recht des Anordnungsstaats voraus. Dies umfasst auch Straftaten gegen juristische Personen, sofern diese im Anordnungsstaat strafrechtlich verantwortlich gemacht werden können (Art. 2 Abs. 2 e-Beweismittelsicherungs-Verordnung), nicht aber Maßnahmen der Gefahrenabwehr.

Die zugrunde liegende Straftat bestimmt, welche Daten von Strafverfolgungsbehörden auf Grundlage einer Herausgabeanordnung erlangt werden können: Zum einen können Straftaten, für die eine Mindesthöchststrafe von 3 Jahren gilt, Anordnungen über Verkehrs- und Inhaltsdaten begründen (Art. 5 Abs. 4 lit. a e-Beweismittelsicherungs-Verordnung). Zum anderen berechtigen bestimmte Kategorien von Straftaten, zB sexueller Missbrauch von Kindern, Terrorismus, Betrug im Zusammenhang mit unbaren Zahlungsmitteln sowie bestimmte Cybercrime-Delikte die Behörden zu Herausgabeanordnungen bezüglich dieser sensiblen Datenkategorien sowie zur Lokalisierung einer verurteilten Person nach den vorstehend genannten Katalogstraftaten, um eine Freiheitsstrafe oder freiheitsentziehende Maßregel der Sicherung von mindestens 4 Monaten zu vollstrecken (Art. 5 Abs. 4 lit. b, lit. c und lit. d e-Beweismittelsicherungs-Verordnung). Für Teilnehmer- und Identifizierungsdaten nach Art. 5 Abs. 3 e-Beweismittelsicherungs-Verordnung kann die Anordnung für alle Straftaten nach dem Recht des Anordnungsstaats ergehen sowie auch zur Lokalisierung einer verurteilten Person, um eine Freiheitsstrafe oder freiheitsentziehende Maßregel der Sicherung von mindestens 4 Monaten zu vollstrecken.

b) Vergleichbare Rechtsgrundlage im Recht des Anordnungsstaats

Eine Anordnung darf nur erlassen werden, wenn sie auch in einem vergleichbaren nationalen Fall im Anordnungsstaat zulässig wäre (Art. 5 Abs. 2 e-Beweismittelsicherungs-Verordnung). Die anordnende Behörde muss demnach prüfen, ob sie dieselben Daten auch in einem rein innerstaatlichen Fall unter denselben Umständen erhalten könnte (Art. 5 Abs. 2 e-Beweismittelsicherungs-Verordnung). Die e-Beweismittelsicherungs-Verordnung regelt allerdings nicht, nach welchem Recht sich die Voraussetzungen des erforderlichen Verdachtsgrads richten.²⁹ Aufgrund der Entsprechungsklausel in Art. 5 Abs. 2 e-Beweismittelsicherungs-Verordnung dürfte auch hierfür das nationale Strafprozessrecht maßgeblich sein.³⁰ Ein neuer Gesetzentwurf zur Einführung einer IP-Adressspeicherung und zur Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren

sieht nunmehr entsprechende Regelungen zu Sicherungsanordnungen vor.³¹ Vorbehaltlich seines Inkrafttretens ist daher künftig mit einer nationalen Rechtsgrundlage iSv Art. 6 Abs. 3 e-Beweismittelsicherungs-Verordnung zu rechnen.³²

c) Erforderlichkeit, Verhältnismäßigkeit und Angemessenheit

Die Anordnungsbehörde muss die Rechte des Verdächtigen oder Beschuldigten berücksichtigen und prüfen, ob die Anordnung auf das unbedingt erforderliche Maß beschränkt ist, um das rechtmäßige Ziel der Erlangung relevanter und notwendiger Beweismittel zu erreichen (Art. 5 Abs. 2 und Abs. 3, Art. 6 Abs. 2 e-Beweismittelsicherungs-Verordnung für Sicherungsanordnungen sowie Erwägungsgrund 38 e-Beweismittelsicherungs-Verordnung).

IV. Maßnahmen des Diensteanbieters beim Erhalt einer Herausgabe- oder Sicherungsanordnung

1. Prüfpflicht

Die Frage einer Prüfpflicht des Diensteanbieters war bereits im Gesetzgebungsverfahren umstritten. Ursprünglich sah der Entwurf vor, dass der Diensteanbieter eine Grundrechtsprüfung anhand der GRCh sowie eine Missbrauchskontrolle der eingehenden Anordnung durchführen und die Herausgabe oder Sicherung gegebenenfalls verweigern müsse.³³ Dieser Ansatz stieß jedoch auf Kritik, da diese Verpflichtung privaten Unternehmen eine quasi-gerichtliche Rolle aufgebürdet hätte.³⁴

Gleichwohl enthalten einige Bestimmungen der Verordnung – etwa Art. 10 Abs. 5 und Abs. 6 e-Beweismittelsicherungs-Verordnung sowie Art. 11 Abs. 4 und Abs. 5 e-Beweismittelsicherungs-Verordnung – Formulierungen, die dahingehend gedeutet werden könnten, dass dem adressierten Diensteanbieter eine formelle oder sogar materiell-rechtliche Prüfpflicht zukommt. Aufgrund der fehlenden Anordnung einer Prüfpflicht in der e-Beweismittelsicherungs-Verordnung sind diese Vorschriften nunmehr iSe Prüfungsrechts, statt einer Prüfpflicht zu verstehen. Hierfür spricht nicht zuletzt Art. 15 Abs. 2 e-Beweismittelsicherungs-Verordnung sowie Erwägungsgrund 71 e-Beweismittelsicherungs-Verordnung, wonach die Anordnungsbehörden für die Gewährleistung der Rechtmäßigkeit einer Anordnung verantwortlich sind.

Dennoch folgt eine wichtige und vom Diensteanbieter innerhalb kurzer Zeit vorzunehmende Pflicht zur faktischen Überprüfung der Datenbestände aus Art. 15 Abs. 1 e-Beweismittelsicherungs-Verordnung iVm § 18 Abs. 2 Nr. 5 und Nr. 6 EBewMG. Hiernach handelt ein Diensteanbieter ordnungswidrig, wenn er feststellt, dass ihm die Herausgabe der ersuchten Daten faktisch unmöglich ist und er die erforderliche Mitteilung an die Anordnungsbehörde nach Art. 10 Abs. 6 e-Beweismittelsicherungs-Verordnung, nicht richtig bzw. nicht unverzüglich tätigt.

Daneben kann sich eine Pflicht zur Prüfung mittelbar aus den datenschutzrechtlichen Vorgaben, insbesondere dem Grundsatz der Rechtmäßigkeit der Verarbeitung und der Rechenschaftspflicht, ergeben.³⁵

2. Fristen

Für die Erfüllung einer Herausgabeanordnung gelten angesichts der zu bewältigenden Datenmengen straffe Fristen. Bei Teilnehmer- und Identifizierungsdaten müssen die angeforderten Informationen spätestens innerhalb von 10 Tagen nach Erhalt der Anordnung übermittelt werden, sofern keine Unterrichtung an die Vollstreckungsbehörde erforderlich ist (Art. 10 Abs. 3 e-Beweismittelsicherungs-Verordnung). Handelt es sich um Ver-

²⁹ Vgl. hierzu Weiß ZRP 2025, 218 (218); Ambos ZfStW 2025, 204 (212).

³⁰ Weiß ZRP 2025, 218 (218).

³¹ Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, BT-Drs. 263/26.

³² REXIN CR 2025, 133 (139 f.).

³³ EU-Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen v. 17.4.2018, COM/2018/225.

³⁴ Esser StraFO 2019, 403 (408 f.).

³⁵ Vgl. hierzu REXIN, CR 2024, 64 (70 f.).

kehrs- oder Inhaltsdaten und ist eine Unterrichtung an die Vollstreckungsbehörde erforderlich, müssen die Daten „nach Ablauf“ von 10 Tagen übermittelt werden, sofern die Vollstreckungsbehörde keinen Ablehnungsgrund geltend gemacht hat (Art. 10 Abs. 2 e-Beweismittelsicherungs-Verordnung). Eine frühere Übermittlung ist bei der Einschaltung der Vollstreckungsbehörde sogar untersagt, es sei denn, die Behörde bestätigt bereits vor Ablauf der Frist, dass sie keinen Ablehnungsgrund geltend machen wird.

Vor besondere praktische Herausforderungen stellt es Diensteanbieter, dass sie in Notfällen die Daten unverzüglich, spätestens jedoch innerhalb von 8 Stunden nach Erhalt der Anordnung übermitteln müssen (Art. 10 Abs. 4 e-Beweismittelsicherungs-Verordnung). Bei der Sicherungsanordnung gilt für alle Datenkategorien, dass die Daten unverzüglich gesichert werden müssen. Die Sicherung ist für 60 Tage aufrechtzuerhalten, es sei denn, die Anordnungsbehörde bestätigt innerhalb dieser Frist, dass ein entsprechendes Herausgabegesuch gestellt wurde. Innerhalb der 60 Tage kann die Sicherung um weitere 30 Tage verlängert werden (Art. 11 e-Beweismittelsicherungs-Verordnung).

3. Drohende Sanktionen und Schutzmöglichkeiten des Diensteanbieters

Aufgrund der kurzen Fristen zur Erfüllung der Anordnungen stehen die Diensteanbieter bezüglich der inhaltlichen und technischen Prüfung der Anordnungen und möglicher Einwände in der Praxis unter erheblichem Zeitdruck.³⁶ Dies gilt nicht zuletzt wegen der erheblichen Geldbußen, denen Diensteanbieter (künftig) ausgesetzt sind, wenn sie die betreffenden Daten nicht oder nicht rechtzeitig sichern bzw. herausgeben (Verstöße gegen Art. 10, 11 und 13 Abs. 4 e-Beweismittelsicherungs-Verordnung). § 18 Abs. 3 Nr. 1 lit. a EBewMG sieht für Ordnungswidrigkeiten nach § 18 Abs. 1 EBewMG (Adressatenbenennung, Vertreterbestellung und Mitteilungspflichten nach §§ 3, 4 EBewMG) einen Bußgeldrahmen von bis zu 500.000 EUR vor. Bei Diensteanbietern mit einem Gesamtumsatz von mehr als 25 Mio. EUR (bei Verstößen nach § 18 Abs. 3 Nr. 1 b EBewMG) bzw. 5 Mio. EUR (bei Verstößen nach § 18 Abs. 3 Nr. 2 EBewMG) kann die Geldbuße sogar bis zu 2% des weltweiten Jahresumsatzes im vorausgegangenen Geschäftsjahr betragen (§ 18 Abs. 4, Abs. 5 und Abs. 6 EBewMG).

Ein Blick auf Art. 18 e-Beweismittelsicherungs-Verordnung und § 13 Abs. 4 EBewMG verdeutlicht jedoch die begrenzten Möglichkeiten der Diensteanbieter, sich vor dem Beginn des Vollstreckungsverfahrens gegen Anordnungen zu wehren: Entsprechende Rechtsbehelfe sind dort lediglich für Personen vorgesehen, deren Daten im Wege einer Herausgabeanordnung angefordert werden. Die Diensteanbieter selbst werden im Kanon dieser Rechtsbehelfe nicht genannt. Zugunsten des Diensteanbieters bestehen neben dem Mitteilungsverfahren nach Art. 10 Abs. 5 bis Abs. 8 iVm Anhang III e-Beweismittelsicherungs-Verordnung jedoch die folgenden Schutzmechanismen:

a) Einwand der Kollision der Herausgabepflichtung mit dem Recht eines Drittstaats

Besteht ein Konflikt der Herausgabeanordnung mit einer Verpflichtung aus dem Recht eines Drittstaats, kann der Diensteanbieter diesen Umstand als begründeten Einwand bereits vor Beginn des Vollstreckungsverfahrens gegen die Anordnung geltend machen. Die Anordnungsbehörde prüft den Einwand und muss eine gerichtliche Überprüfung im Anordnungsstaat beantragen, wenn die Behörde die Anordnung aufrechterhalten will. Bis zum Abschluss des Überprüfungsverfahrens ist die Ausführung der Herausgabeanordnung ausgesetzt (Art. 17

e-Beweismittelsicherungs-Verordnung), die Verpflichtung zur Datensicherung bleibt jedoch weiterhin bestehen (vgl. Art. 17 Abs. 1, 10 Abs. 8, Abs. 9 e-Beweismittelsicherungs-Verordnung).³⁷

b) Ablehnungsgründe der Vollstreckungsbehörde

Ein weiteres Korrektiv ist die Unterrichtung der Vollstreckungsbehörde über Grund und Reichweite der Anordnung, die gleichzeitig zur Übermittlung der Anordnung an den Adressaten erfolgt (Art. 8 e-Beweismittelsicherungs-Verordnung). Die Vollstreckungsbehörde kann nach der Unterrichtung durch die Anordnungsbehörde binnen 10 Tagen Einwände erheben, um nationale Schutzrechte wie Pressefreiheit oder Berufsgeheimnisse zu wahren (Art. 10 Abs. 2 e-Beweismittelsicherungs-Verordnung). Bei Sicherungsanordnungen oder Herausgabeanordnungen zu Teilnehmer- oder Identifizierungsdaten unterbleibt jedoch die Unterrichtung der Vollstreckungsbehörde „vor Ort“ und diese kann dementsprechend auch keine Einwände erheben. Diese bewusst enge Ausgestaltung führt dazu, dass ausländische Behörden in einer Vielzahl von Fällen ohne jede Beteiligung des Vollstreckungsstaats agieren können.

Die unterrichtete Behörde prüft die Anordnung anhand eines Katalogs von Ablehnungsgründen (Grundrechte, Immunitäten und Vorrechte, Pressefreiheit, ne bis in idem, beiderseitige Strafbarkeit; Art. 12 Abs. 1 e-Beweismittelsicherungs-Verordnung). Hierfür ist – außer in Notfällen (Art. 10 Abs. 4 e-Beweismittelsicherungs-Verordnung: spätestens 96 Stunden) – eine Frist von 10 Tagen vorgesehen, während der der Diensteanbieter die Daten nicht herausgeben darf (Art. 10 Abs. 2 S. 1 e-Beweismittelsicherungs-Verordnung). Der Diensteanbieter muss die Daten aber dennoch unverzüglich sichern (Art. 10 Abs. 1 e-Beweismittelsicherungs-Verordnung). Die Unterrichtung entfällt nur dann, wenn hinreichende Anhaltspunkte dafür bestehen, dass sowohl der Begehung- als auch der Wohnort der von der Datenabfrage betroffenen Person im Anordnungsstaat liegen (Art. 8 Abs. 2 e-Beweismittelsicherungs-Verordnung).

c) Rechtsschutz gegen Bußgeldbescheide deutscher Vollstreckungsbehörden

Erhält ein in Deutschland ansässiger Diensteanbieter eine Anordnung aus einem anderen EU-Mitgliedstaat, ist zwischen der freiwilligen Befolgung und der förmlichen Vollstreckung zu differenzieren. In Deutschland ist gem. § 11 Abs. 1 EBewMG die Staatsanwaltschaft bei dem Landgerichtsbezirk des Sitzes des Adressaten die zuständige Vollstreckungsbehörde. Solange der Diensteanbieter freiwillig kooperiert, beschränkt sich sein Rechtsschutz auf die Mitteilung von Fehlern gem. Art. 10 Abs. 5–7 e-Beweismittelsicherungs-Verordnung an die ausländische Behörde.³⁸

Vor der Vollstreckung der Anordnung fordert die Vollstreckungsbehörde die Adressaten nach Art. 16 Abs. 3 e-Beweismittelsicherungs-Verordnung förmlich auf, ihren entsprechenden Verpflichtungen nachzukommen und räumt ihnen die Möglichkeit ein, Einwände nach Art. 16 Abs. 4 und Abs. 5 e-Beweismittelsicherungs-Verordnung (u.a. unzuständige Anordnungsbehörde, unverschuldete faktische Unmöglichkeit der Ausführung, offensichtliche Fehler der Anordnung, Immunitäten oder Vorrechte) gegen die Ausführung der Anordnung geltend zu machen. Auch die Vollstreckungsbehörde prüft den entsprechenden Katalog, erweitert um den Fall einer offensichtlichen Grundrechtsverletzung (Art. 16 Abs. 4 lit. g, Abs. 5 lit. f

³⁶ von der Groeben/F. Meyer, 8. Aufl. 2025, AEUV Art. 82 Rn. 67.

³⁷ Hüttemann NZWiSt 2024, 81 (88); von der Groeben/F. Meyer, 8. Aufl. 2025, AEUV Art. 82 Rn. 67.

³⁸ Babucke wistra 2024, 57 (61).

e-Beweismittelsicherungs-Verordnung). Dieses Korrektiv ist besonders relevant für die Konstellationen, in denen die Vollstreckungsbehörde nach Art. 8 e-Beweismittelsicherungs-Verordnung nicht im früheren Stadium der Anordnungsübermittlung parallel über die Anordnung unterrichtet wurde, um mögliche Einwände geltend zu machen.

Erst wenn die Vollstreckungsbehörde die Anordnung vollstreckt (Art. 16 Abs. 1 S. 2 e-Beweismittelsicherungs-Verordnung), also einen Bußgeldbescheid nach Art. 15 e-Beweismittelsicherungs-Verordnung verhängt, eröffnet sich der nationale Rechtsweg. Für Vollstreckungsverfahren in Deutschland verweist § 17 EBewMG auf §§ 68 ff. OWiG für den Einspruch gegen den Bußgeldbescheid und das anschließende gerichtliche Verfahren sowie die Rechtsmittel.

Im Ergebnis steht dem Diensteanbieter damit ein Rechtsbehelf nur im Falle einer bereits gegen ihn erlassenen Sanktionierung bei Nichtbefolgung einer Herausgabe- oder Sicherungsanordnung zu (Art. 16 Abs. 10 e-Beweismittelsicherungs-Verordnung iVm § 17 EBewMG), nicht aber gegen die Anordnung oder gegen das Vollstreckungsverfahren selbst. Bedenklich erscheint dies insbesondere deshalb, weil der Diensteanbieter gem. Art. 7 e-Beweismittelsicherungs-Verordnung als Adressat einer belastenden Maßnahme anzusehen ist und als solcher das Grundrecht auf effektiven Rechtsschutz aus Art. 47 GRCh hat.³⁹

V. Umsetzungspflichten des Diensteanbieters

1. Benennung eines Adressaten

Diensteanbieter, die am 18.2.2026 bereits Dienste in der EU anbieten, müssen spätestens bis zum 18.8.2026 eine benannte Niederlassung oder einen Vertreter in der EU benennen (Art. 3 Abs. 6 e-Beweismittel-Diensteanbieter-Rechtshilfe-RL). Für EU-ansässige Unternehmen genügt es, eine Niederlassung mit Rechtspersönlichkeit zu bestimmen (Art. 3 Nr. 2 e-Beweismittelsicherungs-Verordnung). Somit ist jeder Diensteanbieter gehalten, einen Kontaktpunkt vorzuhalten, der eingehende Herausgabe- oder Sicherungsanordnungen zügig bearbeitet. Für in Deutschland ansässige Diensteanbieter ist gemäß § 6 Abs. 1 EBewMG das Bundesamt für Justiz als zentrale Behörde vorgesehen, an die die schriftliche Mitteilung über die Benennung einer Niederlassung als Adressat zu richten ist.

2. Weitere Pflichten

Die e-Beweismittelsicherungs-Verordnung bedeutet für Diensteanbieter erheblichen – insbesondere technischen – Implementierungsaufwand. Die Diensteanbieter müssen nach Art. 19 Abs. 3 e-Beweismittelsicherungs-Verordnung Vorkehrungen treffen, dass ihre benannten Niederlassungen oder Vertreter das bereitgestellte dezentrale IT-System nutzen können, um Anordnungen zu empfangen, die angeforderten Daten der Anordnungsbehörde zu übermitteln und mit der Anordnungsbehörde zu kommunizieren. Zudem verpflichtet Art. 13 Abs. 4 e-Beweismittelsicherungs-Verordnung Diensteanbieter dazu, die „dem neuesten Stand der Technik entsprechenden betrieblichen und technischen Maßnahmen“ zu treffen, um die Vertraulichkeit, Geheimhaltung und Integrität der Datensicherung und -herausgabe sicherzustellen.

VI. Ausblick

Mit der e-Beweismittelsicherungs-Verordnung erkennt der europäische Gesetzgeber die wachsende Bedeutung elektronischer

Beweismittel für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen an. Dabei werden die bestehenden Herausforderungen für Strafverfolgungs- und Justizbehörden sowie Diensteanbieter, die sich aus einem bislang fragmentierten Rechtsrahmen bei grenzüberschreitenden Beweismittelersuchen ergeben, adressiert. Vor diesem Hintergrund sind sowohl die e-Beweismittelsicherungs-Verordnung als auch die flankierende e-Beweismittel-Diensteanbieter-Rechtshilfe-RL zu begrüßen.

Es zeichnet sich jedoch ab, dass die e-Beweismittelsicherungs-Verordnung sowohl für Strafverfolgungsbehörden als auch für Diensteanbieter neue Herausforderungen mit sich bringen wird. Um die mit der e-Beweismittelsicherungs-Verordnung verfolgten Ziele in der Praxis zum Erfolg zu führen, ist es daher erforderlich, dass sich Diensteanbieter bereits jetzt mit EPOC und EPOC-PR vertraut machen. Mit Blick auf die kurzen Fristen, komplexen Prüfungsanforderungen und potenziell erheblichen Sanktionsrisiken sollten Diensteanbieter interne Prozesse frühzeitig prüfen und anpassen, um die Anforderungen der e-Beweismittelsicherungs-Verordnung sowie des EBewMG erfüllen zu können. Entsprechende Prozesse müssen nicht nur die weiterhin bestehenden nationalen Beweismittelersuchen, sondern auch internationale Rechtshilfeersuchen berücksichtigen. Zudem sollten Diensteanbieter stets möglichen Rechtsschutz im Blick behalten, um bei Bedarf kurzfristig reagieren zu können. In der Praxis wird sich zeigen, ob die vorgesehenen Rechtsbehelfe im Zusammenhang mit der e-Beweismittelsicherungs-Verordnung ausreichend sind, um den Schutz der Adressaten von Anordnungen sicherzustellen.

Angesichts der stetig zunehmenden Bedeutung elektronischer Beweismittel wird die Zahl der Anordnungen von Strafverfolgungsbehörden zukünftig weiter steigen. Nur durch gut aufgestellte und belastbare Prozesse können Diensteanbieter langfristig eine effiziente und rechtskonforme Bearbeitung entsprechender Anordnungen sicherstellen.

Schnell gelesen ...

- Die e-Beweismittelsicherungs-Verordnung führt mit der Europäischen Herausgabeordnung und der Europäischen Sicherungsanordnung ein einheitliches Verfahren ein, das Strafverfolgungsbehörden in der EU den grenzüberschreitenden Zugriff auf elektronische Beweismittel über standardisierte Bescheinigungen ermöglicht.
- Die Einordnung der ersuchten Informationen in Teilnehmer-, Identifizierungs-, Verkehrs- oder Inhaltsdaten ist der zentrale Schlüssel, weil hiervon Zuständigkeiten, Validierungserfordernisse und Beteiligung einer Vollstreckungsbehörde abhängen.
- Für Diensteanbieter sind die formellen Anforderungen der Anordnungen besonders praxisrelevant, weil Formmängel Klarstellungsmechanismen auslösen können und die Pflichten zur Herausgabe oder Sicherung der Daten in bestimmten Konstellationen erst nach erfolgter Berichtigung greifen.
- Materiell setzt der Erlass von Herausgabe- und Sicherungsanordnungen ein Strafverfahren voraus und ist durch nationale Vergleichbarkeits- sowie Erforderlichkeits- und Verhältnismäßigkeitsanforderungen begrenzt, wobei für Verkehrs- und Inhaltsdaten zusätzliche Schwellen gelten.
- Die e-Beweismittelsicherungs-Verordnung bringt für Diensteanbieter kurze Reaktionsfristen, begrenzte Rechtsschutzmöglichkeiten und erhebliche Sanktionsrisiken mit sich. Diensteanbieter sollten daher frühzeitig die Benennung eines EU-Adressaten klären sowie belastbare interne Prozesse implementieren.

³⁹ Hüttemann NZWiSt 2024, 81 (92).



Anna Lena Nowicki
ist Rechtsanwältin bei DLA Piper UK LLP in Frankfurt/M.



Lisa Fleckenstein
ist Rechtsanwältin bei DLA Piper UK LLP in Frankfurt/M.



Dr. Lucas Blum
ist Rechtsanwalt bei DLA Piper UK LLP in München.



Daniel Werner
ist Rechtsassessor bei DLA Piper UK LLP in München.

EuGH: Tragweite der Ausnahme für Pastiche im Zusammenhang mit Sampling

Kunstfreiheit

RL 2001/29/EG Art. 5 Abs. 3 lit. k, 11, 13; UrhG § 51a S. 1; GRCh Art. 13
Urteil vom 14.4.2026 – C-590/23 – Pelham

Leitsätze der Redaktion

1. Art. 5 Abs. 3 lit. k RL 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft ist dahin auszulegen, dass die in dieser Bestimmung vorgesehene Ausnahme für „Pastiches“ kein Auffangtatbestand ist, sondern Schöpfungen erfasst, die an ein oder mehrere bestehende Werke erinnern, gleichzeitig aber wahrnehmbare Unterschiede diesen gegenüber aufweisen, und die, einschließlich im Wege des „Sampling“, einige ihrer urheberrechtlich geschützten Elemente nutzen, um mit diesen Werken einen als solchen erkennbaren künstlerischen oder kreativen Dialog zu führen, der verschiedene Formen annehmen kann, darunter die einer offenen Nachahmung des Stils dieser Werke, einer Hommage an sie oder einer humoristischen oder kritischen Auseinandersetzung mit ihnen.

2. Art. 5 Abs. 3 lit. k RL 2001/29/EG ist dahin auszulegen, dass es für eine Nutzung „zum Zwecke von“ Pastiches im Sinne dieser Bestimmung genügt, dass der Charakter als „Pastiche“ für denjenigen erkennbar ist, dem das bestehende Werk bekannt ist, dem diese Elemente entnommen sind.

Anm. d. Red.: Das Vorabentscheidungsersuchen zu diesem Verfahren ist abgedruckt in BGH MMR 2024, 171 mAnm Kreutzer. Vgl. zum hierzu bereits ergangenen Instanzenzug: BGH MMR 2009, 253 mAnm Hoeren – Metall auf Metall I; OLG Hamburg MMR 2011, 755; BGH MMR 2013, 464 mAnm Hoeren – Metall auf Metall II; BVerfG MMR 2016, 463 mAnm Hoeren; BGH MMR 2017, 719 (Ls.) – Metall auf Metall III; EuGH MMR 2019, 97 mAnm Apel – Pelham u.a.; BGH MMR 2020, 759 – Metall auf Metall IV; OLG Hamburg MMR 2022, 702 (Ls.). Vgl. ferner EuGH MMR 2019, 596 mAnm Apel; BGH MMR 2024, 171 mAnm Kreutzer; OLG Dresden MMR 2017, 719 (Ls.); EuGH MMR 2019, 588 mAnm Hoeren/Düwel und EuGH MMR 2019, 660 mAnm Hoeren/Düwel.

Schlagworte: Pastiche; Sampling; angemessener Ausgleich; Urheberrecht; Kunstfreiheit

Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 5 Abs. 3 lit. k der RL 2001/29/EG des Europäischen Parlaments und des Rates v. 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

Es ergeht iRe Rechtsstreits zwischen CG und YN, der Rechtsnachfolgerin von RL, einerseits und der Pelham GmbH, SD und UP (im Folgenden zusammen: Pelham u.a.) andererseits wegen der Nutzung einer einem Tonträger der Musikgruppe Kraftwerk, deren Gründungsmitglieder CG und RL sind, entnommenen Rhythmussequenz von etwa zwei Sekunden Dauer in dem von SD und UP komponierten und von Pelham produzierten Musiktitel „Nur mir“.

SD und UP sind die Komponisten des Musikstücks „Nur mir“, das im Jahr 1997 auf Tonträgern von Pelham erschien. CG und der 2020 verstorbene RL sind die Gründungsmitglieder der Musikgruppe „Kraftwerk“, die im Jahre 1977 einen Tonträger veröffentlichte, auf dem sich das Musikstück „Metall auf Metall“ befindet. CG und YN, die Rechtsnachfolgerin von RL, tragen vor, Pelham u.a. hätten etwa zwei Sekunden einer Rhythmussequenz aus dem Titel „Metall auf Metall“ elektronisch kopiert („gesampelt“) und dem Titel „Nur mir“ in fortlaufender Wiederholung unterlegt, obwohl es ihnen möglich gewesen wäre, die übernommene Rhythmussequenz selbst einzuspielen.

CG und YN meinen, dass Pelham u.a. ihr Leistungsschutzrecht als Tonträgerhersteller verletzt habe. Hilfsweise stützen sie sich auf ihr Leistungsschutzrecht als ausübende Künstler, weiter Hilfsweise auf die Verletzung des Urheberrechts von CG an dem Musikwerk. Äußerst Hilfsweise schließlich machen sie geltend, dass Pelham u.a. gegen die Rechtsvorschriften über den wettbewerbsrechtlichen Leistungsschutz verstoßen hätten.

CG und RL erhoben Klage beim LG Hamburg und beantragten Unterlassung, Schadensersatz, Auskunftserteilung und Herausgabe der Tonträger zum Zweck ihrer Vernichtung. Mit Urte. v. 8.10.2004 gab das LG der Klage statt. Die Berufung gegen dieses Urteil von Pelham u.a. wurde vom OLG Hamburg mit Urte. v. 7.6.2006 zurückgewiesen. Auf die Revision von Pelham u.a. zum BGH hob dieser das Urteil des OLG Hamburg mit Urte. v. 20.11.2008 (MMR 2009, 253 mAnm Hoeren) auf und verwies die Sache zu erneuter Prüfung an dieses Gericht zurück. Mit Urte. v. 17.8.2011 (MMR 2011, 755) wies das OLG die Berufung von Pelham u.a. gegen das Urte. v. 8.10.2004 erneut zurück. Mit Urte. v. 13.12.2012 (MMR 2013, 464 mAnm Hoeren) wies der BGH die erneute Revision von Pelham u.a. gegen dieses Urte. v. 17.8.2011 zurück.

Dieses Urteil v. 13.12.2012 und das vorausgegangene Urteil des BGH v. 20.11.2008 sowie das zweite Urteil des OLG Hamburg v. 17.8.2011 wurden vom BVerfG aufgehoben (MMR 2016, 463 mAnm Hoeren), das die Sache an den BGH zurückverwies. Im Rahmen dieses dritten Revisionsverfahrens hat der BGH ein Vorabentscheidungsersuchen u.a. zur Auslegung von Art. 2 lit. c und 5 Abs. 3 lit. d RL 2001/29/EG sowie von Art. 9 Abs. 1 lit. b RL 2006/115/EG an den Gerichtshof gerichtet (MMR 2017, 719 (Ls.)).

Mit Urt. v. 29.7.2019 – Pelham u.a. (MMR 2019, 596 mAnm Apel), hat der Gerichtshof u.a. für Recht erkannt, dass Art. 2 lit. c RL 2001/29/EG unter Berücksichtigung der GRCh dahin auszulegen ist, dass das ausschließliche Recht des Tonträgerherstellers aus dieser Bestimmung, die Vervielfältigung seines Tonträgers zu erlauben oder zu verbieten, ihm gestattet, sich dagegen zu wehren, dass ein Dritter ein – auch nur sehr kurzes – Audiofragment seines Tonträgers nutzt, um es in einen anderen Tonträger einzufügen, es sei denn, dass dieses Fragment in den anderen Tonträger in geänderter und beim Hören nicht wiedererkennbarer Form eingefügt wird. Er hat ferner für Recht erkannt, dass Art. 9 Abs. 1 lit. b RL 2006/11/5/EG dahin auszulegen ist, dass es sich bei einem Tonträger, der von einem anderen Tonträger übertragene Musikfragmente enthält, nicht um eine „Kopie“ dieses anderen Tonträgers im Sinne dieser Vorschrift handelt, da er nicht den gesamten Tonträger oder einen wesentlichen Teil davon übernimmt.

Mit Urt. v. 30.4.2020 (MMR 2020, 759) hob der BGH das Urteil des OLG Hamburg v. 7.6.2006 auf und verwies die Sache an diesen zurück. Mit Urt. v. 28.4.2022 (MMR 2022, 702 (Ls.)) änderte dieses das Urteil des LG Hamburg v. 8.10.2004 ab, indem es bei seiner Beurteilung zwischen drei Zeiträumen unterschied.

Für den ersten Zeitraum, dh den Zeitraum vor Ablauf der Umsetzungsfrist der RL 2001/29/EG am 22.12.2002, verneinte das OLG Hamburg jede Verletzung eines Urheberrechts oder eines verwandten Schutzrechts auf der Grundlage der Bestimmungen des UrhG in ihrer während dieses Zeitraums geltenden Fassung.

Für den zweiten Zeitraum, vom Ablauf der Umsetzungsfrist der RL 2001/29/EG bis zum Inkrafttreten der Schrankenregelung des § 51a UrhG am 7.6.2021, verurteilte das OLG Pelham u.a. zum einen zur Auskunftserteilung über die Zahl der während dieses Zeitraums produzierten und/oder ausgelieferten Tonträger mit Aufnahmen des Musiktitels „Nur mir“ sowie zur Herausgabe der Kopien dieser Tonträger zum Zweck der Vernichtung und stellte zum anderen die Schadensersatzpflicht von Pelham u.a. fest. Es war insb. der Ansicht, dass Pelham u.a. dadurch, dass sie im Jahr 2004 erneut zwei Tonträger mit Aufnahmen dieses Titels veröffentlicht hätten, das Recht von CG und RL als Tonträgerhersteller zur Vervielfältigung ihres Tonträgers verletzt hätten, weil die übernommene Sequenz aus „Metall auf Metall“ in dem Titel „Nur mir“ deutlich wahrnehmbar und für den mit dem ersten Titel vertrauten Hörer erkennbar sei. Außerdem hätten Pelham u.a. mit der Herstellung und Auslieferung der beiden Tonträger im Jahr 2004 das Urheberrecht von CG an der übernommenen Rhythmussequenz verletzt, da diese die Anforderungen an ein urheberrechtlich geschütztes Werk erfülle.

Für den Zeitraum ab dem Inkrafttreten von § 51a UrhG am 7.6.2021 verneinte das OLG jede Verletzung des Urheberrechts und der verwandten Schutzrechte, da es der Ansicht war, dass die Übernahme der Rhythmussequenz aus dem Musiktitel „Metall auf Metall“ im Wege des Sampling eine nach dieser Bestimmung zulässige Nutzung zum Zweck des Pastiche sei.

CG und YN legten beim BGH, dem vorlegenden Gericht (MMR 2024, 171 mAnm Kreutzer), Revision gegen den Teil dieses Urteils v. 28.4.2022 ein, mit dem ihre Anträge zurückgewiesen wurden, soweit sie den Zeitraum nach dem 7.6.2021 betrafen.

Der BGH ist der Auffassung, dass das OLG Hamburg zu Recht einen Eingriff in die Rechte der KI. des Ausgangsverfahrens als Tonträgerhersteller und als ausübende Künstler festgestellt habe, weil Pelham u.a. die betreffende Rhythmussequenz zwar in leicht geänderter, aber beim Hören wiedererkennbarer Form

übernommen hätten. Ohne Rechtsfehler sei auch die Annahme des OLG Hamburg, dass diese Rhythmussequenz ein urheberrechtlich schutzfähiges Werk der Musik darstelle. Das vorlegende Gericht weist jedoch darauf hin, dass nach § 51a S. 1 UrhG die Vervielfältigung, die Verbreitung und die öffentliche Wiedergabe eines veröffentlichten Werks zum Zweck der Karikatur, der Parodie und des Pastiche zulässig sei. Nach § 83 und § 85 Abs. 4 UrhG sei diese Bestimmung auf die Leistungsschutzrechte des ausübenden Künstlers sowie des Tonträgerherstellers entsprechend anwendbar.

Der BGH ist der Auffassung, dass die streitige Übernahme der Rhythmussequenz nicht die Voraussetzungen einer „Karikatur“ oder „Parodie“ erfülle, weil es keinen Anhaltspunkt dafür gebe, dass das Musikstück „Nur mir“ einen Ausdruck von Humor oder eine Verspottung darstelle. Er möchte daher wissen, ob davon ausgegangen werden kann, dass die streitige Übernahme zum Zweck eines „Pastiche“ iSv Art. 5 Abs. 3 lit. k RL 2001/29/EG erfolgt ist. § 51a UrhG sei nämlich im Einklang mit dieser Bestimmung auszulegen, die er in deutsches Recht umsetzen solle.

Insoweit fragt sich der BGH erstens, ob die Schrankenregelung der Nutzung eines Werks oder eines anderen Schutzgegenstands zum Zweck von Pastiche iSv Art. 5 Abs. 3 lit. k RL 2001/29/EG einen Auffangtatbestand jedenfalls für eine künstlerische Auseinandersetzung mit einem vorbestehenden Werk oder sonstigen Bezugsgegenstand einschließlich des Sampling darstellt oder ob für den Begriff des Pastiche einschränkende Kriterien wie das Erfordernis von Humor, Stilmachung oder Hommage gelten.

Zweitens fragt sich der BGH, ob die Feststellung, dass ein Werk oder ein sonstiger urheberrechtlicher Schutzgegenstand „zum Zwecke“ eines Pastiche genutzt werde, eine Absicht des Nutzers voraussetzt, dieses Werk oder diesen Schutzgegenstand zu diesem Zweck zu nutzen, da das OLG Hamburg der Auffassung gewesen sei, dass eine solche Absicht nicht erforderlich sei und es daher keiner entsprechenden Feststellungen bedürfe.

Aus den Gründen

Zur ersten Frage

32 Mit seiner ersten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 5 Abs. 3 lit. k RL 2001/29/EG dahin auszulegen ist, dass die Ausnahme für Pastiche im Sinne dieser Bestimmung einen Auffangtatbestand darstellt, der jedenfalls eine künstlerische Auseinandersetzung mit einem vorbestehenden Werk einschließlich des Sampling umfasst, ohne dass es erforderlich wäre, dass diese Auseinandersetzung einen Ausdruck von Humor, eine Nachahmung des Stils oder eine Hommage darstellt.

33 Nach Art. 5 Abs. 3 lit. k RL 2001/29/EG können die Mitgliedstaaten für die Nutzung zum Zweck von Karikaturen, Parodien oder Pastiche in Bezug auf die in den Art. 2 und 3 vorgesehenen ausschließlichen Rechte – Vervielfältigungsrecht und Recht der öffentlichen Wiedergabe – Ausnahmen oder Beschränkungen vorsehen.

34 Da der Begriff „Pastiche“ in der RL 2001/29/EG nicht definiert ist und Art. 5 Abs. 3 lit. k der Richtlinie hinsichtlich seiner Bedeutung nicht auf die nationalen Rechte verweist, ist dieser Begriff nach stRspr als autonomer Begriff des Unionsrechts anzusehen, der im gesamten Gebiet der Union entsprechend seinem gewöhnlichen Sinn nach dem gewöhnlichen Sprachgebrauch und unter Berücksichtigung des Zusammenhangs, in dem dieser Begriff verwendet wird, und der mit dieser Bestimmung verfolgten Ziele einheitlich auszulegen ist (vgl. idS Urt. v. 3.9.2014 – C-201/13 Rn. 14, 15 und 19 – Deckmyn und Vrij-

heidsfonds, sowie Urt. v. 29.7.2019 – C-516/17 [= MMR 2019, 588 mAnm Hoeren/Düwel] Rn. 62 und 65 – Spiegel Online).

35 Was erstens den gewöhnlichen Sinn des Begriffs „Pastiche“ betrifft, ist ... festzustellen, dass dieser Begriff im gewöhnlichen Sprachgebrauch nur selten anzutreffen ist und dass er zwar üblicherweise verwendet wird, um ein Werk zu bezeichnen, dessen Stil den eines Werks, eines Künstlers oder von Werken derselben künstlerischen Strömung imitiert, gleichwohl aber eine Vielzahl unterschiedlicher Auffassungen zu ihm besteht.

36 So kann nach einigen Auffassungen auch eine mit betrügerischer Absicht erstellte versteckte Imitation als Pastiche eingestuft werden, während andere eine offene, erkennbare Nutzung charakteristischer Merkmale eines oder mehrerer früherer Werke in einer neuen Schöpfung verlangen, die dieses frühere Werk oder diese früheren Werke imitiert, um einen künstlerischen oder kreativen Dialog mit diesen Werken herzustellen.

37 Außerdem beschränken bestimmte Auffassungen den Begriff des Pastiche zwar auf humoristische oder satirische Imitationen und andere auf Stilimitationen, doch kann vielen Auffassungen zufolge die unter diesen Begriff fallende Nutzung unterschiedliche Formen annehmen und mit unterschiedlichen Absichten erfolgen, zB als Hommage an das Werk bzw. die Werke, auf das oder die sich das Pastiche bezieht, als Ausdruck einer Form von Humor oder Kritik oder als eine reine Stilübung.

38 Da der gewöhnliche Sinn dieses Begriffs somit nicht eindeutig ist, ist die Auslegung des Begriffs „Pastiche“ auf den Kontext, in den sich dieser Begriff einfügt, und die mit Art. 5 Abs. 3 lit. k RL 2001/29/EG verfolgten Ziele zu stützen.

39 Was zweitens den Kontext betrifft, in den sich der Begriff „Pastiche“ einfügt, ist festzustellen, dass Art. 5 Abs. 3 lit. k RL 2001/29/EG neben dem Pastiche als Ausnahmen von den in den Art. 2 und 3 dieser Richtlinie genannten ausschließlichen Rechten zur Vervielfältigung und öffentlichen Wiedergabe die „Karikatur“ und die „Parodie“ nennt.

40 Die Zusammenfassung dieser drei Begriffe innerhalb einer einzigen Bestimmung lässt die Annahme zu, dass sie nach der Vorstellung des Unionsgesetzgebers bestimmte wesentliche Merkmale gemeinsam haben, nämlich insb. das Merkmal, an ein bestehendes Werk zu erinnern, gleichzeitig aber ihm ggü. wahrnehmbare Unterschiede aufzuweisen (vgl. idS Urt. v. 3.9.2014 – C-201/13 Rn. 20 – Deckmyn und Vrijheidsfonds).

41 Wie der GA in den Rn. 62 und 69 seiner Schlussanträge im Wesentlichen ausgeführt hat, wollte der Unionsgesetzgeber jedoch durch die gleichberechtigte Aufzählung drei verschiedener Konzepte in Art. 5 Abs. 3 lit. k RL 2001/29/EG drei Nutzungskategorien zulassen, die sich zwar teilweise überschneiden können, aber dennoch so ausgelegt werden müssen, dass die praktische Wirksamkeit jeder dieser Ausnahmen gewährleistet ist. Daher darf der Gerichtshof einen oder mehrere dieser Begriffe nicht als rechtlich überflüssig auslegen.

42 Daraus folgt zum einen, dass das Pastiche zwar ebenso wie die Parodie und die Karikatur einen Ausdruck von Humor oder eine Verspottung darstellen kann (vgl. idS Urt. v. 3.9.2014 – C-201/13 Rn. 20 – Deckmyn und Vrijheidsfonds), jedoch nicht verlangt werden kann, dass dies zwangsläufig der Fall sein muss, da eine solche Auslegung des Begriffs „Pastiche“ zur Folge hätte, dass dieser Ausnahme dieselbe Tragweite verliehen würde wie der Parodie oder der Karikatur, wodurch ihre praktische Wirksamkeit beeinträchtigt würde.

43 Zum anderen kann der Begriff „Pastiche“ nicht dahin ausgelegt werden, dass er jede Schöpfung erfasst, die an ein beste-

hendes Werk erinnert und wahrnehmbare Unterschiede diesem ggü. aufweist, da eine solche Auslegung, wie sich aus Rn. 40 des vorliegenden Urteils ergibt, die beiden anderen in Art. 5 Abs. 3 lit. k RL 2001/29/EG aufgezählten Ausnahmen überflüssig machen würde.

44 Außerdem bietet, wie der GA in den Rn. 69 und 71 seiner Schlussanträge im Wesentlichen ausgeführt hat und wie sich aus Rn. 40 des vorliegenden Urteils ergibt, weder der Kontext von Art. 5 Abs. 3 lit. k RL 2001/29/EG noch allgemeiner der von Art. 5 der RL 2001/29/EG einen Anhaltspunkt dafür, dass der Unionsgesetzgeber die Ausnahme für Pastiche als Auffangbegriff für jede Form der kreativen Nutzung urheberrechtlich geschützten Materials gedacht hätte.

45 Was drittens das mit Art. 5 Abs. 3 lit. k der RL 2001/29/EG verfolgte Ziel betrifft, geht aus den Erwägungsgründen 3 und 31 RL 2001/29/EG hervor, dass Art. 5 Abs. 3 lit. k RL 2001/29/EG darauf abzielt, insb. vor dem Hintergrund der elektronischen Medien einen angemessenen Ausgleich zwischen den Interessen der Inhaber von Urheber- und verwandten Schutzrechten am Schutz ihres Rechts am geistigen Eigentum auf der einen Seite und dem Schutz der Interessen und Grundrechte der Nutzer von Schutzgegenständen, insb. ihrer durch die Art. 11 und 13 GRCh garantierten Meinungsäußerungs- und Kunstfreiheit, sowie dem Allgemeininteresse auf der anderen Seite sichern (vgl. idS Urt. v. 3.9.2014 – C-201/13 Rn. 25 und 26 – Deckmyn und Vrijheidsfonds, sowie Urt. v. 29.7.2019 – C-476/17 [= MMR 2019, 596 mAnm Apel] Rn. 32 – Pelham u.a.).

46 Zwar soll die RL 2001/29/EG, wie sich aus ihren Erwägungsgründen 4, 9 und 10 ergibt, ein hohes Schutzniveau für das Urheberrecht und die verwandten Schutzrechte gewährleisten, indem sie in ihren Art. 2 und 3 ausschließliche Rechte zur Vervielfältigung und öffentlichen Wiedergabe gewährt. Das in Art. 17 Abs. 2 der Charta verankerte Recht des geistigen Eigentums gilt jedoch nicht bedingungslos, sondern muss gegen die anderen Grundrechte abgewogen werden, zu denen die Freiheit der Kunst gehört, die in Art. 13 der Charta garantiert ist und die zur durch Art. 11 der Charta geschützten Freiheit der Meinungsäußerung gehört (vgl. idS Urt. v. 29.7.2019 – C-476/17 [= MMR 2019, 596 mAnm Apel] Rn. 33 und 34 – Pelham u.a., sowie die dort angeführte Rspr.).

47 Folglich müssen bei der Auslegung und Anwendung der in Art. 5 Abs. 3 lit. k RL 2001/29/EG vorgesehenen Ausnahmen in einem konkreten Fall ein angemessener Ausgleich zwischen den Interessen und Rechten der in den Art. 2 und 3 der Richtlinie genannten Personen auf der einen und der freien Meinungsäußerung und der künstlerischen Freiheit der Nutzer urheberrechtlicher Schutzgegenstände auf der anderen Seite sowie das Allgemeininteresse gewahrt werden (vgl. idS Urt. v. 3.9.2014 – C-201/13 Rn. 27 – Deckmyn und Vrijheidsfonds).

48 Insb. ist angesichts des mit Art. 5 Abs. 3 lit. k RL 2001/29/EG verfolgten Ziels und der Tatsache, dass die in dieser Bestimmung vorgesehenen Ausnahmen selbst Rechte zugunsten der Nutzer von Schutzgegenständen umfassen, die die Achtung der Grundfreiheiten gewährleisten sollen, der Begriff „Pastiche“ nicht eng auszulegen, sondern im vollen Einklang mit diesem Ziel und diesen Freiheiten (vgl. idS Urt. v. 29.7.2019 – C-469/17 [= MMR 2019, 660 mAnm Hoeren/Düwel] Rn. 69 bis 71 – Funke Medien NRW und Urt. v. 29.7.2019 – C-516/17 [= MMR 2019, 588 mAnm Hoeren/Düwel] Rn. 53 bis 55 – Spiegel Online).

49 Unter diesen Umständen ist zum einen festzustellen, dass der Begriff „Pastiche“ keine versteckten Imitationen von Schutzgegenständen oder gar Plagiate umfassen kann. Selbst wenn nämlich solche Formen der Nutzung urheberrechtlich geschützter Gegenstände unter bestimmten Voraussetzungen unter die

Freiheit der Meinungsäußerung oder die Kunstfreiheit fallen könnten, wäre eine Auslegung dieses Begriffs, wonach diese Formen nach Art. 5 Abs. 3 lit. k RL 2001/29/EG ohne vorherige Zustimmung der Rechtsinhaber zulässig wären, nicht geeignet, den angemessenen Ausgleich zu verwirklichen, den der Unionsgesetzgeber zwischen dem Schutz des Rechts am geistigen Eigentum dieser Rechtsinhaber und dem Schutz der Grundrechte der Nutzer von Schutzgegenständen sowie des Allgemeininteresses herstellen will. Folglich setzt dieser Begriff voraus, dass es sich um Formen der offenen Nutzung von Schutzgegenständen handelt, die als solche erkennbar sind.

50 Was zum anderen die Frage betrifft, welche Formen der offenen Nutzung von Schutzgegenständen konkret unter den Begriff „Pastiche“ fallen, ist unter Berücksichtigung des mit Art. 5 Abs. 3 lit. k RL 2001/29/EG verfolgten Ziels, die Wahrung der Meinungsäußerungs- und der Kunstfreiheit zu gewährleisten, und der in den Rn. 35 bis 43 des vorliegenden Urteils dargelegten Erwägungen davon auszugehen, dass dieser Begriff Schöpfungen erfasst, die an ein oder mehrere bestehende Werke erinnern, gleichzeitig aber wahrnehmbare Unterschiede diesen ggü. aufweisen, um mit diesen Werken eine als solche erkennbare Form des künstlerischen oder kreativen Dialogs aufzunehmen.

51 Hierzu ist zunächst festzustellen, dass es für die Aufnahme eines solchen Dialogs erforderlich ist, dass die in der neuen Schöpfung genutzten Elemente für das Werk oder die Werke, aus denen sie stammen, charakteristisch sind.

52 Sodann muss, da nur die Nutzung von Elementen eines Werks, die einzeln oder gemeinsam durch das Urheberrecht geschützt sind, die Zustimmung des Rechtsinhabers erfordern kann, die Pastiche-Ausnahme in gewissem Umfang die Nutzung solcher geschützten Elemente ermöglichen, da sie andernfalls keine praktische Wirksamkeit hätte, wie der GA in den Rn. 65 und 66 seiner Schlussanträge im Wesentlichen ausgeführt hat.

53 Schließlich kann der künstlerische oder kreative Dialog mit dem Werk oder den Werken, aus dem bzw. denen die genutzten Elemente stammen, verschiedene Formen annehmen, darunter die einer Imitation des Stils dieser Werke, einer Hommage an sie oder einer humoristischen oder kritischen Auseinandersetzung mit diesen Werken.

54 Im vorliegenden Fall möchte das vorlegende Gericht insb. wissen, ob die Übernahme der Rhythmussequenz aus einem Musiktitel im Wege des Sampling unter die in Art. 5 Abs. 3 lit. k RL 2001/29/EG vorgesehene Ausnahme für Pastiche fallen kann.

55 Insoweit ist zum einen darauf hinzuweisen, dass diese Technik, bei der ein Nutzer – zumeist mit Hilfe elektronischer Geräte – einem Tonträger ein Audiofragment entnimmt und dieses zur Schaffung eines neuen Werks nutzt, eine künstlerische Ausdrucksform ist, die unter die ihrerseits durch Art. 13 GRCh geschützte Freiheit der Kunst fällt (vgl. idS Urt. v. 29.7.2019 – C-476/17 [= MMR 2019, 596 mAnm Apel] Rn. 35 – Pelham u.a.).

56 Zum anderen kann der Tonträgerhersteller sich aufgrund des ihm durch Art. 2 lit. c RL 2001/29/EG eingeräumten ausschließlichen Rechts, die Vervielfältigung seines Tonträgers zu erlauben oder zu verbieten, der Nutzung eines Audiofragments seines Tonträgers durch einen Dritten, um dieses Fragment in beim Hören wiedererkennbarer Weise in einen anderen Tonträger aufzunehmen, grds. widersetzen. Dies steht im Einklang mit dem im zehnten Erwägungsgrund dieser Richtlinie genannten spezifischen Ziel des ausschließlichen Rechts des Tonträgerherstellers,

seine Investitionen zu schützen. Wie nämlich der Unionsgesetzgeber in diesem zehnten Erwägungsgrund ausgeführt hat, sind beträchtliche Investitionen erforderlich, um Produkte wie Tonträger anbieten zu können, sodass den Tonträgerherstellern die Möglichkeit zu geben ist, einen zufriedenstellenden Ertrag zu erzielen (vgl. idS Urt. v. 29.7.2019 – C-476/17 [= MMR 2019, 596 mAnm Apel] Rn. 29 bis 31 – Pelham u.a.).

57 Daher wird der angemessene Ausgleich, der zwischen dem Schutz der Freiheit der Kunst und dem des Urheberrechts und der verwandten Schutzrechte sicherzustellen ist, erreicht, wenn unter die Ausnahme für Pastiche eine Übernahme der Rhythmussequenz eines Musiktitels im Wege des Sampling fällt, sofern das so entnommene Audiofragment zur Schaffung eines Werks genutzt wird, das den in den Rn. 49 bis 53 des vorliegenden Urteils genannten Anforderungen entspricht.

58 Nach alledem ist auf die erste Frage zu antworten, dass Art. 5 Abs. 3 lit. k RL 2001/29/EG dahin auszulegen ist, dass die in dieser Bestimmung vorgesehene Ausnahme für Pastiche kein Auffangtatbestand ist, sondern Schöpfungen erfasst, die an ein oder mehrere bestehende Werke erinnern, gleichzeitig aber wahrnehmbare Unterschiede diesen ggü. aufweisen, und die, einschließlich im Wege des Sampling, einige ihrer urheberrechtlich geschützten Elemente nutzen, um mit diesen Werken einen als solchen erkennbaren künstlerischen oder kreativen Dialog zu führen, der verschiedene Formen annehmen kann, darunter die einer offenen Nachahmung des Stils dieser Werke, einer Hommage an sie oder einer humoristischen oder kritischen Auseinandersetzung mit ihnen.

Zur zweiten Frage

59 Mit seiner zweiten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 5 Abs. 3 lit. k RL 2001/29/EG dahin auszulegen ist, dass es für eine Nutzung „zum Zwecke von“ Pastiche im Sinne dieser Bestimmung erforderlich ist, dass bei dem Nutzer, der sich auf diese Bestimmung berufen möchte, die Absicht festgestellt wird, ein bestehendes Werk zu diesem Zweck zu nutzen, oder ob es genügt, dass der Charakter als „Pastiche“ für denjenigen erkennbar ist, dem dieses Werk bekannt ist und der das erforderliche intellektuelle Verständnis besitzt.

60 Wie sich aus der Antwort auf die erste Frage ergibt, impliziert die Einstufung als Pastiche u.a., dass in der neuen Schöpfung, die verschiedene Formen annehmen kann, geschützte charakteristische Elemente des bestehenden Werks genutzt werden, um mit diesem einen als solchen erkennbaren künstlerischen oder kreativen Dialog zu führen.

61 Wie der GA in Rn. 82 seiner Schlussanträge im Wesentlichen ausgeführt hat, ist es jedoch zur Gewährleistung der Rechtssicherheit erforderlich, die Frage, ob dies der Fall ist, anhand objektiver Kriterien zu prüfen, sodass der Charakter als Pastiche für denjenigen erkennbar sein muss, dem das bestehende Werk bekannt ist, dem diese Elemente entnommen sind.

62 Folglich ist auf die zweite Frage zu antworten, dass Art. 5 Abs. 3 lit. k RL 2001/29/EG dahin auszulegen ist, dass es für eine Nutzung „zum Zwecke von“ Pastiche im Sinne dieser Bestimmung genügt, dass der Charakter als Pastiche für denjenigen erkennbar ist, dem das bestehende Werk bekannt ist, dem diese Elemente entnommen sind. ...

Anmerkung

Prof. Dr. Thomas Hoeren, ITM, Universität Münster

Mit seinem Urteil in der Rs. Pelham u.a. konturiert der EuGH den unionsautonomen Begriff des Pastiche iSv Art. 5 Abs. 3 lit. k InfoSoc-RL erstmals näher. Die Entscheidung ist für das

Musikurheberrecht und darüber hinaus für Remixe, Memes, Mash-ups und Transformationen allgemein von erheblicher Bedeutung. Der Gerichtshof wählt dabei einen Mittelweg: Er weist ein Verständnis des Pastiches als bloßen Auffangtatbestand für jede künstlerische Auseinandersetzung mit vorbestehendem Material zurück, öffnet die Schranke aber ausdrücklich auch für Sampling, sofern die neue Schöpfung mit dem benutzten Werk einen als solchen erkennbaren künstlerischen oder kreativen Dialog führt. Die methodische Grundlage dieses Mittelwegs verdient dabei besondere Aufmerksamkeit. So stützt der EuGH sich auf eine Redundanzvermeidung innerhalb des Art. 5 Abs. 3 lit. k InfoSoc-RL und bricht zugleich mit dem hergebrachten Grundsatz, wonach Schranken des Urheberrechts stets restriktiv auszulegen seien. Das Urteil ergeht in dem seit mehr als 20 Jahren geführten Rechtsstreit um die Übernahme einer etwa zwei Sekunden dauernden Rhythmussequenz aus „Metall auf Metall“ in dem Titel „Nur mir“.

I. Problemaufriss

Der Fall ist längst zu einem Grundtext des europäischen Sampling-Rechts geworden. Nachdem der EuGH bereits 2019 klargestellt hatte, dass die Übernahme eines Audiofragments in wiedererkennbarer Form grds. in das Tonträgerherstellerrecht eingreift, sofern nicht das Fragment in geänderter und beim Hören nicht wiedererkennbarer Form verwendet wird, verlagerte sich der Streit nun auf die Reichweite der 2021 in deutsches Recht eingeführten Pastiche-Schranke des § 51a UrhG. Der BGH wollte wissen, ob diese Schranke gewissermaßen als offene Transformationsklausel verstanden werden könne oder ob sie nur engere Fallgruppen wie Stilnachahmung, Hommage oder humoristische Brechung erfasse. Genau darauf gibt der EuGH nun eine differenzierte Antwort.

II. Kernaussagen des EuGH

Der EuGH lehnt zunächst ausdrücklich ab, den Pastiche als Auffangtatbestand für jede Form kreativer Nutzung urheberrechtlich geschützten Materials zu verstehen. Die Ausnahme sei gerade keine Generalklausel zugunsten freier Kunstaneignung. Damit erteilt der Gerichtshof einer besonders weiten, im deutschen Diskurs teilweise vertretenen Lesart eine klare Absage.

Die tragende Begründung hierfür entnimmt der EuGH dem Gebot praktischer Wirksamkeit (*effet utile*): Würde der Pastiche jede Schöpfung erfassen, die an ein bestehendes Werk erinnert und wahrnehmbare Unterschiede aufweist, wären Parodie und Karikatur als eigenständige Ausnahmen in Art. 5 Abs. 3 lit. k InfoSoc-RL überflüssig. Spiegelbildlich folgt aus derselben Erwägung, dass der Pastiche nicht auf humoristische Formen verengt werden darf, weil er sonst deckungsgleich mit der Parodie wäre und seinerseits keinen eigenständigen Anwendungsbereich besäße. Diese Redundanzvermeidung bildet die methodische Klammer der gesamten Auslegung.

Zugleich fasst der EuGH den Begriff aber keineswegs eng iSb bloßen Stilkopie. Der Gerichtshof formuliert unter Verweis auf die Entscheidungen *Funke Medien* und *Spiegel Online* ausdrücklich, dass der Pastiche-Begriff nicht eng auszulegen sei, weil die Ausnahmen in Art. 5 Abs. 3 lit. k InfoSoc-RL selbst Rechte zugunsten der Nutzer umfassten, die die Achtung der Grundfreiheiten gewährleisten sollen. Das ist methodisch bemerkenswert: Der EuGH löst sich damit endgültig von dem traditionellen Grundsatz, wonach Ausnahmen vom urheberrechtlichen Ausschließlichkeitsrecht stets restriktiv auszulegen seien. An dessen Stelle tritt eine teleologische Auslegung, die den Grundrechtsgehalt der Schranke in die Bestimmung ihrer Reichweite einbezieht.

Vielmehr erfasst der Pastiche nach der Formel der luxemburgischen Richter Schöpfungen, die an ein oder mehrere bestehende Werke erinnern, zugleich aber wahrnehmbare Unterschiede aufweisen und unter Nutzung geschützter Elemente mit diesen Werken einen als solchen erkennbaren künstlerischen oder kreativen Dialog führen. Der EuGH verlangt dabei, dass die in der neuen Schöpfung genutzten Elemente für das Ausgangswerk charakteristisch sind. Damit wird eine eigenständige qualitative Schwelle errichtet: Nicht jede Übernahme irgendeines geschützten Bestandteils genügt – die entnommenen Elemente müssen das Ausgangswerk als solches kennzeichnen. Generische oder stilübliche Elemente, die keinen spezifischen Werkbezug herstellen, dürften damit tendenziell aus dem Anwendungsbereich der Schranke herausfallen.

Zugleich betont der Gerichtshof, dass die Pastiche-Ausnahme in gewissem Umfang die Nutzung urheberrechtlich geschützter Elemente ermöglichen muss, da sie andernfalls keine praktische Wirksamkeit besäße. Diese Aussage ist von erheblicher dogmatischer Tragweite: Der EuGH legitimiert damit ausdrücklich den Zugriff auf den geschützten Kern des Ausgangswerks und beschränkt die Schranke gerade nicht auf die Übernahme gemeinfreier oder nicht schutzfähiger Bestandteile. Für die Anwendungspraxis bedeutet das, dass auch substanzielle Werkentnahmen vom Pastiche-Privileg gedeckt sein können, sofern die übrigen Voraussetzungen – insb. der erkennbare Dialog – erfüllt sind. Dieser Dialog kann unterschiedliche Formen annehmen, namentlich die offene Stilnachahmung, die Hommage sowie die humoristische oder kritische Auseinandersetzung. Gerade diese Offenheit macht deutlich, dass der EuGH keinen kasuistischen Typenzwang errichten, wohl aber eine substanzielle inhaltliche Schwelle sichern will.

Im Sampling-Kontext stellt der EuGH die Pastiche-Ausnahme allerdings ausdrücklich in ein Spannungsverhältnis zum Investitionsschutzgedanken des Tonträgerherstellerrechts. Unter Verweis auf Erwägungsgrund 10 InfoSoc-RL betont er, dass beträchtliche Investitionen für die Herstellung von Tonträgern erforderlich seien und den Herstellern die Möglichkeit gegeben werden müsse, einen zufriedenstellenden Ertrag zu erzielen. Der angemessene Ausgleich wird nach Auffassung des EuGH gerade dadurch erreicht, dass die Pastiche-Ausnahme nur unter den genannten qualifizierten Voraussetzungen eingreift. Damit macht der Gerichtshof deutlich, dass die Abwägung nicht allein zwischen Kreativschutz und Kunstfreiheit verläuft, sondern auch die ökonomische Amortisationserwartung der Rechteinhaber als eigenständiger Belang in die Schrankenkontrolle einfließt.

Von erheblicher praktischer Bedeutung ist ferner die zweite Antwort des EuGH: Für eine Nutzung „zum Zwecke“ eines Pastiches kommt es nicht auf eine subjektive Absicht des Nutzers an. Es genügt, dass der Pastiche-Charakter für denjenigen erkennbar ist, dem das benutzte Werk bekannt ist. Bemerkenswert ist dabei, dass der EuGH den Rezipientenmaßstab ggü. der Vorlagefrage des BGH stillschweigend vereinfacht: Während der BGH zusätzlich zur Werkkenntnis noch das „erforderliche intellektuelle Verständnis“ des Rezipienten als Voraussetzung formuliert hatte (BGH MMR 2024, 171 mAnm Kreutzer, Vorlagefrage 2, Rn. 59), verzichtet der EuGH im Tenor auf dieses kumulative Kriterium und verlangt nur die Bekanntheit des Ausgangswerks. Das senkt die Erkennbarkeitsschwelle: Werkkenntnis genügt, ohne dass ein besonderes ästhetisches oder kulturelles Vorwissen hinzutreten müsste. Damit objektiviert der Gerichtshof die Schrankenprüfung und stärkt die Rechtssicherheit.

III. Bewertung

1. Zutreffende Absage an die Generalklausel

Die wichtigste dogmatische Leistung des Urteils liegt in der Zurückweisung eines schrankenlosen Transformationsbegriffs. Hätte der EuGH jede „künstlerische Auseinandersetzung“ mit vorbestehendem Material genügen lassen, wäre der Pastiche zur Einbruchsstelle für eine kaum noch konturierbare allgemeine Kunstfreiheitsschranke geworden. Das hätte die Systematik des Art. 5 InfoSoc-RL unterlaufen, dessen Schranken gerade abschließend und als Ausnahme vom grundsätzlichen Ausschließlichkeitsrecht ausgestaltet sind. Insofern überzeugt die Aussage des EuGH, dass der Pastiche keine „Restkategorie“ für alle nicht anderweitig erfassbaren Kunstformen sein kann. Dass der EuGH dies nicht nur postuliert, sondern über die Redundanzvermeidung innerhalb des Art. 5 Abs. 3 lit. k InfoSoc-RL systematisch herleitet, verleiht der Begründung eine Stringenz, die über den Einzelfall hinaus als Auslegungsmodell für das gesamte Schrankengefüge fruchtbar gemacht werden kann.

2. Zu Recht keine Reduktion auf Humor oder Stilimitat

Ebenso überzeugend ist jedoch die Gegenbewegung des EuGH, den Pastiche nicht auf humoristische Bearbeitungen oder bloße Stilübungen zu verengen. Eine solche Engführung hätte den eigenständigen Regelungsgehalt der Norm verkürzt und insb. gegenwärtige Kulturtechniken der digitalen Aneignung nur unzureichend erfasst. Gerade Sampling, Mash-up, Fan Art oder Meme operieren typischerweise nicht notwendig mit Spott oder Parodie, sondern mit Kontextverschiebung und Neuverknüpfung. Dass der EuGH hierfür die Formel des „erkennbaren künstlerischen oder kreativen Dialogs“ wählt, ist deshalb funktional richtig.

Darüber hinaus verdient der ausdrückliche Bruch mit dem Grundsatz restriktiver Schrankenauslegung Hervorhebung. Indem der EuGH unter Verweis auf die Rs. Funke Medien und die Rs. Spiegel Online die Grundrechte der Nutzer zum integralen Bestandteil der Auslegungsmethode erhebt, vollzieht er einen methodischen Paradigmenwechsel, der über den Pastiche hinaus für alle grundrechtsrelevanten Schranken des Art. 5 InfoSoc-RL Geltung beansprucht. Die praktische Konsequenz ist erheblich: Gerichte können sich künftig nicht mehr darauf beschränken, Schrankentatbestände aus einem Vorverständnis möglichst enger Auslegung heraus zu bestimmen, sondern müssen deren Grundrechtsgehalt positiv in die Auslegung einbeziehen.

3. Offene Nutzung als Grenze gegenüber Plagiat und verdeckter Imitation

Besonders wichtig ist die vom EuGH gezogene Grenzlinie: Der Pastiche schützt nur offene, als solche erkennbare Nutzungen. Verdeckte Imitationen und Plagiate scheiden aus. Damit wahrt der Gerichtshof den inneren Zusammenhang von Kunstfreiheit und Transparenz der Bezugnahme. Wo der Nutzer das fremde Werk gerade in der Weise aufgreift, dass die Bezugnahme ästhetisch erfahrbar wird, kann die Schranke eingreifen. Wo die Übernahme dagegen verborgen bleiben soll, fehlt der kommunikative Mehrwert, der die Beschränkung der Ausschließlichkeitsrechte rechtfertigen könnte.

4. Stärkung des objektiven Prüfungsmaßstabs

Auch die Abkehr von einem subjektiven Absichtserfordernis verdient Zustimmung. Im Urheberrecht würde eine innere Motivforschung regelmäßig zu kaum beherrschbaren Abgrenzungsproblemen führen. Die vom EuGH gewählte objektive Perspektive – Erkennbarkeit für den mit dem Ursprungswerk vertrauten Rezipienten – ist revisionsfest, rechtspraktisch

handhabbar und dem Werkbezug der Schranke angemessen. Maßgeblich ist damit nicht das Selbstverständnis des Benutzers, sondern die kommunikative Struktur der neuen Schöpfung.

Dass der EuGH dabei das vom BGH zusätzlich geforderte „erforderliche intellektuelle Verständnis“ des Rezipienten stillschweigend fallen lässt und allein auf die Werkkenntnis abstellt, ist dogmatisch konsequent: Ein zusätzliches Verständniskriterium hätte einen unsicheren Bildungsmaßstab in die Schrankenprüfung eingeführt und die objektive Perspektive wieder subjektiviert. Die Vereinfachung auf bloße Werkkenntnis hält den Maßstab schlank und verhindert, dass die Erkennbarkeitsfrage zum Einfallstor für kulturelle Distinktionsurteile wird.

5. Investitionsschutz als eigenständiger Abwägungsbelang

Das Urteil verdient auch insoweit Beachtung, als der EuGH die Abwägung im Sampling-Kontext nicht auf die Achse Kreativschutz/Kunstfreiheit reduziert, sondern den Investitionsschutz des Tonträgerherstellers als eigenständigen Belang einführt. Erwägungsgrund 10 InfoSoc-RL und das spezifische Amortisationsinteresse des Herstellers bilden damit eine ökonomische Gegenposition, die bei der Anwendung der Pastiche-Schranke im Einzelfall zu berücksichtigen ist. Für Fälle massenhafter oder kommerziell motivierter Übernahme dürfte dieser Aspekt künftig erhebliches Gewicht gewinnen, auch wenn der EuGH ihn im vorliegenden Fall nicht zum Hindernis für die Schranken-anwendung erhebt.

6. Offene Frage: Dreistufentest als Korrektivebene

Auffällig ist schließlich, was das Urteil nicht thematisiert: Art. 5 Abs. 5 InfoSoc-RL wird zwar im Rahmenrecht zitiert, aber nicht eigenständig angewendet. Ob der Dreistufentest als zusätzliche Korrekturstufe nach der Feststellung eines Pastiches herangezogen werden kann, bleibt damit offen. Da der EuGH die Pastiche-Schranke bereits tatbestandlich durch das Erfordernis des erkennbaren Dialogs, der Offenheit und der Nutzung charakteristischer Elemente konturiert, ließe sich argumentieren, dass diese Voraussetzungen den Dreistufentest funktional vorwegnehmen. Gleichwohl wäre eine ausdrückliche Klärung wünschenswert gewesen, zumal für Fälle, in denen die tatbestandlichen Voraussetzungen des Pastiches zwar erfüllt sind, die wirtschaftlichen Auswirkungen auf den Rechteinhaber aber ein Ausmaß erreichen, das den Dreistufentest auf den Plan rufen könnte. Hier verbleibt eine Lücke, die der BGH oder künftige Vorlagen schließen müssen.

IV. Folgen für den deutschen Rechtsrahmen

Für § 51a UrhG bedeutet das Urteil eine klare unionsrechtliche Leitplanke. Die Norm darf künftig weder als bloßer Sammelbegriff für freie Benutzung unter neuem Namen noch als enges Annexinstitut zu Parodie und Karikatur verstanden werden. Sie ist vielmehr als besondere Transformationsschranke zu lesen, die einen erkennbaren, offenen Bezug zwischen Altwerk und Neuschöpfung verlangt.

Damit dürfte sich zugleich der deutsche Diskurs verschieben: Nicht jede kreative Aneignung wird unter § 51a UrhG subsumierbar sein; andererseits wird die Vorschrift künftig in digitalen Aneignungskontexten eine weit größere Rolle spielen als ein traditionelles, auf Stilimitate reduziertes Pastiche-Verständnis vermuten ließ. Gerade für Plattformkulturen ist dies zentral, weil der EuGH mit seiner Entscheidung die unionsrechtliche Legitimität solcher Bezugnahmeformen ausdrücklich bestätigt, ohne das Ausschließlichkeitsrecht leer laufen zu lassen.

Besondere Aufmerksamkeit verdient dabei das Kriterium der charakteristischen Elemente: Die deutsche Praxis wird Maßstäbe dafür entwickeln müssen, wann ein übernommenes Element das Ausgangswerk als solches kennzeichnet und wann es lediglich einem generischen Stilrepertoire zuzuordnen ist. Im Bereich der Musikproduktion, in dem standardisierte Patterns, Loops und Sounds allgegenwärtig sind, wird diese Abgrenzung nicht immer einfach sein, aber sie ist unverzichtbar, um die Pastiche-Schranke von einer allgemeinen Freistellung des Sounddesigns abzugrenzen.

V. Prognose für die BGH-Entscheidung

Für das anhängige Revisionsverfahren vor dem BGH spricht nach der Luxemburger Entscheidung mehr für eine Bestätigung des OLG-Ergebnisses für den Zeitraum ab dem 7.6.2021 als für dessen Aufhebung. Der EuGH verweist in seiner Mitteilung selbst auf die vom BGH referierten vorinstanzlichen Feststellungen des OLG Hamburg, wonach die übernommene Sequenz in ein anderes musikalisches Genre übertragen worden sei und trotz Temporeduktion und metrischer Verschiebung als Anspielung auf das Original erkennbar bleibe. Das deutet stark darauf hin, dass Luxemburg die Sache nicht als bloße Tonentnahme, sondern als potenziell dialogische Transformationshandlung liest. Der BGH wird seine frühere, der Vorlage zugrunde liegende Tendenz zu einem weiten Verständnis des Pastiches allerdings vor dem Hintergrund der Ansicht des EuGH korrigieren müssen. Bestätigt er das OLG, dann nicht mit der Formel eines allgemeinen Auffangtatbestands für künstlerische Auseinandersetzungen, sondern mit der engeren Begründung, dass im konkreten Fall ein objektiv erkennbarer kreativer Dialog mit „Metall auf Metall“ vorliegt. Dogmatisch wäre dies die sauberste Lösung: keine Generalschranke, aber ein zulässiges Pastiche im Einzelfall.

Offen bleibt ferner, ob der BGH Anlass sehen wird, den vom EuGH nicht angewendeten Dreistufentest des Art. 5 Abs. 5 InfoSoc-RL eigenständig heranzuziehen. Angesichts der geringen wirtschaftlichen Bedeutung der konkreten Tonentnahme dürfte dies hier fernliegen, aber die Frage wird sich in künftigen Sampling-Fällen mit größerer Dringlichkeit stellen.

VI. Fazit

Der EuGH hat den Pastiche weder domestiziert noch entgrenzt. Die Entscheidung weist den Weg zu einem funktionsgerechten Mittelbegriff: geschützt ist nicht jede kreative Nutzung, wohl aber die offene, erkennbare und dialogische Transformation fremden Materials unter Verwendung für das Ausgangswerk charakteristischer Elemente. Für das Sampling ist das eine vorsichtige, aber folgenreiche Öffnung. Für das Urheberrecht insgesamt ist es ein Versuch, Eigentumsschutz und Kunstfreiheit nicht abstrakt gegeneinander auszuspielen, sondern in einer Schrankenfigur zum Ausgleich zu bringen. Die eigentliche Tiefenwirkung des Urteils liegt dabei weniger im Ergebnis als in der Methode: Der EuGH etabliert mit der Redundanzvermeidung ein Auslegungsmodell, das auf das gesamte Schrankengefüge des Art. 5 InfoSoc-RL übertragbar ist, und vollzieht mit der Abkehr von der restriktiven Schrankenauslegung einen Paradigmenwechsel, dessen Folgen weit über den Pastiche hinausreichen. Dass zugleich offene Fragen verbleiben – namentlich die Rolle des Dreistufentests und die Operationalisierung des Merkmals der Charakteristik – mindert den Wert des Urteils nicht, sondern verweist auf die unvermeidliche Entwicklungsoffenheit einer Schrankendogmatik, die mit der Dynamik digitaler Kreativpraktiken Schritt halten muss. Gerade darin liegt die Stärke des Urteils.

EuGH: Exzessivität von Auskunftsanträgen

Datenverarbeitung

DS-GVO Art. 4 Nr. 2, 12 Abs. 5, 15 Abs. 1, 82 Abs. 1
Urteil vom 19.3.2026 – C-526/24 – Brillen Rottler

Leitsätze der Redaktion

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

Anm. d. Red.: Der Volltext ist abrufbar unter: [BeckRS 2026, 4080](#). Die Entscheidung ist auch veröffentlicht in ZD 2026, 335 mAnm Ligocki/Mekat. Das vorliegende Gericht (AG Arnsberg) ist veröffentlicht in ZD 2024, 648 mAnm Brandt/Goffart. Vgl. ferner AG Darmstadt ZD 2026, 348 mAnm Zieba/Löwer; EuGH MMR 2023, 939 mAnm Hense/Däuble = ZD 2024, 22 mAnm Winnenburg; EuGH ZD 2025, 272 mAnm Wirthensohn; EuGH ZD 2024, 146; EuGH MMR 2024, 400; EuGH ZD 2023, 271; EuGH ZD 2023, 606 mAnm Stief; EuGH ZD 2023, 446 mAnm Mekat/Ligocki; EuGH MMR 2025, 950 mAnm Mekat/Ligocki = ZD 2025, 640 mAnm Mekat/Wellmann; EuGH ZD 2025, 87; EuGH ZD 2024, 208; EuGH ZD 2024, 519 mAnm Pauly/Kienle; BGH MMR 2026, 203 mAnm Ligocki/Wellmann; Ligocki/Sosna/Meyer ZD 2025, 137; EuGH ZD 2024, 150 mAnm Ligocki/Sosna und EuGH MMR 2026, 506 mAnm Briske/Muter – in diesem Heft; OLG Brandenburg ZD 2023, 617; OLG Hamm ZD 2022, 237 und OLG Nürnberg ZD 2022, 463.

Schlagworte: Datenverarbeitung; Rechtsmissbrauch; Sachfremde Zwecke; Immaterieller Schaden; Kontrollverlust

Sachverhalt

Im März 2023 abonnierte TC, eine in Österreich wohnhafte natürliche Person, den Newsletter von Brillen Rottler, einem familiengeführten Optikerunternehmen mit Sitz in Arnsberg. Dabei gab er seine personenbezogenen Daten in die Anmeldemaske auf der Webseite des Unternehmens ein und willigte in die Verarbeitung dieser Daten ein. 13 Tage später richtete TC einen Auskunftsantrag nach Art. 15 DS-GVO an Brillen Rottler. Brillen Rottler wies den Auskunftsantrag innerhalb der gesetzlichen Frist von einem Monat zurück, da sie ihn für missbräuchlich iSv Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO hielt. Sie forderte TC auf, endgültig von seinem Antrag abzusehen.

Nachdem TC seinen Auskunftsantrag weiterverfolgte und darüber hinaus einen Schadensersatzanspruch aus Art. 82 DS-GVO iHv 1.000 EUR geltend machte, erhob Brillen Rottler beim AG Arnsberg, dem vorlegenden Gericht, Klage auf Feststellung, dass TC kein Anspruch auf Schadensersatz zustehe.

TC stützt ihren Feststellungsantrag darauf, dass aus verschiedenen Medienberichten, Blogbeiträgen und Berichten von Rechtsanwälten hervorgehe, dass TC Anträge auf Auskunft über seine personenbezogenen Daten systematisch und rechtsmissbräuchlich allein zu dem Zweck stelle, eine Entschädigung für eine von ihm bewusst provozierte angebliche Verletzung seiner Rechte aus der DS-GVO zu erzwingen. Er gehe nach dem Muster vor, sich zunächst zu einem Newsletter anzumelden, dann Auskunft zu beantragen und schließlich Schadensersatz zu fordern.

TC macht vor dem vorlegenden Gericht geltend, sein Auskunftsantrag an Brillen Rottler sei legitim und entspreche seinem Auskunftsrecht nach Art. 15 DS-GVO; Brillen Rottler wolle ihn unrechtmäßig in seinen Rechten aus der DS-GVO einschränken. Mit einer Widerklage begehrt er die Verurteilung von Brillen Rottler zur Zahlung einer Entschädigung iHv mind. 1.000 EUR für den immateriellen Schaden, der ihm durch die Weigerung des Unternehmens, ihm Auskunft über seine personenbezogenen Daten zu erteilen, entstanden sei.

Das vorlegende Gericht sieht sich als Erstes vor die Frage gestellt, ob ein erster Auskunftsantrag der betroffenen Person als „exzessiver Antrag“ iSv Art. 12 Abs. 5 DS-GVO und damit als Rechtsmissbrauch angesehen werden kann und anhand welcher Umstände ein solcher exzessiver Charakter festgestellt werden kann. Insb. fragt es sich, ob sich ein Verantwortlicher, um einen Auskunftsantrag auf der Grundlage dieser Bestimmung zurückzuweisen, auf öffentliche Informationen stützen kann, aus denen hervorgeht, dass dieselbe Person zahlreiche Auskunftsanträge und Schadensersatzforderungen an andere Verantwortliche gerichtet hat.

Als Zweites wirft das vorlegende Gericht die Frage auf, ob ein Auskunftsantrag nach Art. 15 Abs. 1 DS-GVO und/oder dessen Beantwortung eine „Verarbeitung“ iSv Art. 4 Nr. 2 DS-GVO darstellt. Als Drittes hegt das vorlegende Gericht Zweifel hinsichtlich der Kriterien für die Ersatzfähigkeit von Schäden nach Art. 82 Abs. 1 DS-GVO und insb. hinsichtlich der Frage, ob dieser Artikel ein Recht auf Schadensersatz auch ohne Verarbeitung allein aufgrund der Verletzung des in Art. 15 Abs. 1 DS-GVO vorgesehenen Auskunftsrechts verleiht. Vor diesem Hintergrund hat das AG Arnsberg beschlossen, das Verfahren auszusetzen und dem Gerichtshof Fragen zur Vorabentscheidung vorzulegen.

Aus den Gründen

Zu den Fragen 1 bis 3 und 7

21 Mit seinen Fragen 1 bis 3 und 7, die zusammen und als Erstes zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 12 Abs. 5 DS-GVO dahin auszulegen ist, dass es möglich ist, einen ersten von der betroffenen Person an den Verantwortlichen gerichteten Antrag nach Art. 15 DS-GVO auf Auskunft über personenbezogene Daten als „exzessiv“ im Sinne dieses Art. 12 Abs. 5 DS-GVO anzusehen, und, wenn dem so ist, anhand welcher Umstände ggf. ein solcher exzessiver Charakter festgestellt werden kann.

22 Art. 15 Abs. 1 DS-GVO garantiert insoweit das Recht der betroffenen Person, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden, und, wenn dies der Fall ist, das Recht dieser Person auf Auskunft über diese Daten und die damit verbundenen Informationen (vgl. idS Urt. v. 26.10.2023 –

C-307/22 [= MMR 2023, 939 mAnm Hense/Däuble = ZD 2024, 22 mAnm Winnenburg] Rn. 31 – FT (Kopien der Patientenakte)).

23 Außerdem stellt Art. 12 Abs. 5 DS-GVO den Grundsatz auf, dass der betroffenen Person durch die Ausübung des Rechts auf Auskunft keine Kosten entstehen. Gleichwohl gibt es nach dieser Bestimmung zwei Gründe, aus denen der Verantwortliche entweder ein angemessenes Entgelt in Rechnung stellen kann, bei dem die Verwaltungskosten berücksichtigt werden, oder sich weigern kann, aufgrund des Auskunftsantrags tätig zu werden. Diese Gründe beziehen sich auf Fälle von Rechtsmissbrauch, in denen die Anträge der betroffenen Person als „offenkundig unbegründet“ oder – insb. im Fall häufiger Wiederholung – „exzessiv“ anzusehen sind (Urt. v. 26.10.2023 – C-307/22 [= MMR 2023, 939 mAnm Hense/Däuble = ZD 2024, 22 mAnm Winnenburg] Rn. 31 – FT (Kopien der Patientenakte)).

24 Was erstens die Frage betrifft, ob ein erster Auskunftsantrag der betroffenen Person an den Verantwortlichen nach Art. 15 DS-GVO als „exzessiv“ angesehen werden kann, ist darauf hinzuweisen, dass, da der Begriff „exzessive Anträge“ in der DS-GVO nicht definiert wird, bei seiner Auslegung nach stRspr sowohl der Wortlaut von Art. 12 Abs. 5 DS-GVO entsprechend seinem üblichen Sinn im gewöhnlichen Sprachgebrauch als auch der Zusammenhang dieser Bestimmung und die Ziele zu berücksichtigen sind, die mit der Regelung, zu der sie gehört, verfolgt werden (vgl. Urt. v. 17.11.1983 – 292/82 Rn. 12 – Merck und v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 24 und die dort angeführte Rspr. – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

25 Insoweit bezeichnet, was den Wortlaut von Art. 12 Abs. 5 DS-GVO und insb. den üblichen Sinn des Begriffs „exzessive Anträge“ im gewöhnlichen Sprachgebrauch anbelangt, das Adjektiv „exzessiv“ etwas, das über das gewöhnliche oder vernünftige Maß hinausgeht oder das erwünschte oder zulässige Maß überschreitet (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 43 – Österreichische Datenschutzbehörde (Exzessive Anfragen)). Allein anhand der Verwendung dieses Adjektivs, das sich sowohl auf qualitative als auch auf quantitative Merkmale bezieht, kann daher nicht ausgeschlossen werden, dass ein erster Auskunftsantrag exzessiv sein mag.

26 Zudem ergibt sich zwar aus Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO, dass Anträge „insb. im Fall von häufiger Wiederholung“ exzessiv sein können. Die Häufung von Anträgen einer Person kann daher ein Indiz dafür sein, dass sie exzessiv sind (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 57 – Österreichische Datenschutzbehörde (Exzessive Anfragen)). Wie der GA in Rn. 28 seiner SA im Wesentlichen betont hat, verlangt jedoch, da die häufige Wiederholung in dieser Bestimmung nur beispielhaft angeführt wird, die Einstufung eines Auskunftsantrags als „exzessiv“ nicht, dass der betreffende Antrag notwendigerweise im Zusammenhang mit der Einreichung mehrerer Anträge durch dieselbe betroffene Person stehen muss.

27 In Ansehung einer am Wortlaut orientierten Auslegung von Art. 12 Abs. 5 DS-GVO kann daher nicht ausgeschlossen werden, dass ein erster Auskunftsantrag als „exzessiv“ im Sinne dieser Bestimmung angesehen werden kann.

28 Bestätigung findet diese Feststellung im Regelungszusammenhang von Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO. Insoweit ist darauf hinzuweisen, dass dieser Art. 12 DS-GVO, der sich in Kapitel III DS-GVO über die Rechte der betroffenen Person findet, allgemeine Pflichten des Verantwortlichen in Bezug auf die

Transparenz von Information und Kommunikation aufstellt und die Modalitäten für die Ausübung der Rechte der betroffenen Person festlegt. Nach Art. 12 Abs. 2 S. 1 DS-GVO muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gem. u.a. Art. 15 DS-GVO erleichtern, der den durch die DS-GVO geschaffenen Transparenzrahmen vervollständigt, indem er dieser Person ein Recht auf Auskunft über ihre personenbezogenen Daten gewährt (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 45 und 46 – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

29 Indem Art. 12 Abs. 5 DS-GVO gleichzeitig den Verantwortlichen die Möglichkeit einräumt, bei offenkundig unbegründeten oder exzessiven Anträgen ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten zu verlangen oder sich zu weigern, aufgrund eines Antrags tätig zu werden, sieht er mithin eine Ausnahme von der Pflicht zur Erleichterung u.a. des Auskunftsrechts vor, die eng auszulegen ist (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 33 – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

30 Aus der Rspr. des Gerichtshofs zur Auslegung des Begriffs „exzessive Anfragen“ in Art. 57 Abs. 4 DS-GVO, die auf die vorliegende Rechtssache übertragbar ist, da Art. 57 Abs. 4 DS-GVO einen im Wesentlichen Art. 12 Abs. 5 DS-GVO entsprechenden Wortlaut hat und das gleiche Ziel wie dieser verfolgt, ergibt sich allerdings, dass in Art. 12 Abs. 5 DS-GVO ein allgemeiner Grundsatz des Unionsrechts zum Ausdruck kommt, wonach sich Einzelne nicht in betrügerischer oder missbräuchlicher Weise auf unionsrechtliche Normen berufen dürfen (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 49 – Österreichische Datenschutzbehörde (Exzessive Anfragen)). Die Anwendung der Unionsregelung kann nämlich nicht so weit gehen, dass Vorgänge geschützt werden, die einem missbräuchlichen Zweck dienen (vgl. idS EuGH Urt. v. 19.9.2024 – C-236/23 Rn. 52 und die dort angeführte Rspr. – Matmut).

31 Somit ist die Zahl der Auskunftsanträge der betroffenen Person an den Verantwortlichen für sich allein nicht ausschlaggebend für dessen Recht, von der ihm durch Art. 12 Abs. 5 DS-GVO eingeräumten Möglichkeit Gebrauch zu machen, auf den Antrag nicht tätig zu werden, sodass der Verantwortliche davon auch im Fall eines ersten Auskunftsantrags Gebrauch machen kann, wenn er in Ansehung aller relevanten Umstände des Einzelfalls dartut, dass eine Missbrauchsabsicht der betroffenen Person vorliegt (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 50 – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

32 Diese systematische Auslegung steht im Einklang mit den Zielen, die mit der DS-GVO verfolgt werden. Insoweit ist festzustellen, dass diese Verordnung, wie sich aus ihren Erwägungsgründen 10 und 11 ergibt, ein gleichmäßiges und hohes Schutzniveau für natürliche Personen in der Union gewährleisten und die Rechte der betroffenen Personen stärken und präzise festlegen soll. So sind die Pflichten des Verantwortlichen nach Art. 12 DS-GVO, die u.a. die Mitteilung gem. Art. 15 DS-GVO betreffen, als ein Mechanismus konzipiert, der geeignet ist, die Rechte und Interessen der betroffenen Personen wirksam zu wahren (vgl. idS EuGH Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 38 und 39 sowie die dort angeführte Rspr. – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

33 Im vierten Erwägungsgrund der DS-GVO wird jedoch ausgeführt, dass das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist, da es im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Ver-

hältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden muss. Zudem hat der Gerichtshof bereits hervorgehoben, dass die Mechanismen, die es ermöglichen, einen angemessenen Ausgleich zwischen den verschiedenen berührten Rechten und Interessen zu finden, in der DS-GVO selbst festgelegt sind (Urt. v. 21.12.2023 – C-667/21 [= ZD 2024, 146] Rn. 54 und die dort angeführte Rspr. – Krankenversicherung Nordrhein).

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

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

36 Was zweitens die Umstände betrifft, unter denen der erste Auskunftsantrag der betroffenen Person als „exzessiv“ iSv Art. 12 Abs. 5 DS-GVO eingestuft werden und somit einen Rechtsmissbrauch iSd oben in den Rn. 23 und 30 angeführten Rspr. begründen kann, so ist für den Nachweis einer missbräuchlichen Verhaltensweise zweierlei erforderlich, nämlich zum einen eine Gesamtheit objektiver Umstände, aus denen sich ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wurde, und zum anderen ein subjektives Element, das in der Absicht der betroffenen Person besteht, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden. Bei einer solchen Einstufung müssen außerdem alle Tatsachen und Umstände des Einzelfalls berücksichtigt werden (vgl. idS Urt. v. 21.12.2023 – C-38/21, C-47/21 und C-232/21 [= MMR 2024, 400] Rn. 285 und 286 sowie die dort angeführte Rspr. – BMW Bank u.a.).

37 Was als Erstes das objektive Element einer missbräuchlichen Verhaltensweise anbelangt, ist darauf hinzuweisen, dass eine betroffene Person mit Art. 15 DS-GVO vor dem Hintergrund des 63. Erwägungsgrunds der DS-GVO ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzt und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können soll, um sich insb. der Verarbeitung dieser Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können, damit sie ggf. ihre Rechte auf Berichtigung, auf Löschung und auf Einschränkung der Verarbeitung sowie ihr Widerspruchsrecht und im Schadensfall ihr Recht auf einen Rechtsbehelf ausüben kann (vgl. idS Urt. v. 12.1.2023 – C-154/21 [= ZD 2023, 271] Rn. 37 und 38 – Österreichische Post (Informationen über die Empfänger personenbezogener Daten)).

38 Im vorliegenden Fall stellte TC ... den im Ausgangsverfahren streitigen Auskunftsantrag, nachdem er sich zum Newsletter

von Brillen Rottler angemeldet und dem Unternehmen dabei bestimmte personenbezogene Daten übermittelt hatte, sodass dieser Auskunftsantrag in formaler Hinsicht eine Ausübung des Auskunftsrechts von TC im Hinblick auf die Erreichung des Ziels der Regelung darstellen könnte.

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

40 Was insoweit als Zweites das subjektive Element einer missbräuchlichen Vorgehensweise betrifft, so muss der Verantwortliche, um einen Auskunftsantrag als „exzessiv“ iSv Art. 12 Abs. 5 DS-GVO einstufen zu können, anhand aller relevanten Umstände des Einzelfalls nachweisen, dass eine Missbrauchsabsicht seitens der betroffenen Person vorliegt, wobei eine solche Absicht festgestellt werden kann, wenn diese Person den Antrag zu einem anderen Zweck stellt als dem, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, um anschließend ihre Rechte aus der DS-GVO schützen zu können (vgl. idS Urt. v. 9.1.2025 – C-416/23 [= ZD 2025, 272 mAnm Wirthensohn] Rn. 50 und 56 – Österreichische Datenschutzbehörde (Exzessive Anfragen)).

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

42 Insoweit werden sämtliche Fallumstände zu berücksichtigen sein, insb. der Umstand, dass die betroffene Person personenbezogene Daten freiwillig bereitgestellt hat, der Zweck der Bereitstellung dieser Daten, die zwischen der Datenbereitstellung und dem Auskunftsantrag verstrichene Zeit sowie das Verhalten dieser Person.

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

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

45 Nach alledem ist auf die Fragen 1 bis 3 und 7 zu antworten, dass Art. 12 Abs. 5 DS-GVO dahin auszulegen ist, dass ein erster von der betroffenen Person an den Verantwortlichen gerichteter Antrag nach Art. 15 DS-GVO auf Auskunft über personenbezogene Daten als „exzessiv“ im Sinne dieses Art. 12 Abs. 5 DS-GVO angesehen werden kann, wenn der Verantwortliche in Ansehung aller relevanten Fallumstände nachweist, dass dieser Antrag trotz formaler Einhaltung der in diesen Bestimmungen vorgesehenen Bedingungen von der betroffenen Person nicht gestellt wurde, um sich der Verarbeitung dieser Daten bewusst

zu werden und deren Rechtmäßigkeit zu überprüfen, damit sie anschließend ihre Rechte aus der DS-GVO schützen kann, sondern in missbräuchlicher Absicht wie zur künstlichen Schaffung der Voraussetzungen für die Erlangung eines sich aus der DS-GVO ergebenden Vorteils. Dass die betroffene Person nach öffentlich zugänglichen Informationen etwa mehrere Anträge auf Auskunft über ihre personenbezogenen Daten, gefolgt von Schadensersatzforderungen ggü. verschiedenen Verantwortlichen, gestellt hat, kann für die Feststellung einer solchen missbräuchlichen Absicht berücksichtigt werden.

Zur fünften und zur sechsten Frage

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

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

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

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

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

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

sich aus einer Verarbeitung als solcher ergeben, hätte dies daher den Ausschluss solcher Fälle vom Anwendungsbereich dieser Bestimmung zur Folge, deren praktische Wirksamkeit damit beeinträchtigt würde.

52 IÜ hat der Gerichtshof bereits entschieden, dass der Verstoß des Verantwortlichen gegen die Art. 26 und 30 DS-GVO, von denen der erste den Abschluss einer Vereinbarung über die jeweiligen Funktionen und Beziehungen der Verantwortlichen ggü. betroffenen Personen und der zweite die Führung eines Verzeichnisses der Verarbeitungstätigkeiten betrifft, keine „unrechtmäßige Verarbeitung“ darstellt, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht. Ein solcher Verstoß ist daher unter Rückgriff auf andere von der DS-GVO vorgesehene Maßnahmen zu heilen, u.a. durch Ersatz des vom Verantwortlichen etwaig verursachten Schadens gem. Art. 82 DS-GVO (vgl. idS Urt. v. 4.5.2023 – C-60/22 [= ZD 2023, 606 mAnm Stief] Rn. 66 und 67 – Bundesrepublik Deutschland (Elektronisches Gerichtsfach)).

53 Zweitens findet die oben in Rn. 48 getroffene Feststellung Bestätigung in der teleologischen Auslegung von Art. 82 Abs. 1 DS-GVO, denn dieser Artikel soll die Verwirklichung der Ziele der DS-GVO gewährleisten, zu denen u.a. das in deren elftem Erwägungsgrund genannte Ziel gehört, die Rechte der betroffenen Personen zu stärken und die Verpflichtungen für diejenigen zu verschärfen, die personenbezogene Daten verarbeiten und darüber entscheiden. Wie der GA in Rn. 72 seiner SA im Wesentlichen ausgeführt hat, würden aber diese Rechte, zu denen das Auskunftsrecht, um das es dem vorlegenden Gericht geht, gerade gehört, erheblich geschwächt, wenn Art. 82 Abs. 1 DS-GVO dahin ausgelegt werden sollte, dass er allein Schäden erfasst, die sich aus rechtswidrigen Handlungen ergeben, die eine Datenverarbeitung umfassen.

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

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

Zur achten Frage

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

58 Da die DS-GVO für den Sinn und die Tragweite der in ihrem Art. 82 Abs. 1 DS-GVO enthaltenen Begriffe, insb., was die Begriffe „materieller oder immaterieller Schaden“ und „Schadensersatz“ betrifft, nicht auf das Recht der Mitgliedstaaten verweist, sind diese Begriffe für die Zwecke der Anwendung der DS-GVO als autonome Begriffe des Unionsrechts anzusehen, die in allen Mitgliedstaaten einheitlich auszulegen sind (vgl. idS EuGH Urt. v. 4.5.2023 – C-300/21 [= ZD 2023, 446 mAnm Mekat/Ligocki] Rn. 30 – Österreichische Post (Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten), und v. 4.9.2025 – C-655/23 [= MMR 2025, 950 mAnm Mekat/Ligocki = ZD 2025, 640 mAnm Mekat/Wellmann] Rn. 55 und die dort angeführte Rspr. – Quirin Privatbank).

59 Insoweit ist darauf hinzuweisen, dass nicht davon ausgegangen werden kann, dass jeder „Verstoß“ gegen die Bestim-

mungen der DS-GVO für sich genommen einen Schadensersatzanspruch der betroffenen Person begründet. Nach Art. 82 Abs. 1 DS-GVO hat nämlich „(j)ede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, ... Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“. Daraus geht klar hervor, dass das Vorliegen eines „Schadens“, der „entstanden“ ist, eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadensersatzanspruch darstellt, ebenso wie das Vorliegen eines Verstoßes gegen die DS-GVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. idS Urt. v. 4.5.2023 – C-300/21 [= ZD 2023, 446 mAnm Mekat/Ligocki] Rn. 31 bis 33 – Österreichische Post (Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten), und v. 4.9.2025 – C-655/23 [= MMR 2025, 950 mAnm Mekat/Ligocki = ZD 2025, 640 mAnm Mekat/Wellmann] Rn. 56 und die dort angeführte Rspr. – Quirin Privatbank).

60 Somit muss die Person, die auf der Grundlage von Art. 82 Abs. 1 DS-GVO Ersatz eines immateriellen Schadens fordert, nicht nur den Verstoß gegen Bestimmungen der DS-GVO nachweisen, sondern auch, dass ihr durch diesen Verstoß ein solcher Schaden entstanden ist. Ein entsprechender Schaden kann daher nicht allein deshalb vermutet werden, weil sich der Verstoß ereignet hat (Urt. v. 4.10.2024 – C-200/23 [= ZD 2025, 87] Rn. 141 und die dort angeführte Rspr. – Agentsia po vpisvaniyata).

61 Davon abgesehen hat der Gerichtshof bereits entschieden, dass aus der im ersten Satz des 85. Erwägungsgrund DS-GVO enthaltenen beispielhaften Aufzählung der „Schäden“, die den betroffenen Personen entstehen können, hervorgeht, dass der Unionsgesetzgeber unter den Schadensbegriff insb. auch den bloßen „Verlust der Kontrolle“ über ihre eigenen personenbezogenen Daten infolge eines Verstoßes gegen die DS-GVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten erfolgt sein sollte (Urt. v. 4.10.2024 – C-200/23 [= ZD 2025, 87] Rn. 145 und die dort angeführte Rspr. – Agentsia po vpisvaniyata).

62 Der Gerichtshof hat auch befunden, dass der Begriff „immaterieller Schaden“ nicht allein auf Schäden mit einer gewissen Erheblichkeit beschränkt werden kann. Insb. darf eine nationale Regelung oder Praxis für einen durch einen Verstoß gegen die DS-GVO verursachten immateriellen Schaden keine „Bagatellegrenze“ festlegen. Die betroffene Person muss jedoch nachweisen, dass ihr zum einen tatsächlich ein solcher Schaden – so geringfügig er auch sein mag – entstanden ist und dass zum anderen in den Folgen dieses Verstoßes, die sie erlitten zu haben behauptet, ein Schaden begründet liegt, der sich von der bloßen Verletzung der Bestimmungen der DS-GVO unterscheidet (vgl. idS Urt. v. 14.12.2023 – C-456/22 [= ZD 2024, 208] Rn. 22 und 23 – Gemeinde Ummendorf).

63 So kann das bloße Vorbringen seitens der betroffenen Person einer durch einen Verlust der Kontrolle über ihre personenbezogenen Daten hervorgerufenen Befürchtung nicht zu Schadensersatz nach Art. 82 Abs. 1 DS-GVO führen (vgl. idS Urt. v. 20.6.2024 – C-590/22 [= ZD 2024, 519 mAnm Pauly/Kienle] Rn. 33 und 35 – PS (Fehlerhafte Anschrift)). Beruft sich eine Person, die auf der Grundlage dieser Bestimmung Schadensersatz fordert, auf die Befürchtung, dass ihre personenbezogenen Daten etwa in Zukunft aufgrund eines Verstoßes gegen die DS-GVO missbräuchlich verwendet werden, muss daher das angerufene nationale Gericht prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. idS Urt. v.

4.10.2024 – C-200/23 [= ZD 2025, 87] Rn. 143 und die dort angeführte Rspr. – Agentsia po vpisvanyata).

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

65 Um dem vorlegenden Gericht eine zweckdienliche Antwort zu geben, ist noch darauf hinzuweisen, dass der Kausalzusammenhang zwischen dem behaupteten Verstoß und dem behaupteten Schaden durch die Handlungsweise der betroffenen Person unterbrochen werden kann, sofern sich diese Handlungsweise als die entscheidende Ursache für den Schaden erweist. Eine entsprechende Handlung kann u.a. in einer Entscheidung der geschädigten Person bestehen, allerdings nur, sofern diese Entscheidung für sie nicht zwingend war (vgl. entsprechend Urt. v. 18.12.2025 – C-679/23 P Rn. 151 und 152 sowie die dort angeführte Rspr. – WS u.a./Frontex (Gemeinsame Rückkehraktion)).

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

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

Anmerkung

**RA Christian Sosna / RA Lennart Meyer,
Freshfields PartG mbB, Düsseldorf**

In der Praxis wird zunehmend versucht, das Auskunftsrecht für sachfremde Zwecke zu instrumentalisieren, sei es zur künstlichen Herbeiführung von Schadensersatzansprüchen, zur Schikane des Verantwortlichen oder als prozesstaktisches Mittel zum Auskundschaften der Strategie der Gegenseite. Ein besonders augenfälliges Missbrauchsphänomen (umgangssprachlich als „GDPR-Hopping“ bezeichnet) besteht darin, dass Personen ihre personenbezogenen Daten gezielt zum Gegenstand einer Verarbeitung machen (zB sich für einen Newsletter anmelden), um umgehend Auskunft nach Art. 15 DS-GVO zu verlangen und sodann immateriellen Schadensersatz nach Art. 82 Abs. 1 DS-GVO geltend zu machen, wenn der Verantwortliche die Auskunft nicht oder unvollständig erteilt.

Der EuGH hat nun für den letztgenannten Fall klargestellt, dass bereits ein erster Auskunftsantrag als „exzessiv“ iSv Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO abgelehnt werden kann, wenn der Verantwortliche eine missbräuchliche Absicht des Auskunftersuchenden nachweist (Rn. 35, 45). Zugleich hat der Gerichtshof entschieden, dass Art. 82 Abs. 1 DS-GVO einen

Schadensersatzanspruch auch für Verletzungen des Auskunftsrechts gewährt, ohne dass das schadensbegründende Ereignis selbst in einer Datenverarbeitung bestehen muss (Rn. 48, 55). Schließlich hat er präzisiert, dass der Kausalzusammenhang zwischen DS-GVO-Verstoß und Schaden durch das Verhalten der betroffenen Person unterbrochen werden kann, wenn dieses Verhalten die entscheidende Schadensursache darstellt (Rn. 65–67).

Die Entscheidung stärkt die Verteidigungsmöglichkeiten der Verantwortlichen gegen missbräuchliche Auskunftersuchen und damit zusammenhängende Schadensersatzforderungen betroffener Personen, ohne das Auskunftsrecht als solches zu beschneiden.

1. Exzessivität eines Erstantrags nach Art. 12 Abs. 5 DS-GVO

a) Bestätigung des qualitativen Exzessbegriffs

Der EuGH bestätigt, dass der in Art. 12 Abs. 5 UAbs. 1 S. 2 DS-GVO genannte Fall von „häufiger Wiederholung“ nur ein Beispiel für exzessive Anträge darstellt und damit auch qualitative Exzesse erfasst sind (Rn. 26). Art. 12 Abs. 5 DS-GVO drücke den allgemeinen unionsrechtlichen Grundsatz aus, dass sich Einzelne nicht in betrügerischer oder missbräuchlicher Weise auf unionsrechtliche Normen berufen dürfen (Rn. 30). Entscheidend sei somit nicht allein die Zahl der Auskunftsanträge, sondern ob eine Missbrauchsabsicht der betroffenen Person vorliegt (Rn. 31). Das Urteil bestätigt die Auffassung zahlreicher OLG, die das Merkmal der Exzessivität bereits in der Vergangenheit nicht auf Fälle wiederholter Antragstellung beschränkt, sondern auch auf andere Ausprägungen des Rechtsmissbrauchs erstreckt haben (vgl. OLG Brandenburg ZD 2023, 617 Rn. 15; OLG Hamm ZD 2022, 237 Rn. 9; OLG Nürnberg ZD 2022, 463 Rn. 27).

b) Nachweis einer rechtsmissbräuchlichen Verhaltensweise

Ob ein Auskunftersuchen rechtsmissbräuchlich ist, bestimmt der EuGH anhand eines zweigliedrigen Tests (Rn. 36). Erforderlich sei zum einen ein objektives Missbrauchselement. Trotz formaler Einhaltung der Antragsvoraussetzungen müsse das Ziel des Art. 15 DS-GVO – sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen – verfehlt werden. Zum anderen bedürfe es eines subjektiven Missbrauchselements. Die betroffene Person müsse in der Absicht handeln, sich durch die künstliche Schaffung der Anwendungsvoraussetzungen des Art. 15 DS-GVO einen aus der DS-GVO resultierenden Vorteil zu verschaffen (Rn. 36, 40). Der EuGH betont, dass die Beweislast beim Verantwortlichen liegt (Art. 12 Abs. 5 UAbs. 2 DS-GVO; Rn. 35).

Das Vorliegen des subjektiven Missbrauchselements bestimmt sich anhand aller relevanten Umstände des Einzelfalls (Rn. 40). Als Indizien für eine missbräuchliche Absicht benennt der EuGH die freiwillige Bereitstellung personenbezogener Daten durch die betroffene Person, den Zweck der Datenbereitstellung, die zwischen Datenbereitstellung und Auskunftsantrag verstrichene Zeit sowie das Verhalten der betroffenen Person insgesamt (Rn. 42). Öffentlich zugängliche Informationen über ein systematisches Vorgehen der betroffenen Person gegen verschiedene Verantwortliche können ebenfalls berücksichtigt werden, sofern sie durch zusätzliche relevante Anhaltspunkte bestätigt werden (Rn. 43).

Dass der EuGH hinsichtlich des subjektiven Missbrauchselements auf die Absicht abstellt, einen Vorteil zu erlangen, dürfte dabei dem konkreten, dem EuGH vorgelegten Sachverhalt geschuldet sein. Das subjektive Missbrauchselement dürfte

auch dann zu bejahen sein, wenn die betroffene Person in schlichter Schädigungsabsicht handelt (zB, wenn es ihr nur darauf ankommt, mit dem Auskunftersuchen schikanös Aufwand für den Verantwortlichen zu verursachen). Dafür spricht bereits die einleitende Formel des EuGH, wonach eine Missbrauchsabsicht vorliege, wenn die betroffene Person das Auskunftersuchen zu einem anderen Zweck stellt als dem, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, um anschließend ihre Rechte aus der DS-GVO wahren zu können (Rn. 40).

Diese Formel ist geeignet, neben der Provokation von Schadensersatzansprüchen auch weitere Konstellationen zu erfassen. So kann der Verdacht des Rechtsmissbrauchs ggf. erhärtet werden, wenn ein laufendes Gerichtsverfahren überhaupt keinen Bezug zu einer relevanten Datenverarbeitung durch den beklagten Verantwortlichen hat und kein anderes, irgendwie objektiv fundiertes Interesse an der Auskunft erkennbar ist. Letzteres kann zB der Fall sein, wenn die betroffene Person bereits Kenntnis von den zu beauskunftenden Informationen hat oder sich diese ohne Weiteres selbst beschaffen kann. Auf einen Rechtsmissbrauch deutet es auch hin, wenn die betroffene Person außergerichtlich ein Auskunftersuchen gestellt hat und ihr Vertreter vor Gericht erneut eine Auskunft verlangt, ohne dass sich die Informationsbasis oder die Verarbeitungstätigkeit verändert hat; hier dürfte auch die Vorgabe des EuGH greifen, das Auskunftsrecht „in angemessenen Abständen“ wahrzunehmen (Rn. 37). Anlass zur Annahme eines missbräuchlichen Auskunftersuchens kann überdies bei der Geltendmachung einer Vielzahl individueller Auskunftersuchen durch ein und dieselbe Rechtsanwaltskanzlei oder Legal-Tech-Plattform bestehen. Es ist zu vermeiden, dass der Auskunftsanspruch im Gerichtsverfahren als eine Art „Serviceleistung zu Lasten des Beklagten“ für eine Vielzahl von betroffenen Personen pauschal geltend gemacht wird, um so das Zusammenstellen der anspruchsbegründenden Unterlagen auf den beklagten Verantwortlichen zu verlagern.

2. Weitere Verteidigungsmöglichkeiten

Neben dem Rechtsmissbrauchseinwand kommen weitere Verteidigungsmöglichkeiten gegen Auskunftersuchen in Betracht. Dazu zählt der Einwand des offenkundig unbegründeten Auskunftersuchens iSv Art. 12 Abs. 5 UAbs. 1 S. 2 Var. 1 DS-GVO, der Unverhältnismäßigkeitseinwand auf Grundlage des vom EuGH in Rn. 33 des Urteils nochmals bestätigten Gebots zur Abwägung des Datenschutzrechts mit anderen Grundrechten unter Wahrung des Verhältnismäßigkeitsprinzips (Erwägungsgrund 4 S. 2 DS-GVO; vgl. EuGH ZD 2023, 271 Rn. 47) sowie der Schutz der Rechte und Freiheiten des Verantwortlichen nach Art. 15 Abs. 4 DS-GVO, namentlich seiner Prozessstrategie (dazu eingehend Ligocki/Sosna/Meyer ZD 2025, 137 (138 f.)).

3. Schadensersatz und Unterbrechung des Kausalzusammenhangs

a) Art. 82 Abs. 1 DS-GVO erfasst auch Verstöße gegen Art. 15 DS-GVO

Der EuGH hat entschieden, dass Art. 82 Abs. 1 DS-GVO der betroffenen Person in bestimmten Fällen auch bei Verletzung des Auskunftsrechts einen Schadensersatzanspruch verleihen kann, ohne dass das schädigende Ereignis in einer (rechtswidrigen) Datenverarbeitung bestehen muss (Rn. 48, 55). Er stützt dies auf den Wortlaut des Art. 82 Abs. 1 DS-GVO, der auf einen Verstoß gegen „diese Verordnung“ abstellt, ohne auf eine Verarbeitung Bezug zu nehmen (Rn. 48). In systematischer Hinsicht verweist der EuGH darauf, dass sich Verstöße gegen die in Kapitel III DS-GVO vorgesehenen Rechte gerade

aus der Weigerung ergeben können, auf den Antrag der betroffenen Person tätig zu werden, und dass der Ausschluss solcher Fälle vom Schadensersatzanspruch aus Art. 82 DS-GVO die praktische Wirksamkeit der Betroffenenrechte beeinträchtigen würde (Rn. 51).

b) Unterbrechung des Kausalzusammenhangs

Von besonderer praktischer Bedeutung sind die Ausführungen des EuGH zu den Voraussetzungen eines ersatzfähigen immateriellen Schadens in Form eines Kontrollverlusts. Der Gerichtshof bekräftigt zunächst seine stRspr: Ein Verstoß allein begründet keinen Schadensersatzanspruch; die betroffene Person muss nachweisen, dass ihr tatsächlich ein Schaden entstanden ist, der sich von der bloßen Verletzung der DS-GVO-Bestimmungen unterscheidet (Rn. 62). Das bloße Vorbringen einer durch einen Kontrollverlust hervorgerufenen Befürchtung reicht nicht aus; eine solche Befürchtung muss unter den gegebenen Umständen als begründet nachgewiesen werden (Rn. 63).

Neben diesem Schadenserfordernis konkretisiert der EuGH nun als eigenständige weitere Voraussetzung den Kausalzusammenhang zwischen Verstoß und Schaden. Der Gerichtshof stellt klar, dass dieser Kausalzusammenhang durch die Handlungsweise der betroffenen Person unterbrochen werden kann, sofern sich diese Handlungsweise als die „entscheidende Ursache“ für den geltend gemachten Schaden erweist (Rn. 65). Im Kontext missbräuchlicher Auskunftersuchen bedeutet das: Wer dem Verantwortlichen personenbezogene Daten in der Absicht übermittelt, künstlich die Voraussetzungen für einen Schadensersatzanspruch zu schaffen, scheitert bereits an diesem Kausalitätserfordernis – denn etwaige (nachzuweisende) Befürchtungen infolge des behaupteten Kontrollverlusts oder der Ungewissheit über die Verarbeitung sind dann nicht auf den Verstoß des Verantwortlichen, sondern auf das eigene Verhalten der betroffenen Person zurückzuführen (Rn. 66, 67).

Im Ergebnis formuliert der EuGH damit zwei kumulative Hürden für einen Schadensersatzanspruch wegen verweigerter Auskunft: Der Schaden muss tatsächlich eingetreten und nachgewiesen sein, und er darf nicht maßgeblich durch das eigene Verhalten der betroffenen Person verursacht worden sein.

EuGH: Verbraucherrechtliches Widerrufsrecht bei Unterstützung durch einen Architekten

Fernabsatzvertrag

RL 2011/83/EU Art. 2 Nr. 7, 6 Abs. 1 lit. h, 9 Abs. 1, 10 Abs. 1, 11 Abs. 1, 14 Abs. 4 lit. a, Abs. 5, 15; BGB § 312c Abs. 1 Urteil vom 5.3.2026 – C-564/24 – Eisenberger Gerüstbau GmbH

Leitsätze der Redaktion

1. Art. 2 Nr. 7 RL 2011/83/EU ist dahin auszulegen, dass es für die Einstufung eines Vertrags zwischen einem Verbraucher und einem Unternehmer als „Fernabsatzvertrag“ im Sinne dieser Bestimmung ohne Bedeutung ist, ob der Verbraucher vor und bei Abschluss dieses Vertrags von einem anderen Unternehmer seiner Wahl unterstützt wird, der den Kontakt zwischen dem Verbraucher und dem erstgenannten Unternehmer angebahnt und auf wesentliche Teile des Inhalts des Vertrags Einfluss genommen hat.

2. Art. 2 Nr. 7 RL 2011/83/EU ist dahin auszulegen, dass eine von den Parteien eines Vertrags, der nicht als „Fernabsatzvertrag“ im Sinne dieser Bestimmung eingestuft werden kann, unter ausschließlicher Verwendung von Fernkommunikationsmitteln getroffene Nachtragsvereinbarung über zusätzliche Leistungen, die gegenüber den in dem Vertrag vorgesehenen Leistungen von untergeordneter Bedeutung sind, einen „Fernabsatzvertrag“ im Sinne dieser Bestimmung darstellt, sofern die in dieser Bestimmung vorgesehenen Voraussetzungen erfüllt sind.

3. Die RL 2011/83/EU ist dahin auszulegen, dass in dem Fall, dass ein Verbraucher am Ende der gem. Art. 10 Abs. 1 RL 2011/83/EU verlängerten Widerrufsfrist einen Fernabsatzvertrag zu einem Zeitpunkt widerrufen hat, zu dem die Leistungen, die Gegenstand dieses Vertrags sind und nicht zurückerstattet werden können, bereits erbracht worden waren, der Unternehmer mit Erfolg geltend machen kann, dass der Verbraucher aufgrund seines eigenen Verhaltens das Widerrufsrecht missbräuchlich ausgeübt habe, wenn sich aus der Gesamtheit der Umstände ergibt, dass zum einen die Ausübung des Widerrufsrechts durch den Verbraucher nicht den mit der Richtlinie verfolgten Zielen in Bezug auf die Information des Verbrauchers und die Sicherheit bei Geschäften mit einem Unternehmer entspricht und zum anderen der Verbraucher mit seinem Verhalten darauf abzielt, sich auf Kosten des Unternehmers missbräuchlich einen Vorteil zu verschaffen.

Anm. d. Red.: Der Volltext ist abrufbar unter: [BeckRS 2026, 2859](#). Vgl. ferner EuGH MMR 2019, 364 – slewo; EuGH MMR 2024, 400 – BMW Bank u.a.; EuGH MMR 2026, 500 mAnm Sosna/Meyer – Brillen Rottler/TC – in diesem Heft und EuGH MMR 2019, 299 – Walbusch Walter Busch.

Schlagworte: Fernabsatzvertrag; Verbraucherbegriff; Unterstützung durch einen Architekten; ausschließliche Verwendung von Fernkommunikationsmitteln; akzessorischer Vertrag; Rechtsmissbrauch

Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 2 Nr. 7, 9 Abs. 1 und 14 Abs. 4 lit. a und Abs. 5 RL 2011/83/EU. Es ergeht iRe Rechtsstreits zwischen der Eisenberger Gerüstbau GmbH, einer Gesellschaft deutschen Rechts, und JK über die Zahlung einer Vergütung für die Überlassung und den Aufbau von Gerüsten durch diese Gesellschaft. Eisenberger Gerüstbau vermietet gewerblich Baugerüste, die sie für ihre Kunden auf- und wieder abbaut. JK, die als Bundesbeamtin in Deutschland tätig ist, ist Eigentümerin eines Grundstücks in Berlin, das mit einem mehrgeschossigen Mehrfamilienhaus bebaut ist. Im Jahr 2020 beschloss JK, das Dachgeschoss ihres Hauses für eigene Wohnzwecke um zwei neu zu errichtende Etagen mit insgesamt vier Wohneinheiten aufzustocken. Sie beauftragte hierfür einen Architekten mit der Bauplanung und -überwachung, der auch Leistungsverzeichnisse für die erforderlichen Gewerke erstellen, Angebote bei Fachunternehmen einholen und anschließend bei den Vertragsschlüssen durch die Erstellung von Vertragsentwürfen mitwirken sollte. In dieser Funktion übersandte dieser Architekt Eisenberger Gerüstbau u.a. ein Leistungsverzeichnis über Gerüststellarbeiten mit der Aufforderung, auf dieser Grundlage ein Angebot abzugeben. Eisenberger Gerüstbau versah das erhaltene Leistungsverzeichnis mit Einheitspreisen sowie einem voraussichtlichen Gesamtpreis iHv 45.663,18 EUR brutto, unterschrieb es am 24.4.2020 und sandte es an den Architekten zurück. Der Architekt wählte Eisenberger Gerüstbau als Fachunternehmen für die Ausführung der Gerüststellarbeiten aus. Er entwarf einen entsprechenden Vertrag, der auf das Angebot v. 24.4.2020 Bezug nahm, und übersandte beiden Parteien, dh Eisenberger Gerüstbau und JK, diesen Entwurf am 14.12.2020 per E-Mail. Eine Belehrung darüber, dass JK zum

Widerruf des Vertrags berechtigt sei, enthielt der Entwurf nicht. Eisenberger Gerüstbau unterschrieb den unveränderten Vertragsentwurf am 14.12.2020 und übersandte diesen JK. Diese unterschrieb ihn am 15.12.2020 und schickte das von beiden Parteien unterschriebene Exemplar (im Folgenden: in Rede stehender Vertrag) postalisch zurück an Eisenberger Gerüstbau.

Am 21.1.2021 unterbreitete Eisenberger Gerüstbau JK per E-Mail ein Nachtragsangebot über zwei zusätzliche Absetzbühnen für insgesamt 7.730 EUR brutto für deren Aufbau, Demontage und Vorhaltung für vier Wochen sowie ab der fünften Woche einen zusätzlichen Mietzins iHv insgesamt 517,65 EUR brutto wöchentlich. JK unterschrieb dieses Nachtragsangebot und sandte es am 22.1.2021 per E-Mail zurück an Eisenberger Gerüstbau. Im Januar 2021 begann Eisenberger Gerüstbau mit dem Aufbau des Gerüsts. Ab dem 26.1.2021 überließ Eisenberger Gerüstbau JK das Gerüst zum Gebrauch für die beabsichtigten Bautätigkeiten an dem in Rede stehenden Gebäude. Bis Ende Mai 2021 zahlte JK auf Abschlagsrechnungen der Kl. einen Gesamtbetrag iHv 95.937,84 EUR. Mit Schreiben v. 7.12.2021 erklärte JK ggü. Eisenberger Gerüstbau den Widerruf ihrer auf den Abschluss des in Rede stehenden Vertrags sowie der Nachtragsvereinbarung gerichteten Willenserklärungen, zudem verweigerte sie weitere Zahlungen und forderte ihre Abschlagszahlungen iHv 95.937,84 EUR zurück. Im Dezember 2021 wurden sämtliche von JK beabsichtigten Bauarbeiten, für die das Gerüst benötigt wurde, abgeschlossen. Auf Verlangen von JK wurde das Gerüst schließlich am 20.12.2021 abgebaut.

Eisenberger Gerüstbau verklagte JK vor dem LG Berlin auf Zahlung der ihrer Ansicht nach zum Zeitpunkt der Klageerhebung noch offenen Vergütung, dh eines Betrags iHv 101.000,25 EUR aus dem Vertrag über die Gerüststellung. Im Rahmen dieses Verfahrens erhob JK Widerklage auf Rückerstattung der geleisteten Abschlagszahlungen iHv 95.937,84 EUR. Mit Ur. v. 19.5.2023 wies das LG Berlin die Klage ab und gab der Widerklage in vollem Umfang statt. Eisenberger Gerüstbau legte gegen dieses Urteil Berufung beim KG, dem vorlegenden Gericht, ein. Das vorlegende Gericht ist der Ansicht, dass der unter Einschaltung des Architekten als Verhandlungsgehilfen geschlossene Vertrag nicht in den Anwendungsbereich von § 312c Abs. 1 BGB falle, mit dem Art. 2 Nr. 7 RL 2011/83/EU in deutsches Recht umgesetzt werde. Zwar hätten Eisenberger Gerüstbau auf der einen Seite sowie JK und der Architekt auf der anderen Seite bis zum Abschluss dieses Vertrags ausschließlich über Fernkommunikationsmittel, nämlich postalisch oder per E-Mail, kommuniziert. Allerdings habe sich JK zur Vertragsanbahnung eines Architekten und damit eines Unternehmers bedient, was die Anwendbarkeit des Schutzes nach § 312c BGB ausschließe. Unter diesen Umständen hat das KG beschlossen, das Verfahren auszusetzen und dem Gerichtshof Fragen zur Vorabentscheidung vorzulegen.

Aus den Gründen

Zur ersten und zur zweiten Frage

39 Mit seiner ersten und seiner zweiten Frage, die zusammen zu prüfen sind, möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 2 Nr. 7 RL 2011/83/EU dahin auszulegen ist, dass es für die Einstufung eines Vertrags zwischen einem Verbraucher und einem Unternehmer als „Fernabsatzvertrag“ im Sinne dieser Bestimmung von Bedeutung ist, ob der Verbraucher vor und bei Abschluss dieses Vertrags von einem anderen Unternehmer seiner Wahl unterstützt wird, der den Kontakt zwischen dem Verbraucher und dem erstgenannten Unternehmer angebahnt und auf wesentliche Teile des Inhalts des Vertrags Einfluss genommen hat.

40 Zunächst ist darauf hinzuweisen, dass nach dem Wortlaut von Art. 2 Nr. 7 RL 2011/83/EU drei Voraussetzungen kumulativ

erfüllt sein müssen, damit ein Vertrag als Fernabsatzvertrag eingestuft werden kann. Erstens muss dieser Vertrag zwischen einem Verbraucher und einem Unternehmer iSd Begriffsbestimmungen in Art. 2 Nr. 1 und Nr. 2 RL 2011/83/EU geschlossen werden. Zweitens muss er iRe für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems geschlossen werden. Drittens muss der Vertragsabschluss ohne gleichzeitige körperliche Anwesenheit des Unternehmers und des Verbrauchers erfolgen, und das Vertragsverhältnis zwischen den Parteien muss bis einschließlich zum Zeitpunkt des Abschlusses des Vertrags durch den ausschließlichen Einsatz eines oder mehrerer Fernkommunikationsmittel hergestellt werden.

41 Zwar geht aus dem Vorlagebeschluss nicht eindeutig hervor, an der Erfüllung welcher Voraussetzungen das vorlegende Gericht Zweifel hegt. Das vorlegende Gericht hat jedoch klargestellt, dass JK und der Architekt auf der einen Seite und Eisenberger Gerüstbau auf der anderen Seite bis zum Abschluss des Vertrags ausschließlich über Fernkommunikationsmittel, dh postalisch oder per E-Mail, kommuniziert hätten, woraus sich ergibt, dass es die dritte dieser Voraussetzungen als erfüllt ansieht. Daher sind nur die ersten beiden Voraussetzungen zu prüfen.

42 Als Erstes ist zu prüfen, ob eine Person wie JK, die Eigentümerin eines Grundstücks ist, das mit einem mehrgeschossigen Mehrfamilienhaus bebaut ist, und die einen Unternehmer, nämlich Eisenberger Gerüstbau, in Anspruch genommen hat, um zwei neue Etagen mit insgesamt vier Wohneinheiten errichten zu lassen, in Bezug auf den in Rede stehenden Vertrag als „Verbraucher“ einzustufen ist.

43 Insoweit ist darauf hinzuweisen, dass nach Art. 2 Nr. 1 RL 2011/83/EU jede natürliche Person, die bei von dieser RL erfassten Verträgen zu Zwecken handelt, die außerhalb ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit liegen, als „Verbraucher“ einzustufen ist.

44 Nach stRspr bezweckt die RL 2011/83/EU die Sicherstellung eines hohen Schutzniveaus für Verbraucher, die sich im Vergleich zu Unternehmern in einer unterlegenen Position befinden, da sie als schlechter informiert, wirtschaftlich schwächer und rechtlich weniger erfahren als ihre Vertragspartner angesehen werden müssen (vgl. idS Ur t. v. 27.3.2019 – C-681/17 [= MMR 2019, 364] Rn. 32 – slewo und v. 14.5.2020 – C-208/19 Rn. 39 – NK (Planung eines Einfamilienhauses)).

45 Der Begriff „Verbraucher“ iSv Art. 2 lit. b RL 93/13/EWG des Rates v. 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen (ABl. 1993 L 95, 29), der dem Begriff „Verbraucher“ iSv Art. 2 Nr. 1 RL 2011/83/EU entspricht, hat objektiven Charakter und ist unabhängig von den konkreten Kenntnissen, die die betreffende Person haben mag, oder den Informationen, über die sie tatsächlich verfügt (vgl. idS Ur t. v. 3.9.2015 – C-110/14 Rn. 21 – Costea und v. 8.5.2025 – C-410/23 Rn. 36 – Pielatak).

46 IRd Prüfung, ob die betreffende Person als „Verbraucher“ iSv Art. 2 Nr. 1 RL 2011/83/EU eingestuft werden kann, muss das nationale Gericht sämtliche Umstände des Einzelfalls – insb. die Art der Ware oder Dienstleistung, die Gegenstand des in Rede stehenden Vertrags ist – berücksichtigen, die belegen können, zu welchem Zweck die Ware oder Dienstleistung erworben wird (Ur t. v. 8.6.2023 – C-570/21 Rn. 55 – Begriff des Verbrauchers und die dort angeführte Rspr.).

47 Aus den Erläuterungen des vorlegenden Gerichts geht hervor, dass es wissen möchte, ob es für die Einstufung von JK als Verbraucherin von Bedeutung ist, dass sie von einem anderen Unternehmer ihrer Wahl, im vorliegenden Fall einem Architek-

ten, unterstützt wurde, der auf wesentliche Teile des Inhalts des in Rede stehenden Vertrags Einfluss genommen hat.

48 Insoweit ist zum einen ... der Umstand, dass ein Verbraucher wie im Ausgangsverfahren von einem Unternehmer, im vorliegenden Fall einem Architekten, bei der Anbahnung und dem Abschluss eines Vertrags zwischen diesem Verbraucher und einem anderen Unternehmer unterstützt wurde, nicht geeignet, die oben in Rn. 44 genannte unterlegene Position des Verbrauchers ggü. dem anderen Unternehmer in Frage zu stellen, und dies selbst wenn der Unternehmer, der ihn unterstützt hat, den Kontakt zwischen ihm und dem anderen Unternehmer angebahnt und auf den Inhalt des Vertrags Einfluss genommen hat.

49 Zum anderen ist, wie oben in Rn. 45 ausgeführt, der Begriff „Verbraucher“ iSv Art. 2 Nr. 1 RL 2011/83/EU dahin auszulegen, dass er objektiven Charakter hat und unabhängig ist von den konkreten Kenntnissen, die die betreffende Person haben mag, oder den Informationen, über die sie tatsächlich verfügt. Somit ist der Umstand, dass eine solche Person von einem Unternehmer unterstützt wurde, weder geeignet, ihre Verbrauchereigenschaft in Frage zu stellen, noch bedeutet dies iÜ, dass dem betreffenden Vertrag ein gewerblicher oder beruflicher Zweck beizumessen ist (vgl. idS Ur t. v. 3.9.2015 – C-110/14 Rn. 21 und 25 bis 27 – Costea).

50 Sollte das vorlegende Gericht der Auffassung sein, dass JK für die Zwecke des im Ausgangsverfahren in Rede stehenden Vertrags als Verbraucherin einzustufen ist, ist als Zweites zu prüfen, ob ein solcher Vertrag unter Berücksichtigung der tatsächlichen Umstände, die das vorlegende Gericht in seinem Vorlagebeschluss zu den Modalitäten des Vertragsabschlusses zwischen JK und Eisenberger Gerüstbau und der in diesem Rahmen von dem von JK eingeschalteten Architekten geleisteten Unterstützung dargelegt hat, als iRe für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems iSv Art. 2 Nr. 7 RL 2011/83/EU geschlossen anzusehen ist.

51 Insoweit heißt es im 20. Erwägungsgrund RL 2011/83/EU, dass der Begriff eines für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems von einem Dritten angebotene Fernabsatz- oder Dienstleistungssysteme erfassen sollte, die von Unternehmern verwendet werden, wie etwa eine Online-Plattform, jedoch nicht Fälle, in denen Webseiten lediglich Informationen über den Unternehmer, seine Waren und/oder Dienstleistungen und seine Kontaktdaten anbieten.

52 Im vorliegenden Fall ist festzustellen, dass ... die dem Gerichtshof vorliegenden Akten keine Angaben zu einem von Eisenberger Gerüstbau für den Fernabsatz organisierten Vertriebs- und Dienstleistungssystem enthalten. Die vom vorlegenden Gericht dargelegten tatsächlichen Umstände deuten jedoch darauf hin, dass der in Rede stehende Vertrag nicht iRe solchen Systems geschlossen wurde. Aus diesen Umständen ergibt sich nämlich, dass dieser Vertrag auf der Grundlage eines Vertragsentwurfs geschlossen wurde, der in alleiniger Verantwortung von JK erstellt wurde und in dem die konkreten Leistungen angegeben waren, die sie an Eisenberger Gerüstbau zu vergeben beabsichtigte, wobei der Entwurf diesem Unternehmen per E-Mail zur Unterzeichnung zugesandt wurde und von ihm unverändert unterschrieben wurde. Selbst unter der Annahme, dass dieses Unternehmen über ein für den Fernabsatz organisiertes Vertriebs- und Dienstleistungssystem verfügte, ist daher nicht ersichtlich, dass der im Ausgangsverfahren in Rede stehende Vertrag mittels eines solchen Systems geschlossen worden wäre, was jedoch vom vorlegenden Gericht zu prüfen ist.

53 Nach alledem ist auf die erste und die zweite Frage zu antworten, dass Art. 2 Nr. 7 RL 2011/83/EU dahin auszulegen ist, dass es für die Einstufung eines Vertrags zwischen einem Ver-

braucher und einem Unternehmer als „Fernabsatzvertrag“ im Sinne dieser Bestimmung ohne Bedeutung ist, ob der Verbraucher vor und bei Abschluss dieses Vertrags von einem anderen Unternehmer seiner Wahl unterstützt wird, der den Kontakt zwischen dem Verbraucher und dem erstgenannten Unternehmer angebahnt und auf wesentliche Teile des Inhalts des Vertrags Einfluss genommen hat.

Zur dritten Frage

54 Mit seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 2 Nr. 7 RL 2011/83/EU dahin auszulegen ist, dass eine von den Parteien eines Vertrags, der nicht als „Fernabsatzvertrag“ im Sinne dieser Bestimmung eingestuft werden kann, unter ausschließlicher Verwendung von Fernkommunikationsmitteln getroffene Nachtragsvereinbarung über zusätzliche Leistungen, die ggü. den in dem Vertrag vorgesehenen Leistungen von untergeordneter Bedeutung sind, einen „Fernabsatzvertrag“ im Sinne dieser Bestimmung darstellt.

55 Zur Beantwortung dieser Frage ist zunächst darauf hinzuweisen, dass Art. 2 Nr. 15 RL 2011/83/EU einen „akzessorischen Vertrag“ als einen Vertrag, mit dem der Verbraucher Waren oder Dienstleistungen erwirbt, die im Zusammenhang mit einem Fernabsatzvertrag oder einem außerhalb von Geschäftsräumen geschlossenen Vertrag stehen und bei dem diese Waren oder Dienstleistungen von dem Unternehmer oder einem Dritten auf der Grundlage einer Vereinbarung zwischen diesem Dritten und dem Unternehmer geliefert oder erbracht werden, definiert.

56 Insoweit bestimmt Art. 15 RL 2011/83/EU, wie sich die Ausübung des Rechts auf Widerruf eines im Fernabsatz oder außerhalb von Geschäftsräumen geschlossenen Vertrags auf akzessorische Verträge auswirkt.

57 Allerdings sieht die RL 2011/83/EU keine spezifischen Regeln dafür vor, ob eine Vereinbarung zur Änderung eines anderen Vertrags, dessen rechtliche Einstufung als Fernabsatzvertrag ausgeschlossen worden ist, rechtlich als Fernabsatzvertrag einzustufen ist.

58 Um zu prüfen, ob der Vertrag zur Änderung eines anderen Vertrags als „Fernabsatzvertrag“ iSv Art. 2 Nr. 7 RL 2011/83/EU anzusehen ist, wird das vorlegende Gericht unter diesen Umständen zu prüfen haben, ob die oben in Rn. 40 genannten Voraussetzungen in Bezug auf den Änderungsvertrag, im vorliegenden Fall die Nachtragsvereinbarung zu dem in Rede stehenden Vertrag, erfüllt sind.

59 Daher ist auf die dritte Frage zu antworten, dass Art. 2 Nr. 7 RL 2011/83/EU dahin auszulegen ist, dass eine von den Parteien eines Vertrags, der nicht als „Fernabsatzvertrag“ im Sinne dieser Bestimmung eingestuft werden kann, unter ausschließlicher Verwendung von Fernkommunikationsmitteln getroffene Nachtragsvereinbarung über zusätzliche Leistungen, die ggü. den in dem Vertrag vorgesehenen Leistungen von untergeordneter Bedeutung sind, einen „Fernabsatzvertrag“ im Sinne dieser Bestimmung darstellt, sofern die in dieser Bestimmung vorgesehenen Voraussetzungen erfüllt sind.

Zur vierten Frage

60 Mit seiner vierten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob die RL 2011/83/EU dahin auszulegen ist, dass in dem Fall, dass ein Verbraucher aE der gem. Art. 10 Abs. 1 dieser RL verlängerten Widerrufsfrist einen Fernabsatzvertrag zu einem Zeitpunkt widerrufen hat, zu dem die Leistungen, die Gegenstand dieses Vertrags sind und nicht zurückerstattet werden können, bereits erbracht worden waren, der Unternehmer mit Erfolg geltend machen kann, dass der Verbraucher das Widerrufsrecht missbräuchlich ausgeübt habe.

61 Insoweit bestimmt Art. 6 Abs. 1 lit. h RL 2011/83/EU, dass, bevor der Verbraucher durch einen Vertrag im Fernabsatz gebunden ist, der Unternehmer den Verbraucher in klarer und verständlicher Weise über die Bedingungen, Fristen und Verfahren für die Ausübung des Widerrufsrechts gem. Art. 11 Abs. 1 dieser RL sowie das Muster-Widerrufsformular gem. Anhang I Teil B der RL informiert.

62 IÜ steht dem Verbraucher, sofern nicht eine der Ausnahmen gem. Art. 16 RL 2011/83/EU Anwendung findet, nach Art. 9 Abs. 1 dieser RL eine Frist von 14 Tagen zu, in der er einen Fernabsatz- oder einen außerhalb von Geschäftsräumen geschlossenen Vertrag ohne Angabe von Gründen und ohne andere Kosten als in Art. 13 Abs. 2 und 14 der RL vorgesehen widerrufen kann.

63 Darüber hinaus endet nach Art. 9 Abs. 2 lit. a RL 2011/83/EU unbeschadet von Art. 10 dieser RL die in Art. 9 Abs. 1 der RL vorgesehene Widerrufsfrist bei Dienstleistungsverträgen 14 Tage ab dem Tag des Vertragsabschlusses.

64 Allerdings führt das Versäumnis, die in Art. 6 Abs. 1 lit. h RL 2011/83/EU genannten Informationen zu erteilen, gem. Art. 10 Abs. 1 dieser RL dazu, dass sich die Widerrufsfrist um zwölf Monate nach Ablauf der ursprünglichen Widerrufsfrist verlängert.

65 Zudem sieht Art. 14 Abs. 4 lit. a Ziff. i RL 2011/83/EU vor, dass der Verbraucher nicht für Dienstleistungen aufzukommen hat, wenn der Unternehmer es unterlassen hat, die Informationen gem. Art. 6 Abs. 1 lit. h oder j dieser RL bereitzustellen.

66 Ferner kann der Verbraucher nach Art. 14 Abs. 5 RL 2011/83/EU, sofern in Art. 13 Abs. 2 und Art. 14 dieser RL nichts anderes vorgesehen ist, aufgrund der Ausübung seines Widerrufsrechts nicht in Anspruch genommen werden.

67 Hierzu ist zunächst festzustellen, dass die Vorlagefrage auf der Prämisse beruht, dass JK die Voraussetzungen für die Ausübung des in Art. 9 RL 2011/83/EU iVm Art. 10 Abs. 1 dieser RL vorgesehenen Widerrufsrechts erfüllt.

68 Daher ist zu prüfen, ob sich der Unternehmer in dem Fall, dass ein Verbraucher einen Fernabsatzvertrag wie JK während der gem. Art. 10 Abs. 1 RL 2011/83/EU verlängerten Widerrufsfrist zu einem Zeitpunkt widerruft, zu dem der Unternehmer aufgrund dieses Vertrags bereits Leistungen erbracht hat, die nicht zurückerstattet werden können, auf die Missbräuchlichkeit der Ausübung des Widerrufsrechts durch den Verbraucher berufen kann.

69 Insoweit hat der Gerichtshof entschieden, dass die Anwendung der Unionsregelung nicht so weit reichen kann, dass Vorgänge geschützt werden, die dazu dienen, betrügerisch oder missbräuchlich in den Genuss im Unionsrecht vorgesehener Vorteile zu gelangen (Urt. v. 21.12.2023 – C-38/21, C-47/21 und C-232/21 [= MMR 2024, 400] Rn. 282 – BMW Bank u.a.).

70 Der Nachweis einer missbräuchlichen Praxis setzt zum einen eine Gesamtheit objektiver Umstände voraus, aus denen sich ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Voraussetzungen das Ziel der Regelung nicht erreicht wurde, und zum anderen ein subjektives Element, nämlich die Absicht, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden ...

71 Die Prüfung des Vorliegens einer missbräuchlichen Praxis verlangt, dass das vorlegende Gericht alle Tatsachen und Umstände des Einzelfalls berücksichtigt, einschließlich derjenigen aus der Zeit nach dem Vorgang, dessen missbräuchlicher Charakter geltend gemacht wird ...

72 Es ist daher Sache des vorlegenden Gerichts, gemäß den Beweisregeln des nationalen Rechts – soweit dadurch die Wirksamkeit des Unionsrechts nicht beeinträchtigt wird – zu prüfen, ob die oben in Rn. 70 genannten Tatbestandsmerkmale einer missbräuchlichen Praxis im Ausgangsrechtsstreit vorliegen. Der Gerichtshof kann jedoch iRe Vorabentscheidungsverfahrens ggf. Klarstellungen vornehmen, um dem vorlegenden Gericht eine Richtschnur für seine Auslegung zu geben ...

73 Zum Vorliegen eines oben in Rn. 70 genannten objektiven Elements, das auf eine missbräuchliche Praxis hindeutet, ist festzustellen, dass die RL 2011/83/EU, wie aus ihrem Art. 1 im Licht ihrer Erwägungsgründe 4, 5 und 7 hervorgeht, bezweckt, ein hohes Verbraucherschutzniveau dadurch sicherzustellen, dass die Information und die Sicherheit der Verbraucher bei Geschäften mit Unternehmern garantiert werden. Die RL zielt somit darauf ab, dass die Verbraucher in den Genuss eines weitreichenden Schutzes kommen, indem ihnen insb. bei Vertragsabschlüssen im Fernabsatz bestimmte Rechte, darunter das Widerrufsrecht, gewährt werden. Der Unionsgesetzgeber wollte verhindern, dass die Verwendung von Fernkommunikationstechniken zu einer Verringerung der dem Verbraucher bereitgestellten Informationen führt (vgl. idS Urt. v. 23.1.2019 – C-430/17 [= MMR 2019, 299] Rn. 34 und 35 – Walbusch Walter Busch).

74 Insb. soll Art. 9 RL 2011/83/EU es dem Verbraucher ermöglichen, den seinen Bedürfnissen am besten entsprechenden Vertrag auszuwählen und somit von einem Vertrag zurückzutreten, bei dem sich nach dessen Abschluss innerhalb der für die Ausübung des Widerrufsrechts vorgesehenen Überlegungsfrist herausstellt, dass er solchen Bedürfnissen nicht entspricht. In diesem Rahmen besteht das Ziel von Art. 10 Abs. 1 dieser RL darin, sicherzustellen, dass der Verbraucher Informationen über die Voraussetzungen, die Frist und die Modalitäten für die Ausübung des Widerrufsrechts sowie das Muster-Widerrufsformular erhält, und den Unternehmer, der ihm diese Informationen nicht erteilt, mit Sanktionen zu belegen (vgl. entsprechend Urt. v. 21.12.2023 – C-38/21, C-47/21 und C-232/21 [= MMR 2024, 400] Rn. 288 – BMW Bank u.a.).

75 Wie der GA in den Rn. 54 bis 56 seiner Schlussanträge im Wesentlichen ausführt, werden dieselben Ziele auch mit Art. 14 Abs. 4 lit. a Ziff. i RL 2011/83/EU iVm Art. 14 Abs. 5 RL 2011/83/EU verfolgt, der ausschließt, dass für den Verbraucher, der die in Art. 6 Abs. 1 lit. h dieser RL genannten Informationen nicht erhalten hat, aufgrund der Ausübung seines Widerrufsrechts Kosten anfallen.

76 Insoweit hat der Gerichtshof zwar in Bezug auf das in Art. 14 Abs. 1 RL 2008/48/EG vorgesehene Widerrufsrecht entschieden, dass ein Unternehmer, wenn er dem Verbraucher die in Art. 10 der RL genannten Informationen nicht erteilt hat und dieser beschließt, den Kreditvertrag nach Ablauf der Frist von 14 Tagen nach Abschluss des Vertrags zu widerrufen, zwecks Abschreckung von einem Verstoß gegen die ihm nach der RL ggü. dem Verbraucher obliegenden Pflichten diesem keine missbräuchliche Ausübung seines Widerrufsrechts vorwerfen kann, auch wenn zwischen dem Vertragsschluss und dem Widerruf durch den Verbraucher erhebliche Zeit vergangen ist (Urt. v. 9.9.2021 – C-33/20, C-155/20 und C-187/20 Rn. 126 und 127 – Volkswagen Bank u.a., sowie v. 21.12.2023 – C-38/21, C-47/21 und C-232/21 [= MMR 2024, 400] Rn. 289 und 290 – BMW Bank u.a.).

77 Dementsprechend kann nicht davon ausgegangen werden, dass der bloße Umstand, dass der Verbraucher sein Widerrufsrecht nach Art. 9 Abs. 1 RL 2011/83/EU gegen Ende der gem. Art. 10 Abs. 1 dieser RL verlängerten Widerrufsfrist ausübt, für sich genommen ausreicht, um den Nachweis eines solchen objektiven Elements zu erbringen.

78 Im vorliegenden Fall hat der Verbraucher jedoch nicht nur sein Widerrufsrecht gegen Ende der um zwölf Monate nach Ablauf der ursprünglichen Widerrufsfrist verlängerten Frist ausgeübt, sondern wurde, wie oben in Rn. 52 ausgeführt ... zudem der Vertrag auf der Grundlage eines Entwurfs geschlossen, der in alleiniger Verantwortung des Verbrauchers durch einen Verhandlungsgehilfen seiner Wahl sowie entsprechend dessen Vorgaben für die von dem Unternehmer erwarteten konkreten Leistungen erstellt und anschließend von diesem Unternehmer unverändert unterschrieben wurde.

79 In einem solchen Fall erscheint es aber nicht ausgeschlossen, dass die Ausübung des Widerrufsrechts durch den Verbraucher nicht den oben in Rn. 73 genannten Zielen entspricht.

80 Diese Umstände sprechen für die – letztlich vom vorlegenden Gericht zu treffende – Feststellung, dass ein objektives Element vorliegt, das auf eine missbräuchliche Praxis seitens des Verbrauchers, der den Fernabsatzvertrag widerruft, im vorliegenden Fall JK, hindeutet.

81 Sollte dies der Fall sein, hat das vorlegende Gericht zu prüfen, ob ein subjektives Element, bei dem es sich trotz der vom vorlegenden Gericht geäußerten Zweifel um eine notwendige Voraussetzung für die Feststellung einer missbräuchlichen Praxis iSd oben in den Rn. 69 und 70 angeführten Rspr. handelt, seitens des Verbrauchers vorliegt. Insoweit können Anhaltspunkte von Bedeutung sein, die darauf hindeuten, dass der Zeitpunkt der Ausübung des Widerrufsrechts vom Verbraucher absichtlich allein zu dem Zweck gewählt wurde, um den vollen Nutzen aus der vom Unternehmer vollständig oder fast vollständig erbrachten Leistung ziehen zu können, ohne hierfür als Gegenleistung irgendeine Vergütung zu schulden.

82 Nach alledem ist auf die vierte Frage zu antworten, dass die RL 2011/83/EU dahin auszulegen ist, dass in dem Fall, dass ein Verbraucher aE der gem. Art. 10 Abs. 1 dieser RL verlängerten Widerrufsfrist einen Fernabsatzvertrag zu einem Zeitpunkt widerrufen hat, zu dem die Leistungen, die Gegenstand dieses Vertrags sind und nicht zurückerstattet werden können, bereits erbracht worden waren, der Unternehmer mit Erfolg geltend machen kann, dass der Verbraucher aufgrund seines eigenen Verhaltens das Widerrufsrecht missbräuchlich ausgeübt habe, wenn sich aus der Gesamtheit der Umstände ergibt, dass zum einen die Ausübung des Widerrufsrechts durch den Verbraucher nicht den mit der RL verfolgten Zielen in Bezug auf die Information des Verbrauchers und die Sicherheit bei Geschäften mit einem Unternehmer entspricht und zum anderen der Verbraucher mit seinem Verhalten darauf abzielt, sich auf Kosten des Unternehmers missbräuchlich einen Vorteil zu verschaffen. ...

Anmerkung

RA Robert Briske, M. mel. / RA Jonas Müter, LL.M. (EMLE), Osborne Clarke, Berlin/Hamburg

Die Entscheidung nimmt Stellung zu zentralen Fragen im Zusammenhang mit dem Widerrufsrecht von Verbrauchern. Während der EuGH den Anwendungsbereich des Widerrufsrechts dessen Schutzzweck entsprechend weit zieht, enthält die Entscheidung ein aus Sicht von Unternehmen erfreuliches Korrektiv für Fälle, in denen Verbraucher ihr Widerrufsrecht missbräuchlich ausüben. Die Entscheidung beantwortet damit nicht nur dogmatische Fragen, sondern hat auch eine rechtspolitische Dimension. Diese besteht darin, dass das Widerrufsrecht bei einem rein formalen Fehler einer unterlassenen Widerrufsbelehrung dazu führen kann, dass sich ein Verbraucher nach vollständig erbrachter Leistung innerhalb der verlängerten Widerrufsfrist von einem Jahr und 14 Tagen vom Vertrag und damit seiner Gegenleistungspflicht löst, während er die erbrachte Leistung behalten darf – und zwar ohne Wertersatz.

Dies führt gerade bei regelmäßig teuren Handwerkerleistungen zu erheblichen wirtschaftlichen Auswirkungen für Unternehmer und spiegelbildlich zu einem missbrauchsanfälligen „Einsparpotenzial“ auf Seiten des Verbrauchers (zum rechtspolitischen Gehalt s. ausf. Seiwerth NJW 2025, 1001, der das Problem unter dem Stichwort „Hausbau für lau?“ diskutiert).

1. Sachverhalt und Vorlagefragen

Der Entscheidung liegt eine zuletzt vor dem KG geführte Auseinandersetzung zwischen einem Gerüstbauunternehmen und einer Berliner Grundstückseigentümerin zugrunde, die das Dachgeschoss ihres Wohnhauses aufzustocken plante. Hierzu beauftragte sie (JK) einen Architekten mit der Bauplanung und -überwachung. Dieser entwarf auf Grundlage des Angebots des Gerüstbauers einen Vertrag, den er beiden Parteien übersandte. Eine Widerrufsbelehrung enthielt der Vertrag nicht.

Nach Vertragsschluss überließ der Gerüstbauer JK das Gerüst für die beabsichtigten Bauarbeiten. Gut elf Monate später, als die Bauarbeiten vollständig abgeschlossen waren, erklärte JK den Widerruf des Vertrags, verweigerte weitere Zahlungen und forderte ihre Abschlagszahlungen zurück. Das LG Berlin wies die Klage des Gerüstbauers auf Zahlung der offenen Vergütung ab und verurteilte ihn auf Widerklage zur Rückerstattung der geleisteten Abschlagszahlung. Das KG setzte das Verfahren in der Berufung aus und richtete die nun beantworteten und nachfolgend dargestellten Vorlagefragen an den EuGH.

2. Verbrauchervertrag trotz Einschaltung eines Unternehmers

Mit der ersten Vorlagefrage wollte das KG wissen, ob ein Fernabsatzvertrag iSd Verbraucherrechte-RL auch dann vorliegt, wenn der Verbraucher vor oder bei Vertragsschluss durch einen Unternehmer unterstützt wird, den er unabhängig vom Leistungserbringer beauftragt hat. Das KG hatte sich hier zu Recht skeptisch gezeigt: Zweck des das Fernabsatzrecht regelnden § 312c BGB sei es, die für Distanzgeschäfte typischen Informationsdefizite auf Seiten des Verbrauchers auszugleichen. Derartige Informationsdefizite seien nicht zu erwarten, wenn der Verbraucher bei der Vertragsanbahnung einen Unternehmer als Verhandlungsgehilfen heranzieht, der eine ausreichende Fachkunde in Bezug auf die vertragsgegenständlichen Dienstleistungen aufweist (KG BeckRS 2024, 8645 Rn. 22). Tatsächlich sprechen in der hiesigen Konstellation jedenfalls gute Gründe gegen die Einstufung des Vertrags als Verbrauchervertrag. Die Verbraucherrechte-RL selbst nimmt iRd Informationspflichten des Unternehmers Rücksicht auf die besonderen Bedürfnisse schutzwürdiger Verbraucher (vgl. Erwägungsgrund 34 Verbraucherrechte-RL). Dies sollte auch umgekehrt gelten: Wo die Schutzwürdigkeit aufgrund der Einschaltung eines professionellen Mittlers wie hier des Architekten entfällt, besteht nicht zwingend ein Erfordernis, den Vertragspartner als Verbraucher einzustufen.

Der EuGH teilt diese Bedenken nicht. Es sei ohne Bedeutung, ob der Verbraucher vor und bei Abschluss des Vertrags von einem anderen Unternehmer seiner Wahl unterstützt wird. Diese Unterstützung sei nicht geeignet, die unterlegene Position des Verbrauchers in Frage zu stellen. Das soll selbst dann gelten, wenn der Architekt selbst den Kontakt zu dem Gerüstbauer angebahnt und auf den Inhalt des Vertrags Einfluss genommen hat (Rn. 48). Der Verbraucherbegriff sei rein objektiv zu beurteilen, unabhängig von den konkreten Kenntnissen oder den Informationen, über die die betroffene Person tatsächlich verfügt. Das ist mit Blick auf das von der Richtlinie verfolgte hohe Verbraucherschutzniveau, das sich allein an dem Zweck des Rechtsgeschäfts orientiert, letztlich konsequent, auch wenn jedenfalls in Fällen, in denen – wie hier – der unterstützende Unternehmer sogar den Vertragsentwurf erstellt

hat, bezweifelt werden darf, ob die Einstufung des Vertragspartners als Verbraucher sachgerecht ist.

3. Für den Fernabsatz organisiertes Vertriebssystem

Diesen Punkt greift der EuGH iRd zweiten Vorlagefrage auf. Voraussetzung für einen zum Widerruf berechtigenden Fernabsatzvertrag ist über das Vorliegen eines Verbrauchervertrags hinaus, dass dieser Vertrag iRe für den Fernabsatz organisierten Vertriebs- oder Dienstleistungssystems geschlossen wurde. Die Frage überlässt der EuGH in dem konkreten Fall der Beantwortung durch das nationale Gericht. Er deutet jedoch an, dass er die vorgetragenen Umstände nicht für ausreichend erachtet. Diese deuteten vielmehr darauf hin, dass der Vertrag auf der Grundlage eines Entwurfs geschlossen wurde, der in alleiniger Verantwortung von JK erstellt wurde und in dem die konkreten Leistungen angegeben waren, die sie zu vergeben beabsichtigte (Rn. 52). Der Versand des Vertrags per E-Mail an den Gerüstbauer mache nicht ersichtlich, dass der Vertrag mittels eines Fernabsatzsystems geschlossen worden sei. Dies erscheint sachgerecht. Die gelegentliche Verwendung von Fernkommunikationsmitteln begründet keinen Vertragsschluss „im Rahmen“ eines derartigen Systems, selbst, wenn der Unternehmer ein solches grds. vorhält (vgl. MüKoBGB/Wendehorst, 10. Aufl. 2026, BGB § 312c Rn. 26).

4. Nachtragsvereinbarungen über zusätzliche Leistungen können ebenfalls widerrufliche Fernabsatzverträge sein

Unter den o.g. Voraussetzungen kann eine Nachtragsvereinbarung über zusätzliche Leistungen einen Fernabsatzvertrag auch dann darstellen, wenn der „Hauptvertrag“ keinen solchen Fernabsatzvertrag darstellt. Die Verbraucherrechte-RL kenne insofern keine spezifischen Regeln; Änderungsverträge seien damit grds. eigenständig zu beurteilen. Diese Prüfung hat der EuGH wiederum dem nationalen Gericht überlassen.

Dies ist insofern konsequent, als stets der konkret betrachtete Vertrag maßgeblich für die Feststellung ist, ob der Vertragsschluss iRe Fernabsatzsystems erfolgt ist (MüKoBGB/Wendehorst, 10. Aufl. 2026, BGB § 312c Rn. 26). Für die typische Schutzbedürftigkeit des Verbrauchers macht es in der Regel keinen Unterschied, ob die Parteien zuvor bereits einen Vertrag abgeschlossen hatten, der nicht als Fernabsatzvertrag einzustufen ist. Für den Unternehmer bringt dies die praktisch bedeutsame Konsequenz mit sich, dass er den Verbraucher bei solchen Nachtragsvereinbarungen erneut über das Widerrufsrecht belehren muss. Gerade im Bereich des Handwerks sind derartige Ergänzungsvereinbarungen wirtschaftlich bedeutend (vgl. Seiwerth NJW 2025, 1001).

5. Grenzen des Widerrufsrechts: Korrektiv für rechtsmissbräuchliches Verhalten

Kern der Entscheidung – und von enormer praktischer Bedeutung – sind sodann die Ausführungen des EuGH zum Einwand des Rechtsmissbrauchs. Der EuGH verwehrt dem Verbraucher sein Widerrufsrecht dann, wenn die Ausübung nicht den mit der Verbraucherrechte-RL verfolgten Zielen entspricht und der Verbraucher mit seinem Verhalten darauf abzielt, sich auf Kosten des Unternehmers einen Vorteil zu verschaffen. Ein ähnliches Korrektiv hat der EuGH zuletzt auch Unternehmen zugestanden, die sich mit „exzessiven“ Auskunftsansprüchen nach Art. 15 DS-GVO konfrontiert sehen (EuGH MMR 2026, 500 mAnm Sosna/Meyer – Brillen Rottler/TC – in diesem Heft). Der EuGH konkretisiert damit seine Rspr., wonach die Anwendung einer Unionsregelung nicht so weit reichen kann, dass Vorgänge geschützt werden, die dazu dienen, betrügerisch oder missbräuchlich in den Genuss im Unionsrecht vorgesehener Vorteile zu gelangen (NJW 2024, 809 – VK/BMW Bank GmbH u.a. in Bezug auf das Widerrufsrecht).

Auch in Bezug auf den Nachweis einer solchen missbräuchlichen Praxis knüpft der EuGH an seine vorangegangene Rspr. an. Erforderlich sei zum einen eine Gesamtheit objektiver Umstände, aus denen sich ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Voraussetzungen das Ziel der Regelung nicht erreicht wurde. Zum anderen erfordere er ein subjektives Element, also die Absicht, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden (so auch EuGH MMR 2026, 500 mAnm Sosna/Meyer – Brillen Rottler/TC – in diesem Heft). Das KG hatte in seinem Vorlagebeschluss noch zum Ausdruck gebracht, dass es ein subjektives Element nicht für erforderlich hält (KG BeckRS 2024, 8645 Rn. 45).

Schließlich konkretisiert der EuGH sein Urteil in der Rs. DC/HJ (EuGH Urt. v. 17.5.2023 – C-97/22), in der er entschieden hatte, dass im Falle einer fehlenden Widerrufsbelehrung bei Ausübung des Rechts kein Anspruch des Unternehmers auf Wertersatz bestehe (zu Recht krit. Wallner ZEuP 2024, 436 unter Hinweis auf eine „Verstärkung der Sanktionswirkung durch die verlängerte Widerrufsfrist“ und ein entsprechendes „Alles-oder-nichts“-Ergebnis). Die Auswirkungen dieser Entscheidung werden durch das nunmehr ergangene Urteil gewissermaßen abgemildert.

Die konkrete Bewertung des hiesigen Falls überlässt der EuGH naturgemäß dem vorlegenden Gericht. In seinen Segelanweisungen macht er gleichwohl deutlich, dass er die Grenzen des Rechtsmissbrauchs hier überschritten sieht. In objektiver Hinsicht könne zwar der bloße Umstand, dass der Verbraucher sein Widerrufsrecht gegen Ende der verlängerten Widerrufsfrist ausübe, nicht ausreichen. Hier komme aber noch hinzu, dass der Vertrag auf Grundlage des von der Verbraucherin eingeschalteten Architekten zur Verfügung gestellten Entwurfs zustande gekommen sei, der in alleiniger Verantwortung der JK tätig geworden sei. Insofern findet die Unterstützung durch den Unternehmer, wenn nicht iRd Bewertung der Verbrauchereigenschaft, dennoch Eingang in die Gesamtbetrachtung. Das KG hatte in seinem Vorlagebeschluss weitere Umstände aufgezählt, die ebenfalls für eine Treuwidrigkeit sprächen, u.a., dass der Unternehmer die Belehrung nicht vorsätzlich unterlassen hat, er eine Bauleistung erbracht hat, die aus tatsächlichen oder wirtschaftlichen Gründen nicht zurückgegeben werden kann, und dass der Verbraucher die Leistung nun dauerhaft nutze (KG BeckRS 2024, 8645 Rn. 43).

Der Nachweis des subjektiven Elements begegnet in der Praxis häufig den üblichen Schwierigkeiten. Wie iRd Sittenwidrigkeit, wo die Rspr. keine allzu strengen Anforderungen an den Nachweis stellt und unter Umständen bereits das Vorliegen der objektiven Merkmale eine Vermutung für den subjektiven Tatbestand begründen soll (BeckOK BGB/Wendtland, 77. Ed. 1.2.2026, BGB § 138 Rn. 39), sollte hier ein großzügiger Maßstab angelegt werden. Wenn der Verbraucher einen Vertrag bei fortwährender Nutzung der Vorteile daraus ohne erkennbaren objektiven Grund widerruft, dürfte vieles dafürsprechen, dass dieses Verhalten darauf abzielt, sich auf Kosten des Unternehmers einen Vorteil zu verschaffen. Im Zweifel wird man vom Verbraucher folglich iRe sekundären Darlegungslast Vortrag dazu erwarten dürfen, welche Motive für den Widerruf ausschlaggebend gewesen sein sollen.

6. Fazit und Ausblick

Die Entscheidung ist zu begrüßen. Der EuGH bestätigt die in der deutschen Rspr. durchaus bereits gelebte Praxis (s. dazu zB BeckOGK/Reiter/Schott, 1.4.2026, BGB § 650I Rn. 55 ff.) zur Unterbindung einer rechtsmissbräuchlichen Ausübung von

Verbraucherrechten und gibt Unternehmen ein (nicht nur rechtspolitisch) sinnvolles Korrektiv für Missbrauchsfälle an die Hand. Im Falle eines Widerrufs zu einem Zeitpunkt, in dem der Unternehmer seine Leistung bereits vollständig erbracht hat, ist es jedenfalls idR interessengerecht, wenn der Verbraucher die Leistung – wenn sie ihm zugutekommt – nicht allein aufgrund einer unterlassenen Belehrung „für lau“ bekommt.

Unklar bleibt, wann ein Widerruf „am Ende“ der (verlängerten) Widerrufsfrist erfolgt. Um das vom EuGH entwickelte Korrektiv nicht praktisch zu entwerten, ist eine großzügige Handhabung durch die nationalen Gerichte wünschenswert. Eine rein zeitliche Betrachtung scheint insofern nicht angebracht. Maßgebliches Kriterium sollte hier vor allem der Fortschritt der Leistungserbringung durch den Unternehmer und das Ausnutzen dieser Leistung durch den Verbraucher sein.

Perspektivisch könnte die Entscheidung auch Bedeutung erlangen im Zusammenhang mit der Ausübung des Widerrufsrechts iRv Streamingangeboten oder anderen digitalen Angeboten. Dem EuGH liegt aktuell die Vorlagefrage des ÖOGH vor, ob solche Streamingdienste „digitale Inhalte“ oder aber „digitale Dienstleistungen“ darstellen (ÖOGH Beschl. v. 19.3.2025 – 90b 48/24k). Diese Einstufung hat unmittelbare Auswirkungen auf das Widerrufsrecht, das ein Unternehmer nur bei digitalen Dienstleistungen ausschließen kann. Sollte der EuGH Streaming als digitale Dienstleistungen ansehen, für die das Widerrufsrecht nicht ausgeschlossen werden kann, könnte der Missbrauchseinwand besondere Bedeutung erlangen. Die Bekl. in dem österreichischen Ausgangsverfahren argumentiert folgerichtig, dass eine derartige Bewertung zu missbräuchlichen Ergebnissen führen kann, da Nutzer Streamingdienste, zB bei sportlichen Großereignissen, in Anspruch nehmen und danach ihr Widerrufsrecht ausüben könnten (s. dazu Kuchar GRUR-Prax 2025, 336).

ÖOGH: Speichermedienvergütungspflicht für Cloud-Speicher nach österreichischem Urheberrecht

Vervielfältigungsrecht

öUrhG § 42b Abs. 1, Abs. 2a, Abs. 3 Nr. 1; RL 2001/29/EG Art. 2 lit. a, 5
Urteil vom 16.12.2025 – 4 Ob 15/25x (OLG Wien, HG Wien)

Leitsatz der Redaktion

Nach richtlinienkonformer Auslegung des öUrhG hat derjenige, der als erster Kunde im Inland gewerbsmäßig Speicherplatz in einer Cloud in im Inland oder im Ausland gelegenen Rechenzentren zur Verfügung stellt, dafür eine Speichermedienvergütung zu leisten, soweit nicht nach den Umständen erwartet werden kann, dass den Urhebern durch das Abspeichern in der Cloud nur ein geringfügiger Nachteil entsteht. Die Erheblichkeitsschwelle ist im konkreten Fall überschritten.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 37449. Vgl. ferner EuGH MMR 2022, 647 – Austro-Mechana/Strato und EuGH MMR 2023, 665 – Ocilion IPTV Technologies.

Schlagnote: Speichermedienvergütung; Cloud-Speicher; Vervielfältigungsrecht; gerechter Ausgleich; richtlinienkonforme Auslegung; Privatgebrauch; Erheblichkeitsschwelle

Sachverhalt

Die Kl. ist eine Verwertungsgesellschaft iSd § 42b Abs. 5 öUrhG. Sie macht eigene Ansprüche und ihr von weiteren Verwertungsgesellschaften zum Inkasso abgetretene Ansprüche geltend.

Die Bkl. mit Sitz in Deutschland bietet gewerbsmäßig Cloud-Speicher-Modelle (u.a.) für Privatkunden in Österreich an. Die Cloud-Nutzer können in der vereinbarten Zeit digitale Inhalte im vereinbarten Umfang in Rechenzentren der Bkl. in Deutschland speichern und darauf mit einem geeigneten Endgerät über das Internet – mittels Streaming oder Download – zugreifen.

Die Bkl. hat 620 Kunden in Österreich, überwiegend Privatkunden. Sie benutzen den Cloud-Speicher auch dazu, urheberrechtlich geschützte Werke für den privaten Gebrauch zu vervielfältigen und auf Endgeräte herunterzuladen. Am häufigsten nutzen die Kunden Cloud-Speicher mit 11 GB bis 50 GB Speicherkapazität.

Die Kl. beehrte, gestützt auf § 42b Abs. 1 und Abs. 3 Nr. 1 öUrhG, die Rechnungslegung über die gewerbsmäßigen Cloud-Dienste der Bkl. für Privatkunden in Österreich und die Zahlung der sich aus der Rechnungslegung ergebenden Speichermedienvergütung (Stufenklage). Die gewerbsmäßigen Cloud-Dienste der Bkl. würden den Tatbestand des § 42b Abs. 1 öUrhG erfüllen, weshalb die Bkl. gem. § 42b Abs. 3 Nr. 1 öUrhG eine Speichermedienvergütung zu entrichten habe.

Die Bkl. beantragte die Abweisung des Klagebegehrens. Die Cloud sei kein körperlicher Gegenstand, an dem einem anderen die physische Verfügungsgewalt überlassen werden könne, und damit kein „Speichermedium“, das „in Verkehr kommen“ könne (§ 42b Abs. 1 öUrhG). Die Urheber würden durch die Speichermedienvergütung für die Endgeräte einen gerechten Ausgleich erhalten. Durch Vervielfältigungen urheberrechtlich geschützter Werke in der Cloud zum eigenen oder privaten Gebrauch entstehe den Urhebern nur ein geringfügiger Nachteil (§ 42b Abs. 2a öUrhG).

Das Erstgericht gab dem Rechnungslegungsbegehren (unter rechtskräftiger Abweisung des Mehrbegehrens) für die Zeit seit 1.10.2015 (Inkrafttreten von § 42b Abs. 1, Abs. 3 Nr. 1, Abs. 4 und Abs. 6 bis 9 öUrhG) statt. § 42b Abs. 1 öUrhG sei richtlinienkonform so auszulegen, dass mit dem Zurverfügungstellen von Speicherplatz in einer Cloud ein Speichermedium jeglicher Art in Verkehr komme und die beklagte Anbieterin dafür einen gerechten Ausgleich zu leisten habe. Aufgrund der Kundenanzahl der Bkl. und der von diesen durchschnittlich am häufigsten genutzten Speicherkapazität sei die Erheblichkeitsschwelle des § 42b Abs. 2a öUrhG jedenfalls überschritten.

Das Berufungsgericht bestätigte das Urteil des Erstgerichts.

Aus den Gründen

10 Die Revision ist ... nicht berechtigt.

1. Rechtlicher Rahmen:

11 1.1. Die RL 2001/29/EG ... (InfoRL) gibt den Mitgliedstaaten, soweit hier relevant, den folgenden rechtlichen Rahmen vor:

12 Die Mitgliedstaaten sehen für die Urheber in Bezug auf ihre Werke das ausschließliche Recht vor, die unmittelbare oder mittelbare, vorübergehende oder dauerhafte Vervielfältigung auf jede Art und Weise und in jeder Form ganz oder teilweise zu erlauben oder zu verbieten („Vervielfältigungsrecht“, Art. 2 lit. a InfoRL).

13 Die Mitgliedstaaten können in bestimmten Fällen Ausnahmen vom Vervielfältigungsrecht oder Beschränkungen des Vervielfältigungsrechts vorsehen. ...

14 1.2. Der EuGH legt die Vorgaben der InfoRL, wie sich aus einer vom Berufungsgericht in dieser Sache erwirkten Vorabentscheidung ergibt, wie folgt aus (C-433/20 [= MMR 2022, 647] – Austro-Mechana/Strato):

15 Der Ausdruck „Vervielfältigungen auf beliebigen Trägern“ (Art. 5 Abs. 2 lit. b InfoRL) umfasst (auch) die Erstellung von Sicherungskopien urheberrechtlich geschützter Werke zu priva-

ten Zwecken auf einem Server, auf dem der Anbieter von Cloud-Computing-Dienstleistungen einem Nutzer Speicherplatz zur Verfügung stellt ...

16 Eine nationale Regelung, nach der die Anbieter von Dienstleistungen der Speicherung iRd Cloud-Computing keinen gerechten Ausgleich für Sicherungskopien leisten müssen, die natürliche Personen, die diese Dienste nutzen, ohne Erlaubnis von urheberrechtlich geschützten Werken zum privaten Gebrauch und weder für direkte oder indirekte kommerzielle Zwecke erstellen, ist unter der Voraussetzung zulässig, dass sie – gemeint erkennbar: Auf andere Weise als durch eine Leistung der Anbieter – einen gerechten Ausgleich an die Rechtsinhaber vorsieht ...

17 Der EuGH betont auch den Grundsatz der Technologieneutralität des Urheberrechtsschutzes in der EU: Dieser dürfe im Zuge der technologischen Entwicklung und durch das Aufkommen neuer Formen der Verwertung urheberrechtlich geschützter Inhalte nicht veraltet oder obsolet werden ...

18 Das Unionsrecht stellt es dem nationalen Gesetzgeber somit frei, Ausnahmen vom Vervielfältigungsrecht der Urheber in Bezug auf ihre Werke (Art. 2 lit. a InfoRL) für Fälle vorzusehen, in denen natürliche Personen zum privaten Gebrauch und weder für direkte oder indirekte kommerzielle Zwecke Sicherungskopien urheberrechtlich geschützter Werke auf von Dritten bereitgestellten Cloud-Speichern erstellen und die Urheber – von wem und auf welche Weise immer – einen gerechten Ausgleich erhalten. ...

24 1.4. Kern des Revisionsverfahrens ist die Frage, ob der von der Bkl. angebotene Speicherplatz zum Abspeichern digitaler Inhalte in einer Cloud zum eigenen oder privaten Gebrauch ein „Speichermedium“ ist, das im Inland „gewerbsmäßig in Verkehr gekommen“ ist (§ 42b Abs. 1 öUrhG). Bejahendenfalls hat die Bkl. als diejenige, die das Speichermedium von einer im In- oder im Ausland gelegenen Stelle aus als erste gewerbsmäßig in Verkehr gebracht hat, eine Speichermedienvergütung zu leisten (§ 42b Abs. 3 Nr. 1 öUrhG), soweit nicht nach den Umständen erwartet werden kann, dass den Urhebern durch die Vervielfältigung in der Cloud zum eigenen oder privaten Gebrauch nur ein geringfügiger Nachteil entsteht (§ 42b Abs. 2a öUrhG).

2. Meinungsstand in der Literatur:

25 2.1. Vor der Entscheidung C-433/20, Austro-Mechana/Strato [= MMR 2026, 647], wurden zu im Revisionsverfahren zu klärenden Frage unterschiedliche Ansichten vertreten: ...

28 2.2. Die nach der Entscheidung C-433/20, Austro-Mechana/Strato, veröffentlichte Lit. geht weit überwiegend davon aus, dass das Anbieten von Speicherplatz in einer Cloud eine Verpflichtung zur Leistung einer Speichermedienvergütung auslöst (vgl. zB Fischer MR 2024, 265; Forgó/Škorjanc KuR 2022, 172; Homar in: Thiele/Burgstaller, öUrhG, 4. Aufl., § 42b Rn. 25; Schmitt/Stauderger jUS 2022/41, 98; Walter MR 2022, 87).

29 Eine Pflicht des Cloud-Anbieters zur Leistung einer Speichermedienvergütung wird aber auch weiterhin verneint (vgl. zB Zeemann eCollex 2022/328, 474).

3. Richtlinienkonforme Auslegung der österreichischen Bestimmungen:

30 3.1. Die innerstaatlichen Behörden haben inhaltlich von einer Richtlinie berührte Normen – nach dem Methodenkatalog des nationalen Rechts (4 Ob 124/18s, Punkt 7.3 = RS0114158 (T8); 9 ObA 11/22s, Rn. 43) – so weit wie möglich im Einklang mit der Richtlinie („richtlinienkonform“) auszulegen (RS0111214). Sie haben sich an Wortlaut und Zweck der Richtlinie zu orientieren und Rechtsbegriffe, die in der Richtlinie und im innerstaatlichen Recht übereinstimmen, entsprechend dem unionsrechtlichen Verständnis („autonom“) auszulegen (RS0075866, (auch T10)).

31 Die richtlinienkonforme Interpretation darf aber nicht dazu führen, dass der normative Gehalt der nationalen Regelungen grundlegend geändert wird (RS0111214 (T20); vgl. RS0114158). Sie darf einer nach Wortlaut und Sinn eindeutigen nationalen Regelung keine durch die nationalen Auslegungsregeln nicht erzielbaren abweichenden oder gar entgegengesetzten Sinn geben (RS0114158 (T7)). Sie kann nur insoweit erfolgen, als das nationale Recht dem Rechtsanwender einen Spielraum lässt (RS0114158 (T5)). Die Pflicht zur richtlinienkonformen Interpretation reicht somit grds. nur bis zur Grenze der äußersten Wortlautschränke, erstreckt sich aber zudem auf die nach dem innerstaatlichen interpretativen Methodenkatalog zulässige Rechtsfortbildung durch Analogie oder teleologische Reduktion im Fall einer planwidrigen Umsetzungslücke (RS0114158 (T8); 3 Ob 216/21t Rn. 63; 4 Ob 199/22a Rn. 23).

32 Kurz gefasst: Richtlinienkonforme Interpretation der nationalen Rechtsvorschriften ist geboten, soweit sie nicht zu einer Auslegung contra legem führen würde (vgl. RS0114158 (T9); 3 Ob 216/21t Rn. 63).

33 3.2. Aus der Anwendung dieser Auslegungsgrundsätze auf § 42 Abs. 4 öUrhG iVm § 42 Abs. 1 öUrhG folgt:

34 § 42 Abs. 4 öUrhG iVm § 42 Abs. 1 öUrhG erfasst einzelne Vervielfältigungsstücke auf anderen „Trägern“ als Papier oder einem ähnlichen „Träger“. Die auf die InfoRL zurückgehende nationale Bestimmung verwendet denselben Begriff wie Art. 5 Abs. 2 lit. b InfoRL, der auf Vervielfältigungen auf beliebigen „Trägern“ abstellt. Der Begriff „Träger“ ist daher entsprechend dem unionsrechtlichen Verständnis („autonom“) auszulegen. Das ist jenes des EuGH, nach dem der Begriff „Träger“ auch Server umfasst, auf dem der Anbieter von Cloud-Computing-Dienstleistungen einem Nutzer Speicherplatz zur Verfügung stellt. Die freie Werknutzung nach § 42 Abs. 4 öUrhG iVm § 42 Abs. 1 öUrhG – also die Ausnahme vom Vervielfältigungsrecht der Urheber (Art. 2 lit. a InfoRL) für einzelne von natürlichen Personen zum privaten Gebrauch und weder für unmittelbare noch mittelbare gewerbliche Zwecke hergestellte Vervielfältigungsstücke – umfasst damit (auch) das Abspeichern urheberrechtlich geschützter Inhalte in einer Cloud.

35 3.3. Ausgehend davon führt die Anwendung der eingangs dargelegten Auslegungsgrundsätze auf § 42b Abs. 1, Abs. 2a und Abs. 3 Nr. 1 öUrhG zu dem Ergebnis, das bereits die Vorinstanzen erzielt haben:

36 Nach den Vorgaben der InfoRL in der Auslegung des EuGH hat der österreichische Gesetzgeber dafür zu sorgen, dass die Urheber für das Abspeichern urheberrechtlich geschützter Inhalte in einer Cloud einen gerechten Ausgleich erhalten – von wem und auf welche Weise immer. Entgegen der Ansicht der Bekl. können § 42b Abs. 1 und Abs. 3 Nr. 1 öUrhG so ausgelegt werden, dass den unionsrechtlichen Vorgaben entsprochen wird, ohne dass dadurch einer nach Wortlaut und Sinn eindeutigen Regelung ein durch die nationalen Auslegungsregeln nicht erzielbarer abweichender oder gar entgegengesetzter Sinn gegeben würde.

37 Die moderne Alltagssprache versteht „Medien“ allgemein als Kommunikationsmittel und -konzepte, ohne Beschränkung auf „physische Träger“ (iÜ umfasst gerade der Begriff „Träger“ nach der Rspr. des EuGH auch Speicherplatz in einer Cloud). Speicherplatz in einer Cloud überschreitet vor diesem Hintergrund zumindest nicht die äußerste Wortlautschränke der Wendung „Speichermedien jeder Art, die für solche Vervielfältigungen geeignet sind“ (§ 42b Abs. 1 öUrhG). Der Fachsenat sieht auch keine Anhaltspunkte dafür, dass das gewerbsmäßige Zurverfügungstellen von Speicherplatz in einer Cloud in im Ausland gelegenen Rechenzentren und das Einräumen einer Zugriffsmöglichkeit an Kunden im Inland den äußersten Wortsinn der Wendung „im Inland gewerbsmäßig in Verkehr kommen“ (§ 42b Abs. 1 öUrhG)

überschreiten würde (zumal er in einem anderen Zusammenhang auch bereits ausgesprochen hat, dass das „Inverkehrbringen“ die Einräumung der tatsächlichen oder rechtlichen Verfügungsmacht ist (RS0076899). Zudem kommt das grenzüberschreitende Anbieten von Speicherplatz in einer Cloud funktional und wirtschaftlich betrachtet der Einräumung „physischer Verfügungsmacht“ an „physischen Trägern“ gleich (ähnlich Homar in: Thiele/Burgstaller, UrhG, 4. Aufl., § 42b Rn. 25). Dass auch das Inverkehrbringen im Inland von einer „im Ausland“ gelegenen Stelle die Verpflichtung zur Leistung einer Speichermedienvergütung auslöst, ordnet das Gesetz an (§ 42b Abs. 3 Nr. 1 öUrhG).

38 Dieses Ergebnis ist nach den nationalen Auslegungsregeln auch insofern ohne Weiteres zu erzielen, als ihm weder die Gesetzessystematik noch ein in den Gesetzesmaterialien erklärter Wille des Gesetzgebers so klar widersprechen würden, dass eine richtlinienkonforme Auslegung nicht in Betracht käme. Insb. ist den Gesetzesmaterialien zu den fraglichen Normen kein Hinweis darauf zu entnehmen, dass „Speichermedien jeder Art“ auf „physische Träger“ und „in Verkehr kommen“ auf die Einräumung „physischer Verfügungsgewalt“ beschränkt wäre.

39 Der Zweck der Norm – nämlich einen Ausgleich für bestimmte Ausnahmen vom Vervielfältigungsrecht des Urhebers zu schaffen, unabhängig von der Art des Speichermediums –, stützt sogar das durch die richtlinienkonforme Interpretation erzielte Ergebnis.

40 3.4. Zusammengefasst kommt der Fachsenat in richtlinienkonformer Auslegung von § 42 Abs. 4 öUrhG iVm §§ 42 Abs. 1 und 42b Abs. 1 und Abs. 3 Nr. 1 öUrhG zum Ergebnis, dass derjenige, der als erster Kunden im Inland gewerbsmäßig Speicherplatz in einer Cloud in im Inland oder Ausland gelegenen Rechenzentren zur Verfügung stellt, dafür eine Speichermedienvergütung zu leisten hat – soweit nicht nach den Umständen erwartet werden kann, dass den Urhebern durch das Abspeichern in der Cloud nur ein geringfügiger Nachteil entsteht (§ 42b Abs. 2a öUrhG). Letzteres ist hier, wie noch zu zeigen sein wird (vgl. unten 5. [= Rn. 43]) nicht der Fall. ...

43 5. Angesichts des vom Erstgericht festgestellten Umfangs der Speicherung relevanter Inhalte in der Cloud der Bekl. gibt es auch keine Anhaltspunkte dafür, dass eine nur geringfügige Beeinträchtigung der Interessen der Urheber (§ 42b Abs. 2a öUrhG) vorläge. ...

BGH: Dateiformat PDF als zwingendes Recht

Formmangel

ZPO § 130a Abs. 1, Abs. 2, Abs. 6, 130d S. 1, 294, 522 Abs. 1 S. 2; ERVV § 2 Abs. 1 S. 1
Urteil vom 10.2.2026 – VI ZR 313/24 (LG Oldenburg, AG Varel)

Leitsatz

Bei der Regelung in § 2 Abs. 1 S. 1 ERVV, wonach das elektronische Dokument im Dateiformat pdf zu übermitteln ist, handelt es sich um zwingendes Recht. Bei führender elektronischer Akte ist eine docx-Datei ein nicht formwirksam eingereichtes Dokument (im Anschluss an BAGE 178, 343 Rn. 12, 43 ff. (zu § 46c Abs. 2 ArbGG); BVerwG NVwZ 2023, 1823 Rn. 2 f., 8 ff. (zu § 55a Abs. 2 VwGO); BFHE 2024, 834 Rn. 1, 3 ff. (zu § 52a Abs. 2 FGO)).

Anm. d. Red.: Vgl. ferner BAG MMR 2023, 160 (Ls.); BGH MMR 2022, 670 und BAG MMR 2024, 39.

Schlagworte: Elektronischer Rechtsverkehr; Dateiformat; Heilung von Formmängeln; Unzulässigkeit der Berufung; Zugang zu den Gerichten

Sachverhalt

Der Kl. nimmt nach einem Verkehrsunfall die Bekl. als Gesamtschuldner auf Schadensersatz in Anspruch. Das AG hat die Bekl. ausgehend von einer Haftungsquote von 2/3 des Kl. und 1/3 der Bekl. als Gesamtschuldner zur Zahlung verurteilt und die Klage iÜ abgewiesen.

Die Bekl. haben gegen das Urteil des AG form- und fristgerecht Berufung eingelegt. Im Berufungsverfahren ist die Gerichtsakte elektronisch geführt worden. Einen Tag vor Ablauf der Frist für die Berufungsbegründung hat der Prozessbevollmächtigte der Bekl. eine Berufungsbegründung auf dem sicheren Übermittlungsweg aus seinem besonderen elektronischen Anwaltspostfach im Dateiformat docx eingereicht. Die Klägervertreterin hat mit Schriftsatz v. 23.10.2023 mitgeteilt, dass es sich bei der übermittelten Datei um ein docx-Dokument handle und dass die nicht formgemäß eingereichte Berufungsbegründung daher als nicht eingereicht anzusehen sein dürfte. Am 30.10.2023 ist die Übersendung dieses Schriftsatzes an den Beklagtenvertreter „mit der Bitte um Kenntnisnahme“ verfügt worden. Mit Schriftsatz v. 2.11.2023 hat der Beklagtenvertreter eine Berufungsbegründung im Dateiformat pdf eingereicht.

Mit dem hier angegriffenen Urteil hat das Berufungsgericht ausgehend von einer Haftungsquote von 80% des Kl. und 20% der Bekl. das Urteil des AG abgeändert, die Bekl. in geringerem Umfang zur Zahlung verurteilt und die Klage in weitergehendem Umfang abgewiesen. Mit seiner vom Berufungsgericht zugelassenen Revision beantragt der Kl., die Berufung der Bekl. als unzulässig zu verwerfen.

Aus den Gründen

8 I. Das Berufungsgericht hat ausgeführt, der Zulässigkeit der Berufung stehe nicht entgegen, dass die Berufungsbegründung zunächst als Datei im Format docx eingereicht und erst nach Ablauf der Berufungsbegründungsfrist im zulässigen pdf-Format übermittelt worden sei. Der Formmangel sei rückwirkend gem. § 130a Abs. 6 S. 2 ZPO geheilt worden. ...

9 II. Die ... Revision des Kl. ist begründet. Entgegen der Auffassung des Berufungsgerichts ist die Berufung der Bekl. unzulässig (§ 522 Abs. 1 S. 2 ZPO). Die Berufungsbegründung ist innerhalb der Frist nicht formgerecht eingereicht worden.

10 1. Die nach § 520 Abs. 3 S. 1 ZPO in einem Schriftsatz bei dem Berufungsgericht einzureichende Berufungsbegründung ist gem. § 130d S. 1 ZPO als elektronisches Dokument zu übermitteln.

11 Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet sein (§ 130a Abs. 1, Abs. 2 S. 1 ZPO). Die technischen Rahmenbedingungen für die Eignung zur Bearbeitung durch das Gericht bestimmt auf Grundlage des § 130a Abs. 2 S. 2 Hs. 1 ZPO die VO über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV). Nach § 2 Abs. 1 S. 1 ERVV ist das elektronische Dokument im Dateiformat pdf zu übermitteln.

12 Diese Vorschriften sind nach Wortlaut, Systematik und Zweck eindeutig. Danach handelt es sich bei der Regelung in § 2 Abs. 1 S. 1 ERVV, wonach das elektronische Dokument im Dateiformat pdf zu übermitteln ist, um zwingendes Recht. Dies ergibt sich auch aus der Gesetzesbegründung (vgl. ungeachtet der missverständlichen und teilweise in sich widersprüchlichen Erwägungen BT-Drs. 19/28399, 33 insb. BT-Drs. 19/28399, 40: „Zwingend ist danach nur noch die Übermittlung im Format pdf.“; Bader NZA 2023, 403 f.; s. weiter BVerfG [K] Beschl. v. 16.2.2023 – 1 BvR 1881/21 Rn. 17; zur alten Rechtslage etwa BAG Beschl. v. 1.8.2022 – 2 AZB 6/22 Rn. 10 ff.). Deshalb ist

eine docx-Datei ein nicht formwirksam eingereichtes Dokument (vgl. BAG Ur. v. 25.8.2022 – 6 AZR 499/21 [= MMR 2023, 160 (Ls.)] Rn. 12, 43 ff. (zu § 46c Abs. 2 ArbGG); BVerwG Beschl. v. 4.10.2022 – 20 F 15/22 Rn. 2 f., 8 ff. (zu § 55a Abs. 2 VwGO)). Dies gilt jedenfalls bei führender elektronischer Akte (vgl. BFH Beschl. v. 30.8.2024 – V R 1/24 Rn. 1, 3 ff. (zu § 52a Abs. 2 FGO); s. weiter Senat Beschl. v. 8.3.2022 – VI ZB 25/20 [= MMR 2022, 670] Rn. 15; BeckOK BVerfGG/ Fritzsche, 20. Ed. 1.1. 2026, BVerfGG § 23a Rn. 7 ff.). Abweichendes ist nur für den Fall angenommen worden, dass das Dokument trotzdem für die Bearbeitung durch das Gericht geeignet ist, weil die Papierakte führt, der Schriftsatz druckbar ist und ausgedruckt zur Papierakte genommen wird (vgl. BAG Beschl. v. 29.6.2023 – 3 AZB 3/23 [= MMR 2024, 39] Rn. 11 ff. (zu § 46c Abs. 2 ArbGG); BSG Ur. v. 13.5.2025 – B 12 BA 13/23 Rn. 4, 18 (zu § 65a Abs. 2 SGG); s. weiter Müller NZA 2023, 89 (90 f.); Bader NZA 2023, 403 (406 f.)). Auch der Beschl. des BGH v. 19.10.2022 – 1 StR 262/22 ((zu § 32a Abs. 2 StPO)) betrifft ein Revisionsverfahren mit führender Papierakte (vgl. dazu BFH Beschl. v. 30.8.2024 – V R 1/24 Rn. 10).

13 Danach haben die Bekl. – im Verfahren mit führender elektronischer Akte – die Berufungsbegründung als Dokument im Format docx nicht formwirksam eingereicht.

14 2. Dieser Mangel ist auch nicht geheilt worden. Die später als Dokument im Format pdf eingereichte Berufungsbegründung gilt nicht nach § 130a Abs. 6 S. 2 ZPO als bereits zu dem Zeitpunkt eingegangen, in dem das Dokument zuvor im Format docx eingegangen ist.

15 a) Ist ein elektronisches Dokument für das Gericht zur Bearbeitung nicht geeignet, ist dies dem Absender unter Hinweis auf die Unwirksamkeit des Eingangs unverzüglich mitzuteilen (§ 130a Abs. 6 S. 1 ZPO). Gem. § 130a Abs. 6 S. 2 ZPO gilt das Dokument als zum Zeitpunkt der früheren Einreichung eingegangen, sofern der Absender es unverzüglich in einer für das Gericht zur Bearbeitung geeigneten Form nachreicht und glaubhaft macht, dass es mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt.

16 b) Die Voraussetzungen des § 130a Abs. 6 S. 2 ZPO liegen nicht vor. ...

21 cc) Die Bekl. haben jedenfalls nicht unverzüglich glaubhaft gemacht (§ 294 ZPO), dass die als Dokument im Format pdf nachgereichte Berufungsbegründung mit dem zuerst eingereichten Dokument inhaltlich übereinstimmt.

22 (1) Entgegen der Auffassung der Revisionserwiderung ist eine Glaubhaftmachung nicht entbehrlich, weil es dem Gericht „unproblematisch möglich war zu erkennen, dass der Inhalt der beiden elektronischen Dokumente völlig identisch war.“ Vielmehr handelt es sich bei dem Erfordernis der Glaubhaftmachung um eine unverzichtbare Tatbestandsvoraussetzung, die auch nicht einschränkend auszulegen ist (vgl. BAG Ur. v. 25.8.2022 – 6 AZR 499/21 [= MMR 2023, 160 (Ls.)] Rn. 52 ff., insb. in Abgrenzung zur Wiedereinsetzung; s. weiter etwa BAG Beschl. v. 25.4.2022 – 3 AZB 2/22 Rn. 4, 27, 47 ff.; Ur. v. 3.6.2020 – 3 AZR 730/19 Rn. 30, 35, 37 (jew. zu § 46c Abs. 2 ArbGG)). Es kann hier offenbleiben, ob „für die Fälle, in denen der Inhalt der Schriftsätze von allen Beteiligten mit einem kurzen Blick erfasst werden kann, etwa bei der bloßen Einlegung eines Rechtsmittels ohne jeden Ansatz einer Begründung“, die Entbehrlichkeit der Glaubhaftmachung in Betracht kommt (vgl. BAG Ur. v. 25.8.2022 – 6 AZR 499/21 [= MMR 2023, 160 (Ls.)] Rn. 57 (zu § 46c Abs. 2 ArbGG)). Denn ein solcher Fall liegt hier nicht vor. Die nachgereichte Berufungsbegründung ist drei Seiten lang und muss den Anforderungen des § 520 Abs. 3 S. 2 ZPO genügen.

23 (2) Der im Schriftsatz v. 2.11.2023 enthaltenen Erklärung des Beklagtenvertreters, dass „die Berufungsbegründung vorsorglich nochmals als pdf-Datei übersandt“ werde, kann lediglich noch hinreichend deutlich entnommen werden, dass das zunächst eingereichte und das nachgereichte Dokument einen identischen Inhalt haben (sollen). Allerdings fehlt es an der darüber hinaus erforderlichen Glaubhaftmachung der Identität. Zwar kann dafür eine anwaltliche Versicherung ausreichen (vgl. BAG Beschl. v. 25.4.2022 – 3 AZB 2/22 Rn. 4, 27, 47 ff.; Urt. v. 3.6.2020 – 3 AZR 730/19 Rn. 30, 35, 37 (jew. zu § 46c Abs. 2 ArbGG)). Dafür hätte es jedoch einer Versicherung der Richtigkeit der vorgetragenen Angaben unter Bezugnahme auf die anwaltlichen Standespflichten bedurft. Allein der schriftsätzliche Vortrag relevanter Umstände genügt grds. nicht (vgl. Senat Beschl. v. 20.9.2022 – VI ZB 27/22 Rn. 9; BGH Beschl. v. 11.4.2024 – IX ZB 22/23 Rn. 9 mwN; BAG Beschl. v. 25.4.2022 – 3 AZB 2/22 Rn. 47 ff.).

24 In weiteren Schriftsätzen hat der Beklagtenvertreter ausgeführt, dass nach seiner Auffassung eine Glaubhaftmachung der inhaltlichen Übereinstimmung gerade nicht erforderlich sei, da diese Übereinstimmung ganz offensichtlich vorgelegen habe. Aus der Einreichung ergebe sich insoweit, dass lediglich das Format abgeändert worden sei. Die Datei sei nicht abgeändert worden. Dieser Umstand sei aufgrund des kurzen Schriftsatzes auch ohne Weiteres erkennbar gewesen. Damit hat er ausdrücklich erklärt, nicht glaubhaft machen zu wollen, dass der Inhalt der Dokumente identisch ist.

25 (3) Entgegen der Auffassung des Berufungsgerichts ist den Anforderungen an die Glaubhaftmachung nicht deshalb genügt, weil dem Berufungsgericht der Abgleich der zunächst eingereichten und einsehbaren Datei im Format docx und der nachgereichten Datei im Format pdf möglich geworden ist. Richtig ist zwar der Hinweis des Berufungsgerichts auf die Gesetzesmaterialien, wonach durch die Vorlage eines Papierausdrucks der Inhalt eines nicht bearbeitungsfähigen Dokuments und die Übereinstimmung mit dem nachträglich im richtigen Format eingereichten Dokument glaubhaft gemacht werden kann (vgl. BT-Drs. 17/12634, 26). Daraus ergibt sich aber nicht, dass es für die Glaubhaftmachung ausreicht, wenn das Gericht von Amts wegen prüfen kann, ob sich die zuerst eingereichte Datei für einen solchen Vergleich eignet, und abgleicht, ob der Inhalt der Dokumente identisch ist. Denn dies widerspräche im praktischen Ergebnis nicht nur der gesetzlichen Regelung, wonach die Glaubhaftmachung zwingend ist (s. oben II.2.b.cc.1.). Auch könnte ein solcher Abgleich nur auf Grundlage von technischen Voraussetzungen erfolgen, die für die Arbeit der Gerichte und ihre technische Infrastruktur gerade nicht maßgeblich sind (vgl. dazu BAG Urt. v. 25.8.2022 – 6 AZR 499/21 [= MMR 2023, 160 (Ls.)] Rn. 45; BVerwG Beschl. v. 4.10.2022 – 20 F 15/22 Rn. 10; BFH Beschl. v. 30.8.2024 – V R 1/24 Rn. 1). Daher ist unerheblich, welche technischen Möglichkeiten dem Gericht zur Verfügung stehen oder es sich verschaffen könnte, um eine Datei in einem unzulässigen Format auszuwerten. Weiter ist unerheblich, ob und mit welchem Ergebnis das Gericht einen solchen Abgleich von sich aus vornimmt. Der Absender einer Datei in einem unzulässigen Format kann nicht davon ausgehen, dass sich das Gericht weiter von sich aus damit befasst. Abweichendes ergibt sich daher auch nicht aus dem Hinweis der Revisionserwiderung, dass aktenkundige Tatsachen nicht der Glaubhaftmachung bedürften. Denn das Dokument in einer Datei mit einem unzulässigen Format ist aufgrund der gesetzlichen Vorgaben ebenso wenig aktenkundig wie seine inhaltliche Identität mit einem später eingereichten Aktenbestandteil.

26 3. Durch die formellen Anforderungen, elektronische Dokumente im Dateiformat pdf einreichen zu müssen, und die Sank-

tion, formatfehlerhafte elektronische Dokumente als nicht eingereicht anzusehen, wenn sie nicht auf gerichtlichen Hinweis unverzüglich formgerecht nachgereicht werden und die Übereinstimmung beider Dokumente glaubhaft gemacht wird, wird der Zugang zu den Gerichten für den Rechtsuchenden nach der zu respektierenden Einschätzung des Gesetzgebers nicht unverhältnismäßig erschwert (vgl. BAG Urt. v. 25.8.2022 – 6 AZR 499/21 [= MMR 2023, 160 (Ls.)] Rn. 54; BFH Beschl. v. 30.8.2024 – V R 1/24 Rn. 11 ff.; s. weiter BVerfG [K] Beschl. v. 28.10.2024 – 1 BvR 1996/24). ...

BGH: Teleologische Reduktion des § 1 Abs. 1 Nr. 1 FernUSG

Online-Coaching

FernUSG §§ 1 Abs. 1 Nr. 1, 7 Abs. 1, 12 Abs. 1; BGB § 138 Abs. 1, Abs. 2, 305 ff.

Urteil vom 5.2.2026 – III ZR 137/25 (OLG Oldenburg, LG Osnabrück)

Leitsatz

§ 1 Abs. 1 Nr. 1 FernUSG ist im Wege einer teleologischen Reduktion dahingehend auszulegen, dass der Lehrende und der Lernende als räumlich getrennt anzusehen sind, soweit die Wissensvermittlung über eine physische Distanz und dabei nicht mittels einer bidirektionalen – synchronen – Kommunikation erfolgt, bei der dem Lernenden – wie bei Präsenzveranstaltungen – die Möglichkeit eröffnet ist, ohne besondere Anstrengung Kontakt mit dem Lehrenden aufzunehmen.

Anm. d. Red.: Der Volltext ist abrufbar unter: [BeckRS 2026, 2337](#). Vgl. hierzu auch BGH MMR 2026, 538 (Ls.) und BGH MMR 2026, 538 (Ls.) – beide in diesem Heft. Vgl. ferner BGH MMR 1998, 603; OLG München MMR 2025, 213; OLG Stuttgart MMR 2025, 212; BGH MMR 2025, 725 mAnm Diesler/Klickermann; BGH MMR 2025, 1006 (Ls.); AG Traunstein MMR 2024, 815; Faix MMR 2023, 821; Mertens MMR 2024, 656; OLG Köln MMR 2024, 254 mAnm Demeshko und OLG Celle MMR 2023, 864.

Schlagworte: Fernunterrichtsvertrag; Online-Unterricht; Online-Coaching; räumliche Trennung; teleologische Reduktion; Lernplattform; Videocalls; sekundäre Darlegungslast

Sachverhalt

Die Bekl. bietet auf der von ihr betriebenen Internetplattform sog. Online-Coachings zu verschiedenen Themen an. Die Kl. nimmt die Bekl. auf Rückzahlung von Vergütung für ein solches Coaching und Feststellung der Nichtigkeit des zugrunde liegenden Vertrags in Anspruch. Die Parteien schlossen im Dezember 2022 einen Vertrag über die Teilnahme der Kl. am „F. Trainingsprogramm“ zu einem Preis von 8.092 EUR brutto. Der Vertrag beinhaltete verschiedene Leistungen, insb. Zugänge zu einer Lernplattform mit Videos, zu einer Messenger-Gruppe und zu Video-Calls mit einem Coach sowie die Möglichkeit zur Teilnahme an regelmäßig stattfindenden Videokonferenzen (Live-Calls). Über eine Zulassung für Fernlehrgänge gem. § 12 FernUSG verfügte die Bekl. nicht. Die Kl. hat geltend gemacht, der Vertrag sei nichtig, weil es an der erforderlichen Zulassung nach dem FernUSG fehle. Zudem sei er nach § 138 Abs. 1 BGB nichtig, weil ein auffälliges Missverhältnis von Leistung und Gegenleistung bestehe. Die Klage hat in den Vorinstanzen keinen Erfolg gehabt. Mit der zugelassenen Revision verfolgt die Kl. ihr Klagebegehren weiter.

Aus den Gründen

5 Die Revision hat Erfolg. Sie führt zur Aufhebung des angefochtenen Urteils und zur Zurückverweisung der Sache an das Berufungsgericht.

6 I. Das Berufungsgericht hat zur Begründung seiner Entscheidung im Wesentlichen ausgeführt:

7 Der zwischen den Parteien geschlossene Vertrag über die Teilnahme der Kl. an dem „FBA Unstoppable E-commerce Trainingsprogramm“ sei nicht gem. § 7 Abs. 1 FernUSG nichtig, weil dieses Trainingsprogramm keiner Zulassung gem. § 12 FernUSG bedürfte. Bei dem Trainingsprogramm handele es sich nicht um Fernunterricht gem. § 1 Abs. 1 FernUSG, weil zum einen eine Überwachung des Lernerfolgs nicht geschuldet gewesen sei. Allein die der Selbstkontrolle dienende Möglichkeit des Fragestellens an den Lehrenden könne nicht das Tatbestandsmerkmal der Erfolgsüberwachung erfüllen. Zum anderen könne nicht festgestellt werden, dass der Lehrende und der Lernende ausschließlich oder überwiegend räumlich getrennt gewesen seien.

8 Die Frage, wann von einer räumlichen Trennung auszugehen sei, werde in der Rspr. der Oberlandesgerichte nicht einheitlich beantwortet. Der Berufungssenat schließe sich der Auffassung an, wonach eine räumliche Trennung nur dann vorliege, wenn der Unterricht zu mind. 50% asynchron stattfinde. Der synchrone Online-Unterricht stehe einer Präsenzveranstaltung gleich, weil jederzeit eine Kontaktaufnahme mit der Lehrperson möglich sei. Der Aufenthalt an verschiedenen Orten begründe in diesem Fall nicht die vom Gesetzgeber als nachteilig angesehene räumliche Trennung.

9 Nach dem Ergebnis der versehentlich nicht protokollierten Anhörung der Kl. könne nicht festgestellt werden, dass der Unterricht zu mehr als 50% asynchron stattgefunden habe. ...

10 Dass die Wissensvermittlung zu mind. 50% durch die Lernvideos, also asynchron, hätte erfolgen sollen, lasse sich nicht feststellen. Nach den Angaben der Kl. könne nicht ausgeschlossen werden, dass die Dauer der Live-Calls und der Einzelgespräche diejenige der Lernvideos leicht überstiegen habe, sodass die Wissensvermittlung überwiegend synchron stattgefunden habe.

11 Der Vertrag sei auch nicht nach § 138 Abs. 1 BGB nichtig. Die Kl. habe nicht ausreichend zur Sittenwidrigkeit vorgetragen. Entgegen ihrer Auffassung sei der konkrete Coaching-Markt zum Vergleich mit der vereinbarten Vergütung heranzuziehen. Ob vergleichbare Lernvideos deutlich günstiger erworben werden könnten, sei unerheblich, weil diese Videos nur einen Teil der vereinbarten vertraglichen Leistung ausmachten. Soweit die Kl. behauptete, die Gruppen-Live-Calls hätten keinen qualifizierten Unterricht geboten und Rückfragen seien oft nicht zureichend beantwortet worden, beanstandete sie ein Zurückbleiben der tatsächlichen hinter der geschuldeten Leistung, womit ein auffälliges Missverhältnis von Leistung und Gegenleistung nicht zu begründen sei.

12 II. Dies hält der rechtlichen Nachprüfung nicht in allen Punkten stand.

13 1. Rechtsfehlerfrei allerdings hat das Berufungsgericht angenommen, dass der in Rede stehende Vertrag zwischen den Parteien nicht gem. § 138 Abs. 1 BGB nichtig ist.

14 a) Ein Rechtsgeschäft ist nach § 138 Abs. 1 BGB nichtig, wenn es nach seinem aus der Zusammenfassung von Inhalt, Beweggrund und Zweck zu entnehmenden Gesamtcharakter mit den guten Sitten nicht zu vereinbaren ist. Gegenseitige Verträge können hiernach als wucherähnliche Rechtsgeschäfte sittenwidrig sein, auch wenn der Wuchertatbestand in § 138 Abs. 2 BGB nicht in allen Voraussetzungen erfüllt ist. Dafür muss zwischen Leistung und Gegenleistung objektiv ein auffälliges Missverhältnis bestehen und außerdem mind. ein weiterer Umstand hinzukommen, der den Vertrag bei Zusammenfassung der subjektiven und objektiven Merkmale als sittenwidrig erscheinen lässt (BGH Urt. v. 16.11.2022 – VIII ZR 436/21 Rn. 31 f., mwN).

15 Für die Feststellung eines (auffälligen) Missverhältnisses von Leistung und Gegenleistung kommt es auf die objektiven Werte der Leistungen im Zeitpunkt des Vertragsschlusses an. Die gegenseitigen Leistungen sind nach den vertraglichen Vereinbarungen zu bemessen und nicht danach, was die Parteien sich nachfolgend einander gewährt haben (BGH Urt. v. 21.4.2022 – I ZR 214/20 Rn. 27 und v. 16.11.2022, aaO Rn. 34, jew. mwN). Entscheidend ist der Marktwert, also der marktübliche Preis (BGH Urt. v. 10.11.2016 – IX ZR 119/14 Rn. 18 und v. 23.2.2018 – V ZR 302/16 Rn. 22, jew. mwN; vgl. auch BGH Urt. v. 29.11.2011 – XI ZR 220/10 Rn. 23). Mit Hilfe eines Marktvergleichs lässt sich grds. das verkehrssübliche und wirtschaftlich noch tragbare Entgelt als Vergleichsmaßstab für den auf eine Sittenwidrigkeit zu untersuchenden Austauschvertrag ermitteln (Senat Urt. v. 2.7.1998 – III ZR 287/97 [= MMR 1998, 603]; vgl. auch Senat Urt. v. 12.3.1981 – III ZR 92/79, sowie BGH Urt. v. 16.11.2022, aaO). Das vereinbarte Entgelt ist dabei dem marktüblichen Preis, den die Mehrzahl der übrigen Anbieter für vergleichbare Leistungen fordert, gegenüberzustellen (BGH Urt. v. 29.11.2011, aaO, mwN).

16 b) Danach hat das Berufungsgericht entgegen der Auffassung der Revision zu Recht auch im Streitfall einen Marktvergleich als erforderlich angesehen, um den objektiven Wert der von der Bekl. zu erbringenden Coaching-Leistungen zu bestimmen. Selbst wenn – wie von der Kl. behauptet – der Coaching-Markt insgesamt von „horrenden Preisen“ geprägt sein sollte, ändert dies nichts daran, dass es einen marktüblichen Preis gibt. Seine bloße Höhe vermag es nicht zu rechtfertigen, einen Coaching-Vertrag unabhängig von einem nach Maßgabe der Marktverhältnisse festzustellenden auffälligen Missverhältnis von Leistung und Gegenleistung und einer – im Einzelfall auch nur daraus zu vermutenden – verwerflichen Gesinnung des Anbieters als sittenwidrig zu qualifizieren (vgl. BGH Urt. v. 29.11.2011, aaO zum Darlehensvertrag).

17 c) Daran anknüpfend ist nicht zu beanstanden, dass das Berufungsgericht das Vorbringen der Kl. zur Sittenwidrigkeit für nicht ausreichend erachtet hat. Ohne Erfolg rügt die Revision, das Berufungsgericht habe insoweit Sachvortrag der Kl. samt Beweisangebot übergangen. Die Kl. habe zur Darlegung des auffälligen Missverhältnisses von Leistung und Gegenleistung auf den objektiven Wert der Leistung der Bekl. abgestellt, der sich allenfalls auf einen „Marktwert“ von unter 1.000 EUR belaufe. Sie habe ein Angebot vorgelegt, wonach vergleichbares Videomaterial für 14,99 EUR erworben werden könne, und zur Ermittlung des objektiven Werts zudem die Einholung eines Sachverständigengutachtens beantragt.

18 Gemessen an den oben wiedergegebenen Grundsätzen hat das Berufungsgericht diesem Vorbringen zu Recht keine ausreichende Darlegung eines auffälligen Missverhältnisses von Leistung und Gegenleistung entnommen. Die Bekl. hat unter Verweis auf andere Coaching-Verträge und unter Hinweis auf die Marktsituation das Vorliegen eines derartigen Missverhältnisses bestritten. Ungeachtet der Verwendung des Begriffs „Marktwert“ lässt sich dem Klägervortrag demgegenüber nicht einmal die Behauptung entnehmen, dass die zwischen den Parteien vereinbarte Vergütung für die von der Bekl. (insgesamt) zu erbringenden Leistungen überhaupt vom marktüblichen Preis, den die Mehrzahl der übrigen Anbieter für vergleichbare Leistungen fordert, abweicht. Vielmehr hat die Kl. in den Vorinstanzen die Auffassung vertreten und an der als übergangen gerügten Stelle der Berufungsbegründung auch ausdrücklich ausgeführt, der „konkrete Coaching-Markt“ stelle keine taugliche Vergleichsgrundlage dar, weil er von horrenden Preisen geprägt sei. Sie ist demnach erkennbar selbst davon ausgegangen, dass unter Heranziehung des marktüblichen Preises als Vergleichs-

maßstab kein auffälliges Missverhältnis von Leistung und Gegenleistung besteht. Dies gilt umso mehr, als sie zum marktüblichen (Gesamt-)Preis der von der Bekl. geschuldeten Coaching-Leistungen – wie es für den anzustellenden Marktvergleich erforderlich gewesen wäre – keinen Vortrag gehalten hat. ...

20 2. Von Rechtsfehlern beeinflusst ist hingegen die Annahme des Berufungsgerichts, der zwischen den Parteien geschlossene Vertrag über die Teilnahme der Kl. an dem „FBA Unstoppable E-commerce Trainingsprogramm“ sei nicht gem. § 7 Abs. 1 FernUSG nichtig, weil es sich bei diesem Trainingsprogramm nicht um Fernunterricht gem. § 1 Abs. 1 FernUSG gehandelt und es deshalb keiner Zulassung nach § 12 Abs. 1 FernUSG bedurft habe. Gem. § 1 Abs. 1 FernUSG ist Fernunterricht die auf vertraglicher Grundlage erfolgende, entgeltliche Vermittlung von Kenntnissen und Fähigkeiten, bei der der Lehrende und der Lernende ausschließlich oder überwiegend räumlich getrennt sind (Nr. 1) und der Lehrende oder sein Beauftragter den Lernerfolg überwachen (Nr. 2). Nach dem bisherigen Sachstand ist nicht auszuschließen, dass das Trainingsprogramm diese Voraussetzungen erfüllt.

21 a) Mit der Begründung des Berufungsgerichts lässt sich eine mind. überwiegend räumliche Trennung des Lehrenden und des Lernenden nicht verneinen.

22 aa) Im Ausgangspunkt ist das Berufungsgericht allerdings zutreffend davon ausgegangen, dass nicht bei jeder Wissensvermittlung per Online-Kommunikation eine räumliche Trennung iSv § 1 Abs. 1 Nr. 1 FernUSG gegeben ist (vgl. OLG München WRP 2024, 1260 [= MMR 2025, 213] Rn. 16; OLG Nürnberg WRP 2025, 114 Rn. 24 ff.; AG Traunstein MMR 2024, 815 Rn. 37 f.; Faix MMR 2023, 821 (824 f.); Laukemann/Förster WRP 2024, 24 Rn. 6, 32 f.; Mertens MMR 2024, 656 (657 f.); Schwab/Sablotny NJW 2024, 2802 Rn. 9 ff.; Vennemann, FernUSG, 2. Aufl., § 1 Rn. 10; aA OLG Celle NJW-RR 2025, 113 Rn. 24 ff.; OLG Oldenburg Urte. v. 17.12.2024 – 2 U 123/24 Rn. 7; OLG Stuttgart Urte. v. 4.2.2025 – 6 U 46/24 Rn. 69 ff.; OLG Dresden Urte. v. 30.4.2025 – 12 U 1547/24 Rn. 57 ff.). Zugabe ist der Revision und der von ihr befürworteten Gegenansicht zwar, dass § 1 Abs. 1 Nr. 1 FernUSG nach seinem Wortlaut keine über den Aufenthalt des Lehrenden und des Lernenden in getrennten Räumen hinausgehenden Anforderungen an Fernunterricht stellt. Die Norm ist jedoch im Wege einer teleologischen Reduktion dahingehend auszulegen, dass der Lehrende und der Lernende als räumlich getrennt anzusehen sind, soweit die Wissensvermittlung über eine physische Distanz und dabei nicht mittels einer bidirektionalen – synchronen – Kommunikation erfolgt, bei der dem Lernenden – wie bei Präsenzveranstaltungen – die Möglichkeit eröffnet ist, ohne besondere Anstrengung Kontakt mit dem Lehrenden aufzunehmen.

23 (1) Eine richterliche Rechtsfortbildung im Wege der teleologischen Reduktion, die zu den anerkannten Auslegungsmethoden zählt (vgl. zB BVerfG ZIP 2012, 911 Rn. 57), kommt in Betracht, wenn der Wortlaut der Vorschrift mit Blick auf ihren Normzweck zu weit gefasst ist (BGH Beschl. v. 11.2.2025 – KZR 74/23 Rn. 16; vgl. Beschl. v. 29.11.2013 – BLw 4/12 Rn. 23; s.a. BVerfG ZIP 1997, 1167 (1168)). Sie setzt eine verdeckte Regelungslücke iSe planwidrigen Unvollständigkeit des Gesetzes voraus. Ob eine derartige Lücke besteht, ist vom Standpunkt des Gesetzes und der ihm zugrunde liegenden Regelungsabsicht zu beurteilen. Das Gesetz muss, gemessen an seiner eigenen Regelungsabsicht, unvollständig sein (BGH Urte. v. 7.4.2021 – VIII ZR 49/19 Rn. 36 und v. 21.2.2022 – VIa ZR 8/21 Rn. 57; Beschl. v. 4.9.2024 – IV ZB 37/23 Rn. 19).

24 (2) Diese Voraussetzung ist hinsichtlich § 1 Abs. 1 Nr. 1 FernUSG und des Tatbestandsmerkmals der (mind. überwiegenden)

„räumlichen Trennung“ erfüllt. Die Entstehungsgeschichte sowie Sinn und Zweck der Regelung gebieten mit Blick auf die – zum Zeitpunkt des Inkrafttretens des FernUSG noch nicht bestehende – Möglichkeit, auch bei physischer Distanz Kenntnisse und Fähigkeiten mittels einer bidirektionalen – synchronen – Kommunikation zu vermitteln, eine darauf bezogene einschränkende Auslegung der Norm.

25 Der Gesetzgeber wollte bei der Beschreibung des gesetzlichen Anwendungsbereichs in § 1 Abs. 1 FernUSG auf die „wesentlichen Merkmale des Fernunterrichts“ abstellen. Hierbei sollte das Merkmal der räumlichen Trennung den Fernunterricht von „herkömmlichem Unterricht“ (auch bezeichnet als „Nahunterricht“ oder „Direktunterricht“) abgrenzen, während das Merkmal der Lernerfolgsüberwachung der Abgrenzung von der bloßen Lieferung von Lehrmaterial dienen sollte (vgl. RegE des Fernunterrichtsschutzgesetzes, BT-Drs. 7/4245, 14).

26 Direktunterricht ist dadurch gekennzeichnet, dass die Wissensvermittlung zu einem bestimmten vorgegebenen Zeitpunkt im Wege der direkten Kommunikation zwischen dem Lehrenden und dem oder den Lernenden erfolgt. Das Wesen des Fernunterrichts liegt demgegenüber darin, dass der Lernende sich den Stoff anhand von vom Lehrenden zur Verfügung gestellter Materialien bei freier Zeiteinteilung selbst aneignet (vgl. RegE des FernUSG, aaO, S. 11, 14; VG München NVwZ-RR 1989, 473 (474); Bartl NJW 1976, 1993 (1994); Faix, aaO, S. 824; Laukemann/Förster, aaO Rn. 33). Die Unterscheidung zwischen den beiden Unterrichtsarten ließ sich nach dem Stand der Technik bei Erlass des Gesetzes treffend mit dem Merkmal der „räumlichen Trennung“ erfassen. Der RegE des FernUSG (BT-Drs., aaO) datiert auf den 3.11.1975, das Gesetz wurde am 24.8.1976 verkündet (BGBl I 1976, 2525). Seinerzeit war es technisch noch nicht möglich, über das Internet virtuelle Treffen zu organisieren; die Entwicklung dieser Technologie war für den Gesetzgeber auch nicht absehbar (vgl. AG Traunstein, aaO Rn. 41; Mertens, aaO, S. 657; Schwab/Sablotny, aaO Rn. 9, 12). Demgegenüber kann das Merkmal der „räumlichen Trennung“ nach seinem Zweck aufgrund der heute vorhandenen technischen Möglichkeiten die vom Gesetzgeber intendierte Abgrenzungsfunktion zum klassischen Direktunterricht inzwischen nur dann erfüllen, wenn man – dem Wesen des Fernunterrichts entsprechend – zusätzlich verlangt, dass die Darbietung des Unterrichts und dessen Abruf durch den Lernenden zeitlich versetzt (asynchron) erfolgt oder sich dem Lernenden aus anderen Gründen keine Gelegenheit zum unmittelbaren Austausch mit dem Lehrenden bietet. Andernfalls würde Online-Unterricht zur Anwendung des FernUSG führen, obgleich er in seinen wesentlichen Merkmalen der Lernform des Direktunterrichts entspricht. Dies ist der Fall, wenn der Lehrende und der Lernende in Echtzeit interagieren können, dh iSe bidirektionalen Kommunikation ein unmittelbarer Austausch zwischen beiden möglich ist (vgl. OLG Nürnberg, aaO Rn. 25; Faix, aaO, S. 824; Laukemann/Förster, aaO Rn. 33; Mertens, aaO, S. 657; Schwab/Sablotny, aaO Rn. 15).

27 Das auch von der Revision aufgegriffene Argument der Gegenansicht, die Notwendigkeit, die Teilnehmer von Online-Schulungen vor unseriösen Anbietern zu schützen, sei deutlich größer als bei echten Präsenzveranstaltungen (vgl. OLG Stuttgart WRP 2024, 1408 [= MMR 2025, 212] Rn. 16; OLG Celle, aaO Rn. 27), überzeugt in diesem Zusammenhang nicht. Dabei mag zweifelhaft sein, ob die Teilnehmer eines überwiegend synchron durchgeführten Online-Unterrichts insb. mit Blick auf die im Recht der AGB (§§ 305 ff. BGB) getroffenen – zumindest mittelbar auch für den unternehmerischen Geschäftsverkehr bedeutsamen (vgl. BGH Urte. v. 19.9.2007 – VIII ZR 141/06 Rn. 12) – Regelungen bereits ausreichend geschützt sind (vgl. Positionspapier des Nationalen Normenkontrollrats zum FernUSG vom

6.11.2025, www.normenkontrollrat.bund.de/Webs/NKR/SharedDocs/Downloads/DE/Positionspapiere/2025-11_fernunterrichtsschutzgesetz.html?nn=145276, (abgerufen am 5.2.2026)). Die zur Begründung eines erhöhten Schutzbedürfnisses angeführten – verbliebenen – Unterschiede zum Präsenzunterricht in Bezug auf den organisatorischen Aufwand, die Teilnehmerakquise sowie den persönlichen Kontakt zwischen dem Lehrenden und dem Lernenden ändern nichts daran, dass die Wissensvermittlung in einem synchronen Online-Unterricht, bei dem auch der Lernende ohne besondere Anstrengung Kontakt mit dem Lehrenden aufnehmen kann, „direkt“ und nicht anhand zur Verfügung gestellter Materialien im Selbststudium stattfindet. „Direktunterricht“ ist nach dem gegenstandsbezogenen Schutzkonzept (vgl. Senat Ur. v. 12.6.2025 – III ZR 109/24 [= MMR 2025, 72 mAnm Diesler/Klickermann] Rn. 39) vom FernUSG aber gerade nicht erfasst.

28 Entgegen der Auffassung der Revision führt es zu keiner anderen Beurteilung, dass der Gesetzgeber ausweislich der Begründung des Regierungsentwurfs des FernUSG (aaO, S. 14) die Möglichkeit gesehen hat, dass Unterricht in einen anderen Raum übertragen werden kann. Daraus kann nicht der Wille des Gesetzgebers abgeleitet werden, den Anwendungsbereich dieses Gesetzes auch für Unterrichtsformen zu eröffnen, die ihm aufgrund des damaligen Stands der Technik unbekannt waren und die wesentlichen Merkmale des seinerzeit „herkömmlichen Unterrichts“ erfüllen (aa OLG Celle, aaO; OLG Stuttgart, aaO; OLG Dresden, aaO Rn. 58 ff.). Die in dem RegE als Beispiel für eine (unerhebliche) Überbrückung einer räumlichen Trennung genannte Tonübertragung ist mit den heute vorhandenen Möglichkeiten synchroner bidirektionaler Kommunikation nicht gleichzusetzen.

29 Ebenso wenig steht der teleologischen Reduktion der Norm entgegen, dass der Gesetzgeber das FernUSG in der Vergangenheit mehrfach geändert hat, ohne das Merkmal der „räumlichen Trennung“ aufzugeben oder den aktuellen Gegebenheiten anzupassen (aa OLG Oldenburg, aaO). Es gibt keine Anhaltspunkte dafür, dass dem Gesetzgeber die hier in Rede stehende Abgrenzungsproblematik vor Augen gestanden und er sich insoweit durch Beibehaltung des Wortlauts bewusst für eine Erstreckung des Anwendungsbereichs dieses Gesetzes auch auf synchronen Online-Unterricht entschieden hat.

30 bb) Das Berufungsgericht hat jedoch nicht beachtet, dass es für die Frage, ob es bei einer vertraglich vereinbarten Dienstleistung um Fernunterricht iSv § 1 Abs. 1 FernUSG handelt, auf den Vertragsinhalt ankommt (vgl. Senat Ur. v. 12.6.2025 – III ZR 109/24 [= MMR 2025, 72 mAnm Diesler/Klickermann] Rn. 24 und v. 2.10.2025 – III ZR 173/24 [= MMR 2025, 1006 (Ls.)] Rn. 10 ff.).

31 (1) Das Berufungsgericht hat darauf abgestellt, wie der Unterricht tatsächlich „stattgefunden hat“. Es hat eine Gewichtung der asynchronen und synchronen Unterrichtsteile anhand der Dauer der abrufbaren Lernvideos einerseits sowie der Dauer der durchgeführten Live-Calls und Einzelgespräche andererseits vorgenommen, wie sie sich im Wesentlichen aus den Angaben der Kl. in der mündlichen Verhandlung ergeben haben. Die tatsächliche Gestaltung des Unterrichts ist aber ebenso unerheblich wie der Umfang der von dem Lernenden in Anspruch genommenen Leistungen (vgl. Senat, aaO).

32 (2) Es ist auch nicht ersichtlich, dass die von der Kl. beschriebenen Leistungen nach Art und Umfang den vereinbarungsgemäß von der Bekl. zu erbringenden Leistungen entsprochen hätten. Nach den bislang getroffenen Feststellungen steht zwischen den Parteien vielmehr nicht im Streit, dass der Vertrag über die Teilnahme an dem in Rede stehenden Trainingsprogramm neben dem Zugang zu Lernvideos, zu Video-

Calls mit einem Coach sowie zu regelmäßig stattfindenden Videokonferenzen weitere Leistungen beinhaltet. So hat die Bekl. etwa eine „Vertragsbestätigung“ vorgelegt, in der unter der Überschrift „Produkt“ zehn verschiedene Leistungen schlagwortartig aufgelistet sind, welche die Kl. „als Mitglied von F. „erhalte“.

33 (3) Eine eigene Vertragsauslegung durch den Senat kommt vorliegend nicht in Betracht (vgl. dazu Senat Ur. v. 12.6.2025 [= MMR 2025, 72 mAnm Diesler/Klickermann] Rn. 22 und v. 2.10.2025 – III ZR 173/24 [= MMR 2025, 1006 (Ls.)] Rn. 12). Es fehlt dafür an einer tragfähigen Tatsachengrundlage. Das Berufungsgericht hat in Bezug auf die rechtsgeschäftliche Einigung der Parteien keine hinreichenden Feststellungen getroffen. Dies gilt auch mit Blick auf die o.g. Vertragsbestätigung. Der darin enthaltene Leistungskatalog gibt, wenn er denn den zuvor getroffenen vertraglichen Abreden entspricht, iÜ den Vertragsinhalt nach dem bisherigen Sachstand bereits deshalb nicht vollständig wieder, weil er sich nicht zu den Lernvideos verhält, die nach den Feststellungen des Berufungsgerichts aber ein (wesentlicher) Bestandteil des vereinbarten Trainingsprogramms gewesen sind.

34 b) Mit der Begründung des Berufungsgerichts lässt sich schließlich nicht verneinen, dass eine Überwachung des Lernerfolgs iSv § 1 Abs. 1 Nr. 2 FernUSG stattfindet. Dieses Tatbestandsmerkmal ist erfüllt, wenn dem Teilnehmer ein auf das eigene Verständnis des erlernten Stoffs bezogenes Fragerecht vertraglich eingeräumt ist, wodurch er eine persönliche Lernkontrolle herbeiführen und überprüfen kann, ob er die vermittelten Inhalte zutreffend erfasst hat und richtig anwenden kann (Ur. v. 12.6.2025 [= MMR 2025, 72 mAnm Diesler/Klickermann] Rn. 28 und v. 2.10.2025 – III ZR 173/24 [= MMR 2025, 1006 (Ls.)] Rn. 18). Der vom Berufungsgericht darüber hinaus verlangten „Kontrolle durch den Lehrenden oder seinen Beauftragten“ bedarf es nicht.

35 III. Eine Vorlage an das BVerfG nach Art. 100 Abs. 1 S. 1 GG iVm § 80 BVerfGG ist entgegen der Auffassung der Revisionserwiderung nicht veranlasst. Der Senat ist nicht mit der für eine Vorlage erforderlichen Sicherheit von der Verfassungswidrigkeit des in § 12 FernUSG statuierten Zulassungserfordernisses und der in § 7 Abs. 1 FernUSG angeordneten Nichtigkeit eines Fernunterrichtsvertrags, der von einem Veranstalter ohne entsprechende Zulassung des Fernlehrgangs geschlossen wird, überzeugt (Senat Ur. v. 5.2.2026 – III ZR 74/25).

36 IV. Das Berufungsurteil ist danach aufzuheben (§ 562 Abs. 1 ZPO). Da weitere Feststellungen zu treffen sind, kann der Senat in der Sache nicht selbst entscheiden (§ 563 Abs. 1 S. 1, Abs. 3 ZPO). Für das weitere Verfahren weist er auf Folgendes hin:

37 1. Ob der Lehrende und der Lernende bei der Wissensvermittlung gem. § 1 Abs. 1 Nr. 1 FernUSG nach dem dargestellten Maßstab (s.o. II.2.a.aa. [= Rn. 22]) mindestens überwiegend (räumlich) getrennt sind, hängt von den konkreten Umständen des Einzelfalls ab. Die Würdigung dieser Umstände obliegt grds. dem Tatrichter. Mögliche Anknüpfungspunkte sind bei – wie hier – verschiedenen Unterrichtsleistungen etwa Inhalt und Bedeutung der Teilleistungen für den angestrebten Lernerfolg oder die jeweilige Dauer der nach dem Vertrag vorgesehenen Lerneinheiten (vgl. Senat Ur. v. 12.6.2025 [= MMR 2025, 72 mAnm Diesler/Klickermann] Rn. 26 und v. 2.10.2025 – III ZR 173/24 [= MMR 2025, 1006 (Ls.)] Rn. 16; Faix, aaO, S. 824 f.; Mertens, aaO, S. 657 f). Aufzeichnungen von synchronen Unterrichtsteilen, die nach der getroffenen Vereinbarung den Teilnehmern anschließend zum Abruf zur Verfügung gestellt werden, sind dabei als asynchroner Unterricht zu behandeln (vgl. Senat Ur. v. 12.6.2025 [= MMR 2025, 72 mAnm Diesler/Klickermann]).

38 2. Darlegungs- und beweislasterlastet für die tatbestandlichen Voraussetzungen des § 1 Abs. 1 FernUSG ist nach allgemeinen Grundsätzen derjenige, der sich auf die Anwendbarkeit des FernUSG beruft. Er trägt demnach auch die Darlegungs- und Beweislast dafür, dass der Lehrende und der Lernende bei der Wissensvermittlung iSv § 1 Abs. 1 Nr. 1 FernUSG ausschließlich oder überwiegend räumlich getrennt sind. Die teleologische Reduktion der Vorschrift hat darauf keinen Einfluss, obwohl sie zu einer Einschränkung des nach dem Wortlaut eröffneten Anwendungsbereichs des FernUSG führt.

39 Derjenige, der eine Ausnahme geltend macht, hat deren Voraussetzungen darzulegen und zu beweisen, sofern sich aus dem Gesetz – ausdrücklich oder durch Auslegung – ergibt, dass eine Rechtsfolge für den Regelfall als angemessen bewertet wird (vgl. BGH Urt. v. 13.5.2022 – V ZR 7/21 Rn. 25; s.a. BGH Urt. v. 30.6.2009 – VI ZR 310/08 Rn. 9 ff.) ... Eine entsprechende Wertung ist dem FernUSG in Bezug auf § 1 Abs. 1 [FernUSG] und das Tatbestandsmerkmal der „räumlichen Trennung“ schon deshalb nicht zu entnehmen, weil dem Gesetzgeber seinerzeit, wie ausgeführt (s.o. II.2.a.aa. (2) [= Rn. 24]), die heute vorhandenen technischen Möglichkeiten sowie die damit zusammenhängende Vergleichbarkeit von klassischem Direktunterricht und synchronem Distanzunterricht mittels bidirektionaler Kommunikation unbekannt waren. Die vom Gesetzgeber ursprünglich intendierte Abgrenzungsfunktion von § 1 Abs. 1 FernUSG zum klassischen Direktunterricht spricht insoweit sogar dafür, diese Form des Distanzunterrichts bereits nicht als Ausnahme-tatbestand aufzufassen.

40 3. Nach dem bisherigen Sachstand sind in Bezug auf die Frage der räumlichen Trennung auch die Voraussetzungen einer sekundären Darlegungslast der Bekl. nicht gegeben. Wie ausgeführt (s.o. II.2.a.bb. [= Rn. 30]), ist darauf abzustellen, wie der Lehrende den Lehrstoff nach dem Vertragsinhalt anzubieten hat. Den bislang vom Berufungsgericht getroffenen Feststellungen lässt sich nicht entnehmen, dass der Kl., wie es für die Annahme einer sekundären Darlegungslast erforderlich wäre (vgl. zB Senat Urt. v. 9.6.2022 – III ZR 24/21 Rn. 36), substantiierter Vortrag zum Inhalt des zwischen den Parteien geschlossenen Vertrags unmöglich oder unzumutbar ist. ...

Anmerkung

**RA Florian Stoffel/RA Alexander Diesler, LL.M./
RA Dr. Paul H. Klickermann, FA Urheber- und
Medienrecht, Kläner Rechtsanwälte, Koblenz**

Im hier thematisierten Sachverhalt begehrte die Kl. die Rückstattung von Vergütungen für ein Online-Coaching sowie die Feststellung der Nichtigkeit des zugrunde liegenden Vertrags. Der BGH widmete sich der Frage, inwieweit das FernUSG auf Online-Coaching-Verträge Anwendung findet.

Bei der Beantwortung dieser Frage liegt bereits die zentrale Besonderheit darin, dass das FernUSG aus dem Jahr 1976 stammt, also aus einer Zeit, in der die technische Entwicklung virtueller Echtzeit-Kommunikation für den Gesetzgeber nicht absehbar war. Zielsetzung des Gesetzesentwurfs aus dem Jahre 1975 war der Schutz der Fernunterrichtsteilnehmer vor unseriösen Angeboten und nachteiligen Vertragsgestaltungen. Der Gesetzgeber wollte einheitliche Regelungen schaffen, um dem Fernunterricht eine größere Anerkennung sowie Verbreitung zu verschaffen (BT-Drs. 7/4245 v. 3.11.75) und positiv auf das Qualitätsniveau hinzuwirken. Bei Entstehung des Gesetzes war Fernunterricht dergestalt bekannt, dass kein klassischer Direktunterricht vor Ort stattfand, sondern den Lernenden Fernlernmaterialien an die Hand gegeben wurden, damit diese sich den Stoff anhand der Materialien bei freier Zeiteinteilung selbst aneignen konnten.

Über die Corona-Pandemie und die in diesem Kontext bestehenden Einschränkungen sowie die verstärkte Implementierung von Online-Meetings und Remote-Work im Alltags- und Geschäftsleben entwickelte sich ein immer stärker digitalisierter Markt für Online-Dienstleistungen, so auch für Coachings. Lange war es still um das FernUSG und das Gesetz führte eher ein Schattendasein. Im Kontext des wachsenden Angebots und der Transformation der Coaching- und Beratungsbranche in den Online-Bereich kam es in den letzten Jahren jedoch zu einer Vielzahl gerichtlicher Entscheidungen. Besonders nach den Entscheidungen des OLG Köln (MMR 2024, 254 mAnm Demeshko) sowie des OLG Celle (MMR 2023, 864) zeigte sich die Rspr. uneinheitlich.

1. Zulassung nach FernUSG

Zentraler Anknüpfungspunkt zivilrechtlicher Rückforderungsverlangen ist die gesetzliche Vorgabe, wonach Fernlehrgänge nach § 12 Abs. 1 FernUSG einer Zulassung bedürfen. Fehlt diese, führt dies zwingend zur Nichtigkeit des Vertrags gem. § 7 Abs. 1 FernUSG. Regelmäßig verfügen die Anbieter von Online-Coachings nicht über diese Zulassung, so auch hier. Die Streitigkeiten drehten sich deshalb insb. um die Frage der Anwendbarkeit des FernUSG.

Gem. § 1 Abs. 1 FernUSG liegt Fernunterricht vor, wenn auf vertraglicher Grundlage entgeltlich Kenntnisse vermittelt werden, Lehrender und Lernender ausschließlich oder überwiegend räumlich getrennt sind (Nr. 1) und der Lernerfolg überwacht wird (Nr. 2). Nahezu sämtliche dieser gesetzlich genannten Voraussetzungen waren in der Folge Gegenstand verschiedener gerichtlicher Entscheidungen. Zudem war es überaus strittig, ob das Gesetz ggü. Unternehmern überhaupt anwendbar ist oder nur eine Verbraucherschützende Regelung darstellt.

Nach einer Entscheidung aus dem Jahre 2009 beschäftigte sich der BGH erst im Jahre 2025 erneut mit diesem Gesetz (MMR 2025, 725 mAnm Diesler/Klickermann; Urt. v. 2.10.2025 – III ZR 173/24 = MMR 2025, 1006 (Ls.)). Mit Urt. v. 12.6.2025 (MMR 2025, 725 mAnm Diesler/Klickermann) bestätigte der BGH die weite Interpretation des Merkmals einer Lernerfolgskontrolle und stellte klar, dass hierzu bereits eine auf das Verständnis des Stoffs bezogene Rückfragemöglichkeit ausreiche. Der BGH konnte aufgrund des dortigen Sachverhalts die Frage offenlassen, inwieweit bei einem Vertrag, in welchen jedenfalls auch Beratung und Begleitung erfolgt, eine Schwerpunkt-betrachtung durchzuführen wäre. Entscheidend für die Einordnung des Vertrags sei jedenfalls der Vertragsinhalt, nicht die tatsächliche Umsetzung. Zudem wurde klargestellt, dass der Anwendungsbereich des FernUSG nicht auf Verbrauchergeschäfte beschränkt ist.

2. Räumliche Trennung

Die sehr umstrittene Frage, wann eine räumliche Trennung anzunehmen ist und ob hier neben dem wörtlichen Verständnis auf das Merkmal der Synchronität abzustellen sei, konnte zunächst offengelassen werden. Der BGH wies jedoch bereits darauf hin, dass selbst synchrone Inhalte wie Livecalls dann als asynchron gelten, wenn diese vertragsgemäß aufgezeichnet und zum Abruf zur Verfügung gestellt werden. Gleichzeitig räumte der BGH den Anbietern nach Bereicherungsrecht die Möglichkeit eines Wertersatzanspruchs nach den Grundsätzen der Saldotheorie für bereits geleistete Dienste ein.

Es folgte ein weiteres Urt. v. 2.10.2025 (BGH Urt. v. 2.10.2025 – III ZR 173/24 = MMR 2025, 1006 (Ls.)). Darin bestätigte der BGH die zuvor getroffenen Wertungen, führte diese teilweise weiter aus und konnte wiederum die Frage offenlassen, wie

das Merkmal der überwiegenden räumlichen Trennung zu verstehen sei. Das Kuriosum war hier insgesamt, dass plötzlich eine Vielzahl an Verträgen einem Gesetz unterfallen sollten, das systematisch eigentlich gar nicht auf die betroffenen Verträge ausgelegt wurde, schlicht aufgrund der heutigen technischen Möglichkeiten.

3. Fokus digitales Zeitalter

Im Jahr 2026 kam es bereits zu mehreren Entscheidungen des BGH zum FernUSG, in denen sich der BGH mit verschiedenen Aspekten, u.a. auch der Verfassungsmäßigkeit, auseinandersetzen hatte (BGH MMR 2026, 538 (Ls.) und BGH MMR 2026, 538 (Ls.) – beide in diesem Heft). Der Senat betonte dabei, dass das in § 12 FernUSG statuierte Zulassungserfordernis sowie die in § 7 Abs. 1 FernUSG angeordnete Nichtigkeit nicht gegen die Berufsfreiheit (Art. 12 Abs. 1 GG) oder den Gleichheitssatz (Art. 3 Abs. 1 GG) verstoßen.

Im Urteil III ZR 137/25 positionierte sich der BGH nach anhaltender Unklarheit nun zu dem Merkmal der räumlichen Trennung. So wurde festgestellt, dass der Begriff nicht nur rein wörtlich zu verstehen ist. Neben einer örtlichen Distanz fordert der BGH im Wege einer teleologischen Reduktion, dass die Wissensvermittlung asynchron, also zeitlich versetzt und ohne die Möglichkeit einer synchronen Kommunikation erfolgt. Der BGH erkennt, dass das FernUSG gemessen an seiner Regelungsabsicht planwidrig unvollständig ist und führt aus, dass im Falle synchroner Kommunikationsmöglichkeiten in Echtzeit ohne besondere Anstrengung eine ggü. klassischem Präsenzunterricht gleichwertige Interaktion gegeben ist.

Der BGH katapultiert das FernUSG mit diesen Erwägungen in das digitale Zeitalter und sendet ein klares Signal an die gesamte Online-Dienstleistungsbranche. Zutreffend würdigt das Gericht die fundamental abweichenden Vorstellungen von Fernunterricht in den 1970er Jahren und heutigen Online-Angeboten. Ausgehend davon, dass der Gesetzgeber bei Schaffung des FernUSG die wesentlichen Gesichtspunkte von Fernunterricht in den Gesetzestext aufnehmen wollte, erscheint die Vornahme dieser teleologischen Reduktion angebracht. Der BGH setzt mit seiner zeitgemäßen Betrachtung genau an dem Punkt an, der Online-Coaching-Verträge regelmäßig in ihrer gesamten Charakteristik von der Situation eines Fernunterrichts unterscheiden wird. Gleichzeitig belässt er es weiterhin dabei, dass das FernUSG je nach Einzelfall auch im Online-Bereich angewendet werden kann, nämlich genau dann, wenn es an einer dem Präsenzunterricht gleichwertigen Kommunikation fehlt und die Ausgangslage dadurch mit dem Regelungszweck des FernUSG in Einklang zu bringen ist. Stellen sich hingegen die Sachverhalte – wie es bei vielen Coaching-Angeboten der Fall sein dürfte – fundamental anders als klassischer Fernunterricht dar und die Teilnehmenden haben gleichwertig eines Nah-/Direktunterrichts die Möglichkeit, mit dem Lehrenden in Kontakt zu treten, so entspricht es nur der heutzutage branchenübergreifenden Anerkennung von Online-Kommunikation als gleichwertiges Äquivalent zu physischer Kommunikation, hier am Merkmal der Synchronität anzusetzen.

Richtigerweise führt der BGH auch aus, dass das oftmals angeführte Argument, das FernUSG solle die Teilnehmenden vor unseriösen Anbietern schützen, hier eine Erweiterung auf synchronen Online-Unterricht nicht rechtfertigt.

Wichtig ist zu beachten, dass erneut und eindeutig klargestellt wurde, dass es für die Beurteilung der Kriterien, ob Fernunterricht iSd FernUSG vorliegt, einzig auf die vertragliche Vereinbarung ankommt. Zu denken ist hier zur Differenzierung an Inhalt und Bedeutung der Teilleistungen für den angestrebten Lerner-

folg oder die jeweilige Dauer der nach dem Vertrag vorgesehenen Lerneinheiten. Zudem ist zu betonen, dass die Darlegungs- und Beweislast für das Vorliegen der tatbestandlichen Voraussetzungen des FernUSG und explizit der räumlichen Trennung nach allgemeinen Grundsätzen derjenige trägt, der sich auf die Anwendbarkeit des FernUSG beruft. In der Praxis steht zu vermuten, dass bereits unter Klarstellung dieser Gesichtspunkte deutlicher zwischen berechtigten und unberechtigten Rückforderungsverlangen unterschieden wird.

Insgesamt ist hier besonders auffällig, dass der BGH bei den einzelnen Merkmalen, zu denen er sich in den verschiedenen Urteilen positioniert, stets eine Einzelfallbetrachtung vornimmt. Dieses Vorgehen ist zu begrüßen und zeigt, dass es eben nicht den einen Online-Coaching-Vertrag gibt. Das Urteil kann hier als Chance gesehen werden, einen Mittelweg zu schaffen zwischen zukunftsgerichteter Angebotslandschaft im Online-Segment und einem Paralleldasein des FernUSG für Verträge, in denen Fernunterricht iSd Norm vorliegt.

4. Nationaler Normenkontrollrat

Nicht unerwähnt sollte in diesem Gesamtkontext bleiben, dass sich nach den BGH-Urteilen aus dem Jahr 2025 zwischenzeitlich auch der Nationale Normenkontrollrat zum FernUSG äußerte. Ähnlich wie der BGH hier argumentierte, nahm auch der Normenkontrollrat die massive Diskrepanz zwischen der Situation bei Erlass des Gesetzes und den zwischenzeitlichen Auswirkungen auf den Online-Dienstleistungsbereich in den Blick. Der Normenkontrollrat bezeichnete das FernUSG als veraltet und nicht praxistauglich und empfahl mit Schreiben v. 6.11.2025, das FernUSG ersatzlos abzuschaffen.

Bis es so weit ist, hat der BGH mit dem hier abgebildeten Urteil jedenfalls den Weg für einzelfallgerechte und zeitgemäße Lösungen von Auseinandersetzungen, insb. im Bereich Online-Coaching oder -Beratung geebnet. Das Urteil birgt die Möglichkeit, dass sich der Markt für Online-Dienstleistungen im deutschen Raum weiterentwickeln kann und nicht durch das Korsett einer Regelung um Luft ringen muss, deren zugrundeliegende Erwägungen nunmehr über ein halbes Jahrhundert zurückliegen. Das FernUSG ist aus der Zeit gefallen. Der BGH hat dies erkannt und an entscheidender Stelle das Gesetz um das Merkmal der (A-)Synchronität ergänzt. Darin steckt ein klares Zeichen an die Branche, die in der nun gewonnen Gewissheit wieder positiver betreffend der Zukunftsfähigkeit zB von Online-Coachings gestimmt sein kann.

BGH: Lösungsfrist bei Zahlungsstörungen

Code of Conduct

DS-GVO Art. 5 Abs. 1, 6 Abs. 1 UAbs. 1 lit. f, 40, 82
Urteil vom 18.12.2025 – I ZR 97/25 (OLG Köln, LG Bonn)

Leitsätze

1. Die längstmögliche Speicherdauer von Daten über Zahlungsstörungen, die private Wirtschaftsauskunfteien durch Einmeldungen ihrer Vertragspartner sammeln, um sie zur Grundlage von Bonitätsbeurteilungen zu machen, wird nicht durch die Lösungsfrist von Eintragungen anderer Art über die jeweilige Forderung im öffentlichen Register – hier im Schuldnerverzeichnis – vorgegeben (Abgrenzung zu EuGH Urt. v. 7.12.2023 – C-26/22 und C-64/22 [= ZD 2024, 166 mAnm Schild Rn. 113] – SCHUFA Holding).

2. Verhaltensregeln iSv Art. 40 DS-GVO können im Interesse der Rechtssicherheit und auch mit Blick auf das von Wirtschaftsauskunfteien betriebene Massengeschäft als Orientierung für die nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO vorzunehmende Interessenabwägung herangezogen werden, soweit sie typisiert zu einem angemessenen Interessenausgleich führen – wie das bei der vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum 1.1.2025 genehmigten Ziffer IV.1. lit. b der Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien grundsätzlich der Fall ist – und die Besonderheiten des Einzelfalls bei der konkret vorzunehmenden Interessenabwägung hinreichend berücksichtigt werden (Abgrenzung zu EuGH Urt. v. 7.12.2023 – C-26/22, C-64/22 [= ZD 2024, 166 Rn. 104 f. mAnm Schild] – SCHUFA Holding).

Anm. d. Red.: Die Berufungsinstanz (OLG Köln) ist veröffentlicht in ZD 2025, 400 mAnm Söbbing/Schwarz. Vgl. ferner EuGH ZD 2024, 166 mAnm Schild – SCHUFA; EuGH MMR 2025, 266 mAnm Stief = ZD 2025, 267 mAnm Hanloser – Mousse; BGH MMR 2020, 106 mAnm Hoeren = ZD 2020, 109 mAnm Gräbig – Recht auf Vergessen II; EuGH MMR 2025, 950 mAnm Mekat/Ligocki = ZD 2025, 640 mAnm Mekat/Wellmann – Quirin Privatbank; OLG Brandenburg ZD 2023, 748; EuGH MMR 2025, 421 mAnm Hense/Niekrenz; LG Lübeck ZD 2025, 704 mAnm Söbbing/Schwarz; OLG Köln MMR 2025, 532 mAnm Claes/Jäger und Thiel ZD 2026, 61.

Schlagworte: Wirtschaftsauskunftei; Speicherungsdauer; Öffentliche Register; Berechtigtes Interesse; Code of Conduct

Sachverhalt

Die beklagte SCHUFA Holding AG betreibt eine Wirtschaftsauskunftei. Sie speicherte Daten über drei gegen den Kl. gerichtete unbestrittene Forderungen, und zwar erstens aus einer Rechnung v. 16.11.2018 iHv 150 EUR, titulierte durch Vollstreckungsbescheid und vom Kl. beglichen am 2.12.2020, zweitens aus einer Rechnung v. 31.1.2020 iHv 428,27 EUR, vom Gläubiger mehrfach angemahnt und vom Kl. beglichen am 4.11.2021, sowie drittens aus einer Rechnung v. 9.5.2021 iHv 160,99 EUR, titulierte durch Vollstreckungsbescheid und vom Kl. beglichen im Dezember 2022.

Vor dem LG hat der Kl. von der Bekl. zunächst Löschung der Einträge über die drei erledigten Forderungen und Ersatz immateriellen Schadens sowie vorgerichtlicher Rechtsverfolgungskosten begehrt. Nachdem die Bekl. den Eintrag über die am 2.12.2020 beglichene Forderung nach Ablauf von drei Jahren am 2.12.2023 gelöscht hatte, haben die Parteien den Rechtsstreit bzgl. des diesbezüglichen Lösungsanspruchs vor dem LG übereinstimmend für in der Hauptsache erledigt erklärt. Das LG hat die Klage abgewiesen.

Während des Berufungsverfahrens löschte die Bekl. am 4.11.2024 den Eintrag über die am 4.11.2021 beglichene Forderung sowie später auch den Eintrag über die im Dezember 2022 beglichene Forderung. Hintergrund für die Löschung der zuletzt genannten Forderung war die vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) zum 1.1.2025 genehmigte Ziffer IV.1. lit. b der Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien. Diese sieht – insoweit unverändert zur vorherigen Fassung – im Grundsatz eine Speicherung von personenbezogenen Daten über ausgeglichene Forderungen für drei Jahre vor (Satz 1). Nach der neuen Fassung endet die Speicherung jedoch abweichend davon bereits nach 18 Monaten (Satz 2), wenn 1. der Auskunftei bis zu diesem Zeitpunkt keine weiteren Negativdaten gemeldet worden sind, 2. keine Informationen aus dem Schuldnerverzeichnis oder aus Insolvenz-bekanntmachungen vorliegen und 3. der Ausgleich der Forderung innerhalb von 100 Tagen nach Einmeldung erfolgte.

Die Parteien haben danach den Rechtsstreit auch bzgl. der beiden in die Berufungsinstanz gelangten Lösungsbegehren

übereinstimmend für in der Hauptsache erledigt erklärt. In der Sache hat der Kl. von der Bekl. noch Zahlung immateriellen Schadensersatzes nach Ermessen des Gerichts, aber nicht unter 1.500 EUR, und außergerichtlicher Rechtsverfolgungskosten begehrt. Das Berufungsgericht hat die Bekl. zur Zahlung immateriellen Schadensersatzes von 500 EUR sowie außergerichtlicher Rechtsverfolgungskosten verurteilt (OLG Köln ZD 2025, 400 mAnm Söbbing/Schwarz).

Aus den Gründen

9 B. Die hiergegen gerichtete Revision der Bekl. hat Erfolg. Sie führt zur Aufhebung des Berufungsurteils und Zurückverweisung der Sache an das Berufungsgericht. ...

11 II. Mit der vom Berufungsgericht gegebenen Begründung kann die Unrechtmäßigkeit der Datenspeicherung durch die Bekl. nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO als Voraussetzung für einen Schadensersatzanspruch des Kl. aus Art. 82 Abs. 1 DS-GVO nicht bejaht werden. ...

13 Nach Art. 5 Abs. 1 lit. a DS-GVO sind personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten. ... Nach dem für den im Streitfall allein einschlägigen Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Somit 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, nicht überwiegen (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 75 – SCHUFA Holding (Restschuldbefreiung); NJW 2025, 807 [= MMR 2025, 266 mAnm Stief = ZD 2025, 267 mAnm Hanloser] Rn. 45 – Mousse; BGH Urt. v. 14.10.2025 – VI ZR 431/24 Rn. 34). ...

15 2. Wirtschaftsauskunfteien wie die der Bekl. werden zur Wahrung von berechtigten Interessen iSv Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO tätig. Von der Vorschrift erfasst wird ein weites Spektrum von Interessen, das nicht auf gesetzlich verankerte und bestimmte Interessen beschränkt ist (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 76 – SCHUFA Holding (Restschuldbefreiung); NJW 2025, 807 [= MMR 2025, 266 mAnm Stief = ZD 2025, 267 mAnm Hanloser] Rn. 46 – Mousse; BGH Urt. v. 14.10.2025 – VI ZR 431/24 Rn. 34).

16 a) Neben ihren eigenen wirtschaftlichen Interessen nehmen Wirtschaftsauskunfteien die berechtigten Interessen ihrer Kunden (insb. potenzieller Kreditgeber) wahr (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 82 f. – SCHUFA Holding (Restschuldbefreiung)). Die Analyse einer Wirtschaftsauskunftei kann insoweit, als sie eine objektive und zuverlässige Bewertung der Kreditwürdigkeit der potenziellen Kunden der Vertragspartner der Wirtschaftsauskunftei ermöglicht, Informationsunterschiede ausgleichen und damit Betrugsrisiken und andere Unsicherheiten verringern (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 93 – SCHUFA Holding (Restschuldbefreiung)).

17 b) Dass Kreditgeber Auskünfte zur Kreditwürdigkeit von Verbrauchern einholen dürfen, ist im europäischen Recht anerkannt (vgl. Art. 8 RL 2008/48/EG über Verbraucherkreditverträ-

ge, künftig Art. 18 f. RL (EU) 2023/2225 über Verbraucherkreditverträge; Art. 18 bis 21 RL 2014/17/EU über Wohnimmobilenkreditverträge für Verbraucher; EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 84 f. – SCHUFA Holding (Restschuldbefreiung)). Die Anforderungen an eine Kreditwürdigkeitsprüfung werden allerdings im nationalen Recht geregelt (vgl. EuGH Urt. v. 11.1.2024 – C-755/22 Rn. 22 – Nárókuj). Das deutsche Recht erkennt für Allgemein-Verbraucherdarlehensverträge in § 505b Abs. 1 BGB Kreditwürdigkeitsprüfungen bei Wirtschaftsauskunfteien ausdrücklich an. Eine solche Kreditwürdigkeitsprüfung soll auch verhindern, dass der Verbraucher Kreditverbindlichkeiten eingeht, die seine finanzielle Leistungsfähigkeit übersteigen (vgl. BeckOGK BGB/Knops, 15.11.2025, § 505b Rn. 2), und dient damit mittelbar dem Verbraucherschutz (vgl. auch Erwägungsgründe 54 f. RL (EU) 2023/2225). Auch über den Bereich von Verbraucherdarlehensverträgen hinaus liegen Kreditwürdigkeitsprüfungen zur Vermeidung von Zahlungsausfällen im gesamtwirtschaftlichen Interesse (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 86) – SCHUFA Holding (Restschuldbefreiung)).

18 3. Dem stehen gewichtige Interessen einer von dieser Datenspeicherung betroffenen Person wie dem Kl. ggü.

19 a) Die Verarbeitung von Daten über Zahlungsstörungen, wie etwa die Speicherung, Analyse und Weitergabe dieser Daten an einen Dritten durch eine Wirtschaftsauskunftei stellt einen schweren Eingriff in die Grundrechte der betroffenen Person nach Art. 7 (Achtung des Privat- und Familienlebens) und Art. 8 (Schutz personenbezogener Daten) GRCh dar. Solche Daten dienen nämlich als negativer Faktor bei der Beurteilung der Kreditwürdigkeit der betroffenen Person und stellen daher sensible Informationen über ihr Privatleben dar. Ihre Verarbeitung kann den Interessen der betroffenen Person beträchtlich schaden, da diese Weitergabe geeignet ist, die Ausübung ihrer Freiheiten erheblich zu erschweren, insb. wenn es darum geht, Grundbedürfnisse zu decken (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 94 – SCHUFA Holding (Restschuldbefreiung)).

20 b) Die Folgen für die Interessen und das Privatleben der betroffenen Person sind umso größer und die Anforderungen an die Rechtmäßigkeit der Speicherung dieser Informationen umso höher, je länger die fraglichen Daten durch Wirtschaftsauskunfteien gespeichert werden (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 95 – SCHUFA Holding (Restschuldbefreiung)).

21 4. Nach einer Prüfung, ob die Datenspeicherung der Bekl. zur Verwirklichung der von ihr wahrgenommenen berechtigten Interessen erforderlich ist, muss das Speicherungsinteresse der Bekl. mit dem Löschungsinteresse des Kl. abgewogen werden (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 77 bis 80 – SCHUFA Holding (Restschuldbefreiung)). Die Frage der Erforderlichkeit hat das Berufungsgericht nicht thematisiert. Seine Auffassung, das Löschungsinteresse überwiege stets bereits mit dem Ausgleich der jeweiligen Forderung, hält der rechtlichen Nachprüfung nicht stand.

22 a) In seinem Urteil „SCHUFA Holding (Restschuldbefreiung)“ [= ZD 2024, 166 mAnm Schild] hat der EuGH es als Sache des vorlegenden Gerichts angesehen zu beurteilen, ob bei der in den Ausgangsverfahren in Rede stehenden Verarbeitung personenbezogener Daten die Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO erfüllt sind. Der Gerichtshof hat dem vorlegenden Gericht – dort dem VG Wiesbaden – jedoch sachdienliche Hinweise für diese Prüfung gegeben (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 81). In diesem Rahmen hat der Gerichtshof entschieden, dass Art. 5 Abs. 1 lit. a

DS-GVO iVm Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO dahin auszulegen ist, dass er einer Praxis privater Wirtschaftsauskunfteien entgegensteht, die darin besteht, in ihren eigenen Datenbanken aus einem öffentlichen Register stammende Informationen über die Erteilung einer Restschuldbefreiung zugunsten natürlicher Personen zum Zweck der Lieferung von Auskünften über die Kreditwürdigkeit dieser Personen für einen Zeitraum zu speichern, der über die Speicherdauer der Daten im öffentlichen Register hinausgeht (EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 113 – SCHUFA Holding (Restschuldbefreiung)).

23 Die Löschungsfristen für Insolvenzbekanntmachungen, einer zentralen und länderübergreifenden Veröffentlichung im Internet iSv § 9 Abs. 1 InsO, sind in § 3 InsBekV geregelt. Nach § 3 Abs. 1 S. 1, Abs. 2 InsBekV werden Daten aus einem Insolvenzverfahren einschließlich des Eröffnungsverfahrens spätestens sechs Monate nach Rechtskraft der Entscheidung über die Restschuldbefreiung gelöscht.

24 b) Entgegen der Ansicht des Berufungsgerichts folgt aus dem o.g. Urteil des EuGH nicht, dass bei Daten über Zahlungsstörungen, die private Wirtschaftsauskunfteien aufgrund von Anmeldungen ihrer Vertragspartner speichern, um sie zur Grundlage von Bonitätsbeurteilungen zu machen, die längstmögliche Speicherdauer durch die Löschungsfrist von Eintragungen anderer Art über die jeweilige Forderung im öffentlichen Register – hier im Schuldnerverzeichnis – vorgegeben wird.

25 aa) Die Eintragung eines Schuldners ins Schuldnerverzeichnis ist vom Gerichtsvollzieher etwa dann nach § 882c Abs. 1 S. 1 ZPO von Amts wegen anzuordnen, wenn der Schuldner seiner Pflicht zur Abgabe der Vermögensauskunft nicht nachgekommen ist (Nr. 1) oder eine Vollstreckung nach dem Inhalt des Vermögensverzeichnisses offensichtlich nicht geeignet wäre, zu einer vollständigen Befriedigung des Gläubigers zu führen (Nr. 2). Die Pflicht zur Abgabe einer Vermögensauskunft entsteht nach einer nicht zur Befriedigung des Gläubigers führenden Zahlungsaufforderung durch den Gerichtsvollzieher (§ 802f Abs. 1 ZPO).

26 Die im Schuldnerverzeichnis gespeicherten Angaben bestehen aus persönlichen Daten des Schuldners (§ 882b Abs. 2 ZPO), dem Aktenzeichen und dem Gericht oder der Vollstreckungsbehörde der Vollstreckungssache (§ 882b Abs. 3 Nr. 1 ZPO) sowie – bei Eintragungen auf Anordnung des Gerichtsvollziehers – dem Datum der Eintragungsanordnung und dem gem. § 882c ZPO zur Eintragung führenden Grund (§ 882b Abs. 3 Nr. 2 ZPO).

27 Die Einsicht in das Schuldnerverzeichnis ist nach § 882f Abs. 1 ZPO jedem gestattet, der darlegt, für die nachfolgend genannten Zwecke Angaben nach § 882b ZPO zu benötigen, zB für die Zwangsvollstreckung (§ 882f Abs. 1 Nr. 1 ZPO) oder um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen (§ 882f Abs. 1 Nr. 4 ZPO).

28 Gem. § 882e Abs. 1 ZPO wird eine Eintragung im Schuldnerverzeichnis nach Ablauf von drei Jahren seit dem Tag der Eintragungsanordnung von dem zentralen Vollstreckungsgericht des betreffenden Lands gelöscht. Abweichend davon wird eine Eintragung auf Anordnung des zentralen Vollstreckungsgerichts gem. § 882e Abs. 3 Nr. 1 ZPO bereits dann gelöscht, wenn diesem die vollständige Befriedigung des Gläubigers nachgewiesen worden ist.

29 bb) Die Regelung des § 882e Abs. 3 Nr. 1 ZPO, die bei Nachweis der vollständigen Befriedigung des Gläubigers eine sofortige Löschung des Eintrags im Schuldnerverzeichnis über die be-

treffende Forderung anordnet, ist nicht auf die Speicherung von Daten über Zahlungsstörungen natürlicher Personen durch Wirtschaftsauskunfteien anzuwenden.

30 (1) Die vorliegend in Rede stehende Datenspeicherung der Bekl. unterscheidet sich bereits dadurch wesentlich von derjenigen im Vorlageverfahren an den EuGH, dass die Bekl. dort Daten aus dem öffentlichen Register – den Insolvenzbekanntmachungen – übernommen und parallel gespeichert hatte (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 25 f. – SCHUFA Holding (Restschuldbefreiung)), während sie hier nach den Feststellungen des Berufungsgerichts nicht Daten aus dem Schuldnerverzeichnis, sondern von ihren Vertragspartnern gemeldete Daten über Zahlungsstörungen gespeichert hat. Die Erwägung, dass die für die ursprüngliche Datenspeicherung geltende Lösungsfrist nicht durch eine längere Speicherung an anderer Stelle konterkariert werden soll (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 89, 97 und 99 – SCHUFA Holding (Restschuldbefreiung)), greift deshalb im Streitfall nicht. Es kann daher auch nicht ohne Weiteres von einer Verstärkung des Eingriffs in das Recht der Person auf Achtung des Privatlebens durch das Vorliegen derselben personenbezogenen Daten in mehreren Quellen ausgegangen werden (dazu vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 91 und 100 – SCHUFA Holding (Restschuldbefreiung)).

31 (2) Zwischen dem öffentlichen Schuldnerverzeichnis und der Datensammlung der Bekl. bestehen Gemeinsamkeiten, aber auch gewichtige Unterschiede.

32 (a) Im Ausgangspunkt kann die Einsichtnahme in das Schuldnerverzeichnis einen ähnlichen Zweck erfüllen wie die Einholung einer Bonitätsbeurteilung bei einer Wirtschaftsauskunftei. Dem Schuldnerverzeichnis kommt zum einen, wie aus § 882f Abs. 1 S. 1 Nr. 1 ZPO hervorgeht, eine Funktion iRd Zwangsvollstreckung zu. Ein vollstreckungsbedingtes Einsichtsinteresse besteht danach insb. hinsichtlich der Entscheidung, ob ein Vollstreckungsversuch unternommen werden soll (vgl. Begründung des Entwurfs des Bundesrats eines Gesetzes zur Reform der Sachaufklärung in der Zwangsvollstreckung, BT-Drs. 16/10069, 41). Das Schuldnerverzeichnis ist zum anderen, wie zB aus § 882f Abs. 1 S. 1 Nr. 4 ZPO hervorgeht, auch über Zwecke der Zwangsvollstreckung hinaus ein Auskunftsregister über die Kreditunwürdigkeit einer Person (vgl. BGH Beschl. v. 9.2.2017 – I ZB 56/16 Rn. 16 unter Verweis auf BT-Drs. 16/10069, 20 (37, 40); Beschl. v. 21.9.2023 – V ZB 17/22 Rn. 31).

33 (b) Zudem ist nach den Feststellungen des Berufungsgerichts der Kreis an potenziell ggü. der Bekl. Auskunftsberechtigten nicht deutlich kleiner als der Personenkreis, der nach § 882f Abs. 1 ZPO zu einer Einsicht in das Schuldnerverzeichnis befugt ist, und eine Auskunftserteilung durch die Bekl. nicht von höheren Voraussetzungen abhängig als eine – ebenfalls kostenpflichtige – Einsicht in das Schuldnerverzeichnis. ...

34 (c) Ein erheblicher Unterschied zwischen der Datenspeicherung durch Wirtschaftsauskunfteien und im Schuldnerverzeichnis besteht jedoch mit Blick auf die Art der gespeicherten Informationen. So sind dem Schuldnerverzeichnis keine Informationen über Gläubiger, Höhe und Inhalt der zugrundeliegenden Forderung(en) zu entnehmen. Daher merkt die Revision zu Recht an, dass sich aus dem Schuldnerverzeichnis eher (negative) Anzeichen für eine Kreditunwürdigkeit als (positive) Anzeichen für eine Kreditwürdigkeit einer natürlichen Person ablesen lassen, während Wirtschaftsauskunfteien mit ihren Bonitätsbeurteilungen ein differenzierteres Bild deren finanzieller Situation zeichnen.

35 (d) Darüber hinaus unterscheiden sich auch Beginn und Anlass der Datenspeicherung. So ist anzunehmen, dass Zahlungs-

störungen bei Wirtschaftsauskunfteien, die ihre Informationen (jedenfalls auch) aufgrund einer Einmeldung anderer Privater beziehen, wesentlich früher ersichtlich werden als im Schuldnerverzeichnis, in das ein Eintrag erst dann erfolgen kann, wenn gegen den betroffenen Schuldner eine Forderung rechtskräftig tituliert ist und er seinen vollstreckungsrechtlichen Auskunftspflichten nicht nachgekommen oder die Vollstreckung gegen ihn erfolglos geblieben ist (vgl. BT-Drs. 16/10069, 21).

36 (e) Vor diesem Hintergrund können die vom Gesetzgeber für das Schuldnerverzeichnis getroffenen Wertungen nicht ohne Weiteres auf die Datensammlung der Bekl. übertragen werden. Der Vorschrift des § 882e Abs. 3 Nr. 1 ZPO liegt für das Schuldnerverzeichnis die Wertung zugrunde, dass der Nachweis der vollständigen Befriedigung des Gläubigers das Informationsinteresse des Geschäftsverkehrs beseitigt. Dies ergibt sich im Umkehrschluss aus der Begründung des Gesetzentwurfs zu dieser Vorschrift, nach der der Nachweis einer Stundungsbewilligung oder des Einverständnisses des Gläubigers noch nicht zur Löschung einer Eintragung führe, da dies nicht das Informationsinteresse des Geschäftsverkehrs beseitige (vgl. BT-Drs. 16/10069, 40). Indes lassen sich daraus keine zwingenden Vorgaben für eine Datensammlung wie die der Bekl. ableiten, die zwar umfangreicher ist, aber auch ein differenzierteres Bild der Kredit(-un)würdigkeit eines Schuldners zeichnet als die Datenspeicherung im Schuldnerverzeichnis.

37 (f) Ohne Erfolg verweist die Revisionserwiderung auf eine Bitte des Bundesrats in der vergangenen Legislaturperiode, die Einführung einer gesetzlichen Regelung für die Speicherdauer bei Wirtschaftsauskunfteien zu prüfen, und die ablehnende Gegenäußerung der Bundesregierung dazu (vgl. Begründung des Entwurfs der Bundesregierung eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, BT-Drs. 20/10859, 35 und 39). Ein Wille des Gesetzgebers lässt sich aus diesen Stellungnahmen, die nicht in eine gesetzliche Regelung gemündet haben, nicht ablesen.

38 (3) Schließlich ist die Situation nach Erlangung einer Restschuldbefreiung im Anschluss an ein Insolvenzverfahren, über die der EuGH entschieden hat, mit der vorliegend in Rede stehenden Situation nach Beseitigung einer Zahlungsstörung nicht ohne Weiteres vergleichbar.

39 (a) Soweit die Revisionserwiderung als Argument für eine Gleichbehandlung anführt, bei einer Restschuldbefreiung hätten Gläubiger sogar auf einen Teil ihrer Forderung verzichtet, was bei einer vollständigen Befriedigung nicht der Fall sei, überzeugt dies nicht. Bei der im Streitfall vorzunehmenden Beurteilung kommt es nicht auf die Interessen der von Zahlungsstörungen betroffenen Gläubiger, sondern auf die künftiger Kreditgeber an.

40 (b) Demgegenüber ist der Umstand zu berücksichtigen, dass eine Restschuldbefreiung erst nach einer sog. Wohlverhaltensphase von drei Jahren ab Beendigung des Insolvenzverfahrens zu erlangen ist (vgl. §§ 287 Abs. 2 S. 1, 295, 295a, 296 Abs. 1 S. 1 InsO; BGH Beschl. v. 15.7.2010 – IX ZB 229/07 Rn. 4). Sie soll dem Begünstigten ermöglichen, sich erneut am Wirtschaftsleben zu beteiligen, und hat daher für diese Person im Allgemeinen existenzielle Bedeutung. Dieses Ziel kann durch eine Speicherung dieser Information über längere Zeit gefährdet werden (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 98 – SCHUFA Holding (Restschuldbefreiung)). Im Grundsatz hat zwar auch ein Schuldner, der eine Zahlungsstörung beseitigt hat, ein berechtigtes Interesse an einer ungehinderten Teilnahme am Wirtschaftsleben; er kann aber nicht unmittelbar nach der Begleichung einer ausstehenden Forderung auf eine ähnliche Wohlverhaltensphase verweisen.

41 III. Das angefochtene Urteil ist daher aufzuheben (§ 562 Abs. 1). Die Sache ist zur neuen Verhandlung und Entscheidung an das Berufungsgericht zurückzuverweisen (§ 563 Abs. 1 S. 1 ZPO). Der Senat kann nicht in der Sache selbst entscheiden, weil sie nicht zur Endentscheidung reif ist (§ 563 Abs. 3 ZPO; vgl. dazu ergänzend unter Rn. 51 und 52).

42 C. Für das wiedereröffnete Berufungsverfahren weist der Senat auf Folgendes hin:

43 I. Das Berufungsgericht wird die iRd Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO vorgesehene Erforderlichkeitsprüfung und erneut eine Interessenabwägung vorzunehmen haben. Es erscheint dem Senat möglich, bestimmte Speicherungsfristen als Ergebnis einer typisierten Abwägung festzulegen, soweit dabei die Besonderheiten des Einzelfalls hinreichend berücksichtigt werden.

44 1. In einem ersten Schritt ist die Erforderlichkeit der Datenverarbeitung zu prüfen.

45 a) Dabei ist zu fragen, ob das berechnete Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insb. die durch Art. 7 und 8 GRCh gewährleisteten, eingreifen. Hierbei ist auch der in Art. 5 Abs. 1 lit. c DS-GVO verankerte Grundsatz der Datenminimierung zu berücksichtigen (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 77 f. – SCHUFA Holding (Restschuldbefreiung)). Im Grundsatz trägt die Bekl. als Verantwortliche die Darlegungs- und Beweislast für die Erforderlichkeit der von ihr vorgenommenen Datenverarbeitung (vgl. BGH Urt. v. 14.10.2025 – VI ZR 431/24 Rn. 41).

46 b) Eine kürzere Datenspeicherung könnte zwar grds. als milderes Mittel angesehen werden. Die Bekl. setzt dem die beweisbewehrte Behauptung entgegen, eine empirische Analyse anhand ihres Datenbestands habe ergeben, dass das Risiko einer erneuten Zahlungsstörung auch drei Jahre nach der Erledigung einer Forderung noch etwa um das Achtfache erhöht sei ggü. Personen, bei denen es im Vergleichszeitraum nicht zu einer Zahlungsstörung gekommen sei. Hierüber muss aus Sicht des Senats kein Beweis erhoben werden, weil sich damit keine Aussage über die Erforderlichkeit im Einzelfall treffen ließe. Die im konkreten Fall angemessene Speicherdauer ist – jedenfalls bei der in Rede stehenden Zeitspanne zwischen null und drei Jahren – vielmehr nach normativen Kriterien iRd Interessenabwägung festzusetzen.

47 2. In einem zweiten Schritt ist das Speicherungsinteresse der Bekl. erneut mit dem Lösungsinteresse des Kl. abzuwägen. Soweit hierin grundrechtliche Wertungen einfließen, kommt es im vollharmonisierten Bereich der DS-GVO auf die der GRCh an (vgl. BVerfGE 152, 216 [= MMR 2020, 106 mAnm Hoeren = ZD 2020, 109 mAnm Gräbig] – Recht auf Vergessen II; BGH Urt. v. 24.2.2022 – I ZR 2/21 Rn. 33 – Tina Turner).

48 a) In der obergerichtlichen Rspr. wird überwiegend vertreten, dass Wirtschaftsauskunfteien Daten über Zahlungsstörungen bis zu drei Jahre nach Erledigung der jeweiligen Forderung speichern dürften (vor dem EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] – SCHUFA Holding (Restschuldbefreiung), soweit veröffentlicht: OLG Brandenburg ZD 2023, 748 Rn. 22; danach, soweit veröffentlicht: OLG München Beschl. v. 20.2.2025 – 37 U 4148/24 e Rn. 23; OLG Stuttgart WM 2025, 1379 Rn. 29 bis 42; OLG München ZInsO 2025, 1631 Rn. 36 bis 56; OLG Hamm ZVI 2025, 359 Rn. 42 bis 53; OLG Nürnberg WM 2025, 1886 Rn. 37 bis 53; OLG Dresden WM 2025, 1882 Rn. 37 bis 60; OLG Stuttgart Urt. v. 22.10.2025 – 9 U 141/24 Rn. 42 bis 66; ohne Nennung einer konkreten Frist: OLG Frankfurt/M. ZInsO 2023, 677).

49 b) Die vom HBDI zum 1.1.2025 genehmigte Ziffer IV.1. lit. b der Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien nimmt eine Differenzierung vor, die dem Senat grds. als sachgerecht erscheint.

50 aa) Zwar können Verhaltensregeln iSv Art. 40 DS-GVO, zu denen auch die hier in Rede stehenden gehören, gem. der Rspr. des EuGH bei der Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht berücksichtigt werden, soweit sie zu einer anderen Beurteilung führen würden als derjenigen, die sich nach der genannten Vorschrift ergibt (vgl. EuGH NJW 2024, 417 [= ZD 2024, 166 mAnm Schild] Rn. 104 f. – SCHUFA Holding (Restschuldbefreiung)). Das schließt jedoch nicht aus, solche Verhaltensregeln – im Interesse der Rechtssicherheit und auch mit Blick auf das von Wirtschaftsauskunfteien betriebene Massengeschäft – als Orientierung für die nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO vorzunehmende Interessenabwägung heranzuziehen, soweit sie typisiert zu einem angemessenen Interessenausgleich führen und die Besonderheiten des Einzelfalls bei der konkret vorzunehmenden Interessenabwägung hinreichend berücksichtigt werden. Da die Interessenabwägung normativ an Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO gebunden ist, kann sie sich nicht bis zum 31.12.2024 an den früheren und ab dem 1.1.2025 an den neuen Verhaltensregeln orientieren.

51 bb) Ziffer IV.1. lit. b der Verhaltensregeln in ihrer zum 1.1.2025 genehmigten Fassung nimmt aus Sicht des Senats grds. einen angemessenen Interessenausgleich vor. Im Ausgangspunkt (Satz 1) sieht diese Regelung – wie auch von der überwiegenden obergerichtlichen Rspr. vertreten – eine Speicherung von personenbezogenen Daten über ausgeglichene Forderungen für drei Jahre vor. Die Speicherung endet jedoch abweichend davon bereits nach 18 Monaten (Satz 2), wenn (1) der Auskunftei bis zu diesem Zeitpunkt keine weiteren Negativdaten gemeldet worden sind, (2) keine Informationen aus dem Schuldnerverzeichnis oder aus Insolvenzbekanntmachungen vorliegen und (3) der Ausgleich der Forderung innerhalb von 100 Tagen nach Einmeldung erfolgte. Damit werden Kriterien für eine weniger gewichtige Zahlungsstörung beschrieben, bei der die Speicherdauer ggü. dem Regelfall halbiert ist. Zum Vorliegen dieser Voraussetzungen im Streitfall wird das Berufungsgericht im wiedereröffneten Berufungsverfahren ergänzende Feststellungen zu treffen haben.

52 cc) Dem Schuldner muss es zudem möglich sein, besondere Umstände vorzubringen, die seinem Lösungsinteresse ein wesentlich überdurchschnittliches Gewicht verleihen. In diesem Fall kann die Interessenabwägung ausnahmsweise dazu führen, dass allein eine noch kürzere Speicherdauer als angemessen anzusehen ist. Der Kl. wird im wiedereröffneten Berufungsverfahren Gelegenheit haben, hierzu ergänzend vorzutragen. ...

Anmerkung

Dr. André Reinelt, Bucerius Law School, Hamburg

1. Kontext – Welche Daten darf die SCHUFA wie lange verarbeiten?

Die größte Wirtschaftsauskunftei in Deutschland, die SCHUFA, und ihr (Kern-)Geschäftsmodell, die Erstellung von (externen) Bonitäts-Scores von Verbraucherinnen und Verbraucher, stehen unter dem Druck des Datenschutzes. Soweit der SCHUFA-Score von Dritten maßgeblich für die Entscheidung herangezogen wird, ob ein Vertragsverhältnis begründet, durchgeführt oder beendet wird, ist bereits der Score selbst eine automatisierte Entscheidung und daher nach Art. 22 Abs. 1 DS-GVO grds. verboten (EuGH MMR 2024, 153 mAnm Radtke – SCHUFA Holding (Scoring)). Ebenfalls stehen betrof-

fenen Personen umfassende Auskunftsansprüche nach Art. 15 Abs. 1 lit. h DS-GVO zu, die auch die involvierte Logik umfassen und so ein Recht auf Erklärung begründen (EuGH MMR 2025, 421 mAnm Hense/Niekrenz – Dun & Bradstreet).

Neben dieser Dimension von Transparenz und Kontrolle stellt sich die grundsätzliche Frage, welche Daten die SCHUFA in ihre Score-Formel einbeziehen darf. Oder anders: Welche Daten dürfen für welchen Zeitraum von Auskunftfeien gespeichert und für die Erstellung eines Bonitäts-Scores verwendet werden? Im Fokus stehen dabei Positivdaten wie zB die Einmeldung, dass ein Mobilfunkvertrag abgeschlossen oder beendet worden ist (akzeptiert von BGH ZD 2026, 165; Vorlage zum EuGH von LG Lübeck ZD 2025, 704 mAnm Söbbing/Schwarz – das Verfahren beim EuGH wurde nunmehr wegen einer Klagerücknahme aufgrund eines außergerichtlichen Vergleichs gestrichen). Diskutiert wird auch die Speicherdauer von Negativdaten wie zB der Eintrag einer Restschuldbefreiung nach einer Privatinsolvenz (EuGH ZD 2024, 166 mAnm Schild – SCHUFA Holding (Restschuldbefreiung)). Negativdaten sind auch Gegenstand dieser Entscheidung: Der BGH musste im vorliegenden Fall darüber entscheiden, wie lange Einmeldungen von den Vertragspartnern über Zahlungsausfälle ihrer Kundinnen und Kunden gespeichert werden dürfen und damit den SCHUFA-Score (negativ) beeinflussen können.

Das zentrale Rechtsproblem besteht darin, wie stark die berechtigten Interessen der SCHUFA und des Wirtschaftssystems ggü. den wirtschaftlichen und sozialen Teilhabeinteressen sowie den Grundrechtspositionen betroffener Personen innerhalb der Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu gewichtet sind. Konkret: Müssen Daten zu Zahlungsausfällen sofort nach Forderungsausgleich gelöscht werden oder darf die SCHUFA diese Informationen über diesen Zeitpunkt hinaus für die Score-Berechnung nutzen?

Flankiert wird dies durch die Frage, ob es zulässig ist, dass der Code of Conduct der Auskunftfeien, also Verhaltensregeln nach Art. 40 DS-GVO, eine typisierte Abwägung zur Vereinfachung des Massengeschäfts von Auskunftfeien vornimmt. Die meisten Ober- und Instanzgerichte billigten die dort vorgesehene Speicherdauer von grds. drei Jahren (vgl. Rn. 48). Nur die Vorinstanz (OLG Köln MMR 2025, 532 mAnm Claes/Jäger) sah darin eine unrechtmäßige Datenspeicherung und zog für die Begründung die gesetzgeberische Wertung des § 882e Abs. 3 Nr. 1 ZPO heran, wonach Einträge im Schuldnerverzeichnis unmittelbar nach nachgewiesenem Forderungsausgleich gelöscht werden müssen.

Die Entscheidung des BGH ist in Ergebnis und Begründung erkennbar von dem Leitgedanken getragen, die private Ordnung deutscher Auskunftfeien und das Geschäftsmodell des externen Credit-Scorings rechtlich zu stabilisieren. Die wirtschaftlichen Interessen werden ggü. den sozialen Teilhabechancen von Betroffenen zu stark gewichtet und die Rechtsdurchsetzung auf vulnerable Personen verlagert. Die Entscheidung kann daher auf mehreren Ebenen nicht überzeugen.

2. Systemische Wirtschaftsinteressen versus verdeckte Teilhabechancen

Ein epistemisches Ungleichgewicht zwischen wirtschaftlichen Belangen und den Rechtspositionen von Betroffenen zieht sich durch die gesamten Entscheidungsgründe. Auf der einen Seite werden die wirtschaftlichen Interessen in ihren jeweiligen Dimensionen explizit gemacht (Rn. 16 f.): Es sind gerade nicht nur individuelle wirtschaftliche Interessen der SCHUFA betroffen, die ihren Score gewinnbringend verkaufen möchte. Vielmehr werden auch systemische Belange, nämlich das Interesse des Wirtschaftssystems gegen Unsicherheiten vorzugehen, in

die Waagschale gelegt. Wenn argumentativ diese systemische Position auch dogmatisch in der Abwägung verarbeitet wird, ist abzusehen, dass die Entscheidung bereits im Ausgangspunkt zugunsten dieser wirtschaftlichen Logik ausfallen wird.

Das Gewicht wirtschaftlicher Belange wird damit abgesichert, dass nach Ansicht des BGH die Behauptung der SCHUFA, Betroffene mit Zahlungsstörungen wiesen auch noch drei Jahre danach ein bis zu achtfach höheres Risiko einer erneuten Zahlungsstörung auf, nicht bewiesen werden müsse (Rn. 46). Dabei ist richtig, dass die vorzunehmende Interessenabwägung normativ, genuin nach rechtlichen Gesichtspunkten vorzunehmen ist. Aber jede rechtliche Interessenabwägung hat auch eine tatsächliche Dimension, nämlich wie stark in jedem konkreten Einzelfall die jeweiligen Rechtspositionen betroffen sind (ausf. zur Abwägung T. Möllers Juristische Methodenlehre, 6. Aufl. 2025, S. 391 ff.). Die Frage, welcher genaue statistische Zusammenhang zwischen einer vorherigen und einer zukünftigen Zahlungsstörung besteht, ist deshalb elementar für die Abwägungsgewichtung (ähnlich Schwindt NZI 2026, 187): Ließe sich tatsächlich ein achtfach höheres Risiko nachweisen, wäre das in der Tat ein gewichtiges Argument zugunsten der Informationsinteressen des Wirtschaftssystems. Ist das Risiko jedoch erheblich geringer, nimmt auch das Gewicht in der Gesamtabwägung ggü. den Betroffenenrechten ab.

Diese normative Hervorhebung einer einzigen – hier der wirtschaftlichen – Systemlogik wäre weniger bedenklich, wenn die Rechts- und Interessenpositionen von Betroffenen auf der anderen Seite ebenso explizit adressiert und in die Gewichtung eingestellt werden würden. Das geschieht allerdings nicht, was auch an der Normstruktur des lit. f liegt, die eine überindividuelle Dimension durch Dritinteressen explizit nur auf Seiten des Verantwortlichen anspricht. Die sozial komplexe, ebenfalls systemische Exklusionsdimension eines negativen SCHUFA-Scores, insb. aufgrund von bisherigen Zahlungsausfällen, wird hinter einem „berechtigte[n] Interesse an einer ungehinderten Teilnahme am Wirtschaftsleben“ (Rn. 40) verdeckt.

Über seinen genuin wirtschaftlichen Ursprung als Bonitätsbewertung für die Vergabe von (Bank-)Krediten hat der SCHUFA-Score Einzug in ganz andere Lebensbereiche erhalten. „Hierdurch werden Daten, die in einem bestimmten Bereich und für sehr spezifische Zwecke erhoben wurden, zu wichtigen Referenzgrößen in anderen Kontexten.“ (Mau Berliner Journal für Soziologie 2023, 255 (276 f.)). Die Bonitätsbewertung für die Kreditvergabe war zunächst ein sehr begrenztes Instrument und ist nach und nach in andere soziale Bereiche diffundiert (Ronastas Historical Social Research 2017, 52). Das führt dazu, dass nicht nur in Einzelfällen (so allerdings nicht überzeugend Weichert NJW 2025, 1912 (1912)) einzelne Kreditverträge aufgrund eines schlechten SCHUFA-Scores abgelehnt werden. Vielmehr ist die Bonitätsbewertung der SCHUFA zu einem lebensbereichsübergreifenden Muster sozialer Exklusion geworden: „Bonitätsbewertungen ... stehen stellvertretend für einen grundlegenden Strukturwandel bei der Entscheidungsfindung in unserer digitalisierten Gesellschaft. Solche automatisierten Bewertungssysteme beeinflussen zunehmend unmittelbar die rechtlichen und wirtschaftlichen Lebensverhältnisse, etwa bei der Wohnungssuche, dem Abschluss von Mobilfunkverträgen oder der Kreditbeantragung.“ (Hense/Niekrenz KIR 2025, 240 (241)). Die eingeschränkte Teilhabe am Wirtschaftsleben meint also im Kontext des Kredit-Scorings über den Ausschluss von ökonomischen Interaktionen hinausgehende soziale Exklusion: „Mit der Entscheidung über die Teilnahme am Wirtschaftsleben entscheiden diese Rechenoperationen auch über die Möglichkeiten für gesellschaftliche Teilhabe.“ (Mohabbat Kar/Thapa/Parycek (Un)berechenbar?/Mohabbat Kar/Parycek, 2018, S. 7, 8)

3. Methodisch wenig überzeugende Fallvergleiche

Die systemische Exklusionsdimension von Negativeinträgen macht der EuGH für die Restschuldbefreiung explizit und überträgt die gesetzliche, sechsmonatige Speicherdauer im Insolvenzregister auf das private Bonitäts-Scoring (EuGH ZD 2024, 166 mAnm Schild Rn. 94, 97 – 99). Rein formal nimmt der BGH diese Rspr. zur Kenntnis (Rn. 40). Allerdings verkennt das Gericht die Vergleichbarkeit von Restschuldbefreiung und Zahlungsstörung, sodass es die materiellen Maßstäbe des EuGH fehlerhaft anwendet und wenig überzeugende Vergleichsparameter bildet.

Erstens zeigt sich das zunächst in der Argumentation, mit der der Senat die Anwendung der Abwägungsmaßstäbe des EuGH auf Fälle von Zahlungsstörungen ablehnt. Das Gericht sieht den zentralen Wertungsgesichtspunkt, der für eine Vergleichbarkeit herangezogen werden sollte, im Umstand, dass die Informationen über eine Restschuldbefreiung aus einem öffentlichen Register übernommen werden, die Informationen über Zahlungsstörungen hingegen von den Vertragspartnern der SCHUFA eingemeldet werden (Rn. 30). Der BGH knüpft also an die Art und vor allem an den Ursprung des ursprünglichen Datums an. Er interpretiert die Maßstäbe des EuGH damit in einem formalen Sinne: Kommt das Datum aus einem öffentlichen Register, müssen die gesetzlichen Speicherfristen in der Abwägung im Verhältnis private Auskunft sowie Verbraucherinnen und Verbraucher berücksichtigt werden; stammt es hingegen von den Vertragspartnern, müsse diese Wertung nicht übertragen werden.

Damit verkennt das Gericht, dass der EuGH in der Maßstabsbildung nicht primär auf den formalen Ursprung des Datums abstellt, sondern auf die materielle, in der gesetzlichen Speicherfrist verkörperte Abwägungsentscheidung des Gesetzgebers zwischen Informationsinteresse und Teilhabechancen. Unmissverständlich bringt das der EuGH so zum Ausdruck (EuGH ZD 2024, 166 mAnm Schild Rn. 97): „Er [der deutsche Gesetzgeber] geht daher davon aus, dass nach Ablauf einer Frist von sechs Monaten die Rechte und Interessen der betroffenen Person diejenigen der Öffentlichkeit, über diese Information zu verfügen, überwiegen.“ Ebenso geht es dem europäischen Gericht nicht darum, dass die Speicherdauer des öffentlichen Registers um des Registers wegen (!) konterkariert wird, sondern um den Wertungsgesichtspunkt, dass „diese Daten bei der Bewertung der Kreditwürdigkeit einer solchen Person stets als negativer Faktor verwendet werden.“ (EuGH ZD 2024, 166 mAnm Schild Rn. 98). Dass es dem EuGH bei seiner Maßstabsbildung um die gesellschaftlichen Teilhabechancen der betroffenen Personen und nicht um die Speicherfrist des Registers an sich geht, wird zuletzt noch dadurch deutlich, dass das Gericht selbst für den Zeitraum, in dem die Daten in dem öffentlichen Register verfügbar sind, in der parallelen Verarbeitung durch Auskunfteien einen verstärkenden Eingriff in die Grundrechtspositionen sieht und deshalb eine gesonderte Interessenabwägung notwendig ist (EuGH ZD 2024, 166 mAnm Schild Rn. 100). Käme es dem Gericht auf die Speicherdauer an sich als maßgeblichen Bezugspunkt an, wäre die parallele Verarbeitung im SCHUFA-Score wenig problematisch.

Entgegen dem Fallvergleich anhand formaler Gesichtspunkte betont der BGH, zweitens, mit der Gegenüberstellung von Restschuldbefreiung und Zahlungsstörung materielle Aspekte deutlich stärker (Rn. 38 ff.). Allerdings kann der Verweis auf die dreijährige Wohlverhaltensphase, die bei der bloßen Forderungstilgung nicht besteht, nicht überzeugen. Denn ein solcher Zeitraum, in dem sich ein Schuldner „beweisen“ müsse, spielt für die Maßstabsbildung des EuGH keine Rolle. In den Entscheidungsgründen taucht daher dieser dreijährige Zeitraum weder

ausdrücklich noch der Sache nach auf. Das überzeugt auch in Gänze: Auch hinsichtlich der Restschuldbefreiung wurde vor der EuGH-Entscheidung vertreten, dass von einer Erholung der wirtschaftlichen Verhältnisse erst nach drei Jahren ausgegangen werden könne und deshalb eine Eintragung über die Speicherfrist des Registers hinaus gerechtfertigt sei (Wiedemann VuR 2024, 174 (178)). Indem der EuGH auf eine solche volatile Argumentation nicht einmal eingeht, macht er deutlich, dass ihm die prospektiven Teilhabechancen wichtiger sind als die retrospektive Betrachtung wirtschaftlicher Verhältnisse.

Zuletzt können auch nicht die vom BGH ins Feld geführten Argumente gegen die Vergleichbarkeit der sofortigen Löschfrist aus dem Schuldnerverzeichnis und der Verarbeitung im SCHUFA-Score überzeugen. So mag es zwar sein, dass im Schuldnerverzeichnis weniger Informationen enthalten sind als in den Einmeldungen der Vertragspartner der Auskunfteien (Rn. 34). Daraus zieht das Gericht jedoch die falschen normativen Schlüsse: Wenn der Gesetzgeber selbst bei einer geringeren Eingriffsintensität (wegen weniger Informationen) die Wertung trifft, dass eine sofortige Löschung interessengerecht ist, muss dies erst recht bei weitergehenden Informationen der SCHUFA-Vertragspartner gelten. Dieses Erst-recht-Argument gilt in gleichem Maße für den Einmeldungszeitpunkt Privater (Rn. 35): Wenn die Meldungen von Zahlungsstörungen früher als Eintragungen im Schuldnerverzeichnis erfolgen, wirken sie sich bereits früher negativ auf den SCHUFA-Score aus und entfalten somit länger ihre soziale Exklusionswirkung (ähnl. krit. Radtke NJW 2026, 805 (807)).

Zudem ist der Vergleich des Schuldnerverzeichnisses, das Auskunft über die (negative) Kreditwürdigkeit gibt, und dem Bonitäts-Score, der die (positive) Kreditwürdigkeit differenzierter darstellt, erneut formal und geht am wesentlichen materiellen Bezugspunkt vorbei. Denn der SCHUFA-Score zeichnet – potenziell – lediglich in seiner Gesamtheit, also bei einer Auswertung aller Kriterien und Merkmale, ein differenziertes Gesamtbild der Bonität von Verbraucherinnen und Verbrauchern. Gegenstand der Interessenabwägung des Art. 6 Abs. 1 lit. f DS-GVO, in dessen Rahmen darüber nachgedacht wird, die gesetzliche Wertung des § 882e Abs. 3 Nr. 1 ZPO heranzuziehen, ist hingegen die gesonderte und einzeln zu betrachtende Verarbeitung einer Zahlungsstörung. Diese spezielle Information eines Zahlungsausfalls ist – sowohl nach den alten Scoring-Verfahren als auch nach dem neuen SCHUFA-Score (s. hierzu Thiel ZD 2026, 61) – das zentrale Negativgewichtungskriterium. Mit anderen Worten: Der SCHUFA-Score an sich mag differenzierend sein, weil er sowohl positive als auch negative Bonitätskriterien auswertet. Informationen über Zahlungsausfälle für sich betrachtet, werden allerdings immer als negatives Bonitätskriterium herangezogen.

Schließlich verkennt der BGH, dass das Schuldnerverzeichnis nicht nur dem Informationsinteresse des Geschäftsverkehrs dient. Für das Gericht ist einziger Bezugspunkt dieses Informationsinteresses, was mit dem Nachweis der Forderungstilgung wegfällt (Rn. 36). Für den Senat ist somit erneut in der Argumentation lediglich die wirtschaftliche Dimension des Sachverhalts relevant. Der EuGH stellt jedoch bei seiner Maßstabsbildung für die Abwägung primär auf die Auswirkungen auf die jeweils betroffene Person ab (EuGH ZD 2024, 166 mAnm Schild Rn. 94, 97 – 99). Der BGH übersieht vor diesem Hintergrund, dass § 882e ZPO, der die Löschungstatbestände für das Schuldnerverzeichnis regelt, Ausdruck des informationellen Selbstbestimmungsrechts des Schuldners und damit des Verhältnismäßigkeitsprinzips ist (BeckOK ZPO/Fleck, 59. Ed. 1.12. 2025, ZPO § 882e Rn. 1). Die Regelungen des Schuldnerverzeichnisses konkretisieren den Interessen- und Grundrechts-

ausgleichs zwischen dem allgemeinen Gläubigerschutz und den Rechten und Interessen zahlungsschwacher Personen (Hergenröder DGVZ 2017, 119). Genau dieser Ausgleichsgedanke kann auch auf das private Bonitäts-Scoring übertragen werden (ähnlich Radtke, NJW 2026, 805 (807)).

4. Rechtsdurchsetzungslast bei der strukturell schwächeren Partei

Kritisch zu betrachten ist ebenfalls die Lösung des BGH zu den Auskunft-Verhaltensregeln nach Art. 40 DS-GVO. Das Gericht akzeptiert im Ergebnis die von deutschen Auskunfteien gesetzten Speicherfristen als Ergebnis einer typisierten Abwägung (Rn. 43 ff.). Diese sehen nämlich bei „weniger gewichtigen Zahlungsstörungen“ (Rn. 50) eine Reduzierung der Speicherdauer von drei Jahren auf 18 Monate vor. Neu und positiv zu werten ist, dass der BGH nunmehr prozedurale Anforderungen dahingehend aufstellt, dass betroffene Personen die Möglichkeit haben müssen, besondere Umstände vorzubringen, die dem Lösungsinteresse ein „wesentlich überdurchschnittliches Gewicht verleihen“ und somit im Einzelfall eine sofortige Löschung rechtfertigen (Rn. 52). Dies ist eine maßgebliche Verbesserung ggü. dem bisherigen Zustand.

Allerdings kann die konkrete Ausgestaltung aus Sicht der effektiven Rechtsdurchsetzung nicht überzeugen, weil die typischerweise besonders vulnerable Partei zur Rechtsdurchsetzung aktiv werden muss. Denn der BGH hat nicht nur die Prüfung, ob ein atypischer Einzelfall vorliegt, den Gerichten auferlegt, sondern den Betroffenen die Darlegungs- und Prozessführungslast auferlegt. Damit wurde die Rechtsdurchsetzung ausschließlich auf das Privatrecht verschoben. Da nun im Einzelfall Sonderargumente vorgebracht werden müssen, ist die Frage einer sofortigen Löschung keine Angelegenheit mehr für die jeweiligen Datenschutzbehörden, sondern kann nur noch durch Betroffene selbst ggü. der SCHUFA – regelmäßig iRe Zivilprozesses – geltend gemacht werden.

Da die Last der Rechtsdurchsetzung maßgeblich auf eine von Armut betroffene Person in einer finanziell prekären bzw. überschuldeten Lebenslage verlagert wird, ist mit mehreren strukturellen Durchsetzungshindernissen und -defiziten zu rechnen. Zunächst muss (1.) der individuelle Sonderfall von der betroffenen Person selbst als solcher erkannt werden. Dann muss (2.) die betroffene Person finanzielle Ressourcen für die Prozessführung mobilisieren, was regelmäßig aufgrund ihrer sozio-ökonomischen Positioniertheit schwierig werden wird. Darüber hinaus trägt sie (3.) ein erhebliches Prozessrisiko dahingehend, dass das Gericht ihren Fall nicht als atypischen Sonderfall anerkennen wird. Das ist zwar ein allgemeines Problem bei rechtlichen Abwägungsentscheidungen. Es wird hier jedoch strukturell dadurch verstärkt, dass die Verhaltensregeln einen Ankereffekt dahingehen erzeugen, dass die Abwägungsentscheidung im Normalfall bereits zugunsten der Auskunfteien entschieden worden ist. Hinzu kommt, dass die Verhaltensregeln selbst bereits eine Abstufung vorsehen; die Umstände, die einen atypischen Einzelfall konstituieren, müssen demnach andere sein und in ihrem Abwägungsgewicht schwerer wiegen (Sakowski GRUR-Prax 2026, 96). Schließlich steht das Lösungsbegehren (4.) aufgrund der dreijährigen Speicherfrist von vornherein in einem zeitlich begrenzten Kontext – das Damoklesschwert einer Erledigung schwingt somit immer mit. Betroffene könnten daher angesichts von langen Verfahrensdauern und erwartbaren Berufungen der SCHUFA ein rationales Desinteresse an der individuellen Durchsetzung ihrer Rechtspositionen entwickeln.

5. Fazit – Vorlage an den EuGH

Die Entscheidung des BGH zur Speicherfrist von Zahlungsstörungen überzeugt auf mehreren Ebenen nicht. Sie wird

der sozialen Exklusionsdimension des SCHUFA-Scores nicht gerecht, sie wendet – mit methodisch unsauberen Argumenten – die Maßstäbe des EuGH zur Restschuldbefreiung nicht an und verlagert damit die Rechtsdurchsetzungslast für Ausnahmefallsituationen auf ohnehin schon vulnerable Personen.

Es ist daher bedenklich, dass die ersten Obergerichte diese Rechtsprechungslinie in strukturparalleler Argumentation übernehmen (OLG Dresden Urt. v. 20.1.2026 – 4 U 598/25; OLG München Beschl. v. 21.1.2026 – 20 U 3935/24 e; OLG Koblenz Beschl. v. 22.1.2026 – 2 U 621/25; OLG Frankfurt/M. Beschl. v. 22.1.2026 – 6 U 133/25). Aus Sicht der Betroffenen ist zu hoffen, dass die Instanzgerichte den ihnen überlassenen – begrenzten – Spielraum für eine „(echte) eigene Interessenabwägung“ (Radtke NJW 2026, 805 (807)) dazu nutzen, die Maßstäbe des EuGH zu berücksichtigen. Alternativ käme eine Vorlagefrage an den EuGH in Betracht, die auch dann zulässig wäre, wenn das Gericht von einem acte clair ausginge (EuGH NJW-RR 2021, 775 Rn. 27). Die Gerichte könnten damit einen offenen Konflikt mit dem BGH vermeiden.

OLG Hamburg: Örtliche Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet

Internetveröffentlichung

ZPO § 32

Beschluss vom 3.3.2026 – 7 W 26/26 (LG Hamburg)

Leitsatz der Redaktion

Anders als bei im gesamten Bundesgebiet bekannten Prominenten besteht bei weniger bekannten Persönlichkeiten keine Vermutung, dass sich Persönlichkeitsrechtsverletzungen am gewählten Gerichtsstand auswirken.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2026, 3040. Vgl. ferner BGH MMR 2010, 441.

Schlagworte: Internetveröffentlichung; Persönlichkeitsrechtsverletzungen; Einschränkung des fliegenden Gerichtsstands

Sachverhalt

Die Ag. zu 1) ist ein Karnevalsverein und betreibt die Internetseite www...de. Die Ag. zu 2) und 3) sind Mitglieder der Redaktion eines Festheftes. Der Ast. ist Mitglied der Ag. zu 1) und hat gegen diese einen Aussetzungsbeschluss des AG Köln gegen die Anmeldung eines Vorstandswechsels erwirkt. Inhaltlich liegt dem Streit ein auf einer außerordentlichen Mitgliederversammlung am 29.5.2025 beschlossener Vorstandswechsel bei der Ag. zu 1) zugrunde, gegen den der Ast. geklagt hat.

Der Ast. beantragt,

1. Den Ag. wird untersagt, öffentlich die Behauptung aufzustellen und zu verbreiten bzw. durch Dritte aufstellen und verbreiten zu lassen, A sei 2. Vorsitzende des Karnevalsvereins B und somit Mitglied des geschäftsführenden Vorstands der Ag. zu 1).
2. Die Ag. werden angewiesen, das digital auf den Internetseiten des Vereins veröffentlichte Festheft der Session 2025/26 unverzüglich von allen digitalen Plattformen zu entfernen.

Er ist der Ansicht, die Tatsache, dass seine aus Frechen stammende Schwester in Hamburg lebe, begründe einen direkten Bezug zwischen dem Sitz der Ag. zu 1) in Frechen zum Ort der Störung

in Hamburg. Seinen Anordnungsanspruch leitet der Ast. daraus ab, dass er Verfahrensbeteiligter des Aussetzungsverfahrens vor dem AG Köln sei.

Aus den Gründen

8 II. Die sofortige Beschwerde ist ... nicht begründet. Das LG hat zu Recht ... den Antrag wegen fehlender örtlicher Zuständigkeit zurückgewiesen. Lediglich ergänzend ist auszuführen:

9 Für Veröffentlichungen in Online-Medien setzt der BGH für die autonome internationale Zuständigkeit der deutschen Gerichte zur Entscheidung über Klagen wegen Persönlichkeitsbeeinträchtigungen voraus, dass die als rechtsverletzend beanstandeten Inhalte objektiv einen deutlichen Bezug zum Inland aufweisen (vgl. BGH Urt. v. 2.3.2010 – VIZR23/09 [= MMR 2010, 441]). Danach ist eine Kollision der widerstreitenden Interessen, dh des Interesses des Kl. an der Achtung seines Persönlichkeitsrechts einerseits und des Interesses des Bekl. an der Gestaltung seines Internetauftritts und an einer Berichterstattung andererseits, nach den Umständen des konkreten Falls zu lokalisieren, insb. ist festzustellen, ob aufgrund des Inhalts der beanstandeten Meldung die Verletzung im Inland tatsächlich eingetreten ist oder eintreten kann.

10 Die Übertragung dieser Grundsätze auf die örtliche Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet wird zwar bislang nicht einheitlich gesehen. In der Rspr. wird der ubiquitäre sog. fliegende Gerichtsstand bei Persönlichkeitsrechtsverletzungen im Internet allerdings überwiegend beschränkt auf die örtliche Zuständigkeit der Gerichte an dem Ort, an dem die Beeinträchtigung des Persönlichkeitsrechts durch die Kenntnisnahme von der Veröffentlichung näher liegt. Eine Einschränkung der grds. bundesweit gegebenen Zuständigkeit kommt nach der Rspr. insb. dann in Betracht, wenn sich die Veröffentlichung auf einen örtlich begrenzten Adressatenkreis bezieht oder sonst einen lokalen oder regionalen Bezug aufweist (OLG Hamburg Beschl. v. 29.11.2023 – 7 W 94/23). Angeknüpft wird an die bestimmungsgemäße Abrufbarkeit und damit die bestimmungsgemäße Auswirkung der beanstandeten Inhalte (vgl. u.a. OLG Brandenburg Beschl. v. 16.11.2023 – 1 W 25/23).

11 Vorliegend bezieht sich der Unterlassungsantrag auf eine Veröffentlichung eines in Frechen ansässigen Karnevalsvereins, der Ag. zu 1). Auch der Ast. selbst sowie die weiteren Ag. zu 2) und 3) leben in Frechen. Weder haben die Ag. die in Rede stehende Verlinkung auf die Festschrift, die nach Ansicht des Ast. fehlerhafte Angaben enthält, im Gebiet der Stadt Hamburg vorgenommen, noch hat sich eine Persönlichkeitsrechtsverletzung des Ast., für die ohnehin nach dem eigenen Vortrag keine Anhaltspunkte bestehen, in Hamburg ausgewirkt, da dieser selbst keinen Wohnsitz hier unterhält und auch ansonsten – außer der Tatsache, dass seine Schwester hier lebt – keine Verbindung zur Stadt Hamburg aufweist.

12 Im Vergleich zu Prominenten, die im gesamten Bundesgebiet bekannt sind, sodass Persönlichkeitsrechtsverletzungen keinen besonderen regionalen Bezug aufweisen, besteht für weniger bekannten Persönlichkeiten, wie dies der Ast. ist, keine Vermutung, dass sich Persönlichkeitsrechtsverletzungen am gewählten Gerichtsstand auswirken (s.a. LG Köln Beschl. v. 26.2.2019 – 28 O 359/18; BeckOGK/Lutz, 15.12.2025, ZPO § 32 Rn. 167).

13 Dem Senat erschließt sich darüber hinaus nicht ansatzweise, inwieweit nur mögliche Geschäftsbeziehungen der Ag. zu 1) zu in Hamburg ansässigen Unternehmen einen regionalen Bezug gerade im Hinblick auf die in Rede stehende Rechtsverletzung herstellen sollen. ...

KG: Log-in-Pflicht bei Online-Kündigungsschaltfläche unzulässig

Missbrauchskontrolle

BGB § 312k Abs. 2 S. 3, S. 4, 312m Abs. 1; UKlaG § 2 Abs. 1 S. 1; DDG § 5 Abs. 1; DS-GVO Art. 28, 32, Erwägungsgrund 57; RL (EU) 2022/2555 (NIS-2-RL) Art. 21; RL 2011/83/EU (VRRL) Art. 11a; RL (EU) 2023/2673 Erwägungsgrund 37
Urteil vom 18.11.2025 – 5 UKI 10/25 (LG Berlin II); nicht rechtskräftig

Leitsatz

Eine Kündigungsschaltfläche führt einen Verbraucher nicht unmittelbar zu einer Bestätigungsseite iSd § 312k Abs. 2 S. 3 und S. 4 BGB, wenn ein Verbraucher zunächst eine Kundennummer sowie ein Passwort eingeben muss und erst im Anschluss die Angaben zur Kündigung des Vertrags tätigen kann.

Anm. d. Red.: Die Revision ist beim BGH unter dem Az. I ZR 272/25 anhängig. Vgl. ferner BGH MMR 2025, 538; LG Hamburg MMR 2024, 892; OLG Düsseldorf MMR 2009, 266; Güster/Booke MMR 2022, 450; LG Köln MMR 2023, 381; Sümmernann/Ewald MMR 2022, 713; BGH MMR 2020, 851; BGH MMR 2025, 812; OLG Hamburg MMR 2025, 543; OLG Düsseldorf MMR 2024, 868; OLG Nürnberg MMR 2025, 298 und OLG München MMR 2025, 639.

Schlagworte: Internetdienstleistungen; Webhosting; Abfrage der Kundennummer; Zwischenschritt; eindeutige Identifizierbarkeit; Missbrauchskontrolle

Sachverhalt

Der Kl. ist der Dachverband der 16 Verbraucherzentralen. Die Bekl. bietet auf einer Webseite Verbrauchern den Abschluss von Verträgen im Bereich der Internetdienstleistungen – etwa ein Webhosting – an, die jeweils eine Mindestlaufzeit vorsehen und über die Webseite der Bekl. gekündigt werden können. Zwischen den Parteien steht im Streit, ob die auf der Webseite der Bekl. bereitgestellte Möglichkeit zur Abgabe einer Kündigungserklärung den gesetzlichen Anforderungen entspricht.

Am 20.12.2024 befand sich auf der nachfolgend dargestellten Webseite der Bekl. in der Kopfzeile der Startseite u.a. eine Schaltfläche mit der Bezeichnung „Vertragsbeendigung“. Es folgte eine Einblendung der Webseite. Ein Nutzer wurde nach einer Betätigung der Schaltfläche „Vertragsbeendigung“ auf die nachfolgende Unterseite weitergeleitet, auf der er sich mit seiner Kundennummer und einem Passwort anmelden musste, um den Kündigungsvorgang in einem geschützten Kundenbereich fortzusetzen.

Der Kl. mahnte die Bekl. u.a. wegen eines Verstoßes gegen § 2 UKlaG iVm § 312k BGB erfolglos ab und forderte sie zur Abgabe einer strafbewehrten Unterlassungserklärung auf. Die Abgabe einer Unterlassungserklärung im Hinblick auf den vom Kl. geltend gemachten Verstoß gegen § 312k BGB lehnte die Bekl. ab.

Der Kl. meint, die Bekl. erfülle die sich aus § 312k Abs. 2 BGB ergebenden Pflichten nicht, insb. führe ein Betätigen der Kündigungsschaltfläche nicht unmittelbar zu einer Bestätigungsseite (§ 312k Abs. 2 S. 3 BGB) und die Bestätigungsseite sei zudem nicht ständig verfügbar (§ 312k Abs. 2 S. 4 BGB).

Die Bekl. meint, die Kündigungsschaltfläche auf der Webseite der Bekl. enthalte die in § 312k Abs. 2 S. 1 und S. 2 BGB genannten Vorgaben und führe den Verbraucher zu einer Bestätigungsseite gem. § 312k Abs. 2 S. 3 Hs. 1 BGB; die Bestätigungsseite der Bekl. erfülle auch die weiteren Voraussetzungen des § 312k Abs. 2 S. 4 BGB und enthalte keine Abweichungen zum Nachteil des Verbrauchers, § 312m Abs. 1 BGB. Die Abfrage der Kundennummer und des Passworts auf der Seite der

Bekl. diene der eindeutigen Identifizierbarkeit des Verbrauchers sowie der eindeutigen Zuordnung des betroffenen Vertragsverhältnisses und es werde eine missbräuchliche Kündigung verhindert. Sie meint, da es sich bei den von der Bekl. angebotenen Hosting-Verträgen um kontobasierte Dauerschuldverhältnisse handle, deren laufende Nutzung – etwa zum Anlegen und Verwalten von E-Mail-Konten, zum Zugriff auf gespeicherte Daten, zur DNS-Konfiguration oder zur Kontrolle des Domainstatus – ausschließlich über das eingeloggte Kundenkonto erfolge, stelle die der Abgabe der Kündigungserklärung vorgelagerte Anmeldung keine unzulässige Zugangshürde dar. Mit Blick auf Erwägungsgrund 57 DS-GVO sowie Art. 28, 32 DS-GVO und die noch umzusetzende NIS-2-RL (RL (EU) 2022/2555) sei jedenfalls eine europarechtskonforme Auslegung erforderlich.

Aus den Gründen

18 ... Die Klage ist ... begründet.

19 1. Dem Kl. steht gegen die Bekl. ein Anspruch auf Unterlassung gem. § 2 Abs. 1 S. 1 UKlaG iVm § 312k Abs. 2 S. 3 und S. 4 BGB zu.

20 a) Bei § 312k BGB handelt es sich um ein Verbraucherschutzgesetz iSv § 2 Abs. 1 S. 1 UKlaG.

21 aa) Gem. § 2 Abs. 1 S. 1 UKlaG kann im Interesse des Verbraucherschutzes auf Unterlassung und Beseitigung in Anspruch genommen werden, wer in anderer Weise als durch Verwendung oder Empfehlung von AGB Vorschriften zuwiderhandelt, die dem Schutz der Verbraucher dienen (Verbraucherschutzgesetz). Eine Norm dient dem Schutz der Verbraucher, wenn der Verbraucherschutz ihr eigentlicher Zweck ist. Sie kann auch anderen Zwecken dienen; es genügt aber nicht, wenn der Verbraucherschutz in der Norm nur untergeordnete Bedeutung hat oder eine nur zufällige Nebenwirkung ist. Die Norm muss Verhaltenspflichten des Unternehmers ggü. dem Verbraucher begründen (vgl. zum Ganzen BGH Urt. v. 6.2.2020 – I ZR 93/18 [= MMR 2020, 851] Rn. 15 – SEPA-Lastschrift, mwN).

22 bb) Die für den Streitfall maßgebliche Vorschrift des § 312k BGB fällt unter den Beispielskatalog des § 2 Abs. 2 UKlaG. Es handelt sich bei § 312k Abs. 1 S. 1 BGB um eine Vorschrift des Bürgerlichen Rechts, die iSv § 2 Abs. 2 Nr. 1 lit. c UKlaG für Verträge gilt, die im elektronischen Rechtsverkehr (§ 312i Abs. 1 S. 1 BGB) geschlossen werden können (vgl. BGH Urt. v. 22.5.2025 – I ZR 161/24 [= MMR 2025, 812] Rn. 13; Senat MMR 2025, 538 Rn. 31).

23 b) Die Bekl. hat gegen § 312k Abs. 2 S. 3 und S. 4 BGB verstoßen.

24 aa) Der Anwendungsbereich des § 312k BGB ist vorliegend eröffnet. Nach § 312k Abs. 1 S. 1 BGB hat ein Unternehmer die sich aus § 312k BGB ergebenden Pflichten zu erfüllen, wenn Verbrauchern über eine Webseite ermöglicht wird, einen Vertrag im elektronischen Geschäftsverkehr zu schließen, der auf die Begründung eines Dauerschuldverhältnisses gerichtet ist, das den Unternehmer zu einer entgeltlichen Leistung verpflichtet; es kommt nicht darauf an, dass der Vertrag tatsächlich auf diesem Wege abgeschlossen wurde (vgl. etwa OLG Hamburg Urt. v. 26.9.2024 – 5 UKI 1/23 [= MMR 2025, 543] Rn. 50). ...

25 bb) Die Bekl. hat die sich aus § 312k Abs. 2 S. 3 und S. 4 BGB ergebenden Pflichten nicht erfüllt.

26 (1) Der Kündigungsprozess gem. § 312k BGB ist mehrstufig aufgebaut. Nach § 312k Abs. 2 S. 1 BGB hat der Unternehmer sicherzustellen, dass der Verbraucher auf der Webseite gem. § 312k Abs. 1 S. 1 BGB eine Erklärung zur ordentlichen oder außerordentlichen Kündigung eines auf der Webseite abschließbaren Vertrags über eine Kündigungsschaltfläche abgeben

kann (vgl. dazu bereits Senat MMR 2025, 538 Rn. 37 ff.). Die Kündigungsschaltfläche muss gut lesbar mit nichts anderem als den Wörtern „Verträge hier kündigen“ oder mit einer entsprechenden eindeutigen Formulierung beschriftet sein (§ 312k Abs. 2 S. 2 BGB). Sie muss den Verbraucher nach § 312k Abs. 2 S. 3 BGB unmittelbar zu einer Bestätigungsseite führen, auf der er die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB machen und die Kündigung über die Betätigung einer Bestätigungsschaltfläche erklären kann (§ 312k Abs. 2 S. 3 Nr. 2 BGB). Die Schaltflächen und die Bestätigungsseite müssen gem. § 312k Abs. 2 S. 4 BGB ständig verfügbar sowie unmittelbar und leicht zugänglich sein.

27 Der Begriff der „Schaltfläche“ entspricht demjenigen des § 312j Abs. 3 S. 2 BGB; dieser ist grds. weit zu verstehen und erfasst jedes grafische Bedienelement, das es dem Anwender erlaubt, eine Aktion in Gang zu setzen oder dem System eine Rückmeldung zu geben (Senat MMR 2025, 538 Rn. 36, mwN).

28 (2) Im Streitfall stellt die Bekl. auf der von ihr betriebenen Webseite zwar eine Kündigungsschaltfläche bereit, die mit der Formulierung „Vertragsbeendigung“ beschriftet ist. Um eine Kündigung zu erklären, muss der Verbraucher aber nach dem Betätigen der Schaltfläche seine Kundennummer und sein Passwort eingeben. Die Kündigungsschaltfläche führt den Verbraucher damit nicht gem. § 312k Abs. 2 S. 3 BGB unmittelbar zu einer gem. § 312k Abs. 2 S. 4 BGB ständig verfügbaren Bestätigungsseite.

29 (a) Unmittelbarkeit iSv § 312k Abs. 2 S. 3 BGB ist gewährleistet, wenn der Verbraucher allein durch Betätigen der Kündigungsschaltfläche und ohne weitere Zwischenschritte auf die Bestätigungsseite gelangt (vgl. BeckOK IT-Recht/Föhlisch, 19. Ed. 1.7.2025, BGB § 312k Rn. 13; Staudinger/Thüsing BGB (2024), § 312k Rn. 22; vgl. auch OLG Düsseldorf Urt. v. 23.5.2024 – 20 UKI 3/23 [= MMR 2024, 868] Rn. 18; LG Hamburg MMR 2024, 892 Rn. 32), auf der er die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB tätigen und im Anschluss die Kündigungserklärung durch Betätigung der Bestätigungsschaltfläche gem. § 312k Abs. 2 S. 3 Nr. 2 BGB abgeben kann.

30 Das Tatbestandsmerkmal der ständigen Verfügbarkeit ist an das entsprechende Erfordernis in § 5 Abs. 1 TMG aF (jetzt: § 5 Abs. 1 DDG) angelehnt (vgl. BT-Drs. 19/30840 S. 18). Nach dieser Vorschrift sind die dort genannten Informationen zur Anbieterkennzeichnung u.a. ständig verfügbar zu halten. Für eine ständige Verfügbarkeit in diesem Sinne wird es als erforderlich angesehen, dass der Nutzer jederzeit und ohne Hindernisse auf die Pflichtangaben nach § 5 Abs. 1 TMG aF (bzw. § 5 Abs. 1 DDG) zugreifen kann (vgl. etwa BeckOK IT-Recht/Sesing-Wagenpfeil, 15. Ed. 1.7.2024, TMG § 5 Rn. 53), wobei eine nur vorübergehende technisch bedingte Unerreichbarkeit etwa wegen Wartungsarbeiten unschädlich ist (vgl. OLG Düsseldorf MMR 2009, 266 Rn. 18 und hierauf verweisend BT-Drs. 19/30840 S. 18). An einer ständigen Verfügbarkeit iSd § 5 Abs. 1 TMG aF bzw. § 5 Abs. 1 DDG fehlt es dagegen, wenn die Informationen erst nach Eingabe der persönlichen Daten, Kundenregistrierung, Hinzufügen eines Produktes zum virtuellen Warenkorb oder Abgabe einer Bestellung abrufbar sind (Föhlisch in Hoeren/Sieber/Holzner, MMR-HdB (62. EL Juni 2024), Teil 13.4 Rn. 64).

31 Hiervon ausgehend meint der Begriff der ständigen Verfügbarkeit in § 312k Abs. 2 S. 4 BGB nicht nur eine technische Erreichbarkeit, sondern auch eine einschränkungslose Möglichkeit zur Nutzung der Schaltflächen und der Bestätigungsseite. Nach dem Willen des Gesetzgebers soll durch das Tatbestandsmerkmal vor allem sichergestellt werden, dass der Verbraucher jederzeit und ohne vorherige Anmeldung auf die Schaltflächen

und die Bestätigungsseite zugreifen kann (vgl. BT-Drs. 19/30840 S. 18; BeckOK IT-Recht/Föhlisch, 19. Ed. 1.7.2025, BGB § 312k Rn. 20; Staudinger/Thüsing BGB (2024), § 312k Rn. 32). Dafür muss grds. die Verfügbarkeit der Webseite und währenddessen auch die einschränkungslose Kündigungsmöglichkeit bestehen (vgl. Buschmann/Panfil in Brönneke/Föhlisch/Tonner, Das neue Schuldrecht (2022), § 7 Rn. 40). Dies bedeutet allerdings nicht, dass der Verbraucher jederzeit auch auf die Bestätigungsschaltfläche zugreifen können muss. Denn nach der gesetzlichen Konzeption handelt es sich bei der Bestätigungsschaltfläche um eine nachgelagerte Schaltfläche (vgl. auch BeckOK IT-Recht/Föhlisch, 19. Ed. 1.7.2025, BGB § 312k Rn. 20; Güster/Booke MMR 2022, 450 (451)). ...

32 (b) Das im Streitfall bestehende Erfordernis, nach dem Betätigen der Kündigungsschaltfläche eine Kundennummer und ein Passwort einzugeben, stellt dagegen einen Zwischenschritt dar, der bei typisierender Betrachtung grds. geeignet ist, den Verbraucher etwa dann von der Kündigung abzuhalten, wenn die entsprechenden Daten zum Zeitpunkt der beabsichtigten Kündigung nicht oder nicht ohne Weiteres bereitstehen (so etwa auch LG Köln MMR 2023, 381 Rn. 4). Ein solcher Zwischenschritt ist dem Gesetz nicht zu entnehmen und läuft dem Anliegen des Gesetzgebers entgegen, eine einfache und leicht zugängliche Kündigungsmöglichkeit ohne hohe Hürden zu schaffen (vgl. dazu BGH Urt. v. 22.5.2025 – I ZR 161/24 [= MMR 2025, 812] Rn. 26; Senat MMR 2025, 538 Rn. 45; OLG München Urt. v. 20.3.2025 – 6 U 4336/23 [= MMR 2025, 639] Rn. 37; BT-Drs. 19/30840, 15). Aufgrund des erforderlichen Zwischenschrittes führt ein Betätigen der Kündigungsschaltfläche nicht unmittelbar zu einer Bestätigungsseite, und die Bestätigungsseite ist auch nicht ständig verfügbar, weil eine Eingabe der Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB sowie ein Betätigen der Bestätigungsschaltfläche (§ 312k Abs. 2 S. 3 Nr. 2 BGB) jedenfalls dann nicht (sofort) möglich ist, wenn die angeforderten Daten bei dem Verbraucher nicht vorhanden sind.

33 (c) Eine andere Betrachtung ist nicht deshalb geboten, weil dem Verbraucher nach § 312k Abs. 2 S. 3 Nr. 1 lit. b BGB auf der Bestätigungsseite ermöglicht werden soll, Angaben zu seiner eindeutigen Identifizierbarkeit zu machen. Denn auch insoweit dürfen keine unnötigen Hürden aufgebaut werden; unzulässig ist auch insoweit etwa die Angabe eines Kundenkennworts, die Beantwortung von Sicherheitsfragen, die Identifizierung über Dienste Dritter, die dem Verbraucher möglicherweise nicht oder nicht mehr zugänglich sind. Es muss vielmehr immer auch eine Möglichkeit bestehen, durch Angabe von Namen und ggf. weiteren gängigen Identifizierungsmerkmalen – etwa der Wohnanschrift und dergleichen – eine Kündigung zu erklären (vgl. MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 21; BT-Drs. 19/30840 S. 17).

34 Soweit die Bekl. dagegen darauf abstellt, dass die Eingabe von Kundennummer und Passwort der eindeutigen Identifizierbarkeit diene und eine irrtümliche oder missbräuchliche Kündigung verhindere, übersieht sie, dass Identifizierbarkeit gem. § 312k Abs. 2 S. 3 Nr. 1 lit. b BGB gerade nicht meint, dass die Angaben für den Unternehmer auch eindeutig verifizierbar sind. Für den Unternehmer muss es vielmehr ausreichen, dass er den kündigungswilligen Verbraucher von anderen Verbrauchern unterscheiden kann (vgl. Halder jurisPR-ITR 2/2023 Anm. 3; BeckOK BGB/Maume, 75. Ed. 1.8.2025, BGB § 312k Rn. 26) und durch die Angaben nach § 312k Abs. 2 S. 3 Nr. 1 lit. c BGB eine Zuordnung zu dem zu kündigenden Vertrag vornehmen kann. Der Bekl. dient die Abfrage des Passwortes aber nicht der Identifizierung des Verbrauchers. Es handelt sich vielmehr um eine Maßnahme der Missbrauchs kontrolle, die keine Identifizierung, sondern eine Verifizierung bezweckt.

35 Nach dem in der Gesetzesbegründung zum Ausdruck kommenden Willen des Gesetzgebers, der in dem Tatbestandsmerkmal der Identifizierbarkeit (§ 312k Abs. 2 S. 3 Nr. 1 lit. b BGB) seinen Niederschlag gefunden hat, ist die Eingabe von Log-in-Daten für eine Zuordnung der Kündigungserklärung zu einem bestimmten Verbraucher nicht erforderlich und dementsprechend auch nicht in § 312k Abs. 2 S. 3 BGB enthalten. Die Angaben, die der Verbraucher gem. § 312k Abs. 2 S. 3 BGB tätigen können muss, sind aber als Minimal- und als Maximalvorgabe zu verstehen; ihre Funktion als Minimalvorgabe soll sicherstellen, dass der Verbraucher alle Angaben machen kann, die er für seine Erklärung und deren Rechtswirksamkeit benötigt, und die Beschränkung der zu verlangenden Angaben soll Ausgestaltungen verhindern, bei denen der Unternehmer weitere, für den Verbraucher ggf. nicht ohne Weiteres verfügbare Daten abfragt und so eine einfache und unkomplizierte Kündigung erschwert (vgl. BeckOK BGB/Maume, 75. Ed. 1.8.2025, BGB § 312k Rn. 24; MüKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 19). Das Risiko eines Missbrauchs hat der Gesetzgeber dabei erkannt und aufgrund der Kumulierung der möglichen Angaben nach § 312k Abs. 2 S. 3 Nr. 1 BGB als vernachlässigbar erachtet (vgl. Halder jurisPR-ITR 2/2023 Anm. 3); eine Verifizierung des Verbrauchers erfolgt nach dem Regelungskonzept des § 312k Abs. 2 S. 3 Nr. 1 BGB allein durch die Angaben zur Identifizierbarkeit (§ 312k Abs. 2 S. 3 Nr. 1 lit. b BGB) und der eindeutigen Bezeichnung des Vertrags (§ 312k Abs. 2 S. 3 Nr. 1 lit. c BGB).

36 Ohne Belang ist es daher auch, ob der Verbraucher typischerweise Log-in-Daten schneller zu Hand hat als die Angaben nach § 312k Abs. 2 S. 3 Nr. 1 lit. c BGB für eine Zuordnung des Vertrags. Denn dabei handelt es sich um eine Frage, die der Gesetzgeber zugunsten der Vertragsdaten entschieden hat und die de lege lata hinzunehmen ist (vgl. Halder jurisPR-ITR 2/2023 Anm. 3).

37 (d) Anders als die Bekl. meint, ist bei der Abgabe der Kündigungserklärung gem. § 312k BGB auch nicht in dem jeweiligen Einzelfall ein Vergleich mit der Art und Weise des Vertragsschlusses geboten. Der Gesetzgeber ist zwar davon ausgegangen, dass die Kündigung von im elektronischen Geschäftsverkehr abgeschlossenen Verträgen Verbraucher oft vor besondere Herausforderungen stellte, weil im Vergleich zum einfachen Abschluss eines solchen Vertrags dessen Kündigung direkt über eine Webseite teilweise nicht möglich ist oder häufig durch die Webseitengestaltung erschwert wurde. Die in § 312k BGB vorgesehenen Verpflichtungen des Unternehmers sollen daher Verbraucher in Bezug auf Dauerschuldverhältnisse in die Lage versetzen, Kündigungserklärungen im elektronischen Geschäftsverkehr in vergleichbar einfacher Weise abzugeben wie Erklärungen zum Abschluss entsprechender Verträge (vgl. BT-Drs. 19/30840, S. 15). Zur Erreichung dieses Anliegens hat der Gesetzgeber aber bei der im Gesetzgebungsverfahren gebotenen typisierenden Betrachtung die Voraussetzungen generell abstrakt vorgegeben, die der Unternehmer zu erfüllen hat, um die Abgabe einer Kündigungserklärung des Verbrauchers zu ermöglichen, ohne dass dem Gesetz zu entnehmen ist, dass im jeweiligen Einzelfall eine vergleichende Betrachtung erforderlich oder angezeigt sei.

38 (e) Entgegen der Ansicht der Bekl. ist auch eine einschränkende Auslegung des § 312k Abs. 2 S. 4 BGB nicht geboten.

39 (aa) Richtig ist allerdings zunächst, dass abw. von dem vorstehenden Verständnis zT in Rspr. und Lit. eine einschränkende Auslegung des § 312k Abs. 2 S. 4 BGB erwogen wird. Das Erfordernis zum Einloggen in einen geschützten Kundenbereich stehe nach dieser Auffassung dem Tatbestandsmerkmal der ständigen Verfügbarkeit jedenfalls dann nicht entgegen, wenn die

Nutzung des Dienstes, welcher Gegenstand des Dauerschuldverhältnisses ist, seiner Natur nach ohnehin ein Log-in erfordere (vgl. etwa OLG Nürnberg Ur. v. 30.7.2024 – 3 U 2214/23 [= MMR 2025, 298] Rn. 19 ff. und Rn. 31; Sümmernann/Ewald MMR 2022, 713 (717); Schirnbacher/Schreiber ZdiW 2022, 56 (60)).

40 Der Senat vermag diesem Ansatz jedoch nicht zu folgen. Denn eine derartige einschränkende Auslegung für bestimmte Fallgestaltungen steht nicht nur dem ausdrücklich erklärten und im Gesetzeswortlaut seinen Niederschlag findenden Willen des Gesetzgebers entgegen (vgl. BeckOK BGB/Maume, 75. Ed. 1.8. 2025, BGB § 312k Rn. 39), sondern stellt methodisch eine unzulässige teleologische Reduktion des § 312k Abs. 2 S. 4 BGB dar (zutreffend Halder jurisPR-ITR 1/2025 Anm. 4; vgl. auch ders. jurisPR-ITR 2/2023 Anm. 3). Eine teleologische Reduktion erfordert nämlich, dass der Anwendungsbereich der anzuwendenden Norm planwidrig zu weit gefasst worden ist (stRspr.; vgl. nur BGH Ur. v. 11.11.2011 – V ZR 65/11 Rn. 10). Es gibt aber keinerlei Anhaltspunkte dafür, dass der Gesetzgeber die – praktisch durchaus häufige – Konstellation, dass ein Verbraucher bei der Nutzung des abgeschlossenen Dauerschuldverhältnisses zunächst einen geschützten Kundenbereich aufsucht, wie dies etwa bei Streamingdiensten für Musik, Sportevents, Filme und Serien, bei digitalen Nachrichten- und Zeitungsdiensten oder auf Gaming-Plattformen typischerweise der Fall ist, übersehen haben könnte und dass er sie andernfalls von dem Anwendungsbereich des § 312k Abs. 2 S. 4 BGB ausgenommen hätte (so aber OLG Nürnberg Ur. v. 30.7.2024 – 3 U 2214/23 [= MMR 2025, 298] Rn. 31). Hinzu kommt, dass die Gründe dafür, dass ein Verbraucher die Anmeldedaten zum Zeitpunkt der beabsichtigten Kündigung ggf. nicht parat haben und sich eine Kündigung aus diesem Grunde durch das Erfordernis eines Log-in bzw. der Eingabe von Log-in-Daten erschweren kann, vielfältig sein können (vgl. ausf. zum Ganzen Halder jurisPR-ITR 1/2025 Anm. 4).

41 (bb) Schließlich ist eine andere Betrachtung entgegen der Auffassung der Bekl. nicht mit Blick auf Art. 28, 32 DS-GVO oder auf Art. 21 NIS-2-Richtlinie (RL (EU) 2022/2555) geboten. Insoweit verkennt die Bekl., dass die Vorschrift des § 312k BGB einem Verbraucher ermöglichen soll, im Anwendungsbereich der Norm eine Kündigungserklärung abzugeben. Für die Abgabe einer Kündigungserklärung und deren Zugang bei dem Unternehmer bedarf es jedoch grds. keiner Authentifizierung des Kündigenden; die von der Bekl. geschilderten Schwierigkeiten bei der Löschung von Daten aufgrund einer missbräuchlichen Kündigung – etwa im Fall eines Identitätsdiebstahls – können sich bei einer Kündigung in Schrift- oder Textform gleichermaßen stellen. Im Anwendungsbereich des § 312k BGB kommt hinzu, dass die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB regelmäßig jedenfalls in der Gesamtheit nicht allgemein bekannt sind und das Missbrauchsrisiko eher geringer ist als bei sonstigen (textlichen oder schriftlichen) Erklärungen, bei denen der Unternehmer eine zweifelsfreie Identifizierung auch nicht vornehmen kann (vgl. Halder jurisPR-ITR 2/2023 Anm. 3).

42 Nichts anderes ergibt sich auch aus Erwägungsgrund 57 DS-GVO (VO (EU) 2016/679), der für die Identifizierung einer betroffenen Person auf ein Authentifizierungsverfahren mit Berechtigungsnachweisen verweist. Denn dieser Erwägungsgrund bezieht sich ausdrücklich allein auf eine Anmeldung bei einem Online-Dienst, die iRd § 312k BGB – wie dargelegt – nicht vorgesehen ist. IÜ sieht auch der europäische Gesetzgeber für den Widerruf eines Fernabsatzvertrags (vgl. Art. 11a RL 2011/83/EU – (Verbraucherrechte-RL)) – bei insoweit durchaus vergleichbarer Interessenlage – keine Authentifizierung vor. Nach Art. 11a Abs. 2 lit. b Verbraucherrechte-RL sind neben dem Namen des

Verbrauchers (Art. 11a Abs. 2 lit. a Verbraucherrechte-RL) lediglich Angaben zur Identifizierung des Vertrags zu tätigen (etwa Bestell- oder Vertragsnummer) und die stets erforderliche Beantwortung der Abfrage eines Kundenkennworts wird auch insoweit als unzulässig angesehen (vgl. etwa Wiebe/Sengül WRP 2025, 574 (580) Rn. 41; Halder jurisPR-ITR 18/2025 Anm. 2); allenfalls zulässig ist es, wie etwa Erwägungsgrund 37 RL (EU) 2023/2673 zeigt, in dem Log-in-Bereich eines Kundenkontos eine zusätzliche Kündigungsmöglichkeit ohne weitere Identifizierung zu schaffen.

43 c) Die weiteren Voraussetzungen eines Unterlassungsanspruchs sind ebenfalls gegeben.

44 aa) Neben der bereits durch den Verstoß gegen § 312k Abs. 2 S. 4 BGB indizierten Wiederholungsgefahr setzt ein Unterlassungsanspruch auf Grundlage des § 2 Abs. 1 S. 1 UKlaG voraus, dass er im Interesse des Verbraucherschutzes geltend gemacht wird. Hierfür ist erforderlich, dass der dem Anspruch zugrunde liegende Verstoß die Kollektivinteressen der Verbraucher berührt. Das ist der Fall, wenn der Verstoß in seinem Gewicht und in seiner Bedeutung über den Einzelfall hinausreicht und eine generelle Klärung geboten erscheinen lässt (vgl. BGH Ur. v. 6.2.2020 – I ZR 93/18 [= MMR 2020, 851] Rn. 36 – SEPA-Lastschrift, mwN).

45 bb) Diese Voraussetzungen sind im Streitfall gegeben. Der in Rede stehende Verstoß gegen § 312k Abs. 2 S. 4 BGB berührt die Kollektivinteressen der Verbraucher. Der Kl. beanstandet eine nicht nur den Einzelfall betreffende Verhaltensweise, sondern diese kann eine Vielzahl von Verbrauchern betreffen. Das beanstandete Verhalten geht daher in seinem Gewicht und seiner Bedeutung über den Einzelfall hinaus, sodass eine generelle Klärung geboten ist. ...

KG: Unzulässige Abfrage von Log-in-Daten bei Kündigung von Dauerschuldverhältnissen

Kündigungsschaltfläche

BGB §§ 312i Abs. 1 S. 1, 312k Abs. 2 S. 3, S. 4; UWG §§ 3, 3a, 8 Abs. 1, Abs. 3; DDG §§ 1 Abs. 4 Nr. 1, 5 Abs. 1
Urteil vom 12.11.2025 – 5 U 6/25 (LG Berlin); nicht rechtskräftig

Leitsatz der Redaktion

Die Gestaltung des Kündigungsprozesses für Dauerschuldverhältnisse im elektronischen Geschäftsverkehr nach § 312k Abs. 2 S. 3 und S. 4 BGB ist unzulässig, wenn der Zugang zur Kündigungserklärung von der Eingabe von Login-Daten (vor allem eines Passworts) abhängig gemacht wird.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2025, 32304. Die Revision ist beim BGH anhängig unter Az. I ZR 275/25. Vgl. auch die Parallelentscheidung MMR 2026, 528 – in diesem Heft. Zur Gestaltung der Kündigungsschaltfläche vgl. auch KG MMR 2025, 538 mAnm Halder/Schubert. Dazu auch Pech MMR 2026, 427 – in diesem Heft. Vgl. ferner LG Hamburg MMR 2024, 892; OLG Düsseldorf MMR 2009, 266; Güster/Booke MMR 2022, 450; LG Köln MMR 2023, 381; Sümmernann/Ewald MMR 2022, 713; OLG Hamburg MMR 2025, 543; OLG Düsseldorf MMR 2024, 868; BGH MMR 2025, 812; OLG München MMR 2025, 639 und OLG Nürnberg MMR 2025, 298 und KG MMR 2025, 538.

Schlagworte: Streamingdienst; Kündigungsschaltfläche; Passwortabfrage; wesentliche Hürde; ständige Verfügbarkeit; eindeutige Identifizierbarkeit

Sachverhalt

Der Kl., die Wettbewerbszentrale, nimmt die Bekl. – ein Unternehmen, das einen Streamingdienst für Serien und Filme gegen

Zahlung eines monatlichen Entgelts anbietet – auf Unterlassung und Zahlung in Anspruch. Zwischen den Parteien steht im Streit, ob die auf der Webseite der Bekl. bereitgestellte Möglichkeit zur Abgabe einer Kündigungserklärung den gesetzlichen Anforderungen entspricht; es muss zur Kündigung des Vertrags eine E-Mail-Adresse bzw. Handynummer und ein Passwort eingegeben werden. Auf die tatsächlichen Feststellungen in dem angefochtenen Urteil wird gem. § 540 Abs. 1 S. 1 Nr. 1 ZPO Bezug genommen.

Das LG hat die Klage abgewiesen. Zur Begründung hat es im Wesentlichen ausgeführt, die Bekl. habe die sich aus § 312k BGB ergebenden Pflichten erfüllt, insb. würde die Bestätigungsseite den Vorgaben des § 312k Abs. 2 S. 3 und S. 4 BGB entsprechen.

Der Kl. wendet sich mit der Berufung gegen das Urteil des LG und rügt im Wesentlichen, dass die Passwortabfrage eine unzulässige Hürde darstelle. Die Angabe sei nicht erforderlich, da bereits die E-Mail-Adresse eine eindeutige Identifizierung ermögliche.

Die Bekl. meint im Wesentlichen, nach Eingabe der E-Mail-Adresse bzw. Handynummer und der Eingabe des Passworts sowie der Auswahl, ob die Kündigung sofort oder erst zum Ende des aktuellen Abrechnungszeitraums wirksam werden soll, könne die Kündigung durch einen Klick auf die eindeutig beschriftete Schaltfläche „Kündigung abschließen“ unmittelbar abgesendet werden; ein Log-in sei nicht erforderlich. Die Abfrage von E-Mail-Adresse/Handynummer und Passwort sei zulässig und zudem erforderlich, um den Vertrag eindeutig zuordnen zu können.

Aus den Gründen

7 Die ... Berufung ist begründet. Zu Unrecht verneint das LG einen Verstoß gegen § 312k Abs. 2 S. 3 und S. 4 BGB. ...

14 Die Klage ist ... begründet.

15 1. Dem Kl. steht gegen die Bekl. ein Anspruch auf Unterlassung gem. § 8 Abs. 1 S. 1, Abs. 3 Nr. 2, §§ 3, 3a UWG iVm § 312k Abs. 2 S. 3 und 4 BGB zu.

16 a) Bei § 312k BGB handelt es sich um eine Marktverhaltensregelung iSv § 3a UWG.

17 aa) ... Eine Vorschrift, die dem Schutz von Rechten, Rechtsgütern oder sonstigen Interessen von Marktmittelbewerbern, Verbrauchern oder sonstigen Marktteilnehmern dient, stellt eine Marktverhaltensregelung dar, wenn das geschützte Interesse gerade durch die Marktteilnahme, also durch den Abschluss von Austauschverträgen und den nachfolgenden Verbrauch oder Gebrauch der erworbenen Ware oder in Anspruch genommenen Dienstleistung berührt wird. Nicht erforderlich ist dabei eine spezifisch wettbewerbsbezogene Schutzfunktion in dem Sinne, dass die Regelung die Marktteilnehmer speziell vor dem Risiko einer unlauteren Beeinflussung ihres Marktverhaltens schützt. Die Vorschrift muss aber zumindest auch den Schutz der wettbewerbsbezogenen Interessen der Marktteilnehmer bezwecken; lediglich reflexartige Auswirkungen zu deren Gunsten genügen daher nicht (stRspr.; vgl. nur BGH Urt. v. 10.11.2022 – I ZR 16/22 Rn. 19 – Stickstoffgenerator, mwN). Unerheblich ist, ob die Vorschrift den Schutz aller Marktteilnehmer oder nur der Mitbewerber oder nur der Verbraucher oder nur der sonstigen Marktteilnehmer (vgl. § 2 Abs. 1 Nr. 3 UWG) zum Ziel hat (vgl. etwa Köhler/Odörfer in Köhler/Bornkamm/Feddersen, UWG, 43. Aufl. 2025, § 3a Rn. 1.65). Dem Interesse der Verbraucher und sonstigen Marktteilnehmer dient eine Norm, wenn sie deren Informationsinteresse sowie deren Entscheidungs- und Verhaltensfreiheit in Bezug auf die Marktteilnahme schützt (vgl. zum Ganzen Senat Beschl. v. 12.12.2024 – 5 U 77/22 Rn. 11 f., mwN).

18 bb) Die Vorschrift des § 312k BGB verpflichtet Unternehmer, Verbrauchern eine einfache Möglichkeit zur Kündigung von (bestimmten) Dauerschuldverhältnissen im elektronischen Geschäftsverkehr bereitzustellen. Sie dient damit nicht nur dem Schutz der Verbraucher, sondern ist auch darauf ausgerichtet, das Marktverhalten im Interesse der Marktteilnehmer zu regeln und stellt damit eine Marktverhaltensregelung dar (vgl. etwa Halder jurisPR-ITR 17/2023 Anm. 5; so wohl auch BeckOK BGB/Maume 1.8.2025, § 312k Rn. 46; MÜKoBGB/Wendehorst, 10. Aufl. 2025, BGB § 312k Rn. 38; Staudinger/Thüsing, BGB (2024), § 312k, Rn. 47).

19 b) Die Bekl. hat gegen § 312k Abs. 2 S. 3 und S. 4 BGB verstoßen.

20 aa) Der Anwendungsbereich des § 312k BGB ist vorliegend eröffnet. Nach § 312k Abs. 1 S. 1 BGB hat ein Unternehmer die sich aus § 312k BGB ergebenden Pflichten zu erfüllen, wenn Verbrauchern über eine Webseite ermöglicht wird, einen Vertrag im elektronischen Geschäftsverkehr zu schließen, der auf die Begründung eines Dauerschuldverhältnisses gerichtet ist, das den Unternehmer zu einer entgeltlichen Leistung verpflichtet; es kommt nicht darauf an, dass der Vertrag tatsächlich auf diesem Wege abgeschlossen wurde (vgl. etwa Hanseatisches OLG Hamburg Urt. v. 26.9.2024 – 5 UKI 1/23 [= MMR 2025, 543] Rn. 50). Im Streitfall ermöglicht die Bekl. es (auch) Verbrauchern über die von ihr betriebene Webseite unter Einsatz digitaler Dienste und damit im elektronischen Geschäftsverkehr (§ 312k Abs. 1 S. 1, § 312i Abs. 1 S. 1 BGB iVm § 1 Abs. 4 Nr. 1 DDG) einen auf die Begründung eines Dauerschuldverhältnisses gerichteten Vertrag abzuschließen, durch den sie in Ausübung ihrer gewerblichen Tätigkeit als Unternehmerin (§ 14 BGB) gegen Zahlung eines monatlichen Entgeltes verpflichtet ist, bestimmte digitale Leistungen (Webhosting oder Online-Speicherdienste) zu erbringen.

21 bb) Die Bekl. hat die sich aus § 312k Abs. 2 S. 3 und S. 4 BGB ergebenden Pflichten nicht erfüllt.

22 (1) Der Kündigungsprozess gem. § 312k BGB ist mehrstufig aufgebaut. Nach § 312k Abs. 2 S. 1 BGB hat der Unternehmer sicherzustellen, dass der Verbraucher auf der Webseite gem. § 312k Abs. 1 S. 1 BGB eine Erklärung zur ordentlichen oder außerordentlichen Kündigung eines auf der Webseite abschließbaren Vertrags über eine Kündigungsschaltfläche abgeben kann (vgl. dazu bereits Senat MMR 2025, 538 Rn. 37 ff.). Die Kündigungsschaltfläche muss gut lesbar mit nichts anderem als den Wörtern „Verträge hier kündigen“ oder mit einer entsprechenden eindeutigen Formulierung beschriftet sein (§ 312k Abs. 2 S. 2 BGB). Sie muss den Verbraucher nach § 312k Abs. 2 S. 3 BGB unmittelbar zu einer Bestätigungsseite führen, auf der er die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB machen und die Kündigung über die Betätigung einer Bestätigungsschaltfläche erklären kann (§ 312k Abs. 2 S. 3 Nr. 2 BGB). Die Schaltflächen und die Bestätigungsseite müssen gem. § 312k Abs. 2 S. 4 BGB ständig verfügbar sowie unmittelbar und leicht zugänglich sein.

23 Der Begriff der „Schaltfläche“ entspricht demjenigen des § 312j Abs. 3 S. 2 BGB; dieser ist grds. weit zu verstehen und erfasst jedes grafische Bedienelement, das es dem Anwender erlaubt, eine Aktion in Gang zu setzen oder dem System eine Rückmeldung zu geben (Senat MMR 2025, 538 Rn. 36, mwN).

24 (2) Im Streitfall stellt die Bekl. auf der von ihr betriebenen Webseite zwar eine Kündigungsschaltfläche bereit, die mit der Formulierung „Mitgliedschaft kündigen“ beschriftet ist. Um eine Kündigung zu erklären, muss der Verbraucher aber nach dem Betätigen der Schaltfläche seine E-Mail-Adresse bzw. Han-

dynammer und sein Passwort eingeben. Die Kündigungsschaltfläche führt den Verbraucher damit nicht gem. § 312k Abs. 2 S. 3 BGB unmittelbar zu einer gem. § 312k Abs. 2 S. 4 BGB ständig verfügbaren Bestätigungsseite, auf der (nur) die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB getätigt werden können und die Kündigungserklärung mittels einer ständig verfügbaren Bestätigungsschaltfläche abgegeben werden kann.

25 (a) Unmittelbarkeit iSv § 312k Abs. 2 S. 3 BGB ist gewährleistet, wenn der Verbraucher allein durch Betätigen der Kündigungsschaltfläche und ohne weitere Zwischenschritte auf die Bestätigungsseite gelangt (vgl. BeckOK IT-Recht/Föhlisch, BGB 1.7.2025, § 312k Rn. 13; Staudinger/Thüsing, BGB (2024), § 312k Rn. 22; vgl. auch OLG Düsseldorf Urte. v. 23.5.2024 – 20 UKI 3/23 [= MMR 2024, 868] Rn. 18; LG Hamburg MMR 2024, 892 Rn. 32), auf der er die Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB tätigen und im Anschluss die Kündigungserklärung durch Betätigung der Bestätigungsschaltfläche gem. § 312k Abs. 2 S. 3 Nr. 2 BGB abgeben kann.

26 Das Tatbestandsmerkmal der ständigen Verfügbarkeit ist an das entsprechende Erfordernis in § 5 Abs. 1 TMG aF (jetzt: § 5 Abs. 1 DDG) angelehnt (vgl. BT-Drs. 19/30840 S. 18). Nach dieser Vorschrift sind die dort genannten Informationen zur Anbieterkennzeichnung u.a. ständig verfügbar zu halten. Für eine ständige Verfügbarkeit in diesem Sinne wird es als erforderlich angesehen, dass der Nutzer jederzeit und ohne Hindernisse auf die Pflichtangaben nach § 5 Abs. 1 TMG aF (bzw. § 5 Abs. 1 DDG) zugreifen kann (vgl. etwa BeckOK IT-Recht/Sesing-Wagenpfeil 1.7.2024, § 5 TMG Rn. 53), wobei eine nur vorübergehende technisch bedingte Unerreichbarkeit etwa wegen Wartungsarbeiten unschädlich ist (vgl. OLG Düsseldorf MMR 2009, 266 Rn. 18 und hierauf verweisend BT-Drs. 19/30840, S. 18). An einer ständigen Verfügbarkeit iSd § 5 Abs. 1 TMG aF bzw. § 5 Abs. 1 DDG fehlt es dagegen, wenn die Informationen erst nach Eingabe der persönlichen Daten, Kundenregistrierung, Hinzufügen eines Produktes zum virtuellen Warenkorb oder Abgabe einer Bestellung abrufbar sind (Föhlisch in Hoeren/Sieber/Holz-nagel, MMR-HdB (62. EL Juni 2024), Teil 13.4 Rn. 64).

27 Hiervon ausgehend meint der Begriff der ständigen Verfügbarkeit in § 312k Abs. 2 S. 4 BGB nicht nur eine technische Erreichbarkeit, sondern auch eine einschränkungslose Möglichkeit zur Nutzung der Schaltflächen und der Bestätigungsseite. Nach dem Willen des Gesetzgebers soll durch das Tatbestandsmerkmal vor allem sichergestellt werden, dass der Verbraucher jederzeit und ohne vorherige Anmeldung auf die Schaltflächen und die Bestätigungsseite zugreifen kann (vgl. BT-Drs. 19/30840, 18; BeckOK IT-Recht/Föhlisch 1.7.2025, § 312k BGB Rn. 20; Staudinger/Thüsing, BGB (2024), § 312k Rn. 32). Dafür muss grds. die Verfügbarkeit der Webseite und währenddessen auch die einschränkungslose Kündigungsmöglichkeit bestehen (vgl. Buschmann/Panfil in Brönneke/Föhlisch/Tonner, Das neue Schuldrecht (2022), § 7 Rn. 40). Dies bedeutet allerdings nicht, dass der Verbraucher jederzeit auch auf die Bestätigungsschaltfläche zugreifen können muss. Denn nach der gesetzlichen Konzeption handelt es sich bei der Bestätigungsschaltfläche um eine nachgelagerte Schaltfläche (vgl. auch BeckOK IT-Recht/Föhlisch 1.7.2025, § 312k BGB Rn. 20; Güster/Booke MMR 2022, 450 (451)). Erforderlich ist es zunächst, dass der Verbraucher die Kündigungsschaltfläche bedienen und sodann ohne weitere Hindernisse auf die Bestätigungsseite gelangen kann, um dort die für die Kündigung erforderlichen Daten gem. § 312k Abs. 2 S. 3 Nr. 1 BGB einzugeben. Bei funktionaler Betrachtungsweise ist es daher jedenfalls ausreichend, wenn der Verbraucher erst dann auf die Bestätigungsschaltfläche zugreifen kann, wenn dies für die Abgabe der Kündigungserklärung erforderlich ist.

28 (b) Das im Streitfall bestehende Erfordernis, nach dem Betätigen der Kündigungsschaltfläche neben der E-Mail-Adresse auch ein Passwort einzugeben, stellt dagegen einen Schritt dar, der bei typisierender Betrachtung grds. geeignet ist, den Verbraucher etwa dann von der Kündigung abzuhalten, wenn die entsprechenden Daten zum Zeitpunkt der beabsichtigten Kündigung nicht oder nicht ohne Weiteres bereitstehen (so etwa auch LG Köln MMR 2023, 381 Rn. 4). Ein solcher Schritt ist dem Gesetz nicht zu entnehmen und läuft dem Anliegen des Gesetzgebers entgegen, eine einfache und leicht zugängliche Kündigungsmöglichkeit ohne hohe Hürden zu schaffen (vgl. dazu BGH Urte. v. 22.5.2025 – I ZR 161/24 [= MMR 2025, 812] Rn. 26; Senat MMR 2025, 538 Rn. 45; OLG München Urte. v. 20.3.2025 – 6 U 4336/23 [= MMR 2025, 639] Rn. 37; BT-Drs. 19/30840, 15). Unerheblich ist in diesem Zusammenhang, ob es sich bei der Eingabe von E-Mail-Adresse bzw. Handynummer und Passwort um einen Log-in handelt. Denn ein Betätigen der Kündigungsschaltfläche führt nicht unmittelbar zu einer Bestätigungsseite, die den Vorgaben des § 312k Abs. 2 S. 3 Nr. 1 BGB entspricht (s. sogleich); eine Bestätigungsseite ist damit auch nicht ständig verfügbar iSd § 312k Abs. 2 S. 4 BGB, weil eine Eingabe der Angaben gem. § 312k Abs. 2 S. 3 Nr. 1 BGB sowie ein Betätigen der Bestätigungsschaltfläche (§ 312k Abs. 2 S. 3 Nr. 2 BGB) jedenfalls dann nicht (sofort) möglich ist, wenn die angeforderten Daten – insb. das abgefragte Passwort – bei dem Verbraucher nicht vorhanden sind.

29 (c) Eine andere Betrachtung ist nicht deshalb geboten, weil dem Verbraucher nach § 312k Abs. 2 S. 3 Nr. 1 lit. b BGB auf der Bestätigungsseite ermöglicht werden soll, Angaben zu seiner eindeutigen Identifizierbarkeit zu machen. Die Angabe eines Passwortes dient nämlich nicht der eindeutigen Identifizierbarkeit des Verbrauchers.

30 Bei der Auslegung des Tatbestandsmerkmals der Identifizierbarkeit dürfen ebenfalls keine unnötigen Hürden aufgebaut werden; unzulässig ist auch insoweit etwa die Angabe eines Kundenkennworts, die Beantwortung von Sicherheitsfragen, die Identifizierung über Dienste Dritter, die dem Verbraucher möglicherweise nicht oder nicht mehr zugänglich sind. Es muss vielmehr immer auch eine Möglichkeit bestehen, durch Angabe von Namen und ggf. weiteren gängigen Identifizierungsmerkmalen – etwa der Wohnanschrift und dergleichen – eine Kündigung zu erklären (vgl. MüKoBGB/Wendehorst, 10. Aufl. 2025, § 312k Rn. 21; BT-Drs. 19/30840, 17). Soweit die Bekl. dagegen darauf abstellt, dass die Eingabe von E-Mail-Adresse bzw. Handynummer und Passwort der eindeutigen Identifizierbarkeit diene und eine irrtümliche oder missbräuchliche Kündigung verhindere, übersieht sie, dass Identifizierbarkeit gem. § 312k Abs. 2 S. 3 Nr. 1 lit. b BGB gerade nicht meint, dass die Angaben für den Unternehmer auch eindeutig verifizierbar sind. Für den Unternehmer muss es vielmehr ausreichen, dass er den kündigungswilligen Verbraucher von anderen Verbrauchern unterscheiden kann (vgl. Halder jurisPR-ITR 2/2023 Anm. 3; BeckOK BGB/Maume, 1.8.2025, § 312k Rn. 26) und durch die Angaben nach § 312k Abs. 2 S. 3 Nr. 1 lit. c BGB eine Zuordnung zu dem zu kündigenden Vertrag vornehmen kann. Der Bekl. dient die Abfrage des Passwortes aber nicht der Identifizierung des Verbrauchers. Der Verbraucher identifiziert sich mittels Angabe seiner E-Mail-Adresse bzw. Handynummer, durch die, wie dies auch während der Erörterung in der mündlichen Verhandlung deutlich wurde, bereits eine Vertragszuordnung bei der Bekl. erfolgen kann. Durch die Angabe des Passwortes wird von der Bekl. vielmehr überprüft, ob die Kündigungserklärung auch von dem bei ihr registrierten Verbraucher abgegeben werden soll; es handelt sich um eine Maßnahme der Missbrauchskontrolle, die keine Identifizierung, sondern eine Verifizierung bezweckt.

31 Nach dem in der Gesetzesbegründung zum Ausdruck kommenden Willen des Gesetzgebers, der in dem Tatbestandsmerkmal der Identifizierbarkeit (§ 312k Abs. 2 S. 3 Nr. 1 lit. b BGB) seinen Niederschlag gefunden hat, ist die Eingabe von Log-in-Daten für eine Zuordnung der Kündigungserklärung zu einem bestimmten Verbraucher nicht erforderlich und dementsprechend auch nicht in § 312k Abs. 2 S. 3 BGB enthalten. Die Angaben, die der Verbraucher gem. § 312k Abs. 2 S. 3 BGB tätigen können muss, sind aber als Minimal- und als Maximalvorgabe zu verstehen; ihre Funktion als Minimalvorgabe soll sicherstellen, dass der Verbraucher alle Angaben machen kann, die er für seine Erklärung und deren Rechtswirksamkeit benötigt, und die Beschränkung der zu verlangenden Angaben soll Ausgestaltungen verhindern, bei denen der Unternehmer weitere, für den Verbraucher ggf. nicht ohne Weiteres verfügbare Daten abfragt und so eine einfache und unkomplizierte Kündigung erschwert (vgl. BeckOK BGB/Maume 1.8.2025, § 312k Rn. 24; MüKoBGB/Wendehorst, 10. Aufl. 2025, § 312k Rn. 19). Das Risiko eines Missbrauchs hat der Gesetzgeber dabei erkannt und aufgrund der Kumulierung der möglichen Angaben nach § 312k Abs. 2 S. 3 Nr. 1 BGB als vernachlässigbar erachtet (vgl. Halder jurisPR-ITR 2/2023 Anm. 3); eine Verifizierung des Verbrauchers erfolgt nach dem Regelungskonzept des § 312k Abs. 2 S. 3 Nr. 1 BGB allein durch die Angaben zur Identifizierbarkeit (§ 312k Abs. 2 S. 3 Nr. 1 lit. b BGB) und der eindeutigen Bezeichnung des Vertrags (§ 312k Abs. 2 S. 3 Nr. 1 lit. c BGB). Vor diesem Hintergrund könnte sich ein Unternehmen auch nicht mit Erfolg darauf berufen, es habe für sich die Entscheidung getroffen, eine Identifizierung seiner Kunden alleine oder maßgeblich über ein Passwort herbeizuführen.

32 Ohne Belang ist es daher auch, ob der Verbraucher typischerweise Log-in-Daten schneller zu Hand hat als die Angaben nach § 312k Abs. 2 S. 3 Nr. 1 lit. c BGB für eine Zuordnung des Vertrags. Denn dabei handelt es sich um eine Frage, die der Gesetzgeber zugunsten der Vertragsdaten entschieden hat und die de lege lata hinzunehmen ist (vgl. Halder jurisPR-ITR 2/2023 Anm. 3). Dass die Bekl. möglicherweise bestimmte Daten nicht erhebt oder speichert, fällt in ihren Risikobereich und befreit sie nicht davon, die gesetzlichen Vorgaben des § 312k BGB zu beachten.

33 (d) Anders als die Bekl. wohl meint, ist bei der Abgabe Kündigungserklärung gem. § 312k BGB auch nicht in dem jeweiligen Einzelfall ein Vergleich mit der Art- und Weise des Vertragsschlusses geboten. Der Gesetzgeber ist zwar davon ausgegangen, dass die Kündigung von im elektronischen Geschäftsverkehr abgeschlossenen Verträgen Verbraucher oft vor besondere Herausforderungen stellte, weil im Vergleich zum einfachen Abschluss eines solchen Vertrags dessen Kündigung direkt über eine Webseite teilweise nicht möglich ist oder häufig durch die Webseitengestaltung erschwert wurde. Die in § 312k BGB vorgesehenen Verpflichtungen des Unternehmers sollen daher Verbraucher in Bezug auf Dauerschuldverhältnisse in die Lage versetzen, Kündigungserklärungen im elektronischen Geschäftsverkehr in vergleichbar einfacher Weise abzugeben wie Erklärungen zum Abschluss entsprechender Verträge (vgl. BT-Drs. 19/30840, 15). Zur Erreichung dieses Anliegens hat der Gesetzgeber aber bei der im Gesetzgebungsverfahren gebotenen typisierenden Betrachtung die Voraussetzungen generell abstrakt vorgegeben, die der Unternehmer zu erfüllen hat, um die Abgabe einer Kündigungserklärung des Verbrauchers zu ermöglichen, ohne dass dem Gesetz zu entnehmen ist, dass im jeweiligen Einzelfall eine vergleichende Betrachtung erforderlich oder angezeigt sei. Unerheblich ist es daher, dass ein Verbraucher nur dann einen Vertrag bei der Bekl. abschließen kann, wenn er auf der Webseite der Bekl. eingeloggt ist.

34 (e) Entgegen der Ansicht der Bekl. ist auch eine einschränkende Auslegung des § 312k Abs. 2 S. 4 BGB nicht geboten.

35 Richtig ist allerdings zunächst, dass abweichend von dem vorstehenden Verständnis zT in Rspr. und Lit. eine einschränkende Auslegung des § 312k Abs. 2 S. 4 BGB erwogen wird. Das Erfordernis zum Einloggen in einen geschützten Kundenbereich stehe nach dieser Auffassung dem Tatbestandsmerkmal der ständigen Verfügbarkeit jedenfalls dann nicht entgegen, wenn die Nutzung des Dienstes, welcher Gegenstand des Dauerschuldverhältnisses ist, seiner Natur nach ohnehin ein Log-in erfordere (vgl. etwa OLG Nürnberg Ur. v. 30.7.2024 – 3 U 2214/23 [= MMR 2025, 298] Rn. 19 ff. und Rn. 31; Sümmerrmann/Ewald MMR 2022, 713 (717); Schirnbacher/Schreiber ZdiW 2022, 56 (60)). Hiervon ausgehend könnte die Eingabe von Log-in-Daten den Unternehmer auch davon befreien, eine den Anforderungen des § 312k Abs. 2 S. 3 Nr. 1 BGB entsprechenden Bestätigungsseite bereitzustellen, wenn – wie hier – durch die Eingabe von Log-in-Daten die Identifikation des Verbrauchers und die Zuordnung des Vertrags ermöglicht wird.

36 Der Senat vermag diesem Ansatz jedoch nicht zu folgen. Denn eine derartige einschränkende Auslegung für bestimmte Fallgestaltungen steht nicht nur dem ausdrücklich erklärten und im Gesetzeswortlaut seinen Niederschlag findenden Willen des Gesetzgebers entgegen (vgl. BeckOK BGB/Maume 1.8.2025, § 312k Rn. 39), sondern stellt methodisch eine unzulässige teleologische Reduktion des § 312k Abs. 2 S. 4 BGB dar (zutreffend Halder jurisPR-ITR 1/2025 Anm. 4; vgl. auch ders. jurisPR-ITR 2/2023 Anm. 3). Eine teleologische Reduktion erfordert nämlich, dass der Anwendungsbereich der anzuwendenden Norm planwidrig zu weit gefasst worden ist (stRspr.; vgl. nur BGH Ur. v. 11.11.2011 – V ZR 65/11 Rn. 10). Es gibt aber keinerlei Anhaltspunkte dafür, dass der Gesetzgeber die – praktisch durchaus häufige – Konstellation, dass ein Verbraucher bei der Nutzung des abgeschlossenen Dauerschuldverhältnisses zunächst einen geschützten Kundenbereich aufsucht, wie dies etwa bei Streamingdiensten für Musik, Sportevents, Filme und Serien, bei digitalen Nachrichten- und Zeitungsdiensten oder auf Gaming-Plattformen typischerweise der Fall ist, übersehen haben könnte und dass er sie andernfalls von dem Anwendungsbereich des § 312k Abs. 2 S. 4 BGB ausgenommen hätte (so aber OLG Nürnberg Ur. v. 30.7.2024 – 3 U 2214/23 [= MMR 2025, 298] Rn. 31). Hinzu kommt, dass die Gründe dafür, dass ein Verbraucher die Anmeldedaten zum Zeitpunkt der beabsichtigten Kündigung ggf. nicht parat haben und sich eine Kündigung aus diesem Grunde durch das Erfordernis eines Log-in bzw. der Eingabe von Log-in-Daten erschweren kann, vielfältig sein können (vgl. ausführlich zum Ganzen Halder jurisPR-ITR 1/2025 Anm. 4).

37 c) Die weiteren Voraussetzungen eines Unterlassungsanspruchs sind ebenfalls gegeben.

38 aa) Der festgestellte Verstoß gegen § 312k BGB ist auch geeignet, die Interessen von Verbrauchern iSv § 3a UWG spürbar zu beeinträchtigen. Ob eine Eignung zur spürbaren Interessenbeeinträchtigung besteht, ist nach dem Schutzzweck der jeweils verletzten Marktverhaltensregelung unter Berücksichtigung der Zwecke für die Einordnung der Vorschrift als Marktverhaltensregelung zu beurteilen (vgl. etwa BGH Ur. v. 8.2.2024 – I ZR 91/23 Rn. 50 – Großhandelszuschläge II, mwN), und im Streitfall mit Blick auf den bezweckten Verbraucherschutz ohne Weiteres zu bejahen.

39 bb) Die Wiederholungsgefahr als Voraussetzung für die Zuerkennung eines Unterlassungsanspruchs wird aufgrund der begangenen Verletzung vermutet (vgl. etwa BGH Ur. v. 25.4.1991 – I ZR 134/90 Rn. 21 – Anzeigenrubrik I) und diese Vermutung ist durch die Bekl. nicht widerlegt worden. ...

LG Hamburg: Haftung für KI-generierte Persönlichkeitsverletzung

Unwahre Tatsachenbehauptung

BGB §§ 823 Abs. 1, 1004 Abs. 1 S. 2; GG Art. 2 Abs. 1, 19 Abs. 3

Beschluss vom 23.9.2025 – 324 O 461/25

Leitsatz der Redaktion

Der Account-Betreiber haftet für unwahre Aussagen eines KI-generierten Posts, da er sich die Aussagen durch die Präsentation zu eigen gemacht hat.

Anm. d. Red.: Vgl. ferner Schulz MMR 2026, 400 und LG Kiel MMR 2025, 227.

Schlagworte: Vereinspersönlichkeitsrecht; unwahre Tatsachenbehauptung; KI-generierte Aussage

Aus den Gründen

3 ... 3. Dem Ast. steht ... [ein] Unterlassungsanspruch gegen die Ag. aus §§ 1004 Abs. 1 S. 2 analog, 823 Abs. 1 BGB iVm Art. 19 Abs. 3, 2 Abs. 1 GG zu. Die angegriffene Berichterstattung verletzt den Ast. in seinem Vereinspersönlichkeitsrecht.

4 Der maßgebliche Durchschnittsrezipient entnimmt dem streitgegenständlichen Beitrag des X-Accounts „...“, dass der Ast. staatliche Förderungen bzw. Bundesmittel für seine Tätigkeit erhält. Hierbei handelt es sich um eine prozessual unwahre Tatsachenbehauptung. Der Ast. nimmt in Abrede, unmittelbar oder mittelbar Gelder von staatlichen Institutionen zu erhalten. Die aufgrund der im Kontext bestehenden Ehrabträglichkeit der Behauptung darlegungs- und glaubhaftmachungsbelastete Ag., die im einstweiligen Verfügungsverfahren Gelegenheit zur Stellungnahme hatte, hat hierzu nichts vorgetragen.

5 An der äußerungsrechtlichen Unzulässigkeit der Darstellung ändert sich auch nicht deshalb etwas, weil die Beiträge des besagten Accounts von einer KI erstellt werden.

6 So ist nicht anzunehmen, dass Nutzer der Plattform „X“ allein deshalb Aussagen des Accounts nicht als Tatsachenbehauptungen werten, im Gegenteil verweist die KI selbst darauf, dass ihre Aussagen faktenbasiert erstellt werden, sodass Nutzer ihr besondere faktische Aussagekraft beimessen werden.

7 Für die KI-erstellten Aussagen auf dem Account hat die Ag. als Betreiberin des Accounts einzustehen. ...

VG Köln: Beanstandung eines Twitch-Livestream-Angebots

Jugendmedienschutz

§§ 2 Abs. 1, 3 Nr. 1 und Nr. 2, 5 Abs. 1, Abs. 3 und Abs. 6, 20 Abs. 1, Abs. 2, Abs. 3 und Abs. 6 JMStV; § 118 Abs. 1 S. 1 LMG NRW

Urteil vom 25.11.2025 – 6 K 2650/22; nicht rechtskräftig

Leitsätze der Redaktion

1. Livestreams im Angebot eines Twitch-Kanals sind als Rundfunk einzuordnen, da sie das Kriterium der Linearität erfüllen und iS. „Sendeplans“ inhaltlich und zeitlich in die Abfolge weiterer Sendungen eingebettet sind.

2. Ein Livestream-Angebot, in dem acht Minuten eines jugendschutzrelevanten Films gezeigt werden, ist keine

„Nachrichtensendung“ iSd § 5 Abs. 6 JMStV, wenn die Vorführung unstrukturiert und ohne erkennbare Vermittlung weitergehender Informationen erfolgt und nur einen bloßen Meinungsaustausch mit Zuschauern zum Gegenstand hat.

3. Ein solches Livestream-Angebot stellt auch keine „Sendung zum politischen Zeitgeschehen“ iSd § 5 Abs. 6 JMStV dar, wenn es nach dem Gesamteindruck an einem die Sendung prägenden politischen Bezug fehlt.

4. Die Möglichkeit, der Anbieterpflicht einer Wahrnehmungsschwernis nach § 5 Abs. 1 JMStV durch die Alterskennzeichnung für ein geeignetes Jugendschutzprogramm nachzukommen, ist auf Telemedienanbieter beschränkt. Sie steht daher Anbietern von als Rundfunk einzustufenden Livestream-Online-Angeboten zunächst nicht offen, sondern erst dann, wenn das inhaltsidentische Streaming-Angebot im Anschluss als Telemedium abrufbar ist.

Anm. d. Red.: Der Volltext ist veröffentlicht in MMR 2026, 357. Die Berufung ist beim OVG NRW unter dem Az. 13 A 88/26 anhängig. Vgl. ferner OVG NRW MMR 2016, 144 (Ls.); BVerwG MMR 2017, 788 (Ls.); BVerfG MMR 2021, 795 mAnm Holznaegel; BGH MMR 2021, 892 mAnm Klickermann – Influencer III; BGH MMR 2021, 875 – Influencer I; OLG Karlsruhe MMR 2025, 454 und OLG Frankfurt/M. MMR 2022, 776.

Schlagworte: Livestream; Jugendmedienschutz; Beiladung; USK; Gebührenbefreiung

Anmerkung

RA Prof. Dr. Christian-Henner Hentsch, Leiter Recht und Regulierung beim game, Geschäftsführer VHG, Berlin/TH Köln

1. Aufsicht der Landesmedienanstalten über Influencer

Die Landesmedienanstalten sind inzwischen nach allen Landesgesetzen für die Aufsicht von Telemedien zuständig und damit auch für Influencer und Let's Player. In Zeiten rückläufiger Fernsehdauer und steigender Video-on-Demand (VoD)- und Social Media-Nutzung verlagert sich entsprechend der Fokus der Aufsicht weg vom klassischen Fernsehen hin zu den neuen Angeboten. Bislang lag dabei der Schwerpunkt vor allem auf der Werbekennzeichnung (vgl. BGH MMR 2021, 892 mAnm Klickermann – Influencer III; BGH MMR 2021, 875 – Influencer I; OLG Karlsruhe MMR 2025, 454; OLG Frankfurt/M. MMR 2022, 776). Im vorliegenden Urteil hat die Landesanstalt für Medien Nordrhein-Westfalen (LfM NRW) im Fall Gronkh erstmals – und daher auch etwas überraschend – jugendschutzrechtliche Vorschriften in den Blick genommen. Mit dem Verfahren soll geklärt werden, ob die ursprünglich für Telemedien konzipierten Jugendschutzmaßnahmen auch auf Livestreams anwendbar sind, die als Rundfunk über Internetplattformen wie Twitch verbreitet werden.

Im Mai 2021 zeigte der bekannte Streamer „Gronkh“ in seinem Livestream auf Twitch die ersten acht Minuten des Films „Mortal Kombat“, der von der Freiwillige Selbstkontrolle der Filmwirtschaft (FSK) ab 18 Jahren freigegeben war. Die LfM beanstandete dies als Verstoß gegen § 5 Abs. 1 iVm Abs. 3 und Abs. 4 JMStV, da die Ausstrahlung bereits ab 20:00 Uhr erfolgte und nicht erst nach 22:00 Uhr. Die Unterhaltungssoftware Selbstkontrolle (USK), der One-Stop-Shop für Games und Angebote rund um Games in Deutschland, hatte das Angebot zuvor geprüft und keinen Verstoß festgestellt, insb., weil Twitch die Alterskennzeichnung des Jugendschutzprogramms „JusProg“ nutzt. Gronkh hat gegen die Beanstandung vor dem VG Köln geklagt.

2. Urteil des VG Köln

Kernfrage in diesem Verfahren ist die Anwendbarkeit von § 5 Abs. 3 Nr. 1 HS 2 JMStV auf Rundfunkangebote. Diese Vorschrift erlaubt es Anbietern, ihrer Jugendschutzpflicht durch

eine Alterskennzeichnung nachzukommen, „die von geeigneten Jugendschutzprogrammen nach § 11 Abs. 1 und Abs. 2 [JMStV] ausgelesen werden kann“.

Das Gericht legt diese Norm aus und argumentiert, diese Möglichkeit sei nach Sinn und Zweck sowie der Normsystematik auf Telemedienanbieter beschränkt. § 11 JMStV stehe im III. Abschnitt mit der Überschrift „Vorschriften für Telemedien“ und betreffe ausschließlich technische Jugendschutzprogramme für Internetangebote, nicht jedoch Rundfunkangebote. Das Gericht lehnt zudem eine Anwendung des Nachrichtenprivilegs aus § 5 Abs. 6 JMStV ab. Zwar sei der Filmstart von „Mortal Kombat“ ein tagesaktuelles Ereignis mit Nachrichtenwert, doch fehle es an der erforderlichen „um Objektivität bemühten Unterrichtung“. Die bloße Weiterleitung von Informationen und der sarkastische Kommentar des Streamers reichen nicht aus.

Das VG Köln hat die Berufung beim OVG NRW wegen grundsätzlicher Bedeutung zugelassen; Gronkh hat im Januar 2026 Berufung (Az. 13 A 88/26) eingelegt.

3. Kritische Würdigung der Entscheidung

Das Urteil kann aus gleich mehreren Gründen nicht überzeugen. Es scheint nicht nur der LfM, sondern auch dem Instanzgericht mit diesem Urteil vermutlich um eine höchstrichterliche oder gesetzgeberische Klärung dieser Rechtsfrage zu gehen.

a) Wortlautauslegung

Der Begriff „Angebot“ wird konsistent in § 5 Abs. 1 und Abs. 3 JMStV geregelt und umfasst nach der Legaldefinition des § 3 Nr. 1 JMStV sowohl Sendungen (Rundfunk) als auch Inhalte von Telemedien. Rein nach dem Wortlaut ist somit eindeutig, dass sich der sachliche Anwendungsbereich von § 5 Abs. 1 und Abs. 3 JMStV auf alle elektronischen Medien einschließlich Rundfunksendungen erstreckt. Auch der Wortlaut der Überschrift des Abschnitts I JMStV „Allgemeine Vorschriften“ macht deutlich, dass sich diese Regelungen auf alle vom Geltungsbereich des JMStV erfassten Medien beziehen. Damit können auch Rundfunkprogramme ihrer Jugendschutzpflicht durch technische Jugendschutzprogramme nachkommen.

b) Systematische Auslegung

Auch die systematische Auslegung des VG Köln überzeugt nicht. Zwar verweist § 5 Abs. 3 Nr. 1 HS 2 JMStV auf § 11 Abs. 1 und Abs. 2 JMStV, doch definiert § 3 Nr. 2 JMStV „Anbieter“ ausdrücklich als „Rundfunkveranstalter oder Anbieter von Telemedien“. Der Gesetzgeber hat also beide Anbietergruppen in den Anwendungsbereich des § 5 Abs. 3 JMStV einbezogen und adressiert im Gesetz auch konsequent immer „Anbieter“ und differenziert gerade nicht zwischen Rundfunk und Telemedien (anders als zB in § 5 Abs. 5 JMStV). Die allgemeine Anwendbarkeit ist auch daraus abzuleiten, dass die Überschrift für den Abschnitt in der aktuellen Fassung geändert wurde und keinen Bezug mehr zu Telemedien hat, ohne die hier relevanten Regelungen zu ändern. Historisch ist zu bedenken, dass zur Zeit der Änderung Fernsehen kein Online-Angebot oder Telemedium sein konnte. Das ist erst durch IP-TV in den vergangenen Jahren technisch möglich und zunehmend relevant geworden.

c) Medienkonvergenz und technologieneutraler Gesetzgeber

Eben diese Realität der Medienkonvergenz ignoriert das Gericht bei der Auslegung völlig und geht in seinem Urteil davon aus, dass dem gesamten Medienrecht „die Unterscheidung zwischen Rundfunk und Telemedium“ zugrunde liege (VG Köln MMR 2026, 357 Rn. 75). Gesetzeshistorisch hat der Ge-

setzgeber jedoch mit der Jugendschutzreform 2002 ausdrücklich eine medienkonvergente Regelung angestrebt, die nicht länger zwischen Telemedien und Rundfunk unterscheidet. Dazu wurden im 19. Rundfunkänderungsstaatsvertrag eigens § 5 Abs. 3 und § 11 JMStV technologieneutral neu gefasst. Wenn ein Livestream technisch dual ausgerichtet ist – sowohl als Telemedium als auch als Rundfunk qua Sendeplan qualifiziert – und die Verbreitung auf identische Weise erfolgt, ist es auch nicht verständlich, warum die technischen Jugendschutzmaßnahmen nur für den Telemediendienst gelten sollen.

Das Gericht führt an, die Unterscheidung zwischen Rundfunk und Telemedien sei wegen der „besonderen Breitenwirkung, Aktualität und Suggestivkraft“ des Rundfunks weiterhin sachlich gerechtfertigt. Diese Argumentation mag für klassischen linearen Fernsehrundfunk über DVB-T, -S oder -C überzeugend sein. Für interaktive Livestreams auf Plattformen wie Twitch ist jedoch fraglich, ob die Suggestivkraft tatsächlich höher ist als bei VoD-Angeboten, die ihrerseits unter § 11 JMStV fallen.

d) Absurde Ergebnisse

Letztendlich führt die Rechtsansicht der LfM und des VG Köln zu dem absurden Ergebnis, dass derselbe Inhalt im Livestream verboten sein kann, aber als VoD erlaubt ist, obwohl das VoD für Kinder und Jugendliche leichter zugänglich ist (da nicht an eine feste Sendezeit gebunden). Selbst wenn das VoD direkt während des Streams veröffentlicht würde, wäre es jugendschutzrechtlich unbedenklich, während der Livestream beanstandet wird. Dieses Ergebnis ist mit dem Ziel eines effektiven Jugendmedienschutzes kaum vereinbar. IÜ würde dies auch gegen das verfassungsrechtliche Gleichheitsgebot nach Art. 3 GG verstoßen.

e) Europarechtliche Bezüge

Auch mit Blick auf das zugrunde liegende EU-Recht und die AVMD-RL (RL 2010/13/EU, zuletzt geändert durch Art. 28 VO (EU) 2024/1083) kann das Urteil nicht überzeugen. Anders als der zeitlich frühere Rundfunkstaatsvertrag unterscheidet der europäische Gesetzgeber schon lange nicht mehr zwischen Rundfunk und Telemedien, sondern reguliert Audiovisuelle Medienanbieter medienkonvergent und konsistent. Eine strikte Trennung der Jugendschutzmaßnahmen nach der formalen Qualifikation als Rundfunk oder Telemedium erscheint gerade wegen der technologieneutralen Fassung des Art. 6a Abs. 1 UAbs. 1 S. 1 AVMD-RL, den § 5 Abs. 1 S. 1 JMStV umsetzen soll, also auch europarechtlich problematisch. Das Gericht muss das nationale Recht richtlinienkonform auslegen.

f) Praktische Konsequenzen

In der Praxis verbleibt für Streamer wie Gronkh nach der Entscheidung allein die Sendezeitbeschränkung als Jugendschutzmaßnahme. Dies ist für Livestreams mit interaktiven Elementen und unvorhersehbarem Verlauf kaum praktikabel. Die Möglichkeit, durch technische Maßnahmen wie Alterskennzeichnungen den Jugendschutz zu gewährleisten, wird Rundfunkanbietern im Internetbereich faktisch vorenthalten. Dies führt zu einer Schlechterstellung von Angeboten über Twitch ggü. vergleichbaren, traditionellen Angeboten im Fernsehen.

g) Nachrichtenprivileg

Auch die Auslegung des Nachrichtenprivilegs durch das Gericht erscheint sehr eng. Gerade bei neuen Medienformaten sollte der Begriff der Nachrichtensendung nicht auf klassische Nachrichtenformate beschränkt werden. Die interaktive Auseinandersetzung mit aktuellen Ereignissen in Online-Formaten

kann durchaus eine Form der Unterrichtung und Meinungsbildung darstellen, die von Art. 5 Abs. 1 GG geschützt ist (zuletzt BVerfG Urt. v. 3.11.2025 – 1 BvR 259/24). Gerade mit solchen Formaten werden Menschen erreicht, die klassischen Nachrichtenformaten nicht mehr folgen und insofern ist dies auch demokratiepolitisch sinnvoll.

4. Ausblick

Das VG Köln hat die Berufung wegen der grundsätzlichen Bedeutung der Frage zugelassen, „ob auch Rundfunkanbieter zur Umsetzung des Jugendschutzes ihre Angebote mit einer Alterskennzeichnung für Jugendschutzprogramme kennzeichnen können“. Dies ist zu begrüßen, da die Entscheidung weitreichende Konsequenzen für die Streaming-Landschaft hat. Das Berufungsverfahren bietet nun die Gelegenheit, die Jugendschutzregelungen an die Realität konvergenter Medien anzupassen und die von der Rspr. des BVerfG geforderte technologie neutrale Auslegung zu berücksichtigen.

LG Fulda: Irreführende Preisangabe auf einer Vermittlungsplattform

UWG §§ 3 Abs. 1, Abs. 2, 5 Abs. 2 Nr. 2, 8 Abs. 1 S. 1
Urteil vom 8.8.2025 – 7 O 4/25

Leitsätze der Redaktion

1. Wird in einer Vermietungsplattform einem konkreten Zimmerangebot der Hinweis vorangestellt, dass es sich um Preise einschließlich der USt. handle, aber am Ende des Angebots darauf hingewiesen, es handle sich um Nettopreise, so liegt eine relevante Irreführungsgefahr vor.
2. Der Plattformbetreiber haftet für eine solche irreführende Angabe, auch wenn diese durch den einzelnen Vermieter erfolgt ist.

Anm. d. Red.: Vgl. ferner BGH MMR 208, 39 mAnm Hoffmann und BGH MMR 2005, 461.

Schlagworte: Preisangaben; Irreführung; Haftung

BGH: Keine Vorlagepflicht an das BVerfG zum FernUSG

FernUSG §§ 7 Abs. 1, 12; GG Art. 100 Abs. 1 S. 1; BVerfGG § 80
Urteil vom 5.2.2026 – III ZR 74/25 (LG Berlin II, AG Wedding)

Leitsatz

Der Senat ist nicht mit der für eine Vorlage gem. Art. 100 Abs. 1 S. 1 GG, § 80 BVerfGG erforderlichen Sicherheit von der Verfassungswidrigkeit des in § 12 FernUSG statuierten Zulassungserfordernisses und der in § 7 Abs. 1 FernUSG angeordneten Nich-

tigkeit eines Fernunterrichtsvertrags, der von einem Veranstalter ohne entsprechende Zulassung des Fernlehrgangs geschlossen wird, überzeugt. Aus Sicht des Senats sprechen im Gegenteil gute Gründe dafür, dass die genannten Vorschriften mit dem Grundgesetz im Einklang stehen.

Anm. d. Red.: Der Volltext ist abrufbar unter: [BeckRS 2026, 2970](#). Vgl. auch BGH MMR 2026, 538 (Ls.) und BGH MMR 2026, 516 mAnm Klickermann/Diesler/Stoffel – alle in diesem Heft.

Schlagworte: Vorlagenpflicht an das BVerfG; Überzeugung von Verfassungswidrigkeit eines Gesetzes; Nichtigkeit eines Fernunterrichtsvertrags

BGH: Coaching- und Mentoring-Verträge nach dem FernUSG

BGB § 812 Abs. 1 S. 1 Fall 1; FernUSG §§ 1 Abs. 1, 7 Abs. 1, 12 Abs. 1 S. 1

Versäumnisurteil vom 12.2.2026 – III ZR 73/25 (OLG Stuttgart)

Leitsatz

Ein vertraglich vereinbartes Fragerecht zu den erlernten Kursinhalten ist ausreichend, um das Tatbestandsmerkmal der Lernerfolgskontrolle (§ 1 Abs. 1 Nr. 2 FernUSG) zu erfüllen.

Anm. d. Red.: Der Volltext ist abrufbar unter: [BeckRS 2026, 2614](#). Vgl. ferner BGH MMR 2026, 516 mAnm Klickermann/Diesler/Stoffel und BGH MMR 2026, (Ls.) 538 – alle in diesem Heft.

Schlagworte: Online-Mentoring-Programm; Coaching-Programm; Erklärvideos; Workbooks; Fernunterricht; Einzelfallbetrachtung

LG Frankenthal: Veröffentlichung von Videos ohne Quellenangabe

UrhG §§ 51, 63 Abs. 1, 97 Abs. 1, 94 Abs. 1, 95, 97a Abs. 3
Urteil vom 20.5.2025 – 6 O 269/24

Leitsatz der Redaktion

Bei einer Vervielfältigung oder Verbreitung nach § 51 UrhG ist stets die Quelle deutlich anzugeben. Hierzu gehört, dass jedenfalls der Nachname des Urhebers genannt wird. Darüber hinaus können ggf. weitere, das genutzte Werk identifizierende Merkmale geboten sein. Befindet sich das genutzte Werk im Internet, ist neben Titel und Autor die dortige Fundstelle, zumindest die URL, anzugeben.

Anm. d. Red.: Vgl. hierzu auch LG München I MMR 2026, 74 mAnm Gierschmann; LG Hamburg MMR 2009, 55 mAnm Hoeren und OLG Köln MMR 2014, 263.

Schlagworte: Quellenangabe; Videos; Zitat; YouTube-Reaktion-Video

andernfalls seien kinderfreundliche Voreinstellungen vorrangig (These 4). Schließlich müsse auch die Medienkompetenz verbessert werden (These 5). Anhand dieser Thesen lassen sich die bei Discord geplanten Altersverifikationen bewerten.

2. Umsetzung und Bewertung der Altersverifikation

Discord hat verschiedene Maßnahmen vorgestellt, um die Altersprüfung durchzuführen. Vordergründig möchte Discord auf seine interne Altersschätzung setzen, die auf den gleichen Mechanismen wie die 2024 eingeführten „Sicherheitssysteme“ basiert, die sich zum Aufspüren von Spam-Ringen und Missbrauch bewährt hätten. Es handelt sich dabei um ein maschinelles Lernmodell, das allgemeine Muster der Account-Aktivität analysiert, zB wie lange der Account besteht, ob eine Zahlungsmethode hinterlegt ist oder wie lange man sich auf welchen Servern aufhält. Discord betont, dass weder Nachrichten gelesen noch Postings analysiert werden (Discord Blog v. 24.2.2026). Automatisierte Altersschätzungen existieren seit geraumer Zeit, sind aber in Bezug auf Datenschutz und Eindeutigkeit umstritten (s. dazu Hunter/Steinebach/Yannikos Informatik 2025, 69 (71); Lück/Vogel DSRITB 2024, 163 (172)). Discord ist zwar hinsichtlich Nutzung des Modells transparent. Es bleibt aber fraglich, wie das System die Altersschätzung durchführt, ohne im Hintergrund das Nutzerverhalten zu analysieren. Der Grundsatz der Datenminimierung ist damit nur schwierig einzuhalten. Zudem sind solche Methoden von verschiedenen Profildaten abhängig und nicht für neue oder anonymisierte Accounts geeignet (Hunter/Steinebach/Yannikos Informatik 2025, 69 (71)). Dass diese Methode ihre Schwachstellen hat, zeigt sich auch dadurch, dass Discord ihre interne Altersschätzung in Ländern, die eine Alterskontrolle verpflichtend vorschreiben, nicht einsetzt. Denn ein Rückgriff auf weitere Altersprüfungsmethoden soll erfolgen, wenn die Alterskontrolle in einem Land vorgeschrieben ist oder die Verifizierung aufgrund der automatisierten Altersprüfung kein zuverlässiges Ergebnis erzielen kann.

Als weitere Methode nennt Discord die KI-gestützte Gesichtsalterseinschätzung per Video-Selfie. Die Verarbeitung soll dabei ausschließlich auf dem Endgerät er-

folgen. Auf vergleichbare Verfahren setzte auch Meta zur Einführung ihrer Teen-Konten (vgl. Marquard MMR-Aktuell 2024, 01728). Die BfDI bezeichnete diese Methode als ungenau und plädierte dafür, sie nicht weiter zu verfolgen. Sie beruhe auf Schätzungen und das Analysieren von biometrischen Merkmalen stehe oft nicht im Einklang mit der DS-GVO und KI-VO. Zum einen muss Art. 9 Abs. 1 DS-GVO berücksichtigt werden. Zum anderen sind KI-Systeme, die das Alter bestimmen, regelmäßig als Hochrisikosystem iSd Anhangs III Nr. 1 lit. b KI-VO einzustufen, was wiederum erhöhte Transparenzpflichten begründen würde. Die Verarbeitung am eigenen Endgerät minimiert zwar die Risiken. Jedoch stellt die Analyse des Gesichts weder eine Zero-Knowledge-Lösung dar, noch wird dabei der Grundsatz der Datenminimierung eingehalten.

Trotz des Datenlecks im Oktober 2025 zählt Discord als weitere Altersverifikationsmethode den Ausweis-Upload auf. Auch zu dieser Methode hat die BfDI in ihrem Vortrag v. 1.9.2025 Stellung bezogen. Zur Altersverifikation sollen keinesfalls umfassende Ausweisdaten übermittelt werden, sondern es solle auf Zero-Knowledge-Lösungen zurückgegriffen werden. Dazu wurde insbesondere auf das kommende EUDI-Wallet (European Digital Identity Wallet) verwiesen. Mit diesem Wallet sei es möglich, lediglich das Erreichen eines bestimmten Alters zu übermitteln. Gerade das Datenleck im Oktober 2025 verdeutlicht die Gefahr des leichtfertigen Hochladens von Ausweisdokumenten und sollte schon aus diesem Grund nicht mehr angeboten werden.

Schließlich kündigte Discord die Kreditkartenverifizierung als Option der Altersprüfung an. Diese Methode wurde auf nationaler Ebene bereits im Jahr 2007 vom BGH als unzureichend bewertet (vgl. BGH MMR 2008, 400 (Ls. 5)). Grund dafür sei, dass die Angabe einer Kreditkarte keine effektive Barriere für Minderjährige darstelle. An dieser Auffassung wird sich auch nichts geändert haben, sodass diese Methode nicht ausreichend ist.

3. Fazit

Discord zeigt durch die geplante Einführung verschiedener Altersverifikationsmethoden, dass man die (bevorstehenden) regulatorischen Maßnahmen um-

setzen möchte. In Europa sind zwar keine verpflichtenden Alterskontrollen vorgeschrieben, jedoch muss Discord gem. Art. 28 Abs. 1 DSA geeignete und verhältnismäßige Maßnahmen ergreifen, um ein minderjährigengerechtes Umfeld sicherzustellen. Zu beachten ist außerdem Art. 28 Abs. 3 DSA, wodurch die Online-Plattformen nicht verpflichtet sind, weitere personenbezogene Daten für die Altersbestimmung zu erheben. Eine Risikobewertungs- und Risikominimierungspflicht, wie sie in Art. 34 ff. DSA vorgesehen ist, trifft Discord derzeit nicht.

Gemessen an der These 4 stellt sich damit die Frage, ob Discord überhaupt den erforderlichen Risikograd erreicht, um Altersverifikationsmethoden verhältnismäßig einführen zu können. Die Antwort lautet: Ja. Discord ist bei Minderjährigen eine beliebte Plattform. Zugleich sind auf der Plattform Server und Kanäle mit pornografischen und jugendgefährdenden Inhalten zu finden, auf die Minderjährige derzeit mit einfachen Umgehungsmöglichkeiten zugreifen können. Aus diesem Grund ist der Ansatz von Discord, eine umfassende globale Altersprüfung durchzusetzen, zu begrüßen. Allerdings werfen die geplanten Methoden Fragen auf. Die Altersverifikation mittels Kreditkarten ist nicht sonderlich effizient und bereits durch den BGH abschlägig bewertet worden. Die anderen Methoden der Altersverifikation erscheinen hinsichtlich der Einhaltung des Datenminimierungsgrundsatzes bedenklich. Auch der zusätzliche Einsatz von KI-Systemen zieht weitergehende Pflichten mit sich. Sinnvoll erscheint es deswegen, sich an den Zero-Knowledge-Lösungen der EU zu orientieren, um den Anforderungen gerecht zu werden. Discord könnte sich dahingehend als Anbieter verifizieren lassen. Inwiefern Discord die europäischen Verfahren nutzen wird, bleibt abzuwarten.

■ Vgl. auch Stoklas ZD-Aktuell 2022, 01453; MMR-Aktuell 2026, 01247; Meese MMR-Aktuell 2025, 01528; Langensteiner MMR-Aktuell 2024, 01752; Langensteiner MMR-Aktuell 2025, 01459; MMR-Aktuell 2026, 01214; Etteldorf MMR-Aktuell 2024, 01756; Schmitz-Berndt MMR-Aktuell 2025, 01322 und Meese MMR-Aktuell 2025, 01457.

Dipl.-Jur. Lina Marquard, LL. B., ist Wissenschaftliche Hilfskraft am Institut für Rechtsinformatik (IRI) an der Leibniz Universität Hannover und Rechtsreferendarin am OLG Celle.

GPAl-Taskforce: Sitzung zu aggregierten Risikoprognosen und schädlichen Manipulationen

MMR-Aktuell 2026, 01263

Die Taskforce-Sitzung der Unterzeichner des General-Purpose AI (GPAl) Code of Practice (KI-Verhaltenskodex) vom 27.3.2026 befasste sich mit zwei zentralen Aspekten des Kapitels „Sicherheit und Gefahrenabwehr“: aggregierten Risikoprognosen und dem Systemrisiko schädlicher Manipulationen.

Im Bereich der aggregierten Prognosen diskutierten die Teilnehmenden die Verpflichtung systemrelevanter GPAl-Anbieter, zeitliche Einschätzungen darüber vorzulegen, wann ihre Modelle voraussichtlich höhere Risikostufen erreichen könnten als bisherige Systeme. Die Richtlinie sieht ausdrücklich vor, dass solche Einschätzungen auf gemeinsamen Prognosen oder Umfragen mehrerer Anbieter basieren dürfen. Zudem verweist Maßnahme 3.1 auf die Bedeutung modellunabhängiger Trendanalysen – etwa zur Entwicklung von Rechenaufwand, Datenverfügbarkeit oder Energieverbrauch – als Grundlage für strukturierte, standardisierte Prognoseverfahren.

Zur Unterstützung der Diskussion stellte das Forecasting Research Institute grundlegende Methoden der Prognoseforschung vor. Erörtert wurde ein mögliches Verfahren, bei dem systemrelevante Anbieter zweimal jährlich individuelle Risikoprognosen zu den in Anlage 1.4 definierten systemischen Risiken abgeben. Diese könnten anonymisiert aggregiert werden, um eine branchenweite Einschätzung zu ermöglichen. Offene Fragen betreffen insbesondere die geeignete Frequenz solcher Übungen und deren Auswirkungen auf Compliance-Prozesse. Das Büro für künstliche Intelligenz kündigte an, hierzu einen konkreten Vorschlag vorzulegen.

Der zweite Schwerpunkt betraf das Systemrisiko schädlicher Manipulationen. Die Taskforce diskutierte, wie relevante Risikoszenarien präzisiert werden können, da diese für eine belastbare Risikobewertung unerlässlich sind. Modellbewertungen müssen auf Eigenschaften abzielen, die für konkrete Schadenspfade relevant sind; entsprechend muss die Bewertungskonfiguration die Bedingungen

der jeweiligen Risikoszenarien widerspiegeln.

Translucide präsentierte hierzu eine Einführung, die auf jüngsten Stakeholder-Beiträgen basiert. Vorgeschlagen wurde u.a., Szenarien nach Expositionskontext zu differenzieren – etwa Interaktionen über Chatbots, Drittanwendungen, agentenbasierte Systeme oder KI-generierte Inhalte.

■ Vgl. hierzu auch MMR-Aktuell 2025, 01355 mwN.

BMUKN: Politikempfehlungen für eine ökologisch und ökonomisch nachhaltige KI-Entwicklung

MMR-Aktuell 2026, 01260

Künstliche Intelligenz verändert zentrale Bereiche von Wirtschaft, Verwaltung und Infrastruktur in Deutschland und Europa. In einem Policy Paper des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) werden Handlungsempfehlungen zum nachhaltigen Einsatz von KI gegeben.

Der Bericht hebt hervor, dass ökologische Nachhaltigkeit und wirtschaftliche Leistungsfähigkeit im KI-Einsatz nicht im Widerspruch stehen, sondern sich gegenseitig stärken können. Die deutsche Industrie, geprägt von kleinen und mittleren Unternehmen und einem Fokus auf spezialisierte, aufgabenspezifische Modelle, ist dafür gut aufgestellt.

Viele industrielle Anwendungen – etwa in Wartung, Qualitätskontrolle oder Prozesssteuerung – basieren auf kleineren, energie- und hardwareeffizienten Modellen, die sich gut in bestehende Produktionsumgebungen integrieren lassen und lokale digitale Souveränität ermöglichen. Demgegenüber verursachen sehr große generative Modelle erhebliche Umweltkosten, die mit wachsender Rechenleistung weiter steigen. Gleichzeitig bleibt der Einsatz von KI zur Unterstützung ökologischer Nachhaltigkeitsziele hinter seinem Potenzial zurück. Der Bericht sieht daher sowohl die Notwendigkeit, die ökologischen Auswirkungen rechenintensiver KI zu begrenzen, als auch die Chance, KI gezielt für nachhaltigkeitsorientierte Anwendungen stärker nutzbar zu machen.

Konkret gliedern sich die Empfehlungen in vier Handlungsfelder:

■ Erstens wird gefordert, die Fokussierung auf große generative Modelle zu überwinden. Spezialisierte, energieeffiziente KI-Modelle sollen gezielt gefördert und alternative KI-Paradigmen – etwa neuro-symbolische Ansätze, kausale Modelle, neuromorphe Systeme oder probabilistische Programmierung – strategisch unterstützt werden. Zudem sollen sichere Datenkooperationen zwischen öffentlicher Hand und Unternehmen, etwa über förderiertes Lernen, sowie der Zugang zu zweckgerichteter Recheninfrastruktur gestärkt werden.

■ Zweitens wird mehr Transparenz über ökologische Auswirkungen von KI verlangt. Standardisierte, öffentlich zugängliche und unabhängig geprüfte Umweltberichte sollen den gesamten Modelllebenszyklus einschließlich der Inferenz abdecken. Ergänzend soll die KI-VO um Berichtspflichten zu anwendungsbezogenen Umweltauswirkungen erweitert werden. Nutzerinnen und Nutzer sollen zudem die Möglichkeit erhalten, standardmäßig energieeffiziente Modelle zu wählen.

■ Drittens adressieren die Empfehlungen die Nachhaltigkeit der zugrunde liegenden Infrastruktur. Rechenzentren sollen umfassende, auditierte Umweltkennzahlen veröffentlichen, die reale Betriebsbedingungen widerspiegeln. Öffentliche Investitionen sollen energieeffiziente, auf industrielle Bedarfe zugeschnittene Rechenressourcen fördern sowie netzorientierte Betriebsweisen unterstützen. Rechenzentren sollen in CO₂-Bepreisungssysteme einbezogen und zu zusätzlicher Erzeugung erneuerbarer Energien verpflichtet werden.

■ Viertens wird auf die Wechselwirkungen zwischen KI-Infrastruktur und Energiewende hingewiesen. Kurzfristige regulatorische Eingriffe könnten langfristige Ziele gefährden. Empfohlen wird eine Studie zu wirtschaftlichen und ökologischen Effekten des Rechenzentrumsbaus, um nachhaltige sektorale KI-Lösungen gezielt zu fördern. Ein ökologisch ambitionierter Ausbau von Rechenzentren in Europa könne zudem Märkte für innovative Energie- und Speichertechnologien stärken.

■ Vgl. hierzu auch MMR-Aktuell 2023, 01220.

BA: Cyberkriminalität in Deutschland bleibt auf sehr hohem Niveau

MMR-Aktuell 2026, 01277

Das Bundeskriminalamt (BA) hat das Bundeslagebild Cybercrime 2025 veröffentlicht. Danach ist Deutschland weiterhin stark von Cyberkriminalität betroffen. Der wirtschaftliche Schaden wird auf rd. 202,4 Mrd. EUR geschätzt.

Im Jahr 2025 wurden etwa 335.000 Cybercrime-Fälle registriert, wobei ein Großteil der Taten aus dem Ausland oder anonymen Quellen erfolgte. Experten gehen zudem von einer deutlich höheren Dunkelziffer aus. Im Bereich der schweren Cyberkriminalität bleibt insbesondere Ransomware ein zentrales Problem. Die Zahl der Angriffe ist gestiegen, ebenso die durchschnittlichen Lösegeldforderungen. Gleichzeitig zahlen Betroffene seltener, was auf eine verbesserte Schutzfähigkeit vieler Organisationen hindeutet. Auch DDoS-Angriffe haben deutlich zugenommen. Sicherheitsbehörden gehen zudem gegen internationale Täterstrukturen und sog. Stresser-Dienste vor und konnten im Rahmen mehrerer Operationen Netzwerke teilweise zerschlagen. Ein weiterer Trend ist der zunehmende Einsatz von KI durch Cyberkriminelle, etwa zur effizienteren Durchführung von Angriffen. Gleichzeitig wird KI aber auch als Werkzeug zur besseren Erkennung und Abwehr von Cyberbedrohungen genutzt.

■ Vgl. hierzu MMR-Aktuell 2026, 01207 und MMR-Aktuell 2024, 01285.

Axel Spies USA: FCC gegen Offshore-Callcenter – Neue Risiken für TK-Anbieter mit US-Geschäft

MMR-Aktuell 2026, 01267

Die Federal Communications Commission (FCC) in Washington hat mit einer Notice of Proposed Rulemaking (NPRM) einen regulatorisch wie politisch bemerkenswerten Vorstoß gegen Offshore-Callcenter gestartet. Im Mittelpunkt stehen Kommunikationsanbieter, die Kundenserviceleistungen für US-Kunden aus Drittstaaten erbringen lassen. Für deutsche TK-Anbieter mit US-Geschäft könnte dies eine ganze Reihe von praktischen

Auswirkungen haben, auch wenn sie keine von der FCC lizenzierte Carrier sind. Die FCC begründet die Initiative mit Verbraucherbeschwerden über „communication and other barriers“ bei ausländischen Servicecentern, mit Datenschutz- und Sicherheitsbedenken sowie mit der Bekämpfung illegaler Robocalls. Gleichzeitig verfolgt die Behörde ausdrücklich industriepolitische Ziele und will Arbeitsplätze in die USA zurückholen. Adressaten der NPRM sind zunächst klassische FCC-regulierte Kommunikationsanbieter, insbesondere die Anbieter von „telecommunications services“, CMRS-, VoIP-, Kabel- und Satellitendiensten sowie deren verbundene Internetzugangsanbieter. Damit spricht vieles dafür, dass jedenfalls solche Unternehmen betroffen wären, die selbst einer FCC-Regulierung unterliegen, etwa aufgrund einer US-Präsenz oder einer internationalen Section-214-Autorisierung. Gerade internationale Carrier mit US-Terminierung oder US-Tochtergesellschaften sollten den Fortgang der NPRM aufmerksam beobachten. Ein Aspekt: Auch vertraglich könnten US-Carrier von deutschen Unternehmen Anpassungen oder Zusicherungen für Callcenter-Dienste verlangen.

Allerdings geht die NPRM erkennbar weiter. Die FCC fragt ausdrücklich danach, ob einzelne Pflichten künftig auf sämtliche vom Telephone Consumer Protection Act (TCPA) erfassten Kommunikationsvorgänge ausgeweitet werden sollten. Der TCPA ist das zentrale US-Bundesgesetz zur Regulierung von Telemarketing, automatisierten Anrufen, SMS-Marketing und sonstiger telefonischer Kundenansprache. Das Gesetz enthält insbesondere strenge Vorgaben zu Einwilligungen (consent), automatisierten Wahlsystemen, künstlichen oder aufgezeichneten Stimmen sowie zu Werbeanrufen gegenüber Verbrauchern. Verstöße können erhebliche zivilrechtliche Haftungsrisiken einschließlich Sammelklagen (class actions) auslösen. Sollte die FCC den Anwendungsbereich ihres Vorstoßes tatsächlich auf sämtliche TCPA-relevante Anrufe erstrecken, könnte dies deutlich über klassische FCC-214-Lizenzinhaber hinausreichen. Dann wären auch Unternehmen betroffen, die zwar keinen eigenen regulierten Carrierstatus in den USA besitzen, aber US-Kunden telefonisch betreuen oder Telemarketing betreiben. Ge-

nau hierin liegt derzeit eine der zentralen Rechtsunsicherheiten des Verfahrens. Besonders bemerkenswert ist der Vorschlag, Mitarbeiter in Callcentern müssten „be proficient in American Standard English“ (NPRM Rn. 11 mit Definition in Fn.12) „and otherwise be trained appropriately for resolving issues with U. S. customers“ (NPRM Rn. 4). Gemeint sein dürfte weniger grammatikalisch perfektes Englisch als vielmehr eine sprachliche und kulturelle Kommunikationsfähigkeit, die aus Sicht der FCC eine effektive Kundenbetreuung amerikanischer Verbraucher gewährleistet. Praktisch könnte dies auf verpflichtende Sprachtrainings, Qualitätskontrollen oder standardisierte Sprachtests hinauslaufen. Gerade für große Offshore-Standorte in Asien würde dies zusätzlichen Compliance- und Dokumentationsaufwand bedeuten. Darüber hinaus diskutiert die FCC erstmals auch konkrete quantitative Beschränkungen für Offshore-Callcenter. Die NPRM (NPRM Rn. 33) nennt ausdrücklich ein mögliches Limit von 30 Prozent für den Anteil von Kundenservice-Anrufen, die durch ausländische Callcenter bearbeitet werden dürfen. Die Behörde fragt hierzu u.a., ob sich die Quote auf eingehende und ausgehende Anrufe gemeinsam oder getrennt beziehen soll, über welchen Zeitraum die Einhaltung gemessen werden müsste und welche Arten von Kundenkontakten einzubeziehen wären. Diskutiert werden etwa Kundenservice-, Vertriebs-, Billing-, Retention- oder Debt-Collection-Anrufe. Für international organisierte Customer-Care-Modelle wäre eine solche Quote potenziell hochgradig eingriffsintensiv. Hinzu kommt ein weiterer Vorschlag mit erheblicher Relevanz für internationale Carrier und Gateway-Provider. Die FCC erwägt sog. bond requirements für Anbieter, die Anrufe aus dem Ausland in die USA übermitteln (NPRM Rn. 61 und 67). Insbesondere internationale Gateway-Provider könnten verpflichtet werden, finanzielle Sicherheiten (bonds) zu hinterlegen, um illegale Robocalls besser bekämpfen zu können. Die FCC bittet um Stellungnahmen zu Höhe und Ausgestaltung solcher Sicherheiten, zu möglichen Einbehaltungs- oder Verfallstatbeständen, zu Verfahrensrechten der betroffenen Anbieter sowie zu Nachschusspflichten. Gerade für international tätige Carrier mit US-Voice-Terminierung könnte

dies zusätzliche finanzielle und regulatorische Belastungen bedeuten.

Die neue Callcenter-NPRM zu Offshore-Callcentern adressiert KI-gestützte Customer-Service-Strukturen zwar nicht ausdrücklich im Detail, die FCC verfolgt jedoch sei 2024 parallel bereits ein eigenständiges Regulierungsprojekt zu KI-gestützten Robocalls und KI-generierter Kundenkommunikation gemäß dem TCPA. Für deutsche TK-Anbieter mit KI-basierten Kundenserviceplattformen oder Voice-Bots ist dieses Thema deshalb relevant. Praktisch deutet dies darauf hin, dass die FCC künftig Transparenz- und Disclosure-Pflichten nicht nur für klassische sprachbasierte Callcenter, sondern potenziell auch für KI-gestützte Customer-Service- und Voicebot-Systeme etablieren will. Rechtlich ist keineswegs ausgemacht, dass die FCC diese Vorschläge am Ende tatsächlich umsetzen kann. Die FCC räumt in der NPRM ein, dass Fragen der gesetzlichen Zuständigkeit bestehen. Diskutiert werden insbesondere Kompetenzgrenzen der FCC gegenüber allgemeinen Customer-Service-Aktivitäten sowie mögliche verfassungsrechtliche Probleme, etwa mit Blick auf kommerzielle Kommunikationsfreiheit. In den USA wird bereits kontrovers diskutiert, ob die FCC überhaupt befugt ist, Sprach- oder Standortvorgaben für Kundenservicepersonal zu machen und ob es genug Kapazitäten in US-Callcentern für die Umsetzung der Vorgaben gibt. Bei der FCC können Stellungnahmen bis zum 26.5.2026 eingereicht werden; die Abgabe von Reply Comments ist dann bis zum 22.6.2026 möglich.

■ Vgl. zu Robocalls und TCPA schon Spies MMR-Aktuell 2024, 01314 und Spies MMR-Aktuell 2025, 01483.

RA Dr. Axel Spies

ist Partner der Potomac Law Group in Washington DC und Mitherausgeber der MMR.

Sandra Schmitz-Berndt **UK: Ofcom-Konsultation zu neuen Regeln gegen Cyberflashing und Selbstverletzungsinhalte**

MMR-Aktuell 2026, 01257

Die britische Medienaufsichtsbehörde (Office of Communications – Ofcom)

plant eine Anpassung ihrer Vorschriften und Leitlinien zum Umgang mit illegalen Online-Inhalten iRd Online Safety Act (OSA). Anlass für die Änderungen ist die Neuaufnahme von Straftatbeständen in die Liste prioritärer Tatbestände unter dem OSA im Dezember 2025. Bei den Delikten handelt es sich zum einen um das sog. Cyberflashing, also das Senden einer Fotografie oder eines Films von Genitalien, sowie das Teilen oder die Androhung des Teilens einer intimen Fotografie oder eines Films, und zum anderen um die Förderung oder Unterstützung schwerer Selbstverletzung.

Der OSA unterscheidet bei der Regulierung von rechtswidrigen Inhalten zwischen Priority-Illegal-Content, Illegal Content und Inhalten, die minderjährige Nutzer gefährden können. Dabei umfasst der Priority-Illegal-Content neben Inhalten im Zusammenhang mit Kindesmissbrauch und Terrorismus eine umfangreiche Liste von sog. prioritären Tatbeständen (Priority Offences) in Schedule 7.

Die Straftatbestände des Cyberflashing (Section 66A Sexual Offences Act) und Teilens intimer Aufnahmen (Section 66B Sexual Offences Act) wurden mit dem OSA ins Sexualstrafrecht eingeführt, während die Förderung oder Unterstützung schwerer Selbstverletzung als eigenständiger Straftatbestand in Section 184 OSA (Section 184) enthalten ist. Mit den Online Safety Act 2023 (Priority Offences) (Amendment) Regulations 2025 wurden die Delikte nunmehr in Schedule 7 des OSA und somit unter die prioritären Tatbestände aufgenommen. Damit sind Diensteanbieter u.a. verpflichtet, verhältnismäßige Maßnahmen zu ergreifen, um zu verhindern, dass Nutzer diesen Inhalten ausgesetzt sind.

Im Hinblick auf den Anpassungsbedarf ihrer die gesetzlichen Grundlagen konkretisierenden Regulierungsinstrumente für den Umgang mit illegalen Inhalten hat die Ofcom eine entsprechende Konsultation zu den durch die Gesetzesänderung veranlassten und geplanten Änderungen eingeleitet. Zu den zentralen Vorschlägen gehört insbesondere die Zusammenführung der prioritären Straftatbestände der Förderung oder Unterstützung des Suizids und der Förderung oder Unterstützung schwerer Selbstverletzung zu einer einheitlichen, von den Diensteanbietern im Rahmen ihrer Risikobewertung zu bewertenden Kategorie

„Suizid und Selbstverletzung“. Begründet wird dies damit, dass es sich um vergleichbare Phänomene handelt, die im Online-Kontext gemeinsamen Risikofaktoren unterliegen. Diensteanbieter müssen in der Folge in der Risikobewertung ein einheitliches Gesamtrisikoniveau für diese Kategorie festlegen. Die neu aufgenommenen Sexualstraftatbestände sollen hingegen als eigenständige Risikokategorie geführt werden, die eine eigene Risikoanalyse erfordert.

Zur Unterstützung der Diensteanbieter beabsichtigt die Ofcom das von ihr publizierte „Register of Risks“ um neue Erkenntnisse zu Selbstverletzung und Cyberflashing zu ergänzen. Des Weiteren sollen sowohl die Risk Assessment Guidance and Risk Profiles sowie die Illegal Content Judgements Guidance um Risikofaktoren ergänzt werden, die mit den neu aufgenommenen Phänomenen verbunden sind. In der Folge müssten Anbieter ihre Risikobewertungen im Hinblick auf illegale Inhalte aktualisieren.

Auch wenn die Ofcom davon absieht, eine Konsultation zu den Illegal Content Codes of Practice for User-to-user-Services sowie Illegal Content Codes of Practice for Search Services durchzuführen, schlägt sie vor, die Codes of Practice zu aktualisieren, um sicherzustellen, dass bestehende Maßnahmen auf Cyberflashing sowie Suizid und Selbstverletzung in gleicher Weise Anwendung finden wie auf sonstige prioritäre Straftatbestände. Darüber hinaus wird vorgeschlagen, dass Maßnahmen zum Blockieren und Stummschalten (blocking & muting) bestimmter Inhalte zukünftig auch für Dienste mit einem Risiko von Cyberflashing verpflichtend werden sollten.

Die Konsultation war bis zum 24.4.2026 geöffnet. Mit der Ergänzung des Sexualstrafrechts durch den Data (Use and Access) Act 2025 um eine Strafbarkeit von sog. Deepnudes in Section 66E Sexual Offences Act, die am 6.2.2026 in Kraft trat, erscheint es absehbar, dass eine weitere Ergänzung der prioritären Straftatbestände erfolgen wird.

■ Vgl. auch Ukrow MMR-Aktuell 2025, 01436; Etteldorf MMR-Aktuell 2024, 01502; Etteldorf MMR-Aktuell 2025, 01129 und Meese MMR-Aktuell 2025, 01525.

Dr. Sandra Schmitz-Berndt LL.M., LL.M., ist Wissenschaftliche Mitarbeiterin am Institut für Europäisches Medienrecht e.V. (EMR), Saarbrücken.

**BNetzA: Gemeinsame Roadmap für KI in
Medizinprodukten veröffentlicht**

MMR-Aktuell 2026, 01278

BNetzA, das Hessische Ministerium für Digitalisierung und Innovation sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit haben eine Roadmap für den Einsatz künstlicher Intelligenz in Medizinprodukten vorgestellt. Das Dokument vermittelt eine strukturierte Übersicht über die gesetzlichen Anforderungen der europäischen KI-VO und deren Verknüpfung mit den Vorgaben der Medizinprodukteverordnung. Ziel ist die Schaffung von Rechtsklarheit für Unternehmen bei der Entwicklung sicherer KI-Anwendungen im medizinischen Kontext.

Die Roadmap basiert auf einem simulierten KI-Reallabor-Prozess, dessen Abschlussbericht bereits im März 2026 erschien. Die Beteiligung der Start-ups avisé labs GmbH und Katulu ermöglichte eine praxisnahe Erprobung konkreter Anwendungsfälle unter regulatorischer Begleitung durch die drei Behörden. KI-Reallabore erlauben die Erprobung neuer Technologien unter realistischen Bedingungen und fördern die Skalierung von Innovationen, insbesondere für KMU mit begrenzten Compliance-Ressourcen.

Schwerpunkt der Roadmap sind die Anforderungen an Hochrisiko-KI-Systeme. Sie verdeutlicht das Zusammenspiel zwischen den Regelwerken, ersetzt jedoch nicht die Einzelfallprüfung. Die Anbieter behalten die Verantwortung für die spezifische Umsetzung der Anforderungen. Die Dokumentation dient als Orientierungshilfe, um Innovatorinnen und Innovatoren die Navigation im komplexen regulatorischen Umfeld zu erleichtern und gleichzeitig Patientensicherheit zu gewährleisten.

■ Vgl. hierzu auch MMR-Aktuell 2026, 01222 und MMR-Aktuell 2026, 01281.

**Studie zu Companion-AI: Kritik und Risiken
emotionaler KI**

MMR-Aktuell 2026, 01284

Companion-AI entwickelt sich derzeit zu einer Technologie, die Millionen Menschen emotional an sich bindet – bisher jedoch ohne klare gesellschaftliche und politische Regeln. Das Zentrum für Digitalrechte und Demokratie hat eine Studie veröffentlicht, in der Ramak Molavi Vasse'i die wissenschaftliche Forschung ausgewertet und Vorschläge für einen verantwortungsvollen Umgang erarbeitet hat.

KI-Chatbots übernehmen zunehmend die Rolle von Freunden, Beratern oder sogar Partnern. Sie wirken einfühlsam, sind jederzeit erreichbar und speichern persönliche Informationen. Dadurch entstehen Risiken für die psychische Gesundheit, den Datenschutz und die selbstbestimmte Meinungsbildung.

Besonders problematisch sind Mechanismen, die gezielt Nähe erzeugen, Zustimmung verstärken und eine starke emotionale Bindung fördern. Die Studie empfiehlt deshalb strengere Regeln, etwa einen besseren Schutz sensibler Daten und eine klare Regulierung manipulativer KI-Systeme.

Die zentrale Botschaft: Companion-AI ist bereits Teil unseres Alltags. Deshalb braucht es jetzt demokratische Leitplanken, bevor sich Geschäftsmodelle etablieren, die emotionale Beziehungen gezielt kommerziell ausnützen.

■ Vgl. zur Regelung anthropomorpher KI in China Wang MMR-Aktuell 2026, 01172.

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (V.i.S.d.P.); Nina Himmelstoß, Redakteurin; Ruth Schrödl, Redakteurin; Christine Völker-Albert, Redakteurin; Alexandra Link, Redaktionsassistentin; Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de.

[in de.linkedin.com/showcase/zeitschriftmmr](https://de.linkedin.com/showcase/zeitschriftmmr)

Manuskripte und andere Einsendungen:

Alle Einsendungen sind an die o. g. Adresse zu richten. Es besteht keine Haftung für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigelegt ist. Die Annahme zur Veröffentlichung muss in Textform erfolgen. Mit der Annahme zur Veröffentlichung überträgt die Autorin/der Autor dem Verlag C.H.Beck an ihrem/seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht der Autorin/des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet.

Redaktionsrichtlinie C.H.Beck:

Redaktionsrichtlinien und Werkabkürzungen sind im Zitierportal des Verlags C.H.Beck abrufbar: www.zitierportal.de

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, soweit sie vom Einsendenden oder von der Schriftleitung erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch im Hinblick auf Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form vervielfältigt, verbreitet oder öffentlich wiedergegeben oder zugänglich gemacht, in Datenbanken aufgenommen, auf elektronischen Datenträgern gespeichert oder in sonstiger Weise elektronisch vervielfältigt, verbreitet oder verwertet werden. Der Verlag behält sich auch das Recht vor, das Werk für die automatisierte Analyse insbesondere zur Erkennung von Mustern, Trends und Korrelationen zu verwenden.

Media Sales:

Verlag C.H.Beck GmbH & Co. KG, Media Sales, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.

Media Consultants: Telefon (0 89) 3 81 89-687, Telefax (0 89) 3 81 89-589, E-Mail: mediasales@beck.de.

Auftragsmanagement: Telefon (089) 381 89-609, Telefax (089) 38189-589, E-Mail: anzeigen@beck.de

Verantwortlich für den Anzeigenteil: Simon Holtz.

Verlag: Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: (0 89) 3 81 89-0, Telefax: (089) 38189-398, info@beck.de, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Amtsgericht München, HRA 48 045. Persönlich haftende Gesellschafter: Dr. h. c. Wolfgang Beck (Verleger in München) und C.H.Beck Verwaltungs GmbH, Amtsgericht München, HRB 254521.

Erscheinungsweise: Monatlich.

Bezugspreise 2026: Jahresabo € 599,- (inkl. MwSt.). Vorzugspreis für Mitglieder der davit und Kooperationspartner jährlich € 455,- (inkl. MwSt.). Einzelheft € 61,- (inkl. MwSt.). Versandkosten jeweils zuzüglich. Das Abonnement beinhaltet den Zugang zum Online-Modul MMRDirekt, den Newsletter MMR-Aktuell und die MMR App. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestitelei und -register sind nur mit dem jeweiligen Heft lieferbar.

Hinweise zu Preiserhöhungen finden Sie in den beck-shop AGB unter Ziff. 10.4.

Bestellungen über jede Buchhandlung und beim Verlag.

KundenServiceCenter:

Telefon: (0 89) 3 81 89-750,

Telefax: (0 89) 3 81 89-358.

E-Mail: kundenservice@beck.de

chbeck.de/nachhaltig-produktsicherheit.beck.de

Abbestellung:

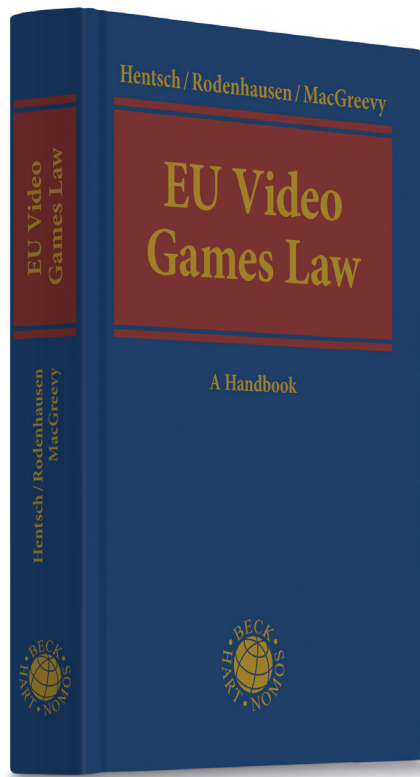
Abbestellfristen finden Sie unter: www.beck-shop.de/mmr-zeitschrift-it-recht-digitalisierung/product/1584

Hinweis gemäß Art. 21 Abs. 1 DS-GVO: Bei Anschriftenänderung kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeauftrag gestellt ist. Hiergegen kann jederzeit mit Wirkung für die Zukunft Widerspruch bei der Post AG eingelegt werden.

Satz: Fotosatz Pfeifer GmbH, 82110 Germering.

Druck: Druckerei C.H.Beck, Bergerstraße 3–5, 86720 Nördlingen.

Your Guide to Playing by the Rules.



Hentsch/Rodenhausen/MacGreevy

EU Video Game Law

2026. Approx. 500 pages.

Hardcover approx. € 190,—

ISBN 978-3-406-83323-6

A co-publication of C.H.BECK, Munich, Hart
Publishing, Oxford, and Nomos, Baden-Baden.

New in May 2026

 beck-shop.de/38341558

The video game industry

has long been the world's largest and fastest-growing media sector. As it continues to evolve and increase in complexity, the demand for sound legal guidance grows accordingly.

Your legal power-up

This new book **explores the legal issues** that arise at every stage of a video game's lifecycle in a practical and focused way, taking into account **commercial and economic conditions**.

It serves as a **comprehensive guide** to both current and emerging legal challenges in the video game industry. As a concise and accessible handbook, it is a valuable manual to both current and emerging legal challenges in the video game industry, covering **key topics** such as:

- Business models and finance
- Platform obligations
- Data protection
- Consumer protection

Written by industry experts

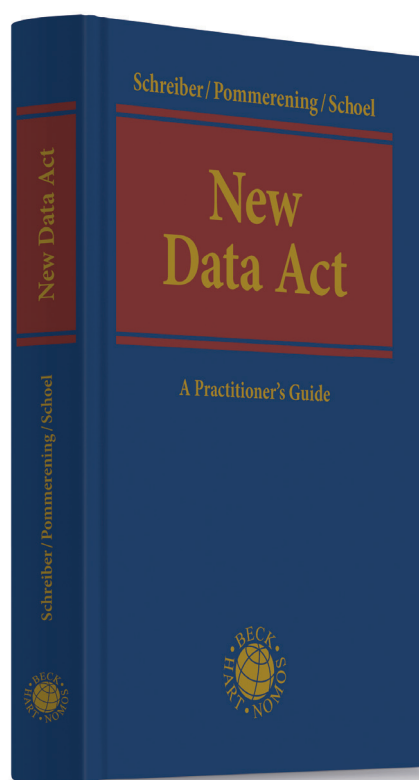
Christian **Henner-Hentsch** is a professor of copyright and media law at TH Köln. Anselm **Rodenhausen** is Vice President Legal & Policy at Video Games Europe. Dara **MacGreevy** is Senior Legal Counsel at Video Games Europe. The authors are renowned and experienced industry experts from all across Europe.

The legal meta

for lawyers and practitioners involved in the video game industry at every level, competition authorities, consumer organisations, data protection authorities, finance institutions.



Mastering the New Data Act.



Schreiber/Pommerening/Schoel

New Data Act

2026. 265 pages.

Hardcover € 130,—

ISBN 978-3-406-83136-2

A co-publication of C.H.BECK, Munich, Hart Publishing, Oxford, and Nomos, Baden-Baden.

New in April 2026

 beck-shop.de/38027144

The advantages at a glance

- concise explanations of new concepts
- practitioner tips
- insights into the relationship with existing data protection law

Regulation (EU) 2023/2854

better known as »EU Data Act«, harmonises rules on fair access to and the use of data. Since September 2025, all businesses that collect and use personal and non-personal data generated by »connected products« are subject to the new legal requirements.

Professional insight

Written in English, this Practitioner's Guide **provides essential guidance to the new EU Data Act** for legal practitioners, specialist IT-lawyers, in-house counsel, public authorities, data protection officers, data intermediaries, EU institutions, on topics including the

- rights and obligations surrounding data sharing
- obligations imposed on data holders
- impact on contract drafting
- sharing of data with authorities
- use of data in smart contracts



HERBSTAKADEMIE 2026

Digitalwirtschaft 2030 –
IT-Recht am Wendepunkt?

9. bis 12. September 2026 in Potsdam

Die 27. DSRI-Herbstakademie führt uns in diesem Jahr in die brandenburgische Landeshauptstadt Potsdam. In unmittelbarer Nähe zu Berlin und in besonderer Atmosphäre am Campus Griebnitzsee freuen wir uns, Sie gemeinsam mit der Deutschen Gesellschaft für Recht und Informatik (DGRI) sowie dem Lehrstuhl für Bürgerliches Recht, IT-Recht und Medienrecht der Universität Potsdam (Prof. Dr. Björn Steinrötter) im September am Campus Griebnitzsee begrüßen zu dürfen.

Wie gewohnt werden aktuelle Entwicklungen des Informationstechnologierechts behandelt. In den »Updates« geben Expertinnen und Experten Überblicke über die Rechtsentwicklung des vergangenen Jahres sowie über aktuelle regulatorische Entwicklungen, insbesondere auf europäischer Ebene.

Abgerundet wird die Herbstakademie durch ein Rahmenprogramm, das vielfältige Gelegenheiten zum fachlichen Austausch und zur Vernetzung bietet.

→ Ausführliche Informationen zum Programm und zur Anmeldung finden Sie unter: www.dsri.de/herbstakademie

THEMENAUZUG

DATENSCHUTZ

- Öffentlichkeitsarbeit von Datenschutz-Aufsichtsbehörden
- Datenschutzrechtliche Systempflichten
- Anonyme Auftragsverarbeitung

DATENSCHUTZ UND KI-VO

- KI-Gesichtserkennung im Fußballstadion
- Rechtliche Chancen zwischen DSGVO und KI-VO

MEDIZIN, GESUNDHEIT UND DISKRIMINIERUNGSSCHUTZ

- Regulierung und Verarbeitung von Neurodaten
- IT- Sicherheitsrecht als Grundpfeiler des Gesundheitsdatenraums

PLATTFORMEN UND CLOUDS

- Aktuelle Entwicklungen zum Digital Markets Act
- Was ist eine „souveräne“ Cloud?

TK-/TELEMEDIENRECHT

- Digital Omnibus vs. Tracking, ePrivacy-Richtlinie und DSGVO
- Werbeeinwilligung und Vertragsauflösung

KI IN BERUFEN UND BRANCHEN

- Einsatz künstlicher Intelligenz im Arbeitsleben
- Regulatorische Aspekte der Datenübertragung und Speicherung

SPEZIFISCHE FRAGEN DES IT-RECHTS

- Transparenzanforderungen an hochriskante KI-Assistenzsysteme
- Identifizierungspflicht von Host Providern?

DATENWIRTSCHAFTSRECHT

- Data Act und der Geschäftsgeheimnisschutz
- Der Dateninhaber und die ihm ohne Weiteres verfügbaren Daten
- Bereichsausnahme des Art. 43 DA für den Datenbankherstellerschutz

RECHTSINFORMATIK & LEGAL TECH

- Hybride Entscheidungsverfahren durch generative KI
- Integrierbarkeit jur. Auslegungsmethoden in ein hybrides KI-System

DIGITALISIERUNG UND RECHT

- KI-Recht im Vergleich zwischen EU und GCC-Staaten
- Vernetzung von Informatik und Recht

IT-SICHERHEIT

- Das novellierte Cybersicherheitsrecht in Deutschland
- Cybersicherheit und Produkthaftung

AGENTIC AI

- Vulnerabilität der Verbraucher im Agentic Commerce
- KI-Agenten als Gamechanger

DATEN UND DATENFLÜSSE

- Praxischeck nach einem Jahr Date Act
- Daten(schutz)rechtliches Zurückbehaltungsrecht

VERWALTUNG

- KI- Training mit Beschäftigendaten
- Künstliche Intelligenz im Rechtsbehelfverfahren

Tagungsentgeld:

inkl. Tagungsband, Vortragsfolien, drei Mittagessen und Erfrischungen: 500,- € (für DGRI-Mitglieder: 470,- €; für WiMi, Studierende, Referendar/innen: 250,- €).

Medienpartner: