

Oberlandesgericht München

Az.: 37 U 530/25 e
24 O 937/24 LG Memmingen



IM NAMEN DES VOLKES

In dem Rechtsstreit

[REDACTED]

- Kläger und Berufungskläger -

Prozessbevollmächtigte:

Rechtsanwälte **BRR Automotive Rechtsanwaltsgesellschaft mbH**, Viktoria-Luise-Platz 7,
10777 Berlin, Gz.: DTS-016254-24

gegen

Meta Platforms Ireland Ltd., vertreten durch ihre Geschäftsführer David Harris, Majella Goss,
Yvonne Cunnane und Anne O'Leary, D04 X2K5, Merrion Road, Dublin 4, Irland

- Beklagte und Berufungsbeklagte -

Prozessbevollmächtigte:

[REDACTED]

wegen Schadensersatz

erlässt das Oberlandesgericht München - 37. Zivilsenat - durch die Vorsitzende Richterin am
Oberlandesgericht [REDACTED], die Richterin am Oberlandesgericht [REDACTED] und den Richter am
Oberlandesgericht [REDACTED] aufgrund der mündlichen Verhandlung vom 14.01.2026 folgendes

Endurteil

I. Auf die Berufung der Klagepartei wird das Urteil des Landgerichts Memmingen vom 30.12.2024, Az. 24 O 937/24 abgeändert und - unter Zurückweisung der Berufung im Übrigen - wie folgt neu gefasst:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., und g. DSGVO dazu zu erteilen,

- welche personenbezogenen Daten von ihr verarbeitet werden und
- zu welchen Verarbeitungszwecken dies geschieht,
- zu den Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten,

dies insbesondere, aber nicht ausschließlich, durch die „Meta-Business-Tools“,

(a) auf Dritt -Webseiten und -Apps die personenbezogenen Daten, die der Identifizierung der Klagepartei dienen, ob direkt oder in gehashter Form übertragen, d.h.

* E-Mail der Klagepartei

* Telefonnummer der Klagepartei

* Vorname der Klagepartei Nachname der Klagepartei

* Geburtsdatum der Klagepartei

* Geschlecht der Klagepartei

* Ort der Klagepartei

* Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID“ genannt)

* IP-Adresse des Clients

* User-Agent des Clients (d.h. gesammelte Browserinformationen)

* interne Klick-ID der Meta Ltd.

* interne Browser-ID der Meta Ltd.

- * Abonnement –ID
- * Lead-ID
- * anon_id

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

(b) auf Dritt -Webseiten

- * die URLs der Webseiten samt ihrer Unterseiten
 - * der Zeitpunkt des Besuchs
 - * der Referrer (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),
 - * die auf der Webseite angeklickten Buttons sowie
 - * weitere von der Meta „Events“ genannte Daten, die die Interaktionen auf der jeweiligen Webseite dokumentieren.

(c) in mobilen Dritt -Apps

- * der Name der App sowie
 - * der Zeitpunkt des Besuchs
 - * die in der App angeklickten Buttons sowie
 - * die von der Meta „Events“ genannte Daten, die die Interaktionen in der jeweiligen App dokumentieren.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gemäß Ziff. 1 sämtliche seit dem 01.01.2021 gespeicherten personenbezogenen Daten der Klagepartei im Sinne von Ziffer 1. a., b. und c. spätestens einen Monat nach Rechtskraft vollständig zu löschen und der Klagepartei die Löschung zu bestätigen.
 3. Die Beklagte wird verurteilt, an die Klagepartei 750 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21.06.2024 zu zahlen.
 4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 280,60 € freizustellen.
 5. Im Übrigen wird die Klage abgewiesen.
- II. Von den Kosten des Berufungsverfahrens und des Verfahrens in erster Instanz trägt die Klagepartei 30 % und die Beklagte 70 %.

- III. Das Urteil ist vorläufig vollstreckbar. Die Beklagte darf die Vollstreckung der Klagepartei durch Sicherheitsleistung in Höhe von 3.000 € abwenden, wenn nicht die Klagepartei vor der Vollstreckung Sicherheit in dieser Höhe leistet. Die Klägerin darf die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110% des vollstreckbaren Betrags abwenden, wenn die Klagepartei zuvor Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrags leistet.
- IV. Die Revision gegen dieses Urteil zum Bundesgerichtshof wird zugelassen.

Beschluss

Der Streitwert wird für das Berufungsverfahren auf 2.500 € festgesetzt.

Gründe:

A.

Die Parteien streiten über Ansprüche auf Schadensersatz, Unterlassung, Feststellung und Löschung sowie Auskunft und Freistellung von vorgerichtlichen Anwaltskosten aufgrund behaupteter Verletzungen der DSGVO. Die in Deutschland wohnhafte Klagepartei nutzt das soziale Netzwerk Instagram seit dem 01.01.2021 unter dem Benutzernamen „[REDACTED]“. Das Konto wurde bis heute nicht gelöscht.

Betreiberin des Netzwerks ist die Beklagte, die bis zum 27. Oktober 2021 unter der Firma „**Facebook Ireland Ltd.**“ auftrat und nunmehr unter „**Meta Platforms Ireland Limited**“ firmiert (nachfolgend: Beklagte).

Die Nutzer der Plattform Instagram können seit 2023 zwischen einem werbefreien Bezahlmodell und einem kostenfreien Modell wählen, bei dem ihnen als Gegenleistung für die kostenlose Nutzung Werbeanzeigen angezeigt werden, die grundsätzlich an ihren Interessen ausgerichtet sind. Die Beklagte verarbeitet Daten der Klagepartei, insbesondere:

- Informationen, die die Kunden bei der Registrierung und Erstellung eines Profils bereitstellen,
- App-, Browser- und Geräteinformationen (vgl. näher die Meta-Datenschutzrichtlinie in Anlage K1, S. 8 f.)

- Informationen über Freunde und Follower des Kunden und deren Nutzungsverhalten in Produkten der Beklagten (a.a.O., S. 6 f.),
- Informationen über Aktivitäten der Kunden auf der jeweiligen Plattform (sog. **On-Plattform-Daten**, a.a.O., S. 7),
- Informationen von Partnern, Anbietern von Mess- und Marketinglösungen und sonstigen Dritten (sog. **Off-Plattform-Daten**, a.a.O., S. 9 f.), dies unabhängig davon, ob der jeweilige Nutzer in einem Meta-Produkt angemeldet ist bzw. überhaupt ein Konto bei der Beklagten besitzt.

Die Beklagte verarbeitet auch solche (Off-Plattform-)Daten, die sie über die streitgegenständlichen **Meta-Business-Tools** erhebt. Die Meta-Business-Tools werden von der Beklagten im allgemeinen Geschäftsverkehr als Werbeprodukt angeboten. Kunden sind Betreiber von Webseiten und Apps, die einzelne oder mehrere Meta-Business-Tools zur Erhöhung ihrer Werbeeffizienz in ihre Webseite/App einbinden und in der Folge bestimmte Daten mit der Beklagten nach Maßgabe der „Nutzungsbedingungen für Meta-Business-Tools“ (Anlage B5) teilen. Zu diesen – in die Webseite oder App des Drittanbieters integrierten – Tools zählen insbesondere „Meta Pixel“ und „App Events über Facebook SDK“ (bzw. „Facebook SDK“), bei deren Einsatz Cookies o.ä. auf dem Endgerät des Internetnutzers gesetzt und ausgelesen werden, sowie seit dem Jahr 2021 zusätzlich serverseitige Tools wie die „Conversions API“ für Webseiten und die „App Events API“ für Apps, die von Drittcookieblockern nicht erfasst werden. Die Conversions API ist, laienhaft erklärt, eine Schnittstelle, die einen Tunnel zwischen den Servern der Beklagte und des Webseitenbetreibers eröffnet und damit Drittcookieblocker bei Browsern umgeht.

Die Beklagte verwendet die Informationen grundsätzlich unter anderem zur Personalisierung des Nutzungserlebnisses und zur Werbung, zur Verbesserung ihrer Produkte, zur Verhinderung schädlichen Verhaltens und zum Schutz von Nutzern ihrer Produkte und zur Unterstützung von Forschenden (vgl. näher die Meta-Datenschutzrichtlinie in Anlage K1, S. 22 ff.). Die Beklagte verkauft die von ihr verarbeiteten Daten nicht, teilt sie aber weltweit mit Werbetreibenden und anderen von ihr sog. Partnern, Anbietern von Mess- und Marketinglösungen, Dienstleistern sowie externen Forschern und sonstigen Dritten (vgl. Datenschutzrichtlinie der Beklagten, Anlage K 1/B 10, S. 48 ff., 72 f.).

Die Beklagte sieht die Möglichkeit vor, die Nutzung von optionalen Cookies auf Webseiten und Apps von Drittanbietern zu erlauben („*Meta Cookies auf anderen Apps und Webseiten*“). Erfolgt diese Zustimmung nicht, nutzt die Beklagte die auf den Webseiten und Apps erhobenen Da-

ten zwar nicht, um relevantere Werbung anzuzeigen, sehr wohl aber - in eingeschränktem Umfang - zu Sicherheits- und Integritätszwecken. Die Klagepartei hat der Nutzung nicht zugestimmt.

Die Beklagte verwendet Informationen von Werbepartnern zu bestimmten Aktivitäten nur dann zur Personalisierung von Werbung, wenn über die Einstellung „*Informationen über Aktivitäten von Werbepartnern*“ ausdrücklich eine Zustimmung erfolgt ist. Zu anderen Zwecken, z.B. zum Schutz der Sicherheit und Integrität der Server oder zur Messung der Effektivität von Werbekampagnen, werden die Daten aber unabhängig von der vorgenommenen Einstellung verarbeitet. Die Klagepartei hat nicht zugestimmt.

Über die Einstellung „*Deine Aktivitäten außerhalb von Meta-Technologien*“ können Nutzer unter anderem die von Drittunternehmen in der Vergangenheit geteilten Daten von ihrem Konto trennen und – bezogen auf konkrete Drittunternehmen – eine Verknüpfung von Informationen für die Zukunft ausschließen. Die Beklagte erhält dann weiterhin Daten und verwendet sie auch, nimmt aber keine Verknüpfung mit dem Benutzerkonto vor.

Die Beklagte entscheidet von Fall zu Fall, wie lange sie Daten behält. Sie behält die Daten, um ihre Produkte bereitstellen zu können, um rechtliche Verpflichtungen zu erfüllen oder ihre Interessen oder die Interessen Dritter zu schützen. In bestimmten Fällen (z.B. zum Zwecke von Schutz, Sicherheit und Integrität, vgl. näher die Meta-Datenschutzrichtlinie in Anlage K1, S. 68 ff.) bewahrt die Beklagte Daten länger auf. Die Aufbewahrungsdauer konkretisiert die Beklagte in ihrer Datenschutzrichtlinie für diese Fälle nicht. In der Datenschutzrichtlinie heißt es dazu „*wir löschen Deine Informationen, sofern wir nicht anderweitig verpflichtet sind, sie aufzubewahren, wie etwa aus rechtlichen Gründen*“ (vgl. Datenschutzrichtlinie Anlage K 1/B 10, S. 67).

Durch Klicken auf „Zustimmen“ oder durch die Nutzung irgendeines Meta-Business-Tools stimmt der Drittanbieter der Möglichkeit zu, Kontaktinformationen seiner Kunden und/oder „Event-Daten“ mit der Beklagten zu teilen. Bestimmte technische Standarddaten werden schon dann an die Beklagte übertragen, wenn ein Nutzer die Webseite oder internetverbundene App eines Dritten aufruft, in die ein streitgegenständliches Business-Tool (v.a. Meta Pixel) eingebunden ist. Das gilt nur dann nicht, wenn das Drittunternehmen die http-Anfrage pausiert oder blockiert, bis der Nutzer über das Cookie-Banner oder die Datenschutzeinstellungen seine Einwilligung erteilt hat. Die Beklagte kontrolliert nicht, ob eine Einwilligung erteilt und wurde und erst recht nicht, ob diese wirksam war.

Die sog. Event-Daten beschreiben Nutzeraktionen auf den Dritt-Webseiten und –Apps: Ein Event kann z.B. das Aufrufen einer Seite („Pages View“), das Absenden eines Suchbefehls („Search“),

das Ausfüllen eines Formulars („Leads“), das in den Warenkorb legen eines Artikels („AddToCart“) oder der Kauf eines Artikels („Purchase“) sein. Die übermittelten Daten ermöglichen es der Beklagten, die Informationen einem bestimmten Nutzer zuzuordnen, sei es unmittelbar oder mittels eines Algorithmus.

Nach den „Nutzungsbedingungen für Meta-Business-Tools“ muss der Drittanbieter in nachprüfbarer Weise sicherstellen, dass ein Endnutzer alle erforderlichen Einwilligungen erteilt, bevor er Meta das Speichern von Cookies oder sonstigen Informationen auf dem Gerät des Endnutzers und den Zugriff hierauf ermöglicht (vgl. Nutzungsbedingungen Anlage B 5). Er muss über eine Rechtsgrundlage für die Offenlegung und Verwendung von Business-Tool-Daten verfügen. Die Beklagte kontrolliert nicht, ob oder wie Drittanbieter ihre gesetzlichen und vertraglichen Verpflichtungen erfüllen. Eine Kontrolle der Einwilligung durch Nutzer der Webseite seitens der Beklagten sehen die Nutzungsbedingungen nicht vor. Vielmehr heißt es im Meta-Hilfebereich für Unternehmen (Anlage B 5, S. 1): *„Metas Systeme sind zwar darauf ausgelegt, potenziell unzulässige Informationen herauszufiltern, die sie erkennen können, aber letztendlich bist du für die Daten verantwortlich, die du mit Meta teilst“*

Die von der Beklagten angebotenen und vertriebenen und verantworteten Meta-Business-Tools laufen – für den Nutzer nicht erkennbar – auf mannigfachen, reichweitenstarken Webseiten und Apps in Deutschland im Hintergrund. Hierzu gehören:

- zahlreiche große Nachrichtenseiten und -Apps (z.B. spiegel.de, bild.de, welt.de, faz.net, stern.de),
- die großen Reiseseiten und -Apps (z.B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de, momondo.de),
- Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, aerzte.de, helios-gesundheit.de, jameda.de),
- Dating- und Erotikseiten (parship.de, lovescout24.de)
- aber auch Seiten mit Inhalten aus der innersten Intimsphäre (krebshilfe.de, tfp-fertility.com, nvve.nl) (Bl. 8, Anlage K2).

Die Klagepartei hat die streitgegenständlichen Ansprüche vorgerichtlich mit Schreiben vom 23.04.2014 gegenüber der Beklagten geltend gemacht (Anlage K 3). Die Beklagte hat auf dieses Schreiben geantwortet (Klageerwiderung Rz. 60).

Die Klagepartei behauptet, von der Einbindung der obengenannten Meta-Business-Tools selbst betroffen zu sein, da sie Internetangebote nutze, in denen Meta-Business-Tools Verwendung finden, die Beklagte verarbeite ihre Daten. Es gebe aufgrund des Vertrages zwischen den Parteien keinen rechtlichen Grund, die Daten, insbesondere Daten, die die Beklagte von Dritten erhalte, zu speichern und zu verarbeiten. Die Klagepartei trägt weiter vor, sie habe keine hinreichende Kenntnis darüber, welche konkreten Daten über sie verarbeitet würden, zu welchen Zwecken diese Daten verarbeitet würden und wie lange eine Speicherung erfolge. Sie beanstandet insbesondere die Verarbeitung der Off-Site-Daten sowie die Unsicherheit darüber, welche ihrer personenbezogenen Daten eigentlich bei der Beklagten gespeichert werden.

Die Klagepartei behauptet, der mit dem Einsatz von Meta-Business auf Drittseiten einhergehende Informationsfluss und die Verarbeitung durch die Beklagte führe bei ihr zu einem Gefühl des Kontrollverlusts über ihre persönlichen Daten und zu einer fortdauernden Verunsicherung hinsichtlich Umfang und Zweck der Datenverarbeitung. Sie empfinde es als belastend, dass ihr Surfverhalten auf Drittwebseiten ohne ihr bewusstes Zutun erfasst und mit ihrem Nutzerprofil bei der Beklagten verknüpft werde. Sie habe wahrgenommen, dass sich Internetrecherchen auf Drittwebseiten in Werbeinhalten innerhalb der Dienste der Beklagten widerspiegeln. Dies erzeuge bei ihr das Gefühl, im Internet fortlaufend beobachtet zu werden, und beeinträchtige ihr Vertrauen in die Kontrolle über die Verwendung ihrer personenbezogenen Daten.

Die **Beklagte** tritt dem entgegen. Sie bestreitet, personenbezogene Off-Site-Daten der Klagepartei in rechtswidriger Weise zu verarbeiten, vielmehr entsprächen ihre Verarbeitungszwecke der DSGVO. Sie stellt insbesondere in Abrede, dass konkrete Off-Site-Daten der Klagepartei verarbeitet oder ihr individuell zugeordnet worden seien. Die Beklagte trägt vor, dass Art und Umfang der Verarbeitung von Off-Site-Daten von den jeweiligen technischen Implementierungen durch die Drittunternehmen sowie von den Entscheidungen und Einstellungen der Nutzer abhingen. Zudem unterscheidet sie zwischen verschiedenen Verarbeitungszwecken und macht geltend, dass Off-Site-Daten – abhängig von der jeweiligen Konstellation – nicht oder nur zu bestimmten Zwecken verarbeitet würden. Sie bestreitet die persönliche Betroffenheit der Klagepartei.

Das Landgericht hat die Klage abgewiesen.

Die Klage sei teilweise unzulässig und im Übrigen unbegründet, weil der geltend gemachte Auskunftsanspruch nach Art. 15 DSGVO bereits durch die Bereitstellung eines elektronischen Self-Service-Tools ordnungsgemäß erfüllt worden sei und insoweit ein Rechtsschutzbedürfnis für eine weitergehende gerichtliche Inanspruchnahme fehle. Weiter habe es angenommen, dass die

Klägerpartei eine konkrete, sie individuell betreffende Verarbeitung personenbezogener Daten durch die Beklagte nicht hinreichend substantiiert dargelegt habe, da sie weder konkret benannt habe, welche Drittwebseiten oder -apps sie genutzt habe, noch inwiefern dort tatsächlich eine Datenübermittlung an die Beklagte erfolgt sei. Mangels eines solchen konkreten Sachvortrags habe das Gericht weder einen Verstoß gegen die DSGVO noch eine Verletzung des allgemeinen Persönlichkeitsrechts oder einen ersatzfähigen immateriellen Schaden feststellen können, weil der Auskunftsanspruch nach Art. 15 DSGVO bereits durch ein zulässiges Self-Service-Tool erfüllt sei und für weitergehende Anträge das Rechtsschutzbedürfnis fehle. Schadensersatz-, Lösungs- und Feststellungsansprüche scheiterten zudem daran, dass der Kläger eine konkrete, ihn individuell betreffende Datenverarbeitung durch die Beklagte nicht hinreichend substantiiert dargelegt hatte und bloße allgemeine Behauptungen zum Tracking nicht ausreichen. Mangels konkreten Vortrags zur tatsächlichen Betroffenheit könne weder ein DSGVO-Verstoß noch ein immaterieller Schaden festgestellt werden

Wegen der tatsächlichen Feststellungen des Landgerichts wird im Übrigen auf das erstinstanzliche Urteil Bezug genommen (§ 540 ZPO).

Gegen dieses Urteil hat die Klagepartei Berufung eingelegt und beantragt, das erstinstanzliche Urteil des Landgerichts vom 30.12.2024 abzuändern und neu zu fassen wie folgt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DSGVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 01.01.2021 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Instagram" unter dem Benutzernamen [REDACTED] der Klagepartei verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business Tools“,

a. auf Dritt-Webseiten und -Apps die personenbezogenen Daten, die der Identifizierung der Klagepartei dienen, ob direkt oder in gehashter Form übertragen, d.h.

- E-Mail der Klagepartei
- Telefonnummer der Klagepartei
- Vorname der Klagepartei
- Nachname der Klagepartei
- Geburtsdatum der Klagepartei
- Geschlecht der Klagepartei
- Ort der Klagepartei
- Externe IDs anderer Werbetreibender (von der Meta Ltd. "externalID" genannt)
- IP-Adresse des Clients
- User-Agent des Clients (d.h. gesammelte Browserinformationen)

- interne Klick-ID der Meta Ltd.
- interne Browser-ID der Meta Ltd.
- Abonnement —ID
- Lead-ID
- anon_id

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

- die URLs der Webseiten samt ihrer Unterseiten
- der Zeitpunkt des Besuchs
- der Referrer (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),
- die auf der Webseite angeklickten Buttons sowie
- weitere von der Meta „Events“ genannte Daten, die die Interaktionen auf der jeweiligen Webseite dokumentieren

c. in mobilen Dritt-Apps

- der Name der App sowie
- der Zeitpunkt des Besuchs
- die in der App angeklickten Buttons sowie
- die von der Meta „Events“ genannte Daten, die die Interaktionen in der jeweiligen App dokumentieren

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 01.01.2021 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat, unter Benennung dieser Dritten,

ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte seit dem 01.01.2021 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

inwieweit die Daten der Klagepartei für eine automatisierten Entscheidungsfindung einschließlich Profiling verwendet wurden und werden. Die Beklagte hat hierfür aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für die betroffene Person zu erteilen.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 01.01.2021 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 01.01.2021 bereits gespeicherten personenbezogenen Daten vollständig zu löschen.
3. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 1.500,00 Eu-

ro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 21.06.2024, zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 Euro freizustellen.

Die Klagepartei macht mit ihrer Berufung geltend:

Die Berufungsbegründung rügt zunächst eine grundlegend fehlerhafte Tatsachenwürdigung des Landgerichts. Dieses habe verkannt, dass sich die Klage nicht gegen einzelne, konkret nachzuweisende Datenverarbeitungsvorgänge richte, sondern gegen die generelle, strukturelle Anwendung der Meta Business Tools mit nicht abstellbaren Voreinstellungen, die bereits als solche gegen Art. 5 Abs. 1 und Art. 25 DSGVO verstoße und einen fortdauernden Eingriff in das Recht auf informationelle Selbstbestimmung begründe. Daraus folge, dass das Landgericht zu Unrecht einen detaillierten Vortrag zu einzelnen Webseiten, Apps oder konkreten Nutzungssituationen verlangt und die Darlegungs- und Beweislast rechtsfehlerhaft der Klagepartei auferlegt habe.

Weiter beanstandet die Berufungsbegründung Rechtsfehler bei der Abweisung der einzelnen Klageanträge: Der Auskunftsanspruch nach Art. 15 DSGVO sei weder erfüllt noch inhaltlich zutreffend begrenzt worden, insbesondere habe das Landgericht zu Unrecht angenommen, es bestehe kein Anspruch auf Auskunft über Drittstaatentransfers und deren „Ob“, und habe die bloße Verweisung auf Self-Service-Tools fälschlich als Erfüllung angesehen. Ebenso sei die Abweisung des Löschungs- bzw. Anonymisierungsanspruchs rechtsfehlerhaft, da Anonymisierung eine zulässige Form der Löschung bzw. zumindest der Einschränkung der Verarbeitung darstelle und sich ausschließlich auf nicht betriebsnotwendige Off-Site-Daten beziehe.

Schließlich rügt die Berufungsbegründung die Ablehnung des immateriellen Schadensersatzes als rechtsirrig: Das Landgericht habe den Schadensbegriff des Art. 82 DSGVO verkannt, indem es den bereits im Kontrollverlust über personenbezogene Daten liegenden Schaden nicht anerkannt und unzulässig zusätzliche Anforderungen gestellt habe. Zudem habe es sich mit dem hilfsweise geltend gemachten Anspruch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG nicht hinreichend auseinandergesetzt und die Tragweite der fortdauernden Überwachungsbedrohung für das Persönlichkeitsrecht der Klagepartei grundlegend unterschätzt

Den ursprünglichen Antrag in Bezug auf die Anonymisierung hat die Klageseite in der mündlichen Verhandlung vom 14.1.2026 fallen gelassen (vgl. Protokoll vom 14.1.2026)

Die Beklagte beantragt, die Berufung der Klagepartei zurückzuweisen.

Sie tritt der Berufung entgegen und verteidigt das angefochtene Urteil als zutreffend. Die Beklagte macht geltend, die Klage sei bereits deshalb abzuweisen gewesen, weil die Klagepartei ihre Anträge nicht hinreichend substantiiert und insbesondere eine individuelle Betroffenheit von einer konkreten Datenverarbeitung nicht dargelegt habe. Es fehle an Vortrag dazu, welche Drittwebseiten oder -apps die Klagepartei wann genutzt habe, ob dort Meta-Business-Tools eingesetzt worden seien und ob es hierbei überhaupt zu einer Übermittlung personenbezogener Daten an die Beklagte gekommen sei; schon deshalb dürfe nicht davon ausgegangen werden, dass im konkreten Einzelfall speicherfähige Daten von Drittunternehmen an die Beklagte übermittelt worden seien. Eine sekundäre Darlegungslast treffe die Beklagte nicht, da sich die maßgeblichen Umstände allein in der Sphäre der Klagepartei befänden.

In der Sache wende sich die Klagepartei sich erkennbar ausschließlich gegen die Verarbeitung sogenannter Business-Tools-Daten zum Zweck personalisierter Werbung. Eine solche Verarbeitung finde im Fall der Klagepartei jedoch nicht statt, da sie keine entsprechende Einwilligung erteilt habe; im Übrigen beruhe eine derartige Verarbeitung – soweit sie überhaupt erfolge – auf einer wirksamen, freiwilligen und jederzeit widerruflichen Einwilligung. Ergänzend macht die Beklagte geltend, die Klagepartei habe weder einen konkreten Verarbeitungszweck benannt noch erläutert, weshalb die – pauschal behaupteten – Verarbeitungszwecke rechtswidrig sein sollten.

Derzeit sei bei der Klagepartei die Einstellung „Meta-Cookies auf anderen Apps und Websites“ auf „nicht erlauben“ gesetzt. In diesem Fall würden etwaige über Business Tools übermittelte Daten ausschließlich zu Zwecken der Sicherheit und Integrität verarbeitet, nicht jedoch zu Werbezwecken. Diese Verarbeitung stütze die Beklagte auf die Rechtsgrundlagen der vertraglichen Notwendigkeit, der berechtigten Interessen sowie des öffentlichen Interesses. Sie diene insbesondere der Abwehr von Sicherheitsbedrohungen, der Erkennung missbräuchlicher oder krimineller Aktivitäten, dem Schutz Minderjähriger sowie der Aufrechterhaltung der Funktionsfähigkeit und Sicherheit der Plattformen (vgl. ergänzende Stellungnahme vom 12.1.2026). Ein Ausschluss solcher Daten von der Sicherheitsverarbeitung würde nach Auffassung der Beklagten erhebliche Sicherheitslücken schaffen. Zudem weist die Beklagte darauf hin, dass eine Erhebung von Daten über Business Tools bereits dann nicht stattfinde, wenn Drittanbieter ihre Webseiten oder Apps entsprechend programmierten; hierzu stelle die Beklagte den Drittunternehmen entsprechende technische Informationen zur Verfügung (Anlage B 18).

Weiter macht die Beklagte geltend, die Klagepartei habe es trotz mehrfacher Hinweise unterlassen, die ihr zur Verfügung stehenden Self-Service-Tools, insbesondere das Tool „Exportiere deine Informationen“, zu nutzen, um sich selbst einen Überblick über etwaige verarbeitete Daten zu

verschaffen. Es sei der Klagepartei ohne Weiteres möglich und zumutbar gewesen, hierdurch konkret vorzutragen, ob und welche Business-Tools-Daten mit ihrem Nutzerkonto verknüpft seien. Es sei nicht sachgerecht, die Beklagte zur Offenlegung entsprechender Informationen heranzuziehen, um erst die Substantiierung des klägerischen Vortrags zu ermöglichen.

Der geltend gemachte Löschungsantrag sei unzulässig, da er nicht hinreichend bestimmt sei; zudem bestehe keine Besorgnis nicht rechtzeitiger Leistung im Sinne des § 259 ZPO. Unabhängig davon könne die Klagepartei Informationen über Aktivitäten außerhalb der Plattform von ihrem Instagram-Konto trennen oder das gesamte Konto löschen

Ein Anspruch auf Geldentschädigung stehe der Klagepartei nicht zu, erst recht nicht in der geltend gemachten Höhe. Ein Anspruch aus Art. 82 DSGVO scheide aus; daneben kämen konkurrierende Ansprüche nach nationalem Recht nicht in Betracht, deren Voraussetzungen im Übrigen ebenfalls nicht vorlägen. Insbesondere habe die Klagepartei keine schwerwiegende, die Erheblichkeitsschwelle überschreitende Verletzung ihres Persönlichkeitsrechts dargelegt. Für sämtliche in Betracht kommenden Ansprüche gelte, dass die Klagepartei über die Datenschutzeinstellungen der Beklagten jederzeit die Kontrolle über ihre Daten habe, sodass von einem Kontrollverlust keine Rede sein könne. Die streitige Verarbeitung beruhe vielmehr auf der wichtigen Aufgabe der Beklagten, die Sicherheit ihrer Nutzer sowie die eigene Sicherheit, insbesondere vor externen Angriffen, zu gewährleisten.

Die Klagepartei erwidert hierauf, dass Gegenstand der Klage die gesamte Datenverarbeitung seitens der Beklagten sei und nicht lediglich diejenige zum Zweck der Bereitstellung personalisierter Werbung. Die Klagepartei stütze sich auf einen Verstoß der Beklagten gegen die Pflicht zur datenschutzkonformen Gestaltung der technischen Systeme, Art. 25, Art. 5 Abs. 1 DSGVO. Zu möglichen Verarbeitungszwecken müsse nicht etwa die Klagepartei vortragen, sondern die Beklagte.

Der Senat verweist ergänzend auf die Schriftsätze der Parteien samt Anlagen.

Der Senat hat die Sach- und Rechtslage mit den Parteivertretern in der mündlichen Berufungsverhandlung vom 14.01.2026 eingehend erörtert. Es wird auf das Protokoll der mündlichen Verhandlung Bezug genommen.

Die Beklagtenseite hat klargestellt, dass sie sich auf eine Einwilligung nur stütze, soweit es darum gehe, die erhobenen Daten zu nutzen, um personalisierte Werbung anzubieten.

In der mündlichen Verhandlung beantragte die Beklagte die Gewährung einer Schriftsatzfrist zu

den Hinweisen des Senats in der mündlichen Verhandlung. Die Beklagte erklärte nicht bis zum 21.1.2026, dass sie bereit sei, die von der Klagepartei gespeicherten Offsite-Daten offen zu legen.

B.

Die Berufung der Klagepartei ist zulässig und teilweise begründet. Die Klage war zulässig (C.) und teilweise begründet (D.). Die beantragte Schriftsatzfrist war nicht zu gewähren (E.).

C.

Die Klage erweist sich als zulässig.

I. Internationale Zuständigkeit

Die internationale Zuständigkeit, die auch in der Berufung von Amts wegen zu prüfen ist (vgl. für die Revision BGHZ 153, 82 (84 ff.) = NJW 2003, 426), folgt aus Art. 17 I lit. c, 18 I Alt. 2 Brüssel Ia-VO, da es sich um eine Verbrauchersache handelt.

II. Löschung

Der auf Löschung bestimmter Daten spätestens einen Monat nach Rechtskraft gerichtete Antrag (s. Ziff. 4 Hs. 1 der Berufungsanträge, Bl. 116 d. BerA) erweist sich bei entsprechendem Verständnis, insbesondere nach Erläuterung in der Verhandlung als zulässig.

Ein Fall der §§ 257 ff. ZPO liegt dabei nicht vor, weil der Anspruch auf Löschung bereits fällig ist (§ 271 Abs. 1 BGB). Dies zumindest, wenn man – im Sinne der Klage – unterstellt, dass die streitgegenständliche Datenverarbeitung unrechtmäßig war (Art. 17 Abs. 1 lit. d) DSGVO).

Dass die Klagepartei entgegen § 260 ZPO („dieselbe Prozessart“) eine einstweilige Regelung dahingehend anstreben könnte, es der Beklagten bis einen Monat nach Rechtskraft zu untersagen, den bestehenden Löschungsanspruch zu erfüllen, lag von vornherein fern.

Die Klagepartei hat in der mündlichen Berufungsverhandlung klargestellt, dass sie eine Löschung *spätestens* einen Monat nach Rechtskraft begehrt. So verstanden, begegnet der Klageantrag keinen Zulässigkeitsbedenken.

D.

Die Klage ist teilweise begründet

Die Anwendung deutschen Rechts folgt vorliegend aus der Rechtswahl der Parteien (Art. 3 Abs. 1, 6 Abs. 2 Rom I-VO – vgl. die Nutzungsvereinbarung in Anlage B2), sie ergäbe sich im Übrigen aus Art. 6 Abs. 1 lit. b Rom I-VO, weil ein Verbrauchervertrag vorliegt.

Der Klagepartei steht

- ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO in Höhe von 750 € (I.)
- ein Löschungsanspruch (II.)
- ein Anspruch auf Auskunft (III.)
- sowie ein Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten zu (dazu IV.).

Im Übrigen war die Klage abzuweisen.

Die Datenschutz-Grundverordnung (im Folgenden DSGVO) ist vorliegend sachlich (Art. 2), räumlich (Art. 3) und auch zeitlich (vgl. Art. 99 Abs. 2) anwendbar.

I. Schadensersatz

Der Klagepartei steht ein Anspruch auf Schadenersatz nach Art. 82 DSGVO in Höhe von € 750 zu.

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter (Art. 82 Abs. 1 DSGVO). Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde (Art 82 Abs. 2 S. 1 DSGVO). Der Verantwortliche wird von der Haftung nach Art. 82 Absatz 2 DSGVO befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 Abs. 3 DSGVO).

Der Senat geht davon aus, dass die Klagepartei einen einheitlichen Anspruch auf (immateriellen) Schadensersatz aus Art. 82 Abs. 1 DSGVO (vgl. hierzu BGH, Urt. v. 18.11.2024 – VI ZR 10/24, NJW 2025, 298 Rn. 16) geltend macht, der sich auf eine Vielzahl einzelner, nicht konkretisierter und auch nicht konkretisierbarer Datenschutzverstöße der Beklagten stützt, aber in einem einheitlichen Geschehen (dem fortlaufenden Einsatz der sog. Meta-Business-Tools) wurzelt.

Mit den Worten des BGH (a.a.O., Rn. 21) erfordert ein derartiger Anspruch nach der Rechtspre-

chung des EuGH „einen Verstoß gegen die Datenschutz-Grundverordnung, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind [...] Die Darlegungs- und Beweislast für diese Voraussetzungen trifft die Person, die auf der Grundlage von Art. 82 I DSGVO den Ersatz eines (immateriellen) Schadens verlangt [...]. Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruchs nach Art. 82 I DSGVO ein Verschulden des Verantwortlichen. Art. 82 DSGVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 III DSGVO dem Verantwortlichen [...].“

1. Verstoß gegen die DSGVO

Für den Senat steht fest, dass die Beklagte mithilfe der Meta-Business-Tools eine potenziell unbegrenzte Menge an Daten der Klagepartei seit 01.01.2021 bis zum Schluss der mündlichen Verhandlung verarbeitet, indem sie die Aktivitäten der Klagepartei auf Dritt-Webseiten und Dritt-Apps verfolgt (so auch EuGH v. 4.7.2023 – C 252/21, GRUR 2023, 1131 Rn. 118 betr. Facebook), ohne dass ihr dies nach der DSGVO erlaubt wäre.

a. Technische Grundlage

Mit der Integration der sog. Meta-Business-Tools (u.a. Meta-Pixel und Conversions API, App Events über Facebook SDK [bzw. Facebook SDK] und App Events API) durch die Anbieter von (Dritt-) Webseiten und Apps werden die technischen Voraussetzungen für eine Übertragung von Kontaktinformationen und Event-Daten an die Beklagte geschaffen. Wann welche technischen Standarddaten, Kontaktinformationen und Event-Daten übertragen werden, hängt insbesondere davon ab, welche Einstellungen der Drittanbieter vornimmt.

Bezogen auf die besonders aussagekräftigen Event-Daten, durch die das Verhalten der Nutzer auf der Webseite oder App abgebildet wird, verlangen die Business-Tools-Nutzungsbedingungen von dem Drittanbieter, die erforderlichen Angaben und Datenschutzbelehrungen zu erteilen und die notwendige Einwilligung einzuholen, bevor Daten übertragen werden. Drittanbieter können definieren, welche „Standard-Events“ (PageView, Lead, StartTrial, AddToCart, Purchase, Subscribe, Contact, Schedule, ViewContent, Donate, Search, AddToWishlist, CompleteRegistration, AddPaymentInfo, InitiateCheckout, FindLocation, SubmitApplication, CustomizeProduct, vgl. Anlage K8 unter Hinweis auf eine Publikation der Beklagten) und welche selbstdefinierten Events gesendet werden (vgl. Anlage K8, Anlage B5, Anlage B20). Ob der jeweilige Drittanbieter diese Vorgaben umsetzt, kontrolliert die Beklagte nicht.

Wie die Beklagte mit den bei ihr eingegangenen Informationen weiter verfährt, hängt von den Datenschutz-Einstellungen des jeweiligen Nutzers ab.

Erlaubt der Nutzer der Beklagten nicht, Cookies und vergleichbare Technologien in anderen Apps und auf anderen Webseiten zu nutzen, so kann er sich dort nicht mehr mit seinem Instagram-Konto anmelden und die dort erhobenen Daten werden nicht verwendet, um relevante Werbung zu zeigen. Sie werden aber in eingeschränktem Umfang genutzt, um für Sicherheit und Integrität zu sorgen und es kann sein, dass die Beklagte aggregierte Informationen zu Aktivitäten erhält, nicht aber die persönliche Cookie-Information des Nutzers (Anlage B7, S. 41).

Entscheidet sich der Nutzer dafür, Werbung mithilfe der Informationen von Werbepartnern zu seinen Aktivitäten relevanter zu machen, erhält er stärker personalisierte Werbung. Entscheidet er sich dagegen, (s. Anlage B7, S. 43), werden die Daten dennoch – für andere Zwecke – verarbeitet (vgl. Duplik), z.B. zum Schutz der Sicherheit und Integrität der Server (a.a.O.) oder zur Messung der Effektivität von Werbekampagnen (Anlage K11, S. 23: „die Conversions API ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben“).

Der Nutzer hat weiter die Möglichkeit, die Verknüpfung künftiger Aktivitäten mit seinem Konto aufzuheben und frühere Aktivitäten zu löschen (Anlage B7, S. 44 ff.). In diesem Fall erhält die Beklagte aber weiterhin Informationen zu seinen Aktivitäten, die für Messungen sowie zur Verbesserung der Werbesysteme verwendet werden (Anlage B7, S. 56). Dass damit auch eine Löschung im System der Beklagten verbunden ist, lässt sich der Datenschutzrichtlinie an keiner Stelle entnehmen.

b. Verarbeitung von personenbezogenen Daten der Klagepartei, Art. 5 Abs. 1, 2 DSGVO

Der Senat geht davon aus, dass die Klagepartei von der streitgegenständlichen Datenverarbeitung mittels sogenannter Business-Tools betroffen war und die Beklagte Daten der Klagepartei infolgedessen verarbeitet, das Bestreiten der Beklagten erweist sich als unzureichend, § 138 Abs. 2, Abs. 3 ZPO.

(i) Vortrag der Klagepartei

Die Klagepartei trägt vor, dass sie im Internet regelmäßig Webseiten bestimmter Kategorien (vgl. Replik S. 37 - 42 i.V.m. Anlage K 13 + 14) aufgesucht habe und weiterhin besuche, in die nach den Erkenntnissen ihrer Prozessbevollmächtigten Meta-Business-Tools integriert seien.

Die Klagepartei hat im Rahmen ihrer informatorischen Anhörung vor dem Landgericht sowie er-

neut vor dem Senat vorgetragen, sie nutze vor allem die Plattformen Instagram und WhatsApp; ein früher bestehender Facebook-Account sei gelöscht worden. Sie habe wahrgenommen, dass ihr nach Internetrecherchen auf externen Webseiten – etwa zu Nachrichten-, Gesundheits- oder Finanzthemen – in Anwendungen der Beklagten entsprechende Werbung angezeigt werde. Der Kläger lehnt bereits seit längerer Zeit alle Cookies ab, soweit möglich ab.

Erst seit einem Gespräch mit ihren Prozessbevollmächtigten habe die Klagepartei ein Bewusstsein dafür, dass Informationen über das Verhalten auf Drittwebseiten und –apps von der Beklagten aufgezeichnet würden.

(ii) Pauschales Bestreiten nicht ausreichend

Das einfache, pauschale Bestreiten der Beklagten ist unwirksam, der Vortrag der Klagepartei gilt damit als zugestanden, § 138 Abs. 3 ZPO.

Nach allgemeinen prozessualen Grundsätzen kann in bestimmten Fällen gegenüber einer Tatsachenbehauptung der darlegungsbelasteten Partei ein einfaches Bestreiten genügen. Das ist z.B. dann der Fall, wenn der Gegner sich zu der behaupteten Tatsache nicht erklären kann oder wenn eine Tatsache zunächst allgemein behauptet wird und von der darlegungsbelasteten Partei eine weitere Substantiierung erwartet werden kann.

Im vorliegenden Fall hätte die Beklagte sich hingegen zum Vortrag der Klagepartei gemäß § 138 Abs. 2 ZPO erklären können und – in Ausübung sekundärer Darlegungslast – müssen, weil die Klagepartei in einem für ihren Vortrag zentralen Punkt – der Frage auf welchen (Dritt-) Webseiten und Apps Meta-Business-Tools zur Anwendung kommen und welche Daten in der Folge von der Beklagten erhoben werden – außerhalb des darzulegenden Geschehensablaufs steht, während die Beklagte als bestreitende Partei alle relevanten Tatsachen kennt (BGH Urt. v. 13.1.2011 – III ZR 146/10, NJW 2011, 1509 Rn. 20). Der Beklagten war substantiierter Gegenvortrag möglich und zumutbar, weil die behaupteten Tatsachen in ihrem Wahrnehmungsbereich gelegen haben (vgl. BGH Urt. v. 15.8.2019 – III ZR 205/17, NJW-RR 2019, 1332 Rn. 23 mwN). Ihr einfaches Bestreiten ist gemäß § 138 Abs. 3 ZPO als unbeachtlich anzusehen (BGH a.a.O.).

Entscheidend ist vorliegend, dass die Beklagte anhand ihres eigenen Systems und der Abfrage des Nutzerkontos ohne weiteres darlegen und überprüfen kann, welche Daten ihr von welchen Drittseiten übermittelt wurden. Demgegenüber wird ein durchschnittlicher Internetnutzer, das ist das Wesen des Surfers im Internet, für einen längeren Zeitraum nicht darlegen können, welche Seiten er konkret besucht hat. Die Klagepartei kann zudem unstreitig nicht wissen, welche Inter-

netseiten und Apps wann mit welchen Meta-Business-Tools ausgestattet sind und welche Daten übertragen werden. Datenschutzrechtliche Sachverhalte sind regelmäßig durch eine strukturelle Informationsasymmetrie geprägt. Die betroffene Person hat weder Einblick in die technischen Abläufe der Datenverarbeitung noch Zugriff auf interne Systeme, Server-Logs oder Datenverknüpfungen. Der maßgebliche Geschehensablauf liegt typischerweise vollständig in der Sphäre der verantwortlichen Stelle, sprich der Beklagten.

Diese Wertung findet ihre gesetzgeberische Bestätigung nach Art. 5 Abs. 2 DSGVO in der der verarbeitenden Seite obliegenden Rechenschaftspflicht und dem damit korrespondierenden eingeräumten Auskunftsrecht aus Art. 15 DSGVO des Betroffenen. Nach dem Wortlaut von Absatz 2 des Art. 5 DSGVO ist der Verantwortliche nach dem in dieser Bestimmung verankerten Grundsatz der „Rechenschaftspflicht“ für die Einhaltung des Absatz 1 dieses Artikels verantwortlich und muss nachweisen können, dass jeder der dort genannten Grundsätze eingehalten worden ist; mithin obliegt ihm hierfür die Beweislast (EuGH Urt. v. 4.5.2023 – C-60/22; ZD 2023, 606 Rn. 53).

Das Auskunftsrecht verdeutlicht zudem, dass der Unionsgesetzgeber die Kenntnis der konkreten Verarbeitungsvorgänge grundsätzlich der verantwortlichen Stelle zuweist und davon ausgeht, dass die betroffene Person ohne Mitwirkung des Verantwortlichen nicht in der Lage ist, Art, Umfang und Zweck der Datenverarbeitung zu überblicken. Das Auskunftsrecht dient der Herstellung der Transparenz und Kontrolle der natürlichen Person, deren Daten verarbeitet werden, nicht jedoch dazu, der betroffenen Person im Zivilprozess die primäre Darlegungslast für außerhalb ihres Wahrnehmungsbereichs liegende Vorgänge aufzuerlegen.

Vorliegend hat die Klagepartei von ihrem Auskunftsrecht bereits vorprozessual Gebrauch gemacht (Anlage K 3). Eine vollständige, nachvollziehbare und systematische Darstellung der von ihr erhobenen, übermittelten, gespeicherten und verwendeten Daten hat die Beklagte der Klagepartei nicht zur Verfügung gestellt. Die Beklagte hat insbesondere nicht ausreichend dargelegt, dass das von ihr zur Verfügung gestellte Selbsthilfetool eine derartige vollständige Darstellung enthält. Die Beklagte hat auch nicht vorgetragen, auf welchen Webseiten und Apps Business-Tools zum Einsatz kommen.

Eine substantiierte Offenlegung der tatsächlich verarbeiteten Daten erfolgte damit nicht.

Ausreichend ist daher, dass der klägerische Vortrag bei verständiger Würdigung greifbare Anhaltspunkte für die behauptete individuelle Betroffenheit erkennen lässt. Das ist angesichts der – unstreitigen – Verbreitung der Meta-Business-Tools und bei Annahme einer üblichen Internetnutzung der Fall. Die Klagepartei hat in Anlage K14 eine Vielzahl weitverbreiteter Internetseiten aufge-

listet, auf denen sie den Meta Pixel nachweisen konnte, die Beklagte hat lediglich angemerkt, dass im Zeitpunkt der Berufungsbegründung auf einzelnen Webseiten der Meta Pixel nicht mehr eingebunden sei. Auch zu der Nutzung des Internets seitens der Klagepartei wurden Angaben gemacht.

Die nähere Aufklärung des in der Sphäre der Beklagten liegenden Geschehens durch substantiiertes Bestreiten obliegt sodann dieser, ohne dass damit eine Umkehr der Beweislast verbunden wäre. Aus Sicht des Senats genügt der klägerische Vortrag für die Annahme der behaupteten Datenschutzverletzung, das Bestreiten der Beklagten ist demgegenüber als pauschales Bestreiten unzulässig.

(iii) Personenbezogene Daten

Der Schutz der DSGVO gilt für alle Daten, die Rückschlüsse auf eine Person zulassen, direkt (z.B. Name) oder indirekt (z.B. durch Kombination von Merkmalen wie E-Mail-Adresse, Standortdaten o.ä.). Besonders sensible Daten (Gesundheit, Genetik) genießen einen höheren Schutz.

Die erhobenen Informationen und Daten sind personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO, weil sie sich auf eine identifizierte oder – direkt oder indirekt – identifizierbare natürliche Person, nämlich die Klagepartei, beziehen. Die Beklagte kann die Verknüpfung zwischen an sich anonymen (Kontakt- und Event-) Daten und den bei ihr vorhandenen Benutzerinformationen herstellen (z.B. über die verwendete IP-Adresse oder individuelle Geräteinformationen; vgl. dazu anschaulich Anlage K 7) und sie damit dem jeweiligen Kunden zuordnen. Dies trifft den Erwägungsgrund 26 zur DSGVO: *„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren [...]“*; s. auch EuGH Ur. v. 19.10.2016 – C-582/14, BeckRS 2016, 82520 zu dynamischen IP-Adressen).

c. Die Datenverarbeitung seitens der Beklagten ist nicht nach Art. 6 Abs. 1 DSGVO gerechtfertigt und daher nicht rechtmäßig.

(i) Beweislast bei Verantwortlichen

Die Beklagte trägt als Verantwortliche gem. Art 5 Abs. 2 DSGVO die Beweislast unter anderem dafür, dass die Daten für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. *„Außerdem obliegt es nach Art. 13 I Buchst. c dieser Verordnung,*

wenn personenbezogene Daten bei der betroffenen Person erhoben werden, dem Verantwortlichen, diese Person über die Zwecke, für die diese Daten verarbeitet werden sollen, sowie über die Rechtsgrundlage für die Verarbeitung zu informieren“ (EuGH Urt. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 95, v. 24.2.2022 – C-175/20, EuZW 2022, 527; Rn. 77).

Anders als die Beklagte meint, muss nicht die Klagepartei bestimmte Verarbeitungszwecke in Frage stellen, sondern hat die Beklagte zu erklären, zu welchem Zweck sie welche Daten erhoben hat und weshalb die Verarbeitung der Daten rechtmäßig sein soll. Die Beklagte verweist in der Berufungsbegründung selbst auf die sog. Einwilligungsleitlinien des Europäischen Datenschutzausschusses, in denen es heißt: „[...] *ist es sehr wichtig, dass die Verantwortlichen vor der Erhebung der Daten die Zwecke bewerten, für die die Daten tatsächlich verarbeitet werden und die Rechtsgrundlage, auf die sich die Verarbeitung stützt. [...] Deshalb sollten Verantwortliche von Anfang an deutlich machen, welcher Zweck auf welche Daten Anwendung findet und auf welcher Rechtsgrundlage die Verarbeitung beruht.*“

(ii) Kein Vortrag der Beklagten zur Rechtfertigung bestimmter Datenverarbeitungsvorgänge

Wie dargestellt setzt eine Rechtfertigung nach Art. 6 DSGVO voraus, dass die verarbeiteten Daten in einem ersten Schritt benannt werden und dass in einem zweiten Schritt jeder einzelne Verarbeitungsvorgang gerechtfertigt wird. Die Beklagte trägt schon nicht vor, welche Daten des Klägers sie überhaupt verarbeitet hat, womit eine Subsumtion unter Art. 6 DSGVO und gegebenenfalls Art. 9 DSGVO von vornherein ausscheidet. Die Beklagte wird damit ihrer Darlegungslast nicht gerecht, die vom Senat als unstreitig zu behandelnde (s.o.) Verarbeitung von Daten der Klagepartei erfolgt also rechtswidrig.

(iii) Hilfsweise: Die von der Beklagten ins Feld geführten Erlaubnistatbestände greifen nicht

Weil die Beklagte nicht offenlegt, welche Daten der Klagepartei sie wie verarbeitet (hat), sind Überlegungen zu einer möglichen Rechtfertigung spekulativ.

Selbst wenn man dies – wie die Beklagte – anders sehen wollte, käme eine Rechtfertigung der streitgegenständlichen Datenverarbeitung nicht in Betracht:

(1) Verarbeitungszwecke

Die Beklagte stützt sich ausweislich ihrer Berufungsbegründung für die Verarbeitungszwecke auf unterschiedliche Rechtsgrundlagen, die sich aus ihrer Datenschutzrichtlinie ergeben sollen. Ein Blick in die als Anlage K1 vorliegende Datenschutzrichtlinie bestätigt diesen Befund. Hier findet sich auf annähernd 70 (!) Seiten (Anlage K1, S. 82 – 150) eine Darstellung zu den Rechtferti-

gungsgründen i.S.v. Art. 6 Abs. 1 DSGVO, den Gründen für die Datenverarbeitung („Warum und wie wir deine Informationen verarbeiten“) und der verwendeten „Informationskategorien“. Für die vorliegend relevante Informationskategorie „Information von Partnern, Anbietern und Dritten“ finden sich dabei – sinngemäß – die folgenden Eintragungen:

<i>Rechtsgrundlage</i>	<i>Verarbeitungszweck</i>
<i>Einwilligung</i>	<i>Personalisierung von Werbeanzeigen</i>
<i>Erfüllung eines Vertrags</i>	<i>Personalisierung der Meta-Produkte</i>
	<i>Bereitstellung und Verbesserung von Meta-Produkten, u.a. Inhalte analysieren</i>
	<i>Förderung von Schutz, Integrität und Sicherheit in und auf den Meta-Produkten</i>
	<i>Übermittlung, Speicherung oder Verarbeitung deiner Informationen weltweit, intern wie extern</i>
<i>Erfüllung einer rechtlichen Verpflichtung</i>	<i>Verarbeitung von Informationen, wenn nach dem Gesetz erforderlich</i>
<i>Berechtigte Interessen</i>	<i>Personalisierung der Meta-Produkte</i>
	<i>Bereitstellung und Verbesserung von Meta-Produkten, u.a. Inhalte analysieren</i>
	<i>Förderung von Schutz, Integrität und Sicherheit in und auf den Meta-Produkten</i>
	<i>Bereitstellung von Messungen, Analysen und anderen Unternehmens-Services für Unternehmen, Werbetreibende und andere Partner:</i>
	<i>Kommunikation, Interaktion und Teilen von Inhalten über die Produkte der Meta-Unternehmen hinweg:</i>
	<i>Business Intelligence und Statistik</i>
	<i>Identifizierung/Personalisierung iRv Meta Audience Network</i>
	<i>Zuschneiden von Werbeanzeigen</i>
	<i>Forschung und Innovation für soziale Zwecke</i>
	<i>Anonymisieren von Informationen</i>
	<i>Beantwortung rechtlicher Anfragen</i>
	<i>Förderung von Schutz, Integrität und Sicherheit außerhalb der Erfüllung von Verträgen</i>
<i>... bei Nutzung nicht bekannter</i>	<i>Förderung von Schutz, Integrität und Sicherheit</i>

*Geräte**Forschung und Innovation für soziale Zwecke**Beantwortung rechtlicher Anfragen**Produktverbesserung**In den öffentlichen Interessen**durchgeführte Aufgaben**Forschung für soziale Zwecke**Förderung von Schutz, Integrität und Sicherheit**Schutz deiner wesentlichen Interessen oder der einer**Schutz wesentlicher Interessen**anderen Person*

Zu ergänzen ist, dass die Beklagte sich ausschließlich auf den Verarbeitungszweck der Sicherheit und Integrität stützt, wenn der Nutzer „Meta Cookies in anderen Apps und auf anderen Websites“ nicht erlaubt (vgl. zuletzt Schriftsatz vom 07.01.2026). Im vorliegenden Fall ist das nicht relevant, weil die Klagepartei die entsprechende Einstellung nicht vorgenommen hat. Die Beklagte hat im Schriftsatz vom 07.01.2026 nur ausgeführt, dass bei der Klagepartei die Einstellung „Meta-Cookies auf anderen Apps und Websites“ derzeit auf „nicht erlauben“ gesetzt sei.

(2) Einwilligung

Die Beklagte stützt sich auf eine Einwilligung ihrer Nutzer nur, um eine Personalisierung von Werbung zu rechtfertigen. Eine derartige Einwilligung erhält die Beklagte mittels der „Information von Werbepartnern zu Deinen Aktivitäten“-Einstellung.

Die Beklagte hat in ihrer Duplik klargestellt, dass sie aus einer Zustimmung, „Meta Cookies in anderen Apps und auf anderen Websites“ einzusetzen, keine Einwilligung im Sinne der DSGVO herleitet.

Wäre der Vortrag der Beklagten so zu verstehen, dass sie bestimmte Datenverarbeitungsvorgänge auf die „Cookie-Banner-Einwilligungen“ auf Drittseiten stützen wollte, so ist hierzu anzumerken, dass die Beklagte zu keiner einzigen Einwilligung auf einer Drittseite konkret vorgetragen hat. Sie hat dem Senat damit die Möglichkeit genommen, die Wirksamkeit der Einwilligung zu prüfen. Das ist von Relevanz, weil eine Willensbekundung in Bezug auf die Einwilligung freiwillig erfolgt sein müsste, für den bestimmten Fall, in informierter Weise und unmissverständlich sowie durch Erklärung oder eine sonstige eindeutige bestätigende Handlung (st. Rspr. EuGH z.B. 4.10.2024 – C-200/23, GRUR-RS 2024, 26255 Rn. 99 ff.). Anders als die Beklagte meint, folgt aus der FashionID-Entscheidung des EuGH nach Auffassung des Senats auch nicht, dass eine wirksame Ein-

willigung zugunsten der Beklagten zu unterstellen ist. Der Drittanbieter ist für das Einholen der Einwilligung verantwortlich, die Beklagte darf die personenbezogenen Daten aber nur verarbeiten, wenn eine wirksame Einwilligung vorliegt. Das hat sie zu überprüfen, was unstreitig nicht geschieht. Unabhängig davon würde die – unterstellt – wirksame Einwilligung auf einer Drittseite nur die Erhebung und Weiterleitung von Daten rechtfertigen, nicht aber die Speicherung und spätere Verwendung seitens der Beklagten.

Auch ist eine Datenverarbeitung nicht über die Datenschutzrichtlinie, der die Klagepartei durch Anlegen eines Nutzerkontos zugestimmt haben könnte, und damit nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO gerechtfertigt. Die Beklagte hat in der Duplik klargestellt, „dass die Datenschutzrichtlinie keinesfalls als Rechtsgrundlage zur Verarbeitung irgendwelcher Daten herangezogen wird“.

(3) Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. b) – f) DSGVO

Auch eine Rechtfertigung der Datenverarbeitung nach Art. 6 Abs. 1 lit. b) – f) DSGVO scheitert zur Überzeugung des Senats – wie dargestellt – schon daran, dass die Beklagte nicht hinreichend genau bezeichnet, welche Daten sie zu welchem Verwendungszweck erhebt. Die Datenschutzrichtlinie (Anlage K 1) bezeichnet diese Ziele auch nur allgemein oder nimmt Bezug darauf, dass sie sich an geltendes Recht halten will. Konkrete Ziele werden nicht bezeichnet. Dass ihr dies angesichts der Menge der betroffenen Daten womöglich nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, verdeutlicht nur den eklatanten Verstoß gegen den Grundsatz der Datenminimierung.

(4) Datenverarbeitung ist nicht erforderlich nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO

Selbst wenn man dies anders sehen und es für ausreichend erachten wollte, dass die Beklagte – ohne auf die konkret verarbeiteten Daten einzugehen – in allgemeiner Form auf ihre Datenschutzrichtlinie verweist, gelangt man nicht zu einer Rechtfertigung der Datenverarbeitung: Die Verarbeitung der personenbezogenen Daten ist für die Erfüllung des Nutzungsvertrages zwischen den Parteien nicht erforderlich i.S.v. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO: Die auch insoweit darlegungs- und beweisbelastete (EuGH Urt. V. 4.7.2023 - C-252/21, GRUR 2023, 1131 Rn. 98) Beklagte hat nicht hinreichend konkret dargestellt, weshalb die Verarbeitung der Daten „objektiv unerlässlich [war], um einen Zweck zu verwirklichen, der notwendiger Bestandteil, der für die betroffene Person bestimmten Vertragsleistung ist“ (EuGH a.a.O.).

Es erscheint bereits zweifelhaft, ob die von der Beklagten in der Berufung angesprochene Personalisierung von Funktionen, Inhalten und Vorschlägen zu Personen, Gruppen und Veranstaltungen notwendiger Bestandteil der Vertragsleistung seitens der Beklagten ist. Jedenfalls aber ist die

streitgegenständliche Verarbeitung von Daten zur Erreichung dieses Zweckes nicht „objektiv unerlässlich“, sondern ließe sich eine hinreichende Personalisierung schon durch Onsite-Daten erreichen.

Zu den von ihr verfolgten Sicherheits- und Integritätszwecken hat die Beklagte in der Berufungsinstanz ergänzend vorgetragen. Wie bereits in erster Instanz fehlt es aber an hinreichend präzisiertem Vortrag zu konkreten, die Klagepartei betreffenden Datenverarbeitungsvorgängen (z.B.: Wann wurde welche IP-Adresse verarbeitet und weshalb war die Verarbeitung im konkreten Fall aus Sicherheitsgründen notwendig?). Sollte der Vortrag der Beklagten so zu verstehen sein, dass alle Daten aus Sicherheits- und Integritätsgründen bis zu 90 Tage aufbewahrt werden, wäre eine solche Vorgehensweise nicht unerlässlich, um den Nutzungsvertrag mit der Klagepartei zu erfüllen.

(5) Keine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO

Die Verarbeitung der personenbezogenen Daten ist auch nicht zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO.

Nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO ist eine Verarbeitung personenbezogener Daten unter den folgenden drei Voraussetzungen rechtmäßig: „Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen“ (EuGH Ur. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 106).

Indem die Beklagte im vorliegenden Verfahren nicht hinreichend genau bezeichnet, welche Daten sie zu welchem Zweck erhoben und verarbeitet hat, ermöglicht sie es dem Senat nicht, eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO zu prüfen. Dies entspricht dem Befund des Bundeskartellamtes, wonach der Vortrag der Beklagten keine hinreichend klare Artikulation der berechtigten Interessen darstellt, die der Abwägungsprüfung mit den Interessen und Rechten der betroffenen Personen zugänglich wäre (BKartA, Beschluss v. 19.02.2019 in Bezug auf Facebook [B6-22/16], Rn. 727 ff., 736 ff., 796 ff.). Auch die im Berufungsverfahren ergänzten, für Nutzer unterhalb der Volljährigkeit relevanten Ausführungen zu den Sicherheits- und Integritätsinteressen der Beklagten, sind allgemein gehalten (s.o.) und ermöglichen keine Prüfung der Rechtfertigung.

Unabhängig davon ist angesichts von Art und Umfang der verarbeiteten Daten mehr als zweifelhaft, ob die von der Beklagten in allgemeiner Form dargestellten Verarbeitungszwecke gegenüber den Interessen und Grundrechten des Nutzers (Art. 7, 8 GRCharta) Vorrang beanspruchen können (vgl. EuGH Ur. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 123 bezogen auf das Ziel der Produktverbesserung).

(6) Keine Rechtfertigung nach Art 6 Abs. 1 UAbs. 1 lit. c) DSGVO

Die Beklagte macht bereits nicht geltend, dass sie gesetzlich verpflichtet ist, personenbezogene Daten präventiv zu erheben und – gleichsam auf Vorrat – zu speichern, um jegliche Anfrage einer nationalen Behörde, die darauf abzielt, bestimmte Daten über ihre Nutzer zu erlangen, beantworten zu können. Eine derartige gesetzliche Verpflichtung liegt auch fern. Eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. c) DSGVO scheidet damit von vornherein aus (vgl. EuGH Ur. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 132).

(7) Keine Rechtfertigung nach Art 6 Abs. 1 UAbs. 1 lit. d) DSGVO

Eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. d) DSGVO kommt bei der gebotenen engen Auslegung von Art. 6 Abs. 1 DSGVO (EuGH Ur. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 93) nur in Betracht, wenn lebenswichtige Interessen zu schützen sind, wobei der Normgeber z.B. die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen im Blick hatte (46. ErwG). Konkreter Vortrag der Beklagten in diese Richtung fehlt, eine Rechtfertigung scheidet in Anbetracht der von der Beklagten angebotenen Dienste wirtschaftlicher und kommerzieller Art aus (EuGH a.a.O. Rn. 137).

(8) Keine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. e) DSGVO

Die Beklagte hat ferner nicht vorgetragen, dass ihr Aufgaben übertragen wurden, die im öffentlichen Interesse liegen oder dass ihr öffentliche Gewalt übertragen wurde, womit auch eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. e) DSGVO ausscheidet (vgl. EuGH a.a.O. Rn. 133).

(9) Umgehen mit sensiblen Daten, Art. 9 DSGVO

Es erscheint nach allgemeiner Lebenserfahrung zwar nicht ganz unwahrscheinlich, dass unter den verarbeiteten Daten auch solche sind, die dem besonderen Schutz des Art. 9 DSGVO unterliegen („sensible Daten“). In einem solchen Fall müsste die Verarbeitung des gesamten Datensatzes an Art. 9 Abs. 2 DSGVO gemessen werden (EuGH Ur. v. 4.7.2023 – C-252/21, GRUR 2023, 1131 Rn. 89), wobei die Beklagte zum Umfang und der Art und Weise der Datenverarbei-

tung nicht konkret vorgetragen hat. Weil die Klagepartei sich aber nur allgemein zu den von ihr genutzten Internetseiten geäußert hat, kann der Senat nicht mit der nötigen Sicherheit davon ausgehen, dass bei Drittanbietern auch sensible Daten i.S.v. Art. 9 Abs. 1 DSGVO erhoben wurden.

d. Verstoß gegen den Grundsatz der Datenminimierung und den Grundsatz der Rechtmäßigkeit der Datenverarbeitung nach Art. 5 f., 25 DSGVO

In dem – so ausgestalteten – Einsatz der Meta-Business-Tools und der anschließenden Verarbeitung der hierdurch erlangten Daten in den Systemen der Beklagten liegt ein Verstoß gegen den Grundsatz der Datenminimierung und den Grundsatz der Rechtmäßigkeit der Datenverarbeitung, der in Art. 5 Abs. 1 lit. b), lit. c), Art. 6 Abs. 1, Art. 25 Abs. 2, S. 1, 3 DSGVO verankert ist. Auf Grundlage des Vortrages der Parteien hat der Senat davon auszugehen, dass die Beklagte ein System bereitstellt, welches personenbezogene Daten der Klagepartei, die durch die Nutzung von (Dritt-) Webseiten und Apps entstehen, in einem erheblichen Umfang und undifferenziert verarbeitet, anstatt die Verarbeitung auf das für den jeweiligen Zweck notwendige Maß zu beschränken.

Der der DSGVO zugrundeliegende Grundsatz der Datenminimierung sichert die Verhältnismäßigkeit der Datenverarbeitung und besagt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (EuGH v. 4.10.2024 – C-446/21, NZA 2024, 1407 Rn. 49 f.; NZA 2023, 1523). Der Verantwortliche darf die Daten nicht allgemein und unterschiedslos erheben, sondern muss von der Erhebung solcher Daten absehen, die für die Zwecke der Verarbeitung nicht unbedingt notwendig sind (EuGH, a.a.O., Rn. 59). In zeitlicher Hinsicht ist der Zeitraum der Datenerhebung als solcher und der Zeitraum, in dem die Möglichkeit besteht, den Betroffenen zu identifizieren, auf das im Hinblick auf den Zweck der beabsichtigten Verarbeitung absolut Notwendige zu beschränken (sog. Speicherbegrenzung, s. EuGH a.a.O. Rn. 52 f.; 24.2.2022 – C-175/20, EuZW 2022, 527).

Art. 5 Abs. 1 lit. a DSGVO sichert, dass Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Zu beachten ist, dass die Rechtsgrundlage, auf der die Datenverarbeitung beruht, so „klar und präzise“ deren Tragweite und Anwendung regeln muss (Erwägungsgrund 41, S. 2), dass die Verarbeitung für die betroffene Person voraussehbar ist (BeckOK DatenschutzR/Schantz, 54. Ed. 1.11.2021, DS-GVO Art. 5 Rn. 6). Dies ist nicht gewährleistet.

Zwischen den Parteien ist unstreitig, dass die von den (Dritt-) Webseiten und Apps stammenden

„Kontaktinformationen“ und/oder „Event-Daten“ (Anlage B5) ungefiltert und damit – in den Worten des EuGH (s.o.) – allgemein und unterschiedslos von der Beklagten verarbeitet werden. Der Senat sieht hierin – wie der EuGH (v. 4.10.2024 – C-446/21, NZA 2024, 1407 Rn. 62 ff.) in einem Facebook betreffenden Fall – einen unverhältnismäßigen Eingriff in die durch Art. 7, 8 GRCharta geschützten Rechte der Klagepartei auf Achtung des Privatlebens und auf Schutz ihrer personenbezogenen Daten. Der EuGH weist zurecht darauf hin, „dass eine solche Verarbeitung besonders umfassend [ist], da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta Platforms Ireland aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht, wird“ (EuGH v. 4.10.2024 - C-446/21, NZA 2024, 1407 Rn. 62; Urt. v. 4.7.2023 – C-252/21, NZA 2023, 1523). Die Beklagte bestreitet die Verarbeitung der Daten im Gesamten nicht ausdrücklich, sondern gibt nur an, dass diese nicht für personalisierte Werbung verwendet werden.

Nachdem der Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO keine Abschreckungs- oder Straffunktion, sondern ausschließlich eine Ausgleichsfunktion erfüllt (BGH Urt. v. 18.11.2024 – VI ZR 10/24, NJW 2025, 298, Rn. 25 m.w.N.), muss der Senat nicht jeden einzelnen Verstoß gegen die DSGVO benennen.

e. Verantwortlicher, Art. 4 Nr. 7 DSGVO

Die Beklagte ist zur Überzeugung des Senats für die Erhebung, Übermittlung, Speicherung und Verwendung dieser Daten verantwortlich i.S.v. Art. 4 Nr. 7 DSGVO. Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Die Verantwortlichkeit der Beklagten für die Speicherung und Verwendung liegt auf der Hand. Wenn Daten über die Business-Tools ins System der Beklagten gelangt sind, ist in der Folge zwangsläufig diese für die weitere Verarbeitung verantwortlich im Sinne von Art. 4 Nr. 7 DSGVO.

Die Beklagte ist – gemeinsam mit dem jeweiligen Drittanbieter – auch für die Erhebung und Übermittlung verantwortlich (EuGH v. 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 79, 96 – *Fashion ID*). Das liegt daran, dass durch die Einbettung der Meta-Business-Tools in eine Webseite oder App quasi eine „dynamische Verweisung“ auf die jeweils aktuelle Version des Tools entsteht. Die Kontrolle über die Programmierung und in der Folge über die Funktionalität des Tools verbleibt damit bei der Beklagten. Diese entscheidet (mit), welche Daten erhoben und übermittelt

werden. Dass eine „gemeinsame Verantwortlichkeit für die Datenverarbeitung mit dem jeweiligen Drittunternehmen gem. der DSGVO betreffend die Erhebung und Übermittlung zusätzlicher Daten an Meta über gewisse Meta-Business-Tools“ besteht, hat die Beklagte eingeräumt (vgl. auch die Nutzungsbedingungen für die Meta-Business-Tools in Anlage B5, dort S. 5).

2. Keine Exkulpation

Art. 82 DSGVO sieht eine Haftung für vermutetes Verschulden vor (BGH v. 11.11.2024 – VI ZR 396/24, GRUR-RS 2025, 32135 Rn. 13; s. auch EuGH Urt. v. 11.4.2024 – C-741/21, NJW 2024, 1561 Rn. 44). Der Senat vermag dem Vortrag der Beklagten keine Anhaltspunkte für eine Exkulpation nach Art. 82 Abs. 3 DSGVO zu entnehmen. Die Beklagte macht geltend, dass sie rechtmäßig gehandelt habe, nicht, dass sie für die – aus Sicht der Klagepartei anspruchsbegründenden – Umstände nicht verantwortlich sei.

3. Kausalität und Schaden

Durch den Verstoß gegen den Grundsatz der Datenminimierung und die Vielzahl der unberechtigten Datenverarbeitungen ist der Klagepartei ein immaterieller Schaden im weiten, autonom unionsrechtlichen Sinne des Art. 82 Abs. 1, Abs. 2 DSGVO (vgl. hierzu EuGH Urt. v. 4.9.2025 – C-665/23, NJW 2025, 3137 Rn. 55; BGH v. 11.11.2024 – VI ZR 396/24, GRUR-RS 2025, 32135 Rn. 25 m.w.N.) entstanden. Der Senat schätzt diesen nach § 287 ZPO auf 750 €.

a. Immaterieller Schaden

Nach aktueller Rechtsprechung des EuGH kann „der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten [...] einen „immateriellen Schaden“ iSv Art. 82 Abs. 1 DS-GVO darstellen, der einen Schadensersatzanspruch begründet, sofern die betroffene Person den Nachweis erbringt, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat“ (EuGH Urt. v. 20.6.2024 – C-590/22, ZD 2024, 519 Rn. 33; zustimmend BGH 11.11.2024 – VI ZR 396/24, GRUR-RS 2025, 32135 Rn. 27 ff.). Zusätzliche spürbare negative Folgen müssen nicht hinzutreten (EuGH Urt. v. 4.10.2024 – C-200/23, NJW 2025, 40, Rn. 156).

b. Kontrollverlust

Für die Klagepartei stellt die Tatsache, dass eine erhebliche Menge personenbezogener Daten, die ihrem Benutzerkonto zugeordnet sind oder die ihr – z.B. mittels eines Abgleiches von IP-Adressen/Geräteinformationen – zugeordnet werden können, sich auf Servern der Beklagten in der ganzen Welt (s. Datenschutzrichtlinie in Anlage K1, S. 72) und bei bestimmten Dritten befinden und ggf. Dritten zur Verfügung gestellt werden können, einen Kontrollverlust dar. Als Dritte,

mit denen Informationen geteilt werden, bezeichnet die Datenschutzrichtlinie der Beklagten (Anlage K1, dort S. 48) Werbetreibende, Unternehmen, die Produkte für die Beklagten vermarkten oder die mit Kundenservice oder Umfragen beauftragt werden, und Forscher, Behörden sowie Strafverfolgungsbehörden (S. 76 Datenschutzrichtlinie).

c. Hinweis auf Verhalten anderer Anbieter entlastet nicht

Dahinstehen kann bei dieser Betrachtung, ob einzelne der streitgegenständlichen Daten bei lebensnaher Betrachtung auch von anderen Anbietern von Internetdiensten erhoben und gespeichert wurden. Denn dann läge jedenfalls eine Intensivierung des Kontrollverlusts vor, die ebenfalls einen immateriellen Schaden darstellt (BGH 11.11.2024 – VI ZR 396/24, GRUR-RS 2025, 32135 Rn. 35).

d. Zusätzliche spürbare negative Folgen

Der Senat ist auf der Grundlage der Anhörung der Klagepartei in der mündlichen Berufungsverhandlung weiter davon überzeugt, dass diese unter dem Gefühl leidet, dass ihr Privatleben konstant überwacht wird. Die Klagepartei hat ausgeführt, sie wolle „nicht das Gefühl haben, beobachtet zu werden, wenn man online ist“. Sie habe das Vorgehen der Beklagten aus den Medien wahrgenommen und empfinde es als belastend, dass Daten über sie gesammelt würden, ohne dass sie wisse, was mit diesen Daten geschehe. Dieses Gefühl habe sie auch konkret erlebt, wenn sie im Internet nach bestimmten Inhalten gesucht habe und ihr anschließend in Anwendungen der Beklagten entsprechende Werbung angezeigt worden sei; dies empfinde sie als „krass“. Das Gefühl der Beobachtung habe sie als negativ beschrieben, vergleichbar mit der Situation, „wie wenn einem einer hinterherläuft und beobachtet“.

Der Senat hält diese Angaben für nachvollziehbar und stimmig und legt sie der Entscheidung zugrunde.

4. Schadenshöhe

Der Senat folgt der Auffassung des Bundesgerichtshofes (Urt. v. 18.11.2024 – VI ZR 10/24, NJW 2025, 298 Rn. 96), wonach *„eine auf Art. 82 DS-GVO gestützte Entschädigung in Geld als 'vollständig und wirksam' anzusehen [ist], wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 I DS-GVO dagegen nicht erfüllen (vgl. EuGH [...]). Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße*

gegenüber derselben Person begangen (EuGH [...]) und ob er vorsätzlich gehandelt hat [...].“

Der Senat schätzt, dass vorliegend ein Betrag von 750 € erforderlich, aber auch ausreichend ist, um den eingetretenen Kontrollverlust und die dargestellten weiteren spürbaren Beeinträchtigungen auszugleichen, § 287 ZPO.

Insbesondere waren hierbei folgende Erwägungen von Bedeutung:

- Die Klagepartei hat sich entschieden, nicht offenzulegen, welche Internetseiten sie besucht. Der Senat geht deshalb davon aus, dass zwar eine ganz erhebliche Menge an Informationen verarbeitet wurde, er kann aber nicht mit der gebotenen Sicherheit feststellen, dass darunter sensible Daten i.S.v. Art. 9 DS-GVO waren.
- Es handelte sich um einen lang andauernden Datenschutzverstoß (seit 1.1.2021).
- Der Vortrag der Parteien erlaubt es dem Senat nicht, das Ausmaß des Kontrollverlustes genau festzustellen. Berücksichtigt hat der Senat aber, in welchem Umfang – ausweislich der Datenschutzrichtlinie der Beklagten (Anlage K 1, S. 48 ff.) - die Daten weitergegeben. Dies umfasst Werbetreibende, Partner der Beklagten - die Analysedienste nutzen -, Handelspartner, Anbieter für Mess- und Marketinglösungen, Dienstleister für die Beklagte, Dritte (externe Forscher, sonstige Dritte - dies dürfte auch Strafverfolgungsbehörden im Ausland umfassen). Der Empfängerkreis ist zwar begrenzt, aber für die Klageseite nicht mehr bestimmbar. Ausweislich der Datenschutzrichtlinie, S. 72 ff., werden die Informationen in die ganze Welt übertragen (Standorte von Meta-Servern, Länder, in denen die Meta-Produkte verfügbar sind, und Empfänger, die ausweislich der Bestimmungen der Beklagten berechtigt sein sollen, ohne dass deren Berechtigung klar definiert ist).
- Es kann daher z.B. nicht ausgeschlossen werden, dass die Daten der Klagepartei bei gegenüber der Beklagten nachgewiesenen „berechtigten Interessen“ auch Staaten oder Organisationen zugänglich gemacht werden, die nicht im Interesse der Klagepartei mit diesen Daten umgehen. Die Grenze zieht die Beklagte hier selbst nur darin, dass sie die Daten nicht „verkauft“.
- Bei der Weitergabe von Daten an Strafverfolgungsbehörden (weltweit) gibt die Beklagte diese weiter, wenn „sie in gutem Glauben davon ausgeht, dass dies notwendig ist“, z.B. bei „verdächtigen Aktivitäten“ (Datenschutzrichtlinie, S. 79 ff).

- Ausweislich der Datenschutzrichtlinie der Beklagten (Anlage K 1, S. 67 ff.) behält die Beklagte Daten so lange, wie sie benötigt werden, um die Produkte der Beklagten bereitzustellen, rechtliche Verpflichtungen zu erfüllen oder bestimmte Interessen zu schützen. Dies wird am Beispiel einer Suche auf Facebook erläutert: Der Suchverlauf wird dabei gespeichert, bis der Nutzer ihn löscht, nur die Informationen zum verwendeten Gerät oder einem Standort werden nach sechs Monaten gelöscht. Es ist damit – auch in zeitlicher Hinsicht – von einem erheblichen Kontrollverlust auszugehen. Dem steht der spätere Vortrag der Beklagten nicht entgegen. Zwar hat sie in ihren Stellungnahmen ausgeführt, personenbezogene Daten würden zu Sicherheits- und Integritätszwecken nicht „auf unbestimmte Zeit“ gespeichert, sondern im Regelfall – sofern eine Untersuchung ohne weitere Maßnahmen abgeschlossen werde – nach bis zu 90 Tagen gelöscht; bei fortdauernden oder vertieften Untersuchungen könne eine längere Aufbewahrung erforderlich sein. Diese Angaben bleiben jedoch abstrakt und lassen weder erkennen, welche konkreten Daten der Klagepartei hiervon erfasst sind, noch, nach welchen überprüfbaren Kriterien die Beklagte im Einzelfall über Dauer und Umfang der Speicherung entscheidet. Auch nach diesem Vortrag verbleibt die Entscheidung über Fortbestand, Zweckbindung und Löschung der Daten einseitig bei der Beklagten und entzieht sich der Kenntnis und Kontrolle der betroffenen Person, was den angenommenen Kontrollverlust nicht entkräftet, sondern bestätigt.
- Es ist auch zu berücksichtigen, dass damit die Klageseite die Dauer der Speicherung teilweise mitbeeinflussen könnte, zum einen durch Löschung des Suchverlaufs oder auch Beendigung der Vertragsbeziehung und damit endgültige Löschung ihres Kontos.
- Der Senat ist auf der Grundlage der Anhörung der Klagepartei zu der Überzeugung gelangt, dass das Gefühl der Überwachung keine übermäßige Belastung für die Klagepartei bedeutet. Dafür spricht auch, dass die Klagepartei Instagram weiter nutzt.
- Eine Überzeugung dahingehend, dass die Klagepartei die Möglichkeit hätte, die Kontrolle über ihre Daten – bei Weiternutzung von Instagram - selbständig zurückzuerlangen, hat sich der Senat schon deshalb nicht bilden können, weil die Beklagte die bei ihr von der Klagepartei vorhandenen Daten nicht benannt hat. Der pauschale Hinweis auf die Möglichkeit, bestimmte Einstellungen vorzunehmen oder Aktivitäten zu trennen (vgl. Anlage B7) führt deshalb nicht weiter.
- Bei der Schätzung des Schadens hat der Senat den Grad des Verschuldens ebenso wenig berücksichtigt wie die Tatsache, dass der Klagepartei mit diesem Urteil ein Unterlas-

sungsanspruch zugesprochen wird (BGH a.a.O.; zuletzt EuGH Urt. v. 4.9.2025 – C-655/23, NJW 2025, 3137 Rn. 73 und Rn. 83).

5. Zinsen

Der Zinsanspruch für den Schadensersatzanspruch folgt aus den §§ 291, 288 BGB. Die Klagepartei hat die Beklagte bereits mit Schreiben vom 23.05.2024 (Anlage K 3) bis 13.06.2024 zur Zahlung eines Schmerzensgelds in Höhe von 5.000 € aufgefordert.

6. § 823 Abs. 1 BGB i.V.m. allgemeinem Persönlichkeitsrecht

Ein darüberhinausgehender Zahlungsanspruch wegen Verletzung des allgemeinen Persönlichkeitsrechts der Klagepartei durch die Beklagte nach § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, Art. 2 Abs. 1 GG steht der Klageseite nicht zu.

a. Schutzzumfang

Zwar kann die schuldhafte Verletzung des allgemeinen Persönlichkeitsrechts einen Anspruch auf eine Geldentschädigung begründen, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann (ständige Rechtsprechung des BGH, s. nur BGH v. 12.3.2024 – VI ZR 1370/20, NJW 2024, 2836 Rn. 70). Das allgemeine Persönlichkeitsrecht schützt auch davor, dass nicht in den persönlichen Nahbereich eingedrungen und/oder ein digitales Persönlichkeitsprofil erstellt und weitergegeben wird.

b. Notwendigkeit eines schwerwiegenden Eingriffs

Der Bundesgerichtshof hat den Entschädigungsanspruch im Spannungsfeld von allgemeinem Persönlichkeitsrecht und Pressefreiheit entwickelt, um zu verhindern, dass schwerwiegende Verletzungen der Würde und Ehre eines Menschen durch Presseveröffentlichungen ohne Sanktion bleiben könnten und dass hierdurch der Rechtsschutz der Persönlichkeit verkümmert (BGH Urt. v. 17.12.2013 – VI ZR 211/12, NJW 2014, 2029 Rn. 40 m.w.N.). Entschädigungen wurden demnach in solchen Fällen zugesprochen, in denen eine Person durch Berichte in Printmedien (s. z.B. BGH Urt. v. 5.12.1995 -VI ZR 332/94, NJW 1996, 984 – *Caroline von Monaco*), im Fernsehen (s. z.B. OLG Hamm Urt. v. 4.2.2004 – 3 U 168/03, GRUR 2004, 970 – *Stefan Raab*) oder im Internet (BGH Urt. v. 17.12.2013 – VI ZR 211/12, NJW 2014, 2029 – www.stern.de) öffentlich bloßgestellt wurden. Bei der Bemessung der Höhe der Entschädigung sollen die „Bedeutung und Tragweite des Eingriffs, also das Ausmaß der Verbreitung der Veröffentlichung, die Nachhaltigkeit und Fortdauer der Interessen- oder Rufschädigung des Verletzten, ferner Anlass und Beweggrund des Handelnden sowie der Grad seines Verschuldens“ berücksichtigt werden (BGH a.a.O.,

Rn. 38).

c. Keine schwerwiegende Verletzung im konkreten Fall belegt

Der vorliegende Fall ist insofern anders gelagert, als mit der informationellen Selbstbestimmung ein anderer (Teil-) Gehalt des allgemeinen Persönlichkeitsrechts betroffen ist. Hier geht es um alltägliche Handlungen, ein Bewegen im virtuellen Raum des Internets. Der Senat geht zwar davon aus, dass auch die Verletzung des Rechts auf informationelle Selbstbestimmung einen Entschädigungsanspruch im o.g. Sinne begründen kann (so wohl auch BGH 12.3.2024 – VI ZR 1370/20, NJW 2024, 2836 Rn. 71). Auch insoweit müsste aber ein schwerwiegender Eingriff in das allgemeine Persönlichkeitsrecht nachgewiesen sein und die Beeinträchtigung dürfte nicht in anderer Weise aufgefangen werden können.

Für den Senat liegt auf der Hand, dass ein „schwerwiegender Eingriff“ im Sinne der Rechtsprechung des Bundesgerichtshofes von der Klagepartei nicht vorgetragen wurde. Entscheidend ist dabei, dass eine Verletzung der Klagepartei im Kernbereich der Persönlichkeit nicht dargelegt ist und sie damit nicht auf diese Weise betroffen ist bzw. dass sie betreffende Daten nicht in die allgemeine Öffentlichkeit gelangt sind oder ein digitales Persönlichkeitsprofil an Dritte gelangt ist. Hierzu bleibt der Vortrag der Klagepartei zu allgemein und unkonkret. Der Umfang der Datenverarbeitung allein (insb. Menge/Art der Daten; Dauer/Zweck der Verarbeitung; s.o.) und die Tatsache, dass von einem vorsätzlichen Verhalten auszugehen ist, begründen die notwendige besondere Schwere des Eingriffs in den Kernbereich des Allgemeinen Persönlichkeitsrechts nicht. Anders als für das Bestreiten der Beklagten in Bezug auf die Datenschutzverletzung kann hier – im Gefüge des § 823 Abs. 1 BGB das bloße allgemeine Behaupten eines Eingriffs nicht genügen. Die von der Klagepartei zitierte, § 100a StPO betreffende Entscheidung des Bundesverfassungsgerichts bestätigt diesen Befund: Das Verfassungsgericht hält fest, dass Akte höchstvertraulicher - und damit den Kernbereich des Persönlichkeitsrechts betreffender – Kommunikation nur einen kleinen Teil der Internetnutzung ausmachen (vgl. BVerfG Urteil v. 6.7.2016 – 2 BvR 1454/13, NJW 2016, 3508). Selbst wenn man deshalb einen ‘quantitativ’ erheblichen Eingriff in das Recht der Klagepartei auf informationelle Selbstbestimmung als bewiesen ansähe, läge die Annahme eines (qualitativ) schwerwiegenden Eingriffs in die Würde und Ehre der Klagepartei fern.

Es kommt hinzu, dass Art. 82 DSGVO für Eingriffe in das Recht auf informationelle Selbstbestimmung einen Schadensersatzanspruch bereithält. Durch die ihr zugesprochene Entschädigung für den von ihr erlittenen Kontrollverlust und durch das an die Beklagte gerichtete Verbot wird die von der Klagepartei erlittene Beeinträchtigung befriedigend aufgefangen.

II. **Löschung**

Die Klagepartei kann aus Art. 17 Abs. 1 lit. d), 12 Abs. 3 DSGVO weiterhin eine Löschung der von ihr hinreichend bestimmt bezeichneten personenbezogenen Daten und die Mitteilung hierüber verlangen.

III. **Auskunft**

Der Klagepartei steht der geltend gemachte Anspruch aus Art. 15 Abs. 1 DSGVO im tenorierten Umfang zu. Art. 15 Abs. 1 DSGVO ist als zentrales Instrument der Transparenz und Kontrolle ausgestaltet und dient der effektiven Wahrnehmung der weiteren Betroffenenrechte nach der DSGVO (EuGH Urt. v. 12.1.2023 – C-154/21 [RW/Österreichische Post AG] Rn. 42). Bei der Auslegung von Art. 15 DSGVO ist zu beachten, dass die Verordnung darauf abzielt, innerhalb der Union ein hohes Datenschutzniveau für natürliche Personen zu gewährleisten (EuGH a.a.O., Rn. 44). Verarbeitung personenbezogener Daten

Die Beklagte verarbeitet personenbezogene Daten der Klagepartei im Sinne von Art. 4 Nr. 1 und Nr. 2 DSGVO.

1. Anspruch aus Art. 15 Abs. 1 DSGVO

Ein Anspruch der Klagepartei auf Auskunft ist im Hinblick auf solche personenbezogenen Daten entstanden, die von der Beklagten verarbeitet werden, Art. 15 Abs. 1 S. 1 DSGVO. Art. 15 Abs. 1 DSGVO verleiht der betroffenen Person ein umfassendes Recht auf Auskunft über sämtliche sie betreffenden personenbezogenen Daten, die von dem Verantwortlichen verarbeitet werden, sowie über die in Art. 15 Abs. 1 lit. a) bis h) DSGVO genannten zusätzlichen Informationen.

Die Beklagte muss diese Daten benennen (S. 1) sowie – entsprechend dem klägerischen Begehren – Informationen erteilen zu:

- den jeweiligen Verarbeitungszwecken (lit. a),
- den Empfängern (s. Art. 4 Nr. 9 DSGVO) oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen (lit. c),
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten (lit. g) sowie

- dem Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Bezogen auf die Information zu den Empfängern hat der EuGH (Urteil vom 12.1.2023 – C-154/21 = NJW 2023, 973) klargestellt: *„Art. 15 I DSGVO ist dahin auszulegen, dass das in dieser Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 V VO (EU) 2016/679 sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen“.*

2. Grenzen des Anspruchs

Der Anspruch der Klagepartei erfasst nach richtiger Ansicht nur solche Daten, die im Zeitpunkt des Auskunftsbegehrens tatsächlich noch vorhanden sind (so zutreffend BeckOK DatenschutzR/Schmidt-Wudy, 54. Ed. 1.11.2025, DS-GVO Art. 15 Rn. 52.2). Das von der DSGVO angestrebte hohe Datenschutzniveau darf nicht zu dem absurden Ergebnis führen, dass Daten alleine zum Zwecke eines potentiellen späteren Auskunftsbegehrens aufbewahrt und damit weiter verarbeitet werden.

Ein Anspruch der Klagepartei aus Art. 15 Abs. 1 lit. c) DSGVO besteht auch nicht, soweit diese Informationen zum Zeitpunkt einer Offenlegung personenbezogener Daten gegenüber Empfängern i.S.v. Art. 4 Nr. 9 DSGVO begehrt.

Die Beklagte muss auch keine Auskunft zu der Frage erteilen, ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat. Ein solcher Anspruch folgt weder aus Art. 15 Abs. 1 lit c) DSGVO, der nur die Weitergabe von Daten an Personen oder Stellen außerhalb des Verantwortlichen meint (Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 9 Rn. 6), noch aus Art. 15 Abs. 2 DSGVO, nach dem nur über die Garantien i.S.v. Art. 46 DSGVO zu unterrichten ist.

3. Erfüllung des Anspruchs

Den Anspruch auf Informationen über das Bestehen einer automatisierten Entscheidungsfindung im Sinne von Art. 15 Abs. S. 2 lit. h) DSGVO hat die Beklagte in ihrem Schreiben (Anlage B8) erfüllt, indem sie eine Negativauskunft erteilt hat. Damit hat die Beklagte ihrer Auskunftspflicht genügt.

Im Übrigen ist keine Erfüllung eingetreten. Richtig ist zwar, dass nach ständiger Rechtsprechung des Bundesgerichtshofes ein Anspruch auf Auskunft erfüllt ist, wenn die Angaben nach dem – ggf. konkludent – erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen (BGH Urt. v. 3.9.2020 – III ZR 136/18 = NJW 2021, 765). Dem Schreiben der Beklagten (Anlage B 8) lässt sich ein solcher Wille nicht ausdrücklich entnehmen (*„wir schreiben Ihnen [...] im Zusammenhang mit dem Auskunftsverlangen Ihrer Mandantschaft“*). Obwohl die Beklagte sich zu dem Auskunftsbegehren der Klagepartei äußert, lässt sich der Wille zu einer Auskunft im geschuldeten Gesamtumfang auch nicht aus den Umständen entnehmen. Im Gegenteil: Indem die Beklagte das Auskunftsverlangen der Klagepartei objektiv sinnverstellend in ihrem Sinne uminterpretiert (*„Meta versteht das Auskunftsverlangen Ihrer Mandantschaft wie folgt“*), verkürzt sie bewusst den Gegenstand der Auskunft. Es kommt hinzu, dass die Beklagte lediglich eine *„Zusammenfassung der mit [den] Konten verknüpften Informationen“* anbietet und eben nicht – wie geschuldet – die Informationen als solche.

Zwar hat die Beklagte mit der Anlage B 8 Informationen für die Klägerin bereitgestellt, die diese befähigen sollen, sich ihrerseits Informationen über die bei der Beklagten über die Klägerin vorhandenen Daten zu erschließen. Auch über dieses ‚Selbsthilfetool‘ wird aber nur eine Zusammenfassung der verarbeiteten Informationen (Anlage 8, S. 3) bzw. der Aktivitäten (a.a.O., S. 4) zur Verfügung gestellt, nicht hingegen eine Auflistung aller personenbezogenen Daten samt der korrespondierenden Metainformationen, wie nach Art. 15 Abs. 1 DSGVO geboten. Auch die allgemein gehaltenen Informationen zu den Kategorien von Empfängern greift nach der im Zeitpunkt des Schreibens bekannten Rechtsprechung des EuGH (s.o., Urteil vom 12.1.2023 – C-154/21 = NJW 2023, 973) zu kurz. Und außerdem soll gelten (Anlage B 8, S. 8): *„Einige Informationen, die du gelöscht hast, werden eventuell aus Sicherheitsgründen vorübergehend gespeichert. Sie erscheinen aber nicht, wenn du auf deine Informationen zugreifst oder sie herunterlädst“*.

Der Auskunftsanspruch der Klagepartei ist damit nicht erfüllt. Etwas anderes konnte die insoweit

beweisbelastete Beklagte jedenfalls nicht nachweisen.

4. Die Beklagte ist Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO (vgl. oben).

IV. Vorgerichtliche Rechtsanwaltskosten

Ein Anspruch auf Freistellung von vorgerichtlichen Anwaltskosten in der tenorierten Höhe beruht auf Art. 82 Abs. 1 DSGVO. Der Senat vermag nicht davon auszugehen, dass das durch Anlage K3 hinreichend dokumentierte außergerichtliche Vorgehen im Zeitpunkt April 2024 ausnahmsweise unzweckmäßig gewesen sein soll.

Der Senat hat einen Gegenstandswert von 1.750 € zugrunde gelegt (Schadensersatz 750 €; Löschung 500,- €; Auskunft 500 €) und die erstattungsfähige 1,3 Geschäftsgebühr nebst Auslagen und MwSt in Höhe 280,60 € errechnet.

E.

Der im Termin zur mündlichen Verhandlung vor dem Senat gestellte Antrag der Beklagten auf Gewährung einer über die bereits gewährte Stellungnahmefrist hinausgehende Schriftsatzfrist war abzulehnen.

Zwar hat der Senat im Termin darauf hingewiesen, dass ein Vortrag zu Rechtfertigungsgründen sich auf konkrete, der Klagepartei zuzuordnende Daten beziehen müsse, und der Beklagten Gelegenheit gegeben, bis zum 21.01.2026 mitzuteilen, ob sie bereit sei, entsprechende Offsite-Daten zu benennen und hierfür Rechtsgrundlagen nach Art. 6 DSGVO darzulegen. Die hierauf erfolgte Stellungnahme der Beklagten vom 21.01.2026 enthält jedoch keinen entscheidungserheblichen neuen Tatsachenvortrag, sondern erschöpft sich in der Wiederholung und Vertiefung der bereits zuvor vertretenen Rechtsauffassung, wonach eine konkrete Benennung einzelner Daten mangels hinreichender Substantiierung des klägerischen Vortrags nicht geschuldet sei und eine entsprechende Verpflichtung unzulässigerweise eine sekundäre Darlegungslast begründen würde.

Eine Schriftsatzfrist nach § 283 ZPO war schon mangels klägerischen neuen oder überraschenden Tatsachenvortrag nicht erforderlich. Ebenso bestand kein Anlass zur Einräumung einer Schriftsatzfrist aus Gründen der Prozessleitung gemäß § 139 ZPO. Der Hinweis des Senats griff

keine neuen rechtlichen Gesichtspunkte auf, sondern knüpfte an den bereits zuvor zwischen den Parteien streitigen Umfangs der Darlegungslast der Klagepartei bzw. einer etwaigen sekundären Darlegungslast hinsichtlich konkreter Datenverarbeitungsvorgänge an. Die Beklagte hatte hierzu bereits umfassend schriftsätzlich vorgetragen und war nicht gehindert, ihren Standpunkt im Termin und in der gewährten Frist zur Stellungnahme, ob sie gewillt ist nun zu den bei ihr gespeicherten Daten darzulegen.

Da der Sach- und Streitstand mit der Stellungnahme der Beklagten vom 21.01.2026 damit entscheidungsreif war und weiterer Vortrag der Parteien keine neuen Erkenntnisse erwarten lässt, war der Antrag auf Gewährung einer Schriftsatzfrist abzulehnen

F.

I. Kosten

Die Entscheidung über die Kosten des Rechtsstreits beruht auf den §§ 92 Abs. 1 S. 1 ZPO. Der Senat hat die Berufungsanträge wie folgt bewertet:

- Schadensersatz: 1.500 €
- Auskunft: 500 €
- Löschung: 500 €

Die Klagepartei unterliegt damit mit 750 € von 2.500 € (=30%).

II. Vorl. Vollstreckbarkeit

Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf §§ 708 Nr. 10, 711 ZPO.

III. Revisionszulassung

Der Senat lässt die Revision zu, da die Sache grundsätzliche Bedeutung im Sinne von § 543 ZPO hat. Dies ist dann anzunehmen, wenn die Sache entscheidungserhebliche, klärungsbedürftige und klärungsfähige Rechtsfragen aufwirft, die sich über den Einzelfall hinaus in einer unbestimmten Vielzahl von Fällen stellen können und deshalb für die Allgemeinheit von besonderer Bedeutung sind, oder wenn andere (tatsächliche oder wirtschaftliche) Auswirkungen des Rechtsstreits auf die Allgemeinheit deren Interessen in besonderem Maße berühren. Die der vorliegenden Entscheidung zugrundeliegenden Rechtsfragen zur Darlegungslast der Klageseite, Beibrin-

gungslast der Beklagten im Rahmen eines Schadensersatzanspruchs nach Art. 82 DSGVO sind bisher vom BGH noch nicht entschieden. Es ist allgemein bekannt, dass schon jetzt eine hohe fünfstellige Zahl vergleichbarer Verfahren geführt wird. Die wirtschaftliche Bedeutung für die Beklagte (und andere Anbieter vergleichbarer Dienstleistungen) liegt vor diesem Hintergrund auf der Hand.

gez.



Vorsitzende Richterin
am Oberlandesgericht



Richterin
am Oberlandesgericht



Richter
am Oberlandesgericht