Beglaubigte Abschrift

Landgericht München I

Az.: 13 O 76/25

IM NAMEN DES VOLKES

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **BK Verbraucherschutz Rechtsanwaltsgesellschaft mbH**, Viktoria-Luise-Platz 7, 10777 Berlin, Gz.: BKD-012182-24

gegen

Meta Platforms Ireland Ltd., vertreten durch d. Geschäftsführer Yvonne Cunnane, Anne O'Leary, Genevieve Hughes, Majella Mungovan, David Harris, Merrion Road, D04 X2K5, Dublin 4, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte [redacted]

wegen Forderung

erlässt das Landgericht München I - 13. Zivilkammer - durch die Richterin am Landgericht [redacted] als Einzelrichterin aufgrund der mündlichen Verhandlung vom 06.02.2026 folgendes

Endurteil

I. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps außerhalb der Netzwerke der Beklagten die nachfolgend aufgeführten personenbezogene Daten der Klagepartei mithilfe der Meta Business Tools zu erheben,

an die Server der Beklagten weiterzugeben, die Daten dort zu speichern und anschließend zu verwenden:

a) über die Business-Tools der Beklagten zur Identifizierung des Klägers übermittelt:

- E-Mail des Klägers in gehashter Form
- Telefonnummer des Klägers in gehashter Form
- Vorname des Klägers in gehashter Form
- Nachname des Klägers in gehashter Form
- Geburtsdatum des Klägers in gehashter Form
- Geschlecht des Klägers in gehashter Form
- Ort des Klägers in gehashter Form
- Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID" genannt) in gehashter oder ungehashter Form
- 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
- Seiten-ID
- Seitenspezifische Nutzungs-ID
- Click-to-WhatsApp(Ad)-ID
- Click-to-Instagram-ID

b) sowie folgende personenbezogene Daten der Klagepartei 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 jewei-

ligen Webseite dokumentieren

c) sowie 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

II. Die Beklagte wird verurteilt, an den Kläger 5.000,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 02.04.2024 zu zahlen.

III. Die Beklagte wird verurteilt den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von 627,13 € freizustellen.

IV. Im Übrigen wird die Klage abgewiesen.

V. Von den Kosten des Rechtsstreits haben der Kläger 25% und die Beklagte 75% zu tragen.

VI. Das Urteil ist vorläufig vollstreckbar, für den Kläger jedoch nur gegen Sicherheitsleistung in Höhe von 110 % des zu vollstreckenden Betrags. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

VII. Der Streitwert wird auf 8.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten über Auskunfts-, Löschungs-, Unterlassungs- und Zahlungsansprüche aufgrund der von der Klägerseite behaupteten Verletzungen datenschutzrechtlicher Vorschriften durch die Beklagte.

Die Klagepartei nutzt ausschließlich privat das Netzwerk „Facebook" unter der E-Mail-Adresse [redacted] seit dem 01.11.2011. Betreiberin des Netzwerks ist die Beklagte.

Um ein Konto auf zu erstellen und zu nutzen, muss ein zukünftiger Nutzer den Nutzungsbedingungen von „Facebook“ zustimmen (vgl. Anlage B1).

Die Nutzung der Plattform ist kostenfrei. Allerdings wird den Nutzern Werbung angezeigt, die auf den Interessen des jeweiligen Nutzers basiert. Dafür nutzt und verarbeitet die Beklagte verschiedene Daten, die sie in ihrer Datenschutzrichtlinie (vgl. Anlage K3) aufführt und auf die sie bei der Registrierung ebenso hinweist wie auf die Cookie-Richtlinie. Zu diesen Daten gehören

- neben den persönlichen Informationen, die der Nutzer bei der Registrierung angibt,
- das Nutzungsverhalten des jeweiligen Nutzers in Produkten der Beklagten (sog. Onsite-Daten),
- Informationen über Freunde und Follower des Nutzers
- und deren Nutzungsverhalten in Produkten der Beklagten sowie
- Informationen über die technischen Geräte, mit Hilfe derer der Kunde die Produkte der Beklagten nutzt.

Zudem sammelt die Beklagte Informationen von Partnern über Handlungen, die seitens des Nutzers sowohl innerhalb als auch außerhalb der Produkte der Beklagten durchgeführt werden. Dazu können z. B. andere besuchte Websites, verwendete Apps oder gespielte Online-Spiele gehören. Unter „Partnern“ versteht die Beklagte „Personen, Unternehmen, Organisationen oder Einrichtungen, die unsere Produkte nutzen oder integrieren, um ihre Produkte und Dienstleistungen zu bewerben, zu vertreiben oder zu unterstützen“ (vgl. Anlage K3).

Um diese sog. Offsite-Daten erheben zu können, hat die Beklagte sogenannte „Meta-Business-Tools“ entwickelt (vgl. Anlage B4). Die Meta-Business-Tools dienen dazu, dass bei Drittanbietern entstandene personenbezogene Informationen an die Beklagte übersandt werden. Dazu zählen u. a. der sog. „Meta-Pixel“ und die „Conversions API“. Meta-Pixel wird in Form eines Programmcodes im Hintergrund des Browsers ausgeführt. Die Conversions API ist ein Meta-Business-Tool, das Marketingdaten direkt vom Server des Gewerbetreibenden an die Meta-Systeme übermittelt, die Werbeanzeigen ausliefern, sodass die Targeting-Methode nicht ausschließlich von Cookies oder browserbasierten Technologien abhängig ist (vgl. Anlage K6). Die Beklagte empfiehlt den Nutzern ihrer Meta-Business-Tools, diese in Kombination zu verwenden (vgl. Anlage K6). Zu den personenbezogenen Informationen, die mithilfe der Meta-Business-Tools erfasst werden, gehören zum einen Kontaktinformationen, mit denen Einzelpersonen identifiziert werden

können, wie Namen, E-Mail-Adressen und Telefonnummern, und zum anderen sog. „Event-Daten“, d. h. sonstige Informationen, die über Personen und ihre Handlungen geteilt werden, die sie auf den Webseiten der Gewerbetreibenden und in deren Apps oder Shops vornehmen (vgl. Anlage B4). Für die Nutzung der Meta-Business-Tools hat die Beklagte Nutzungsbedingungen mit den Drittanbietern vereinbart (vgl. Anlage B4). Nach Ziffer 3.d. der Nutzungsbedingungen ist der Nutzer der Meta-Business-Tools verpflichtet sicherzustellen, dass der Endnutzer alle erforderlichen Einwilligungen erteilt. Eine Kontrolle durch die Beklagte sehen die Nutzungsbedingungen nicht vor. Die Beklagte und der Drittanbieter sind ausweislich Ziffer 5.a.ii. der Nutzungsbedingungen gemeinsam Verantwortliche gemäß Art. 26 DSGVO für die Erhebung personenbezogener Informationen über die Meta-Business-Tools und ihre anschließende Übermittlung an die Beklagte.

Besucht ein Nutzer eine mit einem solchen Tool präparierte Webseite oder App, erhebt und erfasst das Meta-Business-Tool Informationen zum Gerät des Nutzers und die Tätigkeiten des Nutzers auf der Webseite oder in der App. Dies kann der Nutzer auch nicht mit Datenschutzeinstellungen auf der Plattform der Beklagten verhindern. Er kann aber Einfluss darauf nehmen, wie die Beklagte die so in ihren Machtbereich gelangten Daten weiter nutzt. Im Rahmen der Nutzung des Netzwerks Facebook nimmt die Beklagte nämlich auf Folgendes Bezug:

- Bei der Einrichtung des Netzwerks muss der Nutzer den Nutzungsbedingungen zustimmen.

- Im Rahmen der Registrierung verweist die Beklagte den Nutzer auf die Datenschutzrichtlinie (vgl. Anlage K3) sowie auf die Cookie-Richtlinie. Aus der Datenschutzrichtlinie ergibt sich insbesondere, dass diese alle vom Nutzer bereitgestellten Informationen und Geräteinformationen erfasst sowie alle benutzten Meta-Produkte, einschließlich der über die Meta-Business-Tools übersandten Informationen der Drittunternehmen, und diese miteinander verbunden werden. So heißt es etwa:

  > „Partner teilen auch Informationen wie deine E-Mail-Adresse, Cookies und deine Geräte-ID für Werbezwecke mit uns. [...] Wir erhalten diese Informationen unabhängig davon, ob du bei unseren Produkten angemeldet bist bzw. ein Konto auf ihnen hast oder nicht. [...] Partner geben außerdem ihre Kommunikation mit dir an uns weiter, wenn sie uns anweisen, Dienstleistungen für ihr Unternehmen zu erbringen, wie Unterstützung bei der Verwaltung ihrer Kommunikation. [...] Partner nutzen unsere Business-Tools, Integrationen und Meta Audience Network-Technologien, um Informationen mit uns zu teilen. Diese Partner erheben deine Informationen, wenn du ihre Website oder App besuchst oder ihre Dienste nutzt, [...]“.

Sodann hat der Nutzer auf der Plattform der Beklagten die Möglichkeit, folgende Einstellungen zu treffen:

- Deaktivierung bzw. Verwendung optionaler Cookies;
- Informationen von Werbepartnern zu Aktivitäten verwenden/nicht verwenden, um Werbung anzuzeigen.

Dies bedeutet, der Nutzer kann zwar durch die Einstellungen auf der Plattform verhindern, dass die an die Beklagte übermittelten Daten für personalisierte Werbung verwendet werden. Er kann aber nicht verhindern, dass die Beklagte die über Dritte generierten Daten überhaupt erhält.

Die von der Beklagten angebotenen und vertriebenen Meta-Business-Tools laufen auf mannigfachen, reichweitenstarken Webseiten und Apps in Deutschland im Hintergrund. Hierzu gehören (vgl. Anlage K5)

- zahlreiche große Nachrichtenseiten und -Apps (z. B. spiegel.de, bild.de, faz.net, stern.de),
- die großen Reiseseiten und -Apps (z. B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de)
- Seiten und Apps, die medizinische Hilfe bieten (z. B. apotheken.de, shopapotheke.de, docmorris.de, aerzte.de, jameda.de),
- Dating- und Erotikseiten (z. B. parship.de, amorelie.de, orion.de, lovescout24.de),
- aber auch Seiten mit Inhalten aus der innersten Intimsphäre (z. B. krebshilfe.de, tfpfertility.com, niewieder-alkohol.de, nvve.nl).

Der Kläger hat der Option „Meta Cookies in anderen Apps und auf anderen Websites“ nicht zugestimmt sowie in die Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ nicht eingewilligt. Seit Oktober 2025 hat der Kläger die Einstellung „weniger stark personalisierte Werbung“ im Angebot der Beklagten eingestellt.

Mit Schreiben vom 04.03.2024 forderte der Klägervertreter von der Beklagten u.a. eine Unterlassungserklärung (vgl. Anlage K7). Mit Schreiben vom 16.07.2025 (vgl. Anlage B7) nahm die Beklagte zum Auskunftsverlangen der Klagepartei im hiesigen Verfahren Stellung.

Die Klagepartei behauptet, auf zahlreichen reichweitenstarken Webseiten und Apps in Deutschland laufe „Meta Pixel“ im Hintergrund. Hierzu würden zahlreiche große Nachrichtenseiten und -Apps, die großen Reiseseiten und -Apps, Seiten und Apps, die medizinische Hilfe bieten, Dating-

und Erotikseiten, aber auch Seiten mit Inhalten aus der innersten Intimsphäre laufen. Die Beklagte zeichne über die Business-Tools das Nutzerverhalten jedes Nutzers auf. Hinsichtlich der technischen Einzelheiten wird auf die Ausführungen in Abschnitt D. der Klageschrift Bezug genommen.

Auch die Klagepartei selbst nutze regelmäßig zahlreiche Webseiten und Apps, auf denen Meta Business Tools vorzufinden seien und mit deren Hilfe sensible Daten der Klägerin i. S. v. Art. 9 Abs. 1 DSGVO verarbeitet würden.

Die Klagepartei ist der Meinung, durch die Einbindung der Meta-Business-Tools auf den Webseiten und in den Apps von Drittanbietern werde die Beklagte alleinige „Verantwortliche" i. S. v. Art. 28 DSGVO für sämtliche Webseiten und Apps, auf denen der Code der Beklagten laufe. Eine „Auslagerung" dieser Verantwortung an die Webseitenbetreiber, die die entsprechenden Einwilligungen einholen sollen, sei nicht möglich.

Die Verarbeitung von Daten, die der Beklagten von Drittanbietern zur Verfügung gestellt würden, sei rechtswidrig. Eine wirksame Einwilligung i. S. v. Art. 6 DSGVO liege nicht vor. Die Tatbestandsvoraussetzungen sämtlicher neben der Einwilligung in der DSGVO enthaltenen Rechtfertigungsgründe seien nicht erfüllt.

Die Klagepartei ist der Auffassung, ihr stünde ein Anspruch aus § 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1, Art. 1 GG zu. Das Recht auf informationelle Selbstbestimmung der Klagepartei sei verletzt.

Die bei der Klagepartei entstandene Ungewissheit, in welchem Ausmaß sie nun aktuell von der Beklagten überwacht werde oder nicht, inwieweit ein Persönlichkeitsprofil von ihr erstellt und inwieweit ein solches auch zur Verhaltenssteuerung eingesetzt werde, stelle eine kausal auf der Geschäftspraxis der Beklagten beruhende Rechtsverletzung dar. Wer nicht ausmachen könne, welche ihn betreffenden Informationen anderen bekannt sind, sei bereits einem schwerwiegenden Eingriff in seine informationelle Selbstbestimmung ausgesetzt.

Hilfsweise stützt die Klagepartei ihren Anspruch auf Art. 82 DSGVO.

Die Klagepartei ist der Auffassung, dass die Beklagte verpflichtet sei, der Klägerin mitzuteilen, auf welchen Webseiten und Apps die Beklagte die personenbezogenen Daten der Klägerin erfasst hat und wie sie diese verarbeitet hat. Solange sie sich einer Auskunft verweigere, läge eine Umkehr der Beweislast vor.

Die Klagepartei beantragt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1, Abs. 3 Satz 1 DSGVO zu erteilen, welche personenbezogenen Daten des Klägers seit dem 25.05.2018

   - durch die Software-Tools „Meta Business Tools“ erfasst wurden,
   - nach Erfassung an die Server der Beklagten weitergeleitet wurden,
   - dort gespeichert und anschließend verwendet wurden,

   und weiterhin im Zusammenhang mit den so beauskunfteten Daten Auskunft zu jedem Datum gem. Art. 15 Abs. 1 lit. a., c., g. und h. DSGVO darüber zu erteilen,

   - zu welchen Zwecken die Daten verarbeitet wurden,
   - welchen Empfängern oder Kategorien von Empfängern die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
   - welche Herkunft die Daten haben,
   - inwieweit die Daten des Klägers für eine automatisierte 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, die Daten gem. dem Antrag zu 1. nach Auskunftserteilung zu löschen.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers mit Hilfe der Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden.

4. Die Beklagte wird verurteilt, an den Kläger eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 02.04.2024, zu zahlen.

5. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten i. H. v. 1.295,43 Euro freizustellen.

Zur Konkretisierung des Unterlassungsantrags zu 3. teilt die Klagepartei mit, dass sich die personenbezogenen Daten, die – von dem Kläger unbemerkt – über die Meta Business Tools erfasst, an die Server der Beklagten weitergeleitet und anschließend von der Beklagten gespeichert und verwendet werden, ausweislich der von der Beklagten angewandten technischen Kategorisierung wie folgt konkretisieren lassen. Zur Identifizierung des Klägers können über die Business-Tools übermittelt werden:

- E-Mail des Klägers in gehashter Form
- Telefonnummer des Klägers in gehashter Form
- Vorname des Klägers in gehashter Form
- Nachname des Klägers in gehashter Form
- Geburtsdatum des Klägers in gehashter Form
- Geschlecht des Klägers in gehashter Form
- Ort des Klägers in gehashter Form
- Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID" genannt) in gehashter oder ungehashter Form
- 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
- Seiten-ID

- Seitenspezifische Nutzungs-ID
- Click-to-WhatsApp(Ad)-ID
- Click-to-Instagram-ID

Zur Nachverfolgung der Aktivitäten des Klägers können über die Business Tools erfasst werden:

- 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
- 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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, dass zahlreiche andere Unternehmen ähnliche Tools anböten. Die Anzahl der Webseiten Dritter, die die streitgegenständlichen Business-Tools nutzen, stelle lediglich einen Bruchteil des gesamten Internets dar.

Die Beklagte behauptet, die Meta-Business-Tools hätten lediglich den Zweck, dass Drittunterneh-

men ihre Produkte und Dienstleistungen effektiver bewerben könnten. Drittunternehmen würden keine personenbezogenen Daten i. S. v. Art. 9 DSGVO übermitteln. Eine Übermittlung sei Drittunternehmen entsprechend den Nutzungsbedingungen für die Business-Tools verboten. Hinsichtlich der Einzelheiten wird auf die Anlagen B4 und B5 Bezug genommen. Eine Nutzung der Tools sei nur in Übereinstimmung mit geltenden Gesetzen, Verordnungen und Branchenrichtlinien zugelassen. Im Übrigen seien die Systeme der Beklagten dahingehend ausgestaltet, die als potenziell unzulässig erkannten Informationen herauszufiltern. Die Klagepartei habe eine Übermittlung personenbezogener Daten i. S. d. Art. 9 DSGVO auch nicht substantiiert dargelegt.

Die Beklagte ist der Meinung, sie stelle Drittunternehmen die Nutzung der streitgegenständlichen Business-Tools lediglich zur Verfügung. Die Drittunternehmen seien für die Erhebung der Daten, Offenlegung der Erhebung der Daten und Übermittlung der Daten an die Beklagte verantwortlich. Das Verhalten der Drittunternehmen sei der Beklagten nicht zurechenbar.

Darüber hinaus könne jeder Nutzer im Hilfebereich der Beklagten seine Informationen über Aktivitäten außerhalb der Plattform herunterladen.

Die Klage sei im Übrigen unsubstantiiert. Es werde weder angeführt, welche Daten die Beklagte unzulässigerweise verarbeitet habe noch welche Webseiten die Klägerin besucht habe, auf denen eine unzulässige Datenerhebung erfolgt sei. Dies gelte insbesondere hinsichtlich der Behauptung, die Beklagte verstoße gegen Art. 9 DSGVO.

Ein Unterlassungsanspruch könne weder auf Art. 17 DSGVO noch Art. 18 DSGVO gestützt werden.

Ein Schadensersatzanspruch aus Art. 82 DSGVO stehe dem Kläger schon mangels Verstoßes gegen Vorschriften der DSGVO nicht zu. Im Übrigen fehle es auch an einem tatsächlich eingetretenen Schaden.

Die Klagepartei könne nicht mit demselben Antrag zugleich Geldentschädigung nach nationalem Recht und nach Art. 82 DSGVO geltend machen. Im Übrigen lägen die Voraussetzungen für eine Geldentschädigung wegen einer Verletzung des Persönlichkeitsrechts nicht vor.

Wegen der weiteren Einzelheiten des Vorbringens der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 06.02.2026 verwiesen.

Entscheidungsgründe

Die teilweise zulässige Klage ist im tenorierten Umfang begründet.

Das Landgericht München I ist international zuständig. Die internationale Zuständigkeit folgt aus Art. 17 Abs. 1 lit. c, 18 Abs. 1 Alt. 2 der Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12.12.2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (Brüssel Ia-VO).

I.

Der Klageantrag unter Ziffer 2. hinsichtlich der Löschung der Daten ist nicht hinreichend bestimmt i. S. d. § 253 Abs. 2 Nr. 2 ZPO und demnach unzulässig.

Die Beklagtenpartei hat mit Schreiben vom 16.07.2025 (vgl. Anlage B7) bereits Auskunft erteilt, sodass die Klagepartei genau darlegen könnte, welche bei der Beklagten gespeicherten Daten gelöscht werden sollen. Die Klagepartei hätte hierzu über das Selbstbedienungstool die Auskunft erholen können und dann konkret die Löschung genau dieser Daten beantragen können. Dies hat die Klagepartei trotz Hinweis der Beklagten auf die fehlende Bestimmtheit nicht getan.

Im Übrigen ist die Klage zulässig. Insbesondere ist der Antrag unter Ziffer 4. zulässigerweise in das Ermessen des Gerichts gestellt.

II.

Der Klagepartei steht kein Anspruch auf die mit Antrag unter Ziffer 1. begehrte Auskunft nach Art. 15 Abs. 1 DSGVO zu.

1.

Entgegen den Ausführungen der Klagepartei begehrt die Klagepartei mit dem Auskunftsantrag keine Auskunft darüber, auf welchen Webseiten Meta-Business-Tools implementiert sind. Dies kann das Gericht nicht aus dem Klageantrag nicht erkennen. Vielmehr begehrt die Klagepartei Auskunft über die Erfassung und Verarbeitung der Daten der Klagepartei.

2.

Diesen Auskunftsanspruch hat die Beklagte erfüllt.

Erfüllt i. S. d. § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist.

Die Beklagte hat nach ihrem erklärten Willen (vgl. Anlage B7) vollständig Auskunft erteilt. Die Beklagte hat in diesem Schreiben in zulässiger Weise auf ihr Self-Service-Tool verwiesen. Wie die Klagepartei hierüber an die begehrte Information kommt, ist in dem Schreiben ausführlich dargelegt. Eine Auskunftserteilung über ein elektronisches Auskunftssystem ist ausweislich Erwägungsgrund 63 zur DSGVO eine zulässige Art und Weise der Erteilung der Auskunft nach Art. 15 DSGVO (so auch Bäcker, in: Kühling/Buchner, DS-GVO / BDSG, 4. Aufl. 2024, Art. 15 DSGVO, Rn. 31). So heißt es in Erwägungsgrund 63 zur DSGVO: „Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde“. Damit hat der europäische Gesetzgeber die Möglichkeit eines Selbstbedienungstools gerade vorgesehen (vgl. auch LG Stuttgart, Urteil vom 24.10.2024 – 12 O 170/23).

Darüber hinaus hat die Beklagte dargelegt, für welche Zwecke sie die Nutzerdaten verarbeitet. Zusätzlich hat die Beklagte in Anhang 1 zum Schreiben vom 27.08.2025 (vgl. Anlage B7) Auskunft erteilt, an welche Unternehmen die personenbezogenen Daten der Klagepartei wann weitergeleitet wurden.

In den Schriftsätzen vom 27.08.2025 und 09.01.2026 wurde seitens der Beklagten schließlich ausdrücklich erklärt, dass sie ihre Erklärung für vollständig hält.

III.

1.

Der Unterlassungsantrag der Klagepartei ist zulässig und in dem von der Klagepartei konkretisierten Umfang, wie tenoriert, begründet.

a) Gegenüber der Zulässigkeit des Antrags bestehen keine Bedenken.

Nicht zu überzeugen vermag das Gericht insbesondere das Argument, es handele sich bei dem

gestellten Unterlassungsantrag letztlich um einen verkappten Leistungsantrag, da der eigentliche Schwerpunkt der Forderung der Klageseite darin liege, eine "aktive Handlung" herbeizuführen, z. B. dass die Beklagte zukünftig technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten der Klagepartei zu implementieren habe (vgl. hierzu Landgericht Aachen, Urteil vom 26. Februar 2025, 12 O 53/24; Landgericht Oldenburg, Urteil vom 28. Oktober 2024, 5 O 2845/23; Landgericht Oldenburg, Urteil vom 28. Oktober 2024, 5 O 2937/23). Dieses Vorbringen überzeugt nicht. Die Klägerseite beantragt ein reines Unterlassen der Erhebung und Verarbeitung der streitgegenständlichen Daten. Dem kann die Beklagte auch tatsächlich durch ein reines Unterlassen nachkommen, etwa durch den Verzicht auf den Einsatz der Business-Tools. Die Notwendigkeit zu einem aktiven Tun in der Form von Umprogrammierungen o.ä. erwächst in keiner Weise aus dem Antrag der Klägerseite, sondern nur aus der ggf. bestehenden Intention der Beklagten, trotz eines ggf. bestehenden Unterlassungsanspruches mit der Verwendung der Tools fortzufahren - und hierzu Programmänderungen durchzuführen, die ihr dies möglicherweise erlauben könnten. Diese geschäftlich bedingte Intention der Beklagtenseite muss sich die Klägerseite nicht zurechnen lassen (s. LG Lübeck, Urteil vom 27. November 2025 – 15 O 15/24 –, Rn. 79 juris).

In der von der Klagepartei konkretisierten Form gemäß S. 4-6 der Klageschrift vom 18.12.2024 ist der Antrag auch hinreichend bestimmt i.S.d. i. S. d. § 253 Abs. 2 Nr. 2 ZPO. Mit der Angabe der spezifischen Einzeldaten ist für eine potenzielle Vollstreckung hinreichend klar ersichtlich, welche personenbezogenen Daten gemeint sind. Der Antrag der Klagepartei war daher hier im Sinne einer Zulässigkeit auszulegen.

b) Auf das streitgegenständliche Vertragsverhältnis ist materiell-rechtlich deutsches Recht anzuwenden. Der Vertrag unterliegt nach Art. 3 Abs. 1, Art. 6 Abs. 2 der Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.06.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO) dem von den Parteien ausweislich der Nutzungsbedingungen (vgl. Anlage B1) gewählten deutschen Recht (BGH, Urteil vom12.07.2018 – III ZR 183/17); sie ergäbe sich im Übrigen aus Art. 6 I lit. b Rom I-VO, da ein Verbrauchervertrag vorliegt.

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

c) Zu einem mit vergleichbarem Umfang gestellten Unterlassungsantrag führt das Oberlandesgericht Dresden in seinem Urteil vom 03.02.2026, Az. 4 U 292/25, aus (s. OLG Dresden, Urteil vom

3. Februar 2026 – 4 U 292/25 –, juris Rn. 139-183):

„Der Antrag, mit dem die Klagepartei die Unterlassung begehrt, Daten mit Hilfe der Business-Tools zu erheben und die erhobenen Daten, weiterzugeben, zu speichern und anschließend zu verwenden, ist zulässig, insbesondere hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Ein Klageantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens der Klagepartei nicht durch vermeidbare Ungenauigkeit auf die Beklagtenseite abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (vgl. BGH, Urt. v. 18.11.2024, VI ZR 10/24 m.w.N., juris). Dies bedeutet bei einem Unterlassungsantrag insbesondere, dass dieser nicht derart undeutlich gefasst sein darf, dass die Entscheidung darüber, was der Beklagtenpartei verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (vgl. BGH, a.a.O.). Eine hinreichende Bestimmtheit ist bei einem Unterlassungsantrag für gewöhnlich gegeben, wenn eine Bezugnahme auf die konkrete Verletzungshandlung erfolgt oder die konkret angegriffene Verletzungsform antragsgegenständlich ist und der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchen Merkmalen des angegriffenen Verhaltens die Grundlage und der Anknüpfungspunkt für den Rechtsverstoß und damit das Unterlassungsgebot liegen soll (st. Rspr.; vgl. BGH, a.a.O. m.w.N.). Die Verwendung auslegungsbedürftiger Begriffe im Klageantrag ist zulässig, wenn über ihren Sinngehalt zwischen den Parteien kein Streit besteht und objektive Maßstäbe zur Abgrenzung vorliegen, oder wenn die Klagepartei den auslegungsbedürftigen Begriff hinreichend konkret umschreibt und gegebenenfalls mit Beispielen unterlegt oder ihr Begehren an der konkreten Verletzungshandlung ausrichtet. Eine auslegungsbedürftige Antragsformulierung kann hinzunehmen sein, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (st. Rspr., vgl. BGH, a.a.O.).

An diesen Anforderungen gemessen ist der Antrag der Klagepartei, die Beklagte solle es unterlassen, personenbezogene Daten der Klägerseite zu erheben, an ihre Server weiterzuleiten, zu speichern und zu verwenden, die außerhalb ihrer Netzwerke mittels der von ihr vertriebenen Business-Tools auf Drittseiten und -Apps erhoben und an sie übertragen werden, hinreichend bestimmt. Er lässt sich unter Heranziehung des Klagevorbringens sinn-

gemäß dahingehend auslegen, dass die Klagepartei sich dagegen wendet, dass ihre (sämtliche) personenbezogenen Daten über eine auf Drittwebseiten bzw. -Apps implementierte Software an die Beklagte gelangen und dort von ihr für eigene Zwecke genutzt werden. Entsprechend dem in den sog. Scraping-Fällen als hinreichend bestimmt angesehenen Unterlassungsbegehren begehrt sie eine Unterlassung jeglicher Verarbeitung ihrer durch Business-Tools erhobenen Daten durch die Beklagte. Dies gilt auch für Daten, die von Drittunternehmen übermittelt werden, die hierfür zuvor eine Einwilligung der Klagepartei eingeholt haben. Dem zur Auslegung des Antrags heranzuziehenden Vorbringen der Klagepartei ist deutlich zu entnehmen, dass sie auch für diesen Fall von einer rechtswidrigen Verarbeitung ausgeht.

Die Klagepartei ist zur Konkretisierung ihres Antrags auch nicht gehalten, einzelne Webseiten oder Apps zu benennen, deren Nutzung die Datenübertragung an die betroffene Plattform infolge eines von der Beklagten zur Verfügung gestellten Trackingtools ausgelöst haben könnte. Die Beklagte bestreitet nicht, dass zahlreiche Webseiten (aus dem Bereich Nachrichten, Medien, Shopping) ihre Business-Tools implementiert haben. Für einen regelmäßigen Nutzer des Internets, der online einkauft, Reisen bucht und sich über Nachrichten, Wetter, Politik oder/ und Gesundheitsfragen informiert, ist es schlechterdings nicht möglich, nur Webseiten aufzusuchen, die Business-Tools nicht verwenden. Von der Klagepartei kann nicht verlangt werden vorzutragen, welche Werbetreibende die Business-Tools der Beklagten implementiert haben, denn dies ist mangels Kenntnis nicht möglich (vgl. hierzu LG Berlin II, Urt. v. 04.04.2024 - 39 O 67/24, Rn 79 - juris; vgl. OLG München, Urt. v. 18.12.2025, a.a.O.). Der Klagepartei ist es auch grundsätzlich nicht zumutbar, näher zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten und mit diesen Tools versehenen Homepages vorzutragen. Zum einen kann schon naturgemäß niemand mit vertretbarem Aufwand rekonstruieren, welche Homepages zu welchem Zeitpunkt er in der Vergangenheit besucht hat; auch ist niemand verpflichtet, entsprechende Verlaufsprotokolle in seinen Rechnern vorzuhalten (vgl. LG Braunschweig, Urt. v. 04.06.2025 - 9 O 2615/23, Rn 95 - juris). Zum anderen wäre der Klagepartei aber auch selbst dann, wenn dieses Wissen vorhanden wäre, kein weitergehend substantiierter Vortrag möglich, da sie keinen vollständigen Überblick darüber hat, auf welchen Homepages zu welchem Zeitpunkt welche Business-Tools der Beklagten aktiv waren und welche Daten hierüber an die Beklagte übermittelt wurden. Faktisch wäre die Klagepartei entsprechend gezwungen, ihr gesamtes Internetnutzungsverhalten offen zu legen, was ersichtlich im eklatanten Widerspruch zum Normzweck der DSGVO stünde (vgl. LG Braunschweig, a.a.O., Rn 95 - ju-

ris). Für die Zulässigkeit des Unterlassungsantrags ist es angesichts dessen ausreichend, wenn mit einiger Wahrscheinlichkeit jedenfalls feststeht, dass die Klagepartei als Internetnutzerin von der streitigen Datenverarbeitung erfasst wurde und wird (so auch LG Braunschweig, a.a.O., Rn. 90, - juris).

Dies ist hier mit Blick auf die oben zitierten (Dritt-)Nutzungsbedingungen der Beklagten ausreichend bestimmt dargelegt. Der Unterlassungsantrag konkretisiert die inkriminierte Verletzungshandlung, nämlich die behauptete unrechtmäßige Verarbeitung von an die Beklagte mittels Business-Tools gelangter Daten trotz fehlender Einwilligung der Klagepartei bzw. auf Grundlage einer unwirksamen Einwilligung (soweit Dritte Daten an die Beklagte übertragen). Ob Daten an die Beklagte zumindest teilweise unabhängig von ihrer Auswahlentscheidung auf Webseiten von Drittunternehmen oder auch bei fehlender Einwilligung zum Zweck der Bereitstellung personalisierter Werbung auf der Plattform der Beklagten übertragen werden, ist für die Zulässigkeit des Unterlassungsbegehrens unerheblich, genauso wie die Frage, ob eine solche Datenverarbeitung für die Funktionsweise der Webseiten erforderlich ist und/oder hierfür rechtfertigende Gründe vorliegen (i.d.S. auch OGH Österreich, Urt. v. 26.11.2025 - 6 Ob 189/24y, Rn. 78 ff, Rn. 82, BeckRS 2025, 34948; a.A. OLG München, a.a.O., S. 23). So verstanden gibt es auch keine Auslegungsprobleme im Vollstreckungsverfahren, da die Klagepartei die Datenverarbeitung durch die Beklagte mittels Daten, die über Business Tools an sie gelangen, in Gänze unterlassen wissen will.

Entgegen der Auffassung der Beklagten besteht für einen solchen Antrag auch ein Rechtsschutzbedürfnis. Zwar kann die Klagepartei ihr Konto bei der Beklagten ohne weiteres selbst löschen, indem sie die Löschung ihres Kontos initiiert. Allerdings ist das Rechtsschutzziel – die Untersagung einer unrechtmäßigen Verarbeitung ihrer Daten – mit dem dann erreichten Ergebnis nicht identisch. Dieses Rechtsschutzziel ist auch besonders schützenswert, weil die DSGVO allen europäischen Bürgern ein einheitliches und hohes Datenschutzniveau bezüglich aller auf dem europäischen Markt zugelassener Anwendungen – und somit auch Social-Media-Plattformen – gewährleisten soll. Würde man die Klagepartei auf das Löschen ihres Nutzerprofils verweisen, so würde man zugleich diese Regelungsabsicht ad absurdum führen (LG Aschaffenburg, Urt. v. 20.10.2025 - 31 O 98/24, S. 28, Anlagen K zum Schriftsatz vom 21.01.2026; LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, GRUR-RS 2025, 32563, Rn. 99). Auch der Verweis auf die Möglichkeit der Klagepartei, über die Schaltfläche „Deine Aktivitäten außerhalb der Meta Technologien“ selbst die Verarbeitung einzuschränken, verfängt nicht: Zwar führen die Einstellungen „Be-

stimmte Aktivitäten trennen“ dazu, dass Aktivitäten von Apps und Websites, die der Nutzer auswählen muss, nicht mehr in seinen Konten gespeichert werden; „Frühere Aktivitäten löschen“ dazu, dass die von Drittunternehmen geteilten Informationen über Aktivitäten vom Konto des Nutzers getrennt werden und „Verknüpfung mit künftigen Aktivitäten aufheben“ dazu, dass Informationen, die Unternehmen und Organisationen zu Interaktionen mit dem Nutzer an die Beklagte übermitteln, zukünftig nicht mehr verknüpft werden. Der Transfer personenbezogener Daten von Drittunternehmen an die Beklagte bleibt davon aber unberührt.

b)

Der Antrag ist auch begründet, die Klagepartei hat einen Anspruch auf die begehrte Unterlassung.

aa) Zwar ergibt sich der Anspruch nicht unmittelbar aus den Vorschriften der DSGVO (EuGH, Urt. v. 04. 09. 2025 – C-655/23 –, LS 1 und Rz. 52, - juris; vgl. Senat, Urt. v. 14.12.2021 - 4 U 1278/21, Rn 46 - juris). Der Rückgriff auf nationale Vorschriften ist insoweit aber möglich (EuGH, a.a.O) und ergibt sich nach deutschem Recht wegen der Verletzung des allgemeinen Persönlichkeitsrechts der Klagepartei aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 Art. 1 Abs. 2 GG; § 823 Abs. 2 BGB i.V.m. Art. 6 DSGVO, jeweils i.V.m. § 1004 Abs. 1 S. 2 BGB analog. Der Unterlassungsanspruch setzt voraus, dass eine konkrete (Erstbegehungs- oder Wiederholungs-)Gefahr dafür besteht, dass die Beklagte gegenwärtig über die Meta Business-Tools gesammelte personenbezogene Daten der Klagepartei verarbeitet, die Beklagte Verantwortliche für diese Verarbeitung ist und sie eine Rechtfertigung gem. Art. 6 DSGVO für diese Datenverarbeitung nicht darlegt und beweist. Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr wird durch das festgestellte rechtsverletzende Verhalten indiziert (vgl. Senat, Beschl. v. 24.06.2024 – 4 U 168/24 –, Rn. 18, m.w.N., -juris).

Da es sich bei diesen Verarbeitungsvorgängen um interne Abläufe in den Systemen der Beklagten handelt, trifft sie dabei eine sekundäre Darlegungslast zu den Datenverarbeitungsvorgängen bei der Erhebung und Verarbeitung personenbezogener Daten mittels Business-Tools. Die Klagepartei hat demgegenüber nicht darzulegen, welche konkreten Webseiten sie aufgesucht hat und auf welchen dieser Webseiten Business-Tools zum Einsatz kommen [...]. Schon aus diesem Grund kann von ihr [...] auch nicht verlangt werden, darzulegen und zu beweisen, dass sie auf diesen Webseiten die Einwilligung in

die Datenerhebung über Business-Tools verweigert hat. Zwingende Voraussetzung für eine Datenübermittlung an die Beklagte ist die Cookie-Einwilligung des Nutzers auf Drittwebseiten ohnehin nicht, weil unstreitig die Implementierung der Business-Tools auf zahlreichen Drittwebseiten fehlerhaft ist, so dass dort Daten auch dann an die Beklagte weitergeleitet werden, wenn der Nutzer eine solche Einwilligung nicht erteilt hat. Nachdem unstreitig ist, dass die Klagepartei bei der Beklagten als Nutzer registriert ist und dass auf einer erheblichen Anzahl namhafter und reichweitenstarker Webseiten in Deutschland die Business-Tools der Beklagten in ihren verschiedenen Ausprägungen zum Einsatz kommen, ist vielmehr davon auszugehen, dass auch von der Klagepartei Business-Tool-Daten erhoben werden. Soweit sich die Beklagte darauf beruft, dass dies ausnahmsweise nicht der Fall ist, trägt sie auch hierfür die Darlegungslast (vgl. hierzu auch [OLG Dresden], Urt. v. 11.02.2025 – 4 U 1283/24 –, juris, und mit überzeugender Begründung: LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, Rn. 88-92 m.w.N., -juris).

bb) Bei Anwendung dieser Maßstäbe hat die Beklagte die Behauptung, die ihr seitens ihrer Geschäftspartner über Business-Tools übermittelten personenbezogenen Daten der Klagepartei verarbeite sie auch bei fehlender Einwilligung des Nutzers, nicht substantiiert bestritten. Hierfür ist nicht entscheidend, ob sie die von Drittunternehmern übermittelten Daten verarbeitet, um der Klagepartei personalisierte Werbung zu zeigen. Entscheidend ist vielmehr, dass sie diese Daten auf ihrer Plattform jedenfalls vorübergehend speichert und mit den sog. onsite-Daten der Klagepartei zusammenführt, bevor diese in einem weiteren Schritt durch Zuweisung von Ad-IDs, Hash-Werten und Cookie-IDs pseudonymisiert werden. Diese Zusammenfassung in für die Beklagte auswertbaren individuellen Nutzerprofilen stellt ein Verknüpfen i.S.d.Art. 4 Nr. 2 DSGVO dar, weil hiermit eine inhaltliche Umgestaltung erfolgt und die verknüpften Daten einen neuen Aussagewert erhalten (vgl. hierzu Schaffland/Holthaus in: Schaffland/Wiltfang, DS-GVO/BDSG, 6. Erglfg. 2025, Art. 4 EUV 2016/679, Rn. 116). Die hiermit einhergehende Bildung individueller Nutzerprofile stellt zugleich ein Profiling der Nutzer im Sinne von Art. 4 Nr. 4 DSGVO dar, weil die mit der o.a Verknüpfung verbundene Erstellung eines Profils einer Person durch Auswertung von Daten und Bewertungen aufgrund von Algorithmen zur Erstellung eines Persönlichkeits-, Verhaltens- oder Bewegungsprofils durch Sammlung von Daten, unter anderem durch (im Internet) hinterlassene (Cookies), getätigte und veröffentlichte Informationen z. B. zu sozialen Kontakten, politischer Einstellung, persönlichem Weltbild, persönlichen Vorlieben, finanziellen Verhältnissen, gesundheitlicher Situation und weiteren Angaben ein modellhaftes, auf Algorithmen beruhendes Gesamtbild der individuellen Persönlichkeit ergeben (vgl. auch in-

soweit Schaffland/Wiltfang, aaO, Art. 4 EUV 2016/679, Rn. 125). Dies steht zur Überzeugung des Senats aufgrund des Sachvortrags der Parteien und in Würdigung der vorgelegten NB-MBT sowie der Nutzungsbedingungen für Plattform-Nutzer (im Folgenden NB-PN) fest.

(1) Die hiergegen gerichtete Behauptung der Beklagten, es sei technisch ausgeschlossen, dass über auf Drittwebseiten, -Apps und Servern implementierte Business-Tools Daten von Nutzern wie der Klagepartei mit ihr geteilt werden, die nicht von einer Einwilligung des Nutzers in diese Verarbeitung umfasst sind, ist weder ausreichend dargelegt noch bewiesen.

Nach Ziff. 1 und 2 der NB-MBT vom 25.04.2023 (vgl. Anl. B5) werden bei Implementierung von Business-Tools auf Drittwebseiten, -Apps und Servern sowohl Kontaktinformationen (definiert unter Ziff. 1. a. i.) als auch Event-Daten (definiert unter Ziff. 1. a. ii.) an die Beklagte übermittelt; dies - unstreitig - zumindest dann, wenn die Drittunternehmen eine „Cookie-Einwilligung" ihres Kunden eingeholt haben. Keine Daten werden hingegen nach dem Vortrag der Beklagten (nur) dann übermittelt, wenn und soweit die Business-Tools Verwender ihre Cookie-Einstellungen bzw. -Banner entsprechend den Nutzungsbedingungen der Beklagten und auch im übrigen datenschutzkonform konfiguriert haben, und der Nutzer diese abgelehnt hat. Ob alle diese Voraussetzungen zutreffen, überprüft die Beklagte freilich nicht.

Nach den NB-MBT (vgl. dort Ziff. 2 a) kann die Beklagte sämtliche Business-Tools-Daten für eine Reihe von Zwecken verwenden, insbesondere auch die übermittelten Kontaktinformationen mit von ihr selbst vergebenen Nutzer-IDs abgleichen und mit den Event-Daten kombinieren. Entsprechend dem Hinweis unter Ziff. iv am Ende ihrer Nutzungsbedingungen definiert die Beklagte als „abgeglichene Daten" Event-Daten, die mit abgeglichenen Nutzer-IDs kombiniert wurden. Somit kann sie den betreffenden Nutzer eindeutig identifizieren und ihm sämtliche Interaktionen zuordnen. Im Anschluss an diesen Abgleichprozess werden - lediglich - die von Dritten übermittelten Kontaktinformationen von ihr gelöscht (vgl. Ziff. 2 a i.1. Satz 2 NB-MBT), was nach dem Verständnis des Senats jedoch keine Auswirkungen auf die zuvor von der Beklagten in ihren Systemen erfolgte Identifizierung und Zuordnung zu einem bestimmten Nutzer wie der Klagepartei hat. Dies wird auch durch Ziff. 2. a. bestätigt, insbesondere unter v. der NB-MBT. Dabei verarbeitet die Beklagte die ihr von Dritten übermittelten Daten auch nicht ausschließlich für drittbezogene (Werbe-)Zwecke. Aus der Regelung unter Ziff. 2. a. v. 2. NB-MBT ergibt sich vielmehr,

dass sie die übermittelten Event-Daten verwenden kann, „um die Funktionen und Inhalte (einschließlich Werbeanzeigen und Empfehlungen) zu personalisieren, die wir Personen auf und außerhalb von unseren Meta-Produkten zeigen." Nach Ziff. 2. a. v. 3. NB-MBT ist die Beklagte ferner berechtigt, „um das Erlebnis für Nutzer von Meta-Produkten zu verbessern", Event-Daten zu verwenden, „um den Schutz und die Sicherheit auf und außerhalb von Meta-Produkten zu fördern, sowie für Forschungs- und Entwicklungszwecke und für den Erhalt der Integrität der Meta-Produkte sowie für deren Bereitstellung und Verbesserung."

(2) Auch die in den Nutzungsvertrag mit der Klagepartei (NB-PN) einbezogenen Erläuterungen zur „Deine Aktivitäten außerhalb von Meta-Technologien"- Einstellung („Off-site Aktivitäten" bzw.„Third-Party Activity Data") bestätigen eine fortlaufende Verarbeitung der ihr übermittelten Business-Tools Daten, unabhängig von der Einwilligung eines Nutzers. Entsprechend den Ausführungen unter Ziff. IV und den Informationen in der abgebildeten Infobox (vgl. Anl. B7) verwendet die Beklagte über ihre optionalen Cookies in anderen Apps und Websites geteilte Informationen des Nutzers zur Verbesserung des Nutzungserlebnisses in Meta-Produkten mittels personalisierter Werbeanzeigen, zur Erbringung von Diensten außerhalb der Meta-Plattformen, zur Verbesserung von Meta-Produkten und zur Unterstützung der Business-Tools-Verwender bei Analysen und Messungen ihrer Anzeigenperformance. Bei einem Nutzer, der optionale Cookies auf Dritt-Apps und -Websites erlaubt, verwendet die Beklagte die individuellen Cookie-Informationen zur Anzeige von relevanter Werbung. Die Einstellungen des Nutzers für Werbung und seine Werbepräferenzen werden dabei „berücksichtigt", ohne dass die Beklagte näher erläutert, in welcher Form dies geschieht. Ein Nutzer, der - wie die Klagepartei - Cookies der Beklagten über die Plattform-Einstellungen nicht erlaubt, wird zwar bei den Dritt-Websites und -Apps von seinen Plattform-Konten abgemeldet. Selbst nach dem Beklagtenvorbringen folgt hieraus indes nicht zwingend, dass die Beklagte über ihre Business-Tools keine personenbezogenen Daten dieses Nutzers mehr erhält. Denn sie bestätigt, dass sie die Informationen in eingeschränktem Umfang für „Sicherheit und Integrität", und nicht für die Anzeige von für den Nutzer relevanter Werbung verwendet. Darüber hinaus könne sie aber auch weiterhin „aggregierte" Informationen zu Aktivitäten in diesen Apps und auf diesen Websites erhalten, während (nur) „persönliche" Cookie-Informationen darin nicht enthalten sein sollen. Zudem wird in den NB-PN ausdrücklich darauf hingewiesen, dass die Beklagte im Fall einer Kontentrennung, und zwar bezogen auf zukünftige und vergangene Aktivitäten, auch weiterhin Informationen zu den Aktivitäten von Apps und Websites erhalte, die sie für Messun-

gen sowie zur Verbesserung ihrer Werbesysteme verwenden könne (vgl. Infobox: „Das solltest du wissen“).

Bestätigt wird eine fortlaufende Verarbeitung von personenbezogenen Daten auch durch die für die Nutzung von Instagram/Facebook geltende, 146 Seiten (!) umfassende Datenschutzrichtlinie der Beklagten (Anl. B10). Im Unterpunkt „Wie teilen wir Informationen mit Dritten?“ (vgl. S. 46) wird ausgeführt, dass die Beklagte „bestimmte Informationen“ mit einer Reihe von Parteien teile, darunter Werbetreibende, die Anzeigen in Produkten der Beklagten schalten, Unternehmen, die die Beklagte damit beauftrage, ihre Produkte für sie zu vermarkten, bzw. mit Dienstleistungen wie Kundenservice oder Umfragen, Forscher, die diese Informationen für Zwecke wie Innovationen, technologische Fortschritte oder Sicherheitsverbesserungen nutzen (vgl. S. 46ff). Auch der weitere Passus:

„Wir bestätigen Werbetreibenden außerdem, welche Werbeanzeigen du gesehen hast, die dich zu einer Handlung veranlasst haben, beispielsweise zum Herunterladen der App eines Werbetreibenden. Wir teilen mit diesen Werbetreibenden und ihren Anbietern jedoch keine Informationen, die für sich genommen dazu verwendet werden können, dich zu kontaktieren oder identifizieren (wie z. B. dein Name oder deine E-Mail-Adresse), es sei denn, du gibst uns deine Einwilligung dazu. ...“ (vgl. S. 48) lässt darauf schließen, dass auch ohne Einwilligung des Nutzers bestimmte nutzerbezogene Datenkategorien an Geschäftspartner der Beklagten weitergegeben werden, wenn auch nicht solche, die seine eindeutige direkte Identifizierung ermöglichen.

(3) Die Beklagte kann sich nicht mit Erfolg darauf berufen, die Privatsphäre der Nutzer sei gewahrt, da sie personenbezogene Daten aggregiere, also einzelne Datenpunkte zu Gruppen zusammenfasse, so dass Erkenntnisse aus den gesammelten Informationen mehrerer Personen und nicht aus denen einer einzelnen Person gewonnen werden. Dagegen steht, dass schon wegen der Vielzahl der durch Off-site Aktivitäten bzw. Third-Party Activity Data gewonnenen Datenpunkte und Informationen es zumindest nicht ausgeschlossen erscheint, dass einzelne Nutzer und/oder ihm zugeordnete Events identifizierbar bleiben. Welche Daten konkret aggregiert und von der Beklagten genutzt werden, sei es für eigene Zwecke, sei es, indem sie sie weiterleitet bzw. teilt, wird durch die Datenschutzbedingungen nur beispielhaft und damit unzureichend erläutert wie folgt:

„Partner, die unsere Analysedienste nutzen

Menschen setzen auf unsere Produkte, wie Unternehmenskonten, professionelle Tools und

Facebook-Seiten, um ihre Unternehmen zu betreiben und zu bewerben. Unternehmen nutzen unsere Analysedienste, um mehr darüber zu erfahren, wie Personen ihre Inhalte, Features, Produkte und Dienste verwenden. Wir verwenden die von uns erfassten Informationen über dich, um diese Dienste bereitzustellen. Wir geben diese Informationen in zusammengefassten Berichten an Partner weiter, die ihnen Aufschluss darüber geben, wie gut ihre Inhalte, Features, Produkte und Dienste abschneiden. So können sie die Erfahrung der Nutzer mit diesen Inhalten, Produkten und Diensten besser verstehen. Diese Berichte aggregieren z. B. folgende Informationen:

Wie viele Personen mit den Inhalten, Produkten oder Diensten unserer Partner interagiert haben

Allgemeine demografische Daten und Interessen der Personen, die mit ihnen interagiert haben

Wie Personen die Produkte und Dienste unserer Partner nutzen, um sich mit Meta-Produkten zu verbinden, und ihre Verbindungs- und Netzwerkleistung

Werbetreibende erhalten auch andere Informationen. ...“

Dass sämtliche nutzerbezogene Informationen aggregiert werden, wird von der Beklagten auch nicht hinreichend substantiiert in Abrede gestellt, da sie hierzu in der Datenschutzerklärung unter „Wie verwenden wir deine Informationen?“ in wesentlichen Punkten unklar und einschränkend mitteilt, „um weniger Informationen zu verwenden, die mit einzelnen Nutzern verknüpft“ seien, diese „in einigen Fällen de-identifiziert, zusammenfasst oder anonymisiert, so dass der Nutzer damit nicht mehr identifizierbar“ sei. Soweit sie in diesem Zusammenhang zur Klarstellung darauf hinweist, dass sie die über Cookies und ähnliche Technologien gesammelten Daten einer Person nicht zur Anzeige von Werbung verwende, wenn diese Person „Meta-Cookies in anderen Apps und auf anderen Websites“ nicht ausdrücklich zulasse [...], bezieht sie sich ausschließlich auf (eigene) Werbe- und nicht auf andere, in ihren Nutzungsbedingungen genannten Zwecke, die hierüber hinausgehen.

(4) Schließlich ist auch das Hashen (Verschlüsseln) der von Partnern der Beklagten übermittelten Daten nicht geeignet, ihre Behauptung zu stützen, sie verarbeitete bei fehlender Einwilligung ihrer Nutzer keine personenbezogenen Daten, die ihr mittels Business Tools übermittelt werden. Drittunternehmen übermitteln der Beklagten zwar Kontakt- und Eventdaten ihrer Kunden in gehashter Form bei Vorliegen einer „Cookie-Einwilligung“. Den

*NB-MBT und den Parametern für Kund:innen Informationen lässt sich aber entnehmen, dass die Beklagte, die ihren Geschäftspartnern die für die Verschlüsselung dieser Daten zu verwendende Technologie im Einzelnen verbindlich vorschreibt, diese Technologie selbst verwendet. Da sie ihre eigenen Nutzerdaten mit demselben Verfahren hasht und die Hashes vergleicht, ermöglicht dies eine Zuordnung in den meisten Fällen. Dass sie die erfolgte Verschlüsselung der Daten rückgängig machen kann, um sie für ihre Zwecke, darunter auch - aber nicht nur - personalisierte Werbung verwenden zu können, wird durch die NB-MBT und die detaillierten Regelungen in den Parametern für Kund*innen-Informationen belegt.*

(5) Dem Vortrag der Beklagten, sie verarbeite Business Tools Daten von Nutzern, die „Meta-Cookies auf anderen Apps und Websites“ nicht ausdrücklich zulassen, nur zu Sicherheits- und Integritätszwecken, steht bereits entgegen, dass er ihren eigenen Nutzerinformationen widerspricht, die eine Verarbeitung auch zu "weiteren eigenen Zwecke wie Messungen und Verbesserung unserer Werbesysteme" zulässt. Abgesehen davon ist der diesbezügliche Sachvortrag der Beklagten geprägt von unbestimmten Begriffen wie „gewisse“ bzw. „eingeschränkte“ Verarbeitung, „Integritätszwecke“, die nicht näher erläutert werden sowie von Verallgemeinerungen wie „einige Informationen“, “im Großen und Ganzen“, und ist zudem in wesentlichen Punkten widersprüchlich und nicht nachvollziehbar. So bleibt beispielsweise im Dunkeln, wie die Beklagte ohne einen Datenabgleich ermitteln will, ob die ihr übermittelten Daten einem Nutzerprofil zuzuordnen sind und dieser Nutzer eine Einwilligung in die Verarbeitung seiner Daten erteilt hat oder nicht.

(6) Die Beklagte hat zu diesem Punkt im Verlauf des Verfahrens eingeräumt, an sie gelangte personenbezogene Daten (zumindest) für einen Abgleich in ihren Systemen zu nutzen, um festzustellen, ob es sich um Daten eines bei ihr registrierten Nutzer handelt. Bereits der Abgleich zur Prüfung, ob es sich um einen bei ihr registrierten Nutzer handelt, stellt eine Verarbeitung im Sinne des Art 4 Ziff. 2 DSGVO dar. Nach dem Vorstehenden betrifft der Abgleich zudem Kontaktinformationen und Event-Daten, die sie automatisch entschlüsselt bzw. de-hasht [...]. Der weitere Umgang der Beklagten mit den ihr übermittelten personenbezogenen Daten bleibt allerdings in jeder Hinsicht unklar und wird auch durch den - nach entsprechenden Hinweisen des Senats - ergänzten Vortrag nicht weiter aufgeklärt. Sie verweist lediglich darauf, sie müsse zumindest eine „gewisse“ Verarbeitung von Business-Tools Daten vornehmen, um festzustellen, ob sie diese einem bestimmten Nutzerkonto zuordnen könne und um die Einstellungen des Nutzers zu erkennen und anzuwenden. Es erschließt sich bereits nicht, aus welchem Grund die Beklagte nicht nur

*übermittelte Kontaktinformationen für den Abgleich mit Nutzerkonten ("abgeglichene Nutzer-ID") nutzt, sondern darüber hinaus auch eine weitere Verarbeitung der Event-Daten in Form einer Kombination beider vornimmt, so jedenfalls nach den NB-MBT und den Parametern für Kund*innen-Informationen (s.o.). Zudem führt sie „zur Klarstellung" weiterhin aus, dass bei Daten, die keinem registrierten Nutzer zugeordnet werden können, anschließend eine Speicherung nicht erfolge (ausgenommen bestimmte Daten für Sicherheits- und Integritätszwecke). Im Umkehrschluss folgt hieraus aber, dass sie umgekehrt Daten, die sie einem registrierten Nutzer wie der Klagepartei zuordnen kann, anschließend speichert. Zwar behauptet sie, bei Nutzern, die „Meta Cookies auf anderen Apps und Webseiten" nicht zugelassen haben, die über Cookies und andere Technologien gesammelten Daten einer Person nicht „zur Anzeige von Werbung" zu verwenden. Andere Zwecke, die sie nach ihren eigenen Nutzungsbedingungen verfolgt, werden indes nicht genannt. Ihr ohnehin allgemein gehaltener, unscharfer und durch kein Beweisangebot untersetzter Vortrag lässt sich daher bereits nicht mit den NB-MBT und der Datenschutzrichtlinie in Übereinstimmung bringen. Er verhält sich insbesondere auch nicht zu der Frage, wie die Beklagte mit den an sie gelangten Daten der Nutzer weiter verfährt, die auf Drittwebseiten, -Apps und Servern ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten erteilt, jedoch der Nutzung durch die Beklagte auf den von ihr betriebenen sozialen Netzwerken widersprochen haben. Hierzu lässt die Beklagte lediglich vortragen, nach der Verarbeitung könne „Meta dann entscheiden, welche weiteren Maßnahmen in Bezug auf diese spezifischen Daten ergriffen werden, abhängig von den Einstellungen des Nutzers", ohne aber diese Maßnahmen und ihre technische Umsetzung näher zu beschreiben. Abgesehen davon konnte die Beklagte auch auf Nachfrage des Senats nicht darstellen, ob und ggfls. wie lange die Daten, die von Drittunternehmen übermittelt werden und die sich auf konkrete Nutzer beziehen, bei ihr zunächst zwischengespeichert werden, bevor sie darüber entscheidet, ob sie diese bei Vorliegen der entsprechenden Einwilligungserklärungen für personenbezogene Werbung verwendet oder nicht.*

(7) Dies gilt auch hinsichtlich der besonderen Kategorien personenbezogener Daten (im folgenden BKD) i.S.d. Art 9 Abs. 1 DSGVO, da die Datenverarbeitung über die Business-Tools der Beklagten insofern nicht zwischen „einfachen" und „sensiblen" personenbezogenen Daten unterscheidet, als sie nicht extrahiert, ob Daten sensibel sind oder nicht (vgl. OGH Wien, a.a.O., Rn. 98 und 99, EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 71, 73; - juris). Zwar untersagt die Beklagte den Verwendern ihrer Business-Tools die Übermittlung von BKD wie Gesundheits- oder Finanzdaten, Informationen von oder über Kin-

*dern unter 13 sowie nicht zugelassene IDs wie etwa Sozialversicherungs- oder Kreditkartennummern (vgl. NB-MBT, Abschnitt 1. h., Richtlinie Unzulässige Informationen, „Parameter für Kund*innen-Informationen“). Bei Verstößen hiergegen steht jedoch zumindest für den Zeitraum bis zu den vorstehend zitierten Entscheidungen fest, dass die automatisiert ablaufende Datenverarbeitung der Beklagten sensible Daten objektiv umfasste und der gesamte Verarbeitungsvorgang als “Verarbeitung besonderer Kategorien personenbezogener Daten“ zu beurteilen ist (vgl. OGH, a.a.O., EuGH, a.a.O.), was eine für ein Unterlassungsbegehren ausreichende Erstbegehungs-, aber auch eine Wiederholungsgefahr indiziert. Im Übrigen ist kaum vorstellbar, dass bei der Übermittlung von diesen Drittwebseiten an die Beklagte keine sensiblen Daten enthalten sind. Denn schon allein das Aufsuchen oder Registrieren auf entsprechenden Drittwebseiten sowie die dort getätigten Aktionen, wie z.B. Online-Bestellungen, können Rückschlüsse auf Gesundheit, sexuelle Orientierung, Finanzen und Weltanschauung eines Nutzers zulassen.*

(8) Ohne Erfolg beruft sich die Beklagte angesichts dessen darauf, sie habe "freiwillig" Maßnahmen wie eine Kategorisierung der Datenquellen, eine automatisierte Filterung sowie erweiterte Datenbeschränkungen wie beispielsweise das „Core Set-up“ implementiert, die dazu dienen sollten, den Erhalt und die Nutzung potentiell sensibler Daten zu verhindern, die nach den NB-MBT nicht zulässig seien und die Drittunternehmen möglicherweise unzulässigerweise zu übermitteln versuchen. Dass diese Maßnahmen vor der Übertragung sensibler Daten an die Beklagte bei einer automatisierten Datenverarbeitung mittels Business-Tools ausreichend Schutz bieten, erscheint bereits deshalb zweifelhaft, weil die Beklagte an anderer Stelle vortragen lässt, nur die Drittunternehmen hätten die Möglichkeit, sicherzustellen, dass der Browser der Person oder der Server des Drittunternehmens eine HTTP-Anfrage erst dann ausführe, wenn die Person ihre Einwilligung zu nicht notwendigen Cookies erteilt habe, was die Beklagte selbst nicht kontrolliere. Auch in der Richtlinie „Unzulässige Informationen“ (Anl. B6) weist die Beklagte darauf hin, dass ihre Systeme "die eigenen Mechanismen des Verwenders zur Einhaltung dieser Regeln lediglich ergänzen“, was für sich genommen bereits belegt, dass die implementierten Maßnahmen allein nicht ausreichen, um das Teilen von sensiblen Daten mit der Beklagten gänzlich und zuverlässig zu unterbinden. Schließlich steht die damit einhergehende Behauptung einer automatischen Ausfilterung besonders geschützter Daten nach Art. 9 Abs. 1 DSGVO auch in Widerspruch zu den tatbestandlichen Feststellungen in den "Schrems-Verfahren" (vgl. OGH aaO.; EuGH aaO.), worauf die Beklagte durch den Senat auch hingewiesen wurde.

cc) Die Beklagte ist als Verantwortliche i.S.d. Art. 4 Ziff. 7 DSGVO für die Erhebung von über Business-Tools auf Drittseiten erlangten Daten und deren anschließende Weiterverarbeitung passivlegitimiert. Gemäß Art. 4 Ziff. 7 DSGVO ist Verantwortlicher diejenige 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. Eine gemeinsame Verantwortung besteht nach Art. 26 Ziff. 1 Satz 1 DSGVO, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verwendung festlegen. Das Ziel dieser Bestimmungen liegt darin, durch eine weite Definition des Begriffs des „Verantwortlichen" einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten (Urteile v. 13.05.2014, Google Spain und Google, C-131/12, EU:C:2014:317, Rn. 34, und vom 0506.2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, Rn. 28). Der EuGH hat für die insoweit dem Art. 4 Ziff. 7 entsprechende Vorschrift des Art. 2 Buchst. d der Richtlinie 95/46 entschieden, dass eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als für die Verarbeitung Verantwortlicher im Sinne von Art. 2 lit. d der Richtlinie 95/46 angesehen werden kann (EuGH, Urt. v. 29.07.2019 – C-40/17 –, juris, Rz 68; Urt. v. 10.07.2018, Jehovan todistajat, C-25/17, EU:C:2018:551, Rn. 68). Indem die Beklagte Drittunternehmern ihre Business-Tools anbietet, mit deren Hilfe sie unstreitig möglichst viele Daten der Drittseitennutzer für ihre eigenen Zwecke erhalten möchte, wird sie auch für die Datenerhebung auf Drittseiten zur Mitverantwortlichen im Sinne des Art. 26 DSGVO (vgl. EuGH, Urteil vom 29.07.2019 - C-40/17 - juris; vgl. LG Stuttgart, Urteil vom 05.02.2025 - 27 O 190/23 - juris; vgl. OGH Wien, Urteil vom 26.11.2025 - 6 Ob 189/24y, Beck-RS 34948, Beck-Online); vgl. OLG München, Urt. v. 18.12.2025 - 14 U 1068/25e, juris).

Diese Verantwortlichkeit kann sie weder durch vertragliche Vereinbarungen mit den Drittanbietern auf diese abwälzen, noch kann sie sich durch etwaige Belehrungen der Drittanbieter im Hinblick auf deren datenschutzrechtlichen Pflichten von der eigenen Verantwortlichkeit freizeichnen, schon weil sie selbst gegenüber ihren Business-tools-Kunden die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO feststellt [...]. Aus denselben Gründen kann sich die Beklagte daher auch nicht darauf berufen, entsprechend ihren NB-MBT unter Ziff. 5. hinsichtlich bestimmter Verarbeitungszwecke (Abgleich-, Messung- und Analysedienste) lediglich als Auftragsverarbeiter i.S.d. Art. 4 Nr. 9 DSGVO der Drittunternehmer tätig zu werden. Nimmt eine Stelle - wie hier die Beklagte - aus Eigeninteresse auf die

Verarbeitung Einfluss und wirkt auf diese Weise neben einem anderen Beteiligten an der Entscheidung über Zweck und Mittel der Verarbeitung mit, führt dies regelmäßig zu einer (gemeinsamen) Verantwortlichkeit (EuGH, Urt. v. 29.7.2019, a.a.O.; Simitis/Hornung/ Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 26 Rn. 25, Art. 4 Nr. 7, Rn. 24, m.w.N., beck-online; BeckOK DatenschutzR/Spoerr, 54. Ed. 01.11.2025, DS-GVO Art. 26 Rn. 18-22, m.w.N. beck-online).

dd) Bei den von der Klagepartei aufgezählten und unstreitig von der Beklagten auch verarbeiteten Daten handelt es sich ausnahmslos um „personenbezogene Daten“ im Sinne der Legaldefinition in Art. 4 Ziffer 1 DSGVO. Der Begriff der personenbezogenen Daten ist weit zu verstehen und umfasst alle Arten von Informationen sowohl objektiver als auch subjektiver Natur unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten natürlichen Person verknüpft ist, so dass sie aufgrund dessen direkt oder indirekt identifiziert oder identifizierbar ist. (vgl. EuGH, Urt. v. 20.122017 - C-434/16, juris Rn. 34 f. - Nowak; BGH, Urt. v. 18.12.2025 – I ZR 115/25 –, m.w.N., Rn. 22ff, juris). Die übermittelten Daten sind zur Identifizierung des Nutzers geeignet, was die Beklagte ausdrücklich nicht bestreitet. Die Identifizierung des Nutzers auf Webseiten und Apps Dritter erfolgt durch verschiedene Techniken. Dafür werden "Third Party Cookies", "First Party Cookies", die "Klick-ID" sowie "automatisiertes Advanced Matching" und "manuelles Advanced Matching" verwendet (vgl. LG Braunschweig, Urt. v. 04.06.2025 – 9 O 2615/23 –, Rn. 106, juris mit Verweis auf BKartA Beschl. v. 06.02.2019 Az. B6-22/16 Rn. 575 ff; https://www.bundeskartell-amt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=2).

ee) Die Verarbeitung der personenbezogenen Daten der Klagepartei durch die Beklagte ist rechtswidrig. Die Beklagte hat keine Rechtfertigungsgründe für die Verarbeitung nachgewiesen i.S.d. Art 6 Ziff. 1 DSGVO, deren Nachweis ihr nach Art. 7 Ziff. 1 DSGVO obliegt. Die Erhebung und Verarbeitung personenbezogener Daten verstößt darüber hinaus gegen das in Art. 5 Ziff. 1 a DSGVO normierte Rechtmäßigkeits- und Transparenzgebot, gegen den Grundsatz der Datenminimierung gem. Art. 5 Absatz 1 lit. c DSGVO sowie gegen zulässige Speicherfristen, Art 5 Ziff. 1 lit. e) DSGVO. Erst recht liegen keine die Verarbeitung von BKD i.S.d. Art 9 DSGVO rechtfertigende Gründe vor.

(1) Damit der Rechtfertigungsgrund einer Einwilligung der Klagepartei als betroffene Person greift, muss die Beklagte nachweisen, dass die Weitergabe von Daten der Klagepartei an sie von einer auf konkrete Zwecke bezogenen freiwilligen Einwilligung gedeckt ist, vgl. Art. 6, Art 7 Ziff. 2 und 4 DSGVO. Dieser Nachweis ist ihr nicht gelungen. Dies betrifft die im Unterlassungsantrag genannten Verarbeitungsvorgänge der Datenerhebung mittels Business-Tools bei den Drittunternehmen, der Weitergabe an die Server der Beklagten, die Speicherung und die anschließende Verwendung. Unstreitig hat die Klagepartei der Beklagten weder über die "Meta-Cookies in anderen Apps und auf anderen Webseiten" noch über die Schaltfläche "Informationen über deine Aktivitäten" eine Einwilligung zur Nutzung von Business-Tool-Daten erteilt. Eine solche Einwilligung nimmt die Beklagte auch nicht für sich in Anspruch, sie beruft sich auch nicht auf eine vor dem 25.05.2018 erklärte Einwilligung, die ohnehin unter der Geltung der DSGVO keine rechtfertigende Wirkung mehr entfalten könnte (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 114 - juris). Die Beklagte kann sich auch nicht auf eine etwaig erteilte Einwilligung der Klagepartei auf Drittwebseiten und -Apps berufen, da sich diese nur auf Datenverarbeitungszwecke des Webseiten- bzw. App-Betreibers als Business-Tools Verwender, aber nicht auf diejenigen des Anbieters dieser Technologien bezieht (vgl. EuGH, Urt. v. 29.7.2019 – C-40/17 (Fashion ID) a.a.O., Rn. 97). Es obliegt somit nicht den Drittunternehmen, eine Einwilligung des Nutzers für eine Verarbeitung von Daten für Zwecke der Beklagten einzuholen. Ob die Klagepartei die (Nicht-)Erteilung einer Einwilligung hierin auf Drittseiten substantiiert dargelegt hat, ist daher nicht entscheidend.

(2) Die Beklagte kann sich auch nicht mit Erfolg darauf berufen, sie verarbeite Business-Tools Daten als für die Erfüllung der Verträge mit geschäftsfähigen Nutzern erforderlich gemäß Art. 6 Ziff. 1 lit. b DSGVO. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 98, - juris). Entscheidend ist dabei, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen. Zudem ist bei einem Vertrag, der mehrere Dienstleistungen oder mehrere eigenständige Elemente

einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit des Rechtfertigungstatbestandes für jede dieser Dienstleistungen gesondert zu beurteilen (vgl. EuGH, a.a.O., Rn. 100). Dass die Verwendung der Business-Tools und die Verarbeitung der durch sie gewonnenen personenbezogenen Daten zur Nutzung der sozialen Plattform unerlässlich wäre, lässt sich nicht feststellen. Der Betrieb und die Nutzung der streitgegenständlichen Plattform sind vielmehr ohne Einbindung der Business-Tools möglich, was nicht zuletzt die Einführung des Bezahlmodells seit dem 03.11.2023 verdeutlicht. Für fernliegend hält der Senat die Annahme, die Verarbeitung von Business-Tools-Daten sei aus Sicherheits- und Integritätszwecke geboten. Insoweit fehlt es aber schon an nachvollziehbaren, hinreichend konkreten Sachvortrag, dass der Hauptgegenstand des Vertrags, der hier in der Nutzung der Social-media-Plattform der Beklagten liegt, ohne die zusätzliche und außerhalb des eigentlichen Vertragszwecks liegende, umfassende Verarbeitung von Off-site Daten ihrer Geschäftspartner nicht erfüllt werden könnte, diese also objektiv unerlässlich für den mit der Klagepartei bestehenden Nutzungsvertrag sind.

(3) Die nach Art. 6 Ziff. 1 lit. f DSGVO vorzunehmende Interessenabwägung ergibt gleichfalls kein zugunsten der Beklagten überwiegendes Interesse an der Verarbeitung von Business-Tool-Daten (vgl. zu den Voraussetzungen EuGH, Urt. v. 04.07.2023, C-252/21, a.a.O., Rn. 114, -juris).

(a) Dem berechtigten Interesse der Beklagten an einem "profitablen Dienst" kommt kein höheres Gewicht zu, als dem Recht der Nutzer auf Datensicherheit und -minimierung sowie informationelle Selbstbestimmung. Der EuGH (a.a.O.) hat insoweit bereits entschieden, dass auch wenn die Dienste eines sozialen Online-Netzwerks unentgeltlich sind, der Nutzer dieses Netzwerks vernünftigerweise nicht damit rechnen müsse, dass dessen Betreiber seine personenbezogenen Daten ohne seine Einwilligung zum Zweck der Personalisierung der Werbung verarbeitet oder sogar noch umfänglicher nutzt. Daher sei davon auszugehen, dass die Interessen und Grundrechte eines solchen Nutzers bereits gegenüber dem Interesse dieses Betreibers an einer solchen Personalisierung der Werbung, mit der er seine Tätigkeit finanziert, überwiegen, so dass die von ihm zu solchen Zwecken vorgenommene Verarbeitung nicht unter Art. 6 Ziff. 1 lit. f DSGVO fallen könne (vgl. EuGH, Urt. v. 4.07.2023, a.a.O., Rn. 117, juris). Davon ausgehend kann erst recht die der Nutzung der Plattform der Beklagten vorgelagerte oder gar unabhängig von einer Plattformnutzung erfolgte Verarbeitung von personenbezogenen Daten nicht gemäß Art. 6 Ziff.1 lit. f DSGVO gerechtfertigt sein.

(b) Soweit die Beklagte auch insoweit geltend macht, die Speicherung der Off-Site-Daten sei zu Sicherheits- und Integritätszwecken notwendig, trägt dies den Rechtfertigungsgrund des berechtigten Interesses nicht. Denn sie bezieht sich auch in diesem Zusammenhang auf die Datenerhebung mittels Business-Tools, die wiederum als „Einfallstor" für kriminelle Aktivitäten bzw. Ausnutzung der Systeme diene und der sie durch eine Speicherung/Auswertung dieser Daten begegnen müsse. Diese Begründung ist nicht geeignet, die Verarbeitung von individualisierten und/oder individualisierbaren Nutzerdaten auf ihrer Plattform zu rechtfertigen (so auch LG Stuttgart, Urt. v. 05.02.2025 - 27 O 190/23 -, Rn. 85, -juris; LG Lübeck, Urt. v. 10.01.2025 - 15 O 269/23 -, Rn. 130, -juris). Im Übrigen widerspricht der Vortrag der Beklagten, dass die Daten nur zu Sicherheits- und Integritätszwecken genutzt werden ihren eigenen Informationen [...], in denen sie mitteilt, dass sie trotz „Trennung" und/oder „Verknüpfung mit künftigen Aktivitäten aufheben" weiterhin Informationen zu den Aktivitäten erhält und diese für „Messungen sowie zur Verbesserung ihrer Werbesysteme" verwendet. Schließlich steht dieser Vortrag auch nicht im Einklang mit den Informationen, die die Beklagte ihren Nutzern erteilt. Dort heißt es u.a.:

„Berechtigte Interessen

Wir verarbeiten deine Informationen so, wie es für unsere berechtigten Interessen bzw. die von anderen erforderlich ist. Zu unseren Interessen zählen u.a. die Bereitstellung eines innovativen, personalisierten, sicheren und profitablen Dienstes für unsere Nutzer und Partner und die Reaktion auf rechtliche Anfragen. Wir verarbeiten deine Informationen jedoch nicht, wenn deine Interessen oder Grundrechte und Grundfreiheiten unsere überwiegen. Wenn wir uns auf berechtigte Interessen berufen, hast du das Recht, der Verwendung bestimmter Informationen durch uns zu widersprechen."

Sicherheits- und Integritätszwecke finden hier keine Erwähnung.

(c) Bei der gebotenen Gesamtabwägung nach Art 6 Abs. 1 lit f) DSGVO ist zudem zu berücksichtigten, dass die von der Beklagten angegebene Speicherpraxis mit wesentlichen Grundgedanken der DSGVO nicht im Einklang steht. Die auch nach Vortrag der Beklagten bestehende längerfristige Speicherung von abgeglichenen Daten, also Nutzer-IDs und Event-Daten, begründet sie mit Sicherheits- und Integritätsprozessen, für die sie nach ihrem Sachvortrag „aufgrund deren Komplexität und Feinheiten" keinen „konkreten Zeitrahmen" angeben könne, da sie sicherstellen müsse, dass „schwerwiegende oder böswillige Aktivitäten keine negativen Auswirkungen auf die Nutzer, Produkte oder Systeme von Me-

ta haben“. Die „maximalen Aufbewahrungsfristen“ lege sie im Rahmen eines umfassenden, funktionsübergreifenden Überprüfungsprozesses fest, Daten werden „in der Regel bis zu 90 Tage aufbewahrt“, u.U. auch länger. Eine solche Speicherpraxis verstößt gegen Art. 5 Ziff. 1 lit. e DSGVO. In EG 39 S. 8 wird gefordert, „dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt“. Dass die Speicherung sämtlicher zunächst zu Zwecken wie Verbesserung des Erlebnisses für Nutzer von Meta-Produkten, Förderung von Schutz und die Sicherheit auf und außerhalb von Meta-Produkten, für Forschungs- und Entwicklungszwecke, Erhalt der Integrität der Meta-Produkte, für deren Bereitstellung und Verbesserung übermittelter personenbezogener Daten für einen unbestimmten Zeitraum nunmehr mit Sicherheits- und Integritätsprozessen und -interessen begründet wird, ist nicht nachvollziehbar und für den Senat nicht überzeugend.

(d) Schließlich verstößt die streitgegenständliche Datenverarbeitung auch gegen den Grundsatz der Datenminimierung, Art. 5 Ziff 1 lit. c DSGVO, der verlangt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist ("limited to what is necessary"). Aus diesem Grundsatz folgt, dass der Verantwortliche nicht allgemein und unterschiedslos personenbezogene Daten erheben darf und er von der Erhebung von Daten absehen muss, die für die Zwecke der Verarbeitung nicht unbedingt notwendig sind (EuGH, Urt. v. 04.10.2024 - C-446/21, a.a.O.). Die Beklagte erhält über ihre Business-Tools - wie bereits ausgeführt - umfassende Off-site Daten ihrer Nutzer über deren Tätigkeiten und verfolgt allgemein auch das Navigationsverhalten der Nutzer (vgl. EuGH a.a.O.; Bundeskartellamt, NZKart 2024, 651 [655]; vgl. Hense, K&R 2023, 556-562 m.w.N.). Eine solche Verarbeitung ist besonders umfassend, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von der Beklagten aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird (EuGH a.a.O., und MMR 2023, 669 [678, Rn. 118] - M. Plat - forms/Sosna, GSZ 2024, 53 [57]). Es steht dem Grundsatz der Datenminimierung entgegen, wenn - wie hier - sämtliche personenbezogenen Daten, die ein Verantwortlicher wie der Betreiber einer Onlineplattform für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden.“

Diesen Ausführungen des OLG Dresden schließt sich das Gericht in vollem Umfang an, wobei für den vorliegenden Fall der Nutzungsvertrag mit der Klagepartei (im zitierten Urteil NB-MBT) nicht vorliegt. Vergleichbare Informationen zur Verwendung der Business-Tools und der dadurch weitergeleiteten Daten ergeben sich für den vorliegenden Fall aus der Datenschutzrichtlinie (Anlage K3), der der Kläger unstreitig zugestimmt hat, in Verbindung mit den in der zitierten Entscheidung ebenfalls zugrunde gelegten Nutzungsbedingungen (Anlage B1). Auch ansonsten ist der hiesige Fall den dort zugrundegelegten Tatsachenfeststellungen vergleichbar, insbesondere betreffend die Verarbeitung von Daten durch die Beklagte, die ihr trotz fehlender Zustimmung des Nutzers zu Cookies übermittelt werden.

c) Eine Einschränkung der Unterlassungsverpflichtung wegen einer möglicherweise noch in der Zukunft erteilten Einwilligung oder eines sich in der Zukunft ergebenden Rechtfertigungsgrundes hält das Gericht nicht für erforderlich. Die Klagepartei hat gegenüber der Beklagten keine Einwilligung in die streitgegenständliche Datenverarbeitung erteilt. Eine möglicherweise - auch wenn nach den Aussagen des Klägers zu seinem Online-Verhalten unwahrscheinliche - gegenüber Drittanbietern erteilte Einwilligung bezieht sich allein auf die dortige Datenerhebung, erfasst indes die Weiterverarbeitung durch die Beklagte nicht (s.o.). Wird zu einem späteren Zeitpunkt eine wirksame Einwilligung erteilt oder ergibt sich ein Rechtfertigungsgrund für eine Datenverarbeitung durch die Beklagte, ist dies ggf. durch eine Vollstreckungsabwehrklage nach § 767 Abs. 2 ZPO geltend zu machen, die auch gegen einen Unterlassungsanspruch gerichtet werden kann (OLG Köln, Urt. v. 26.06.2019 – I-15 U 91/19 –, Rn. 57, juris; OLG Dresden, a.a.O. Rn. 183).

IV.

Die Klage ist hinsichtlich des Zahlungsanspruchs in tenoriertem Umfang begründet. Dem Kläger steht ein Schadensersatzanspruch nach Art. 82 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) in Höhe von 5.000,00 € zu.

1.

Zum anwendbaren Recht s.o.

2.

Dem Kläger steht aufgrund von Datenschutzverstößen ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO in Höhe von 5.000,00 € zu.

a) Das Gericht geht davon aus, dass der Kläger einen einheitlichen Anspruch auf Schadenersatz aus Art. 82 Abs. 1 DSGVO (vgl. BGH, Urteil vom 18.11.2024 – VI ZR 10/24) geltend macht, der sich auf eine Vielzahl einzelner, nicht konkretisierter Datenschutzverstöße der Beklagten stützt, aber in einem einheitlichen Geschehen (dem fortlaufenden Einsatz der sog. Meta-Business-Tools) wurzelt. Ein derartiger Anspruch erfordert nach der Rechtsprechung des EuGH einen Verstoß gegen die DSGVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. EuGH, Urteil vom 04.10.2024 – C-507/23; EuGH, Urteil vom 11.04. 2024 – C-741/21; EuGH, Urteil vom 25.01.2024 - C-687/21; BGH, Urteil vom 18.11.2024 – VI ZR 10/24). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft dabei die Person, die auf der Grundlage von Art. 82 Abs. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH, Urteil vom 11.04.2024 – C-741/21; EuGH, Urteil vom 25.01.2024 – C-687/21; BGH, Urteil vom 18.11.2024 – VI ZR 10/24). 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 (vgl. EuGH, Urteil vom 11.04.2024 – C-741/21; EuGH, Urteil vom 21.12.2023 – C-667/21; BGH, Urteil vom 18.11.2024 – VI ZR 10/24).

Nach ständiger Rechtsprechung des EuGH erfordert ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DSGVO einen Verstoß gegen Vorschriften der DSGVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. nur EuGH, Urt. v. 04.10.2024 - C-200/23, DB 2024, 2952 Rn. 140; BGH Urt. v. 18.11.2024 - VI ZR 10/24, BGHZ 242, 180 Rn. 21). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft grundsätzlich die Person, die auf der Grundlage von Art. 82 Ziff. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH a.a.O Rn. 141, BGH, a.a.O m.w.N). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruches nach Art. 82 Ziff. 1 DSGVO ein Verschulden des Verantwortlichen. Art. 82 DSGVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DSGVO dem Verantwortlichen (vgl. EuGH, Urt. v. 11.04.2024 - C-741/21, NJW 2024, 1561 Rn. 44 ff. BGH, a.a.O m.w.N). Der europäische Gerichtshof stützt sich auf den 146. Erwägungsgrund, der auf „Schäden“ abstellt, „die einer Person aufgrund einer Verarbeitung entstehen“. Zwar muss der Schaden nicht eine gewisse

Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urt. v. 04.05.2023 - C - 300/21, 49, 50 - juris). Allerdings muss der Schaden tatsächlich und sicher entstanden sein (vgl. EuGH, Urt. v. 04.04.2017 - C - 337/15, Rn 91 - juris; vgl. OLG Dresden, Urt. v. 10.12.2024 - 4 U 732/24, Rn 17 - juris). Im Anschluss an die mittlerweile gefestigte Rechtsprechung des Bundesgerichtshofes (Urt. v. 18.11.2024 - VI ZR 10/24 - juris) und des EuGH (Urt. v. 04.09.2025 (C-655/23; Rn 60 - juris) kann bereits ein Kontrollverlust über personenbezogene Daten als Schaden angesehen werden, sofern die betroffene Person nachweist, dass sie tatsächlich einen solchen Schaden - so geringfügig er auch sein mag - erlitten hat, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (vgl EuGH, Urt. v. 04.09.2025 - C-655, Rn 60 - juris; s. insgesamt OLG Dresden a.a.O., Rn. 193 f.).

b) Die Beklagte verarbeitet die personenbezogenen Daten der Klagepartei ohne Rechtsfertigungsgrund gemäß Art. 6 Ziff. 1 DSGVO (s.o.).

aa) Zur Überzeugung des Gerichts steht fest, dass die Beklagte mithilfe der Meta-Business-Tools eine potenziell unbegrenzte Menge an Daten des Klägers verarbeitet, indem sie dessen Aktivitäten auf Dritt-Webseiten und Dritt-Apps verfolgt (vgl. auch EuGH, Urteil vom 04.07.2023 – C-252/21). Über die sog. Meta-Business-Tools erhält die Beklagte Daten, d. h. Kontaktinformationen und/oder Event-Daten (z. B. Besuche auf einer Webseite, Installation einer App, Kauf eines Produkts) von ihren Vertragspartnern, den sog. Drittanbietern.

Bestimmte technische Standarddaten gelangen automatisch an die Beklagte, wenn der Kläger eine Webseite aufruft, deren Anbieter die Business-Tools in seine Webseite eingebettet hat. Nach einer vereinfachten Darstellung des EuGH (vgl. EuGH, Urteil vom 29.07.2019 – C-40/17) ist es „eine Eigenart des Internets, dass der Browser des Internetbesuchers Inhalte aus verschiedenen Quellen darstellen kann. […] Hierzu übermittelt der Browser dem Server des Drittanbieters die IP-Adresse des Rechners dieses Besuchers sowie die technischen Informationen des Browsers, damit der Server feststellen kann, in welchem Format der Inhalt an welche Adresse auszuliefern ist. […]“.

Weitere (sog. Event-)Daten werden dann automatisch an die Beklagte übertragen, wenn der Drittanbieter bei der Einbettung der Business-Tools in seine Webseite oder App eine entsprechende Einstellung vorgenommen hat. Die Meta-Business-Tools-Nutzungsbedingungen verlangen in diesem Fall von dem Drittanbieter, die erforderlichen Angaben und Datenschutzbelehrungen zu erteilen und die notwendige Einwilligung einzuholen (vgl. Anlage B4). Die Beklagte über-

prüft dies nicht.

bb) 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 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.

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, werden die Daten dennoch – für andere Zwecke – verarbeitet, etwa zum Schutz der Sicherheit und Integrität der Server oder zur Messung der Effektivität von Werbekampagnen (vgl. Anlage K6).

Der Nutzer hat weiter die Möglichkeit, die Verknüpfung künftiger Aktivitäten mit seinem Konto aufzuheben und frühere Aktivitäten zu löschen. In diesem Fall erhält die Beklagte aber weiterhin Informationen zu seinen Aktivitäten, die für Messungen sowie zur Verbesserung der Werbesysteme verwendet werden.

cc) Aufgrund des von der Klagepartei geschilderten Surf- und Nutzerverhaltens ist davon auszugehen, dass der Kläger Seiten von Drittanbietern besucht, auf welchen Meta-Business-Tools geschaltet sind, und er demnach von der streitgegenständlichen Datenverarbeitung betroffen ist. Die Behauptung des Klägers, er verbringe wöchentlich mehrere Stunden im Internet und nutze eine Reihe von Webseiten und Apps, auf denen die Meta-Business-Tools vorzufinden seien, ist hinreichend substantiiert. Nachdem die Beklagte genau weiß, von welchen Drittseiten sie Informationen über Aktivitäten der Klägerin erhalten hat, könnte sie den Vortrag der Klagepartei konkret bestreiten.

Der Kläger kann und muss nicht wissen, auf welchen (Dritt-)Webseiten und Apps Meta-Business-Tools Verwendung finden, er darf sich insoweit auf Vermutungen stützen (vgl. BGH, Beschluss vom 20.05.2015 – IV ZR 127/14). Die Beklagte kann sich hingegen nicht auf ein pauschales Bestreiten beschränken, sie müsste konkret vortragen, weil (nur) sie es kann (vgl. § 138 Abs. 1, Abs. 2 ZPO). Dass der Kläger sich um eine gewisse Plausibilisierung seiner Vermutung

bemüht, indem er – gestützt auf Nachforschungen ihrer Prozessbevollmächtigten – vorträgt, dass allein Meta Pixel auf der ganz überwiegenden Mehrzahl der meistbesuchten 100 Webseiten Deutschlands verbaut sei (vgl. Anlagen K1, K4 und K5), gereicht ihm nicht zum Nachteil. Das pauschale Bestreiten dieses Vortrags als unsubstantiiert ist unwirksam.

dd) Der Kläger muss sich auch nicht darauf verweisen lassen, dass er die Möglichkeit hätte, durch den Abschluss einer kostenpflichtigen Abo-Version eine werbefreie Version des Angebots der Beklagten zu erhalten. Dass ihm dann keine Werbung mehr angezeigt wird, ändert nichts daran, dass die Beklagte weiterhin die persönlichen Daten erhält, die über Business-Tools über den Kläger von Drittanbietern an die Beklagte weitergegeben werden.

c) Der Kläger hat hierdurch einen Kontrollverlust über seine Daten erlitten. Er hat keine Kenntnis davon und keine Kontrolle darüber, auf welchen Webseiten welche Daten über Business-Tools der Beklagten erheben und weitergeben.

Wie bereits ausgeführt, ist die Datenverarbeitung durch die Beklagte besonders umfassend, da sie potenziell unbegrenzte Daten über die Online-Aktivitäten der Nutzer betrifft und das Gefühl auslösen kann, dass das Privatleben der Nutzer kontinuierlich überwacht wird (vgl. EuGH, Urt. v. 04.10.2024 - C-446/21 -, Rn 62, - juris). Dieses Gefühl des ständigen Überwachtwerdens ist eine nachteilige Folge, die über einen "bloßen" Kontrollverlust und die hiermit verbundenen Unannehmlichkeiten hinausgeht und daher einen immateriellen Schaden begründet (vgl. Meyer MMR 2025, 173 (177) m.w.N.). So berichtet der Kläger in seiner persönlichen Anhörung, dass es ihm mehrfach so vorkam, als ob ihm für Dinge, die er zuvor online recherchiert hatte, später auf Facebook Werbung angezeigt wurde.

Dies gilt umso mehr, als nach dem hier zugrunde zu legenden Vorbringen anzunehmen ist, dass auch bei verweigerter Einwilligung eines Nutzers über Business-Tools erlangte Daten zu einem Profiling im Sinne des Art. 22 DSGVO verwendet werden. Nach der Rechtsprechung des EuGH (Urt. v. 04.10.2024 – C-446/21 (Schrems) – juris, dort Rn 63) stellt das Erstellen detaillierter Profile der Nutzer in Verbindung mit der zeitlich unbegrenzten Weiterverarbeitung einen schweren Eingriff in die Grundrechte der betroffenen Nutzer, insbesondere auf Achtung ihres Privatlebens und den Schutz personenbezogener Daten dar (EuGH aaO. Rn 63). Dies gilt nach Auffassung des Gerichts auch in den Fällen – wie hier –, in denen nicht nachgewiesen ist, dass die über Business-Tools erlangten Daten für Zwecke der personalisierten Werbung verwendet werden. Dass vorliegend überdies nicht ausgeschlossen werden kann, dass durch die Business-Tools auch BKD im Sinne von Art. 9 Abs. 1 DSGVO von der streitgegenständlichen Datenverarbeitung betrof-

fen sind, verstärkt diesen Eindruck und kann dazu führen, dass Nutzer davon absehen, Webseiten etwa zu Gesundheitsthemen oder zum Sexualleben zu besuchen. Anders als in den sog. Scraping-Fällen werden vorliegend zwar die über die Business-Tools erlangten Daten nicht im Internet veröffentlicht, sondern lediglich bei der Beklagten verknüpft und gespeichert. Im Unterschied zu den Scraping-Sachverhalten, bei denen es im Wesentlichen um die Verknüpfung von Telefonnummer und/oder E-Mail-Anschrift mit einem Facebook-Nutzerkonto geht, erfasst die Verarbeitung von Daten aus den Business-Tools aber eine unabsehbare Vielzahl personenbezogener Daten, darunter je nach Einzelfall auch Gesundheitsdaten oder Daten zur sexuellen Orientierung. Des Weiteren ist die nicht bestehende Möglichkeit der Klagepartei, durch eigenes Handeln die Kontrolle über diese Daten zurückzuerlangen zu berücksichtigen (zu diesen Kriterien vgl. OLG Dresden, Urt. v. 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688 Rn. 20, beck-online). Insofern kann vorliegend nicht außer Betracht bleiben, dass weder durch die Änderung der Datenschutzeinstellungen noch durch die Löschung des Kontos eine vollumfängliche Löschung der bei der Beklagten gespeicherten Daten möglich wäre. Das Gericht geht nach alledem davon aus, dass bereits dieser abstrakt bestehende Kontrollverlust in Verbindung mit dem nachvollziehbar hieraus abgeleiteten Unsicherheitsgefühl für einen immateriellen Schaden ausreicht, ohne dass die Klagepartei diesen noch weiter individualisieren müsste. Die sehr umfassende Verarbeitung von personenbezogenen Daten durch die Beklagte sowie das allgemeine Gefühl der Beobachtung im privaten Umfeld sind ohne weiteres geeignet, bei jedem davon betroffenen Nutzer negative Gefühle in Form von Sorge und Ärger auszulösen, weshalb diese Empfindungen bei der Bemessung des immateriellen Schadens berücksichtigt werden können, ohne dass es auf weiteren Vortrag ankommt, welche Daten genau erhoben worden sind (so wohl auch Ehmann/Selmayr/Nemitz, 3. Aufl., DS-GVO Art. 82 Rn. 17; Kühling/Buchner/Bergt, 4. Aufl., DS-GVO Art. 82 Rn. 18c). Das unbestimmte Gefühl einer Überwachung ihres Verhaltens nicht nur im Internet liegt nachvollziehbar darin begründet, dass die Klägerseite nicht weiß und auch nicht wissen kann, welche und wie viele Daten die Beklagte aus ihrer Privat- und Intimsphäre über sie gesammelt hat und auch nicht weiß und wissen kann, was die Beklagte mit diesen Daten macht (so auch LG Leipzig, Urt. v. 04.07.2025 - 5 O 2351/23 -, Rn. 72 ff., Juris; s. OLG Dresden, a.a.O., Rn. 197).

Eine Überzeugung dahingehend, dass der Kläger die Möglichkeit hätte, die Kontrolle über seine Daten selbständig zurückzuerlangen, hat sich das Gericht schon deshalb nicht bilden können, weil die Beklagte die bei ihr 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.

d) Die Schadenshöhe schätzt das Gericht im Rahmen seines Ermessens nach § 287 ZPO auf 5.000 EUR.

Im Rahmen der nach § 287 ZPO vorzunehmenden Schadensschätzung sind im Rahmen des Art. 82 DS-VGO allgemein die Art, Schwere, Dauer des Verstoßes, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der betroffenen personenbezogenen Daten in die Erwägung mit einzubeziehen.

aa) Eine auf Art. 82 DSGVO gestützte Entschädigung in Geld ist als vollständig und wirksam anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 I DS-GVO dagegen nicht erfüllen (vgl. BGH, Urteil vom 18.11.2024 – VI ZR 10/24).

Folglich darf weder die Schwere des Verstoßes gegen die DSGVO, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen und ob er vorsätzlich gehandelt hat. Schließlich wurde bei der Schätzung des Schadens der Grad des Verschuldens nicht berücksichtigt.

Der Kläger hat zumindest Themenkreise dargelegt, zu denen er im Internet aktiv ist, auch wenn er die entsprechenden konkreten Webseiten nicht vollständig offengelegt hat. Er hat dies im Rahmen seiner informatorischen Anhörung bestätigt. Das Gericht geht deshalb davon aus, dass eine erhebliche Menge an Informationen verarbeitet wurde und darunter auch sensible Daten i. S. v. Art. 9 DSGVO waren. Demgegenüber ist zwar der Empfängerkreis der Daten vorliegend begrenzt: Er umfasst die Beklagte und solche Dritte, mit denen sie bestimmte Informationen teilt. Frei im Internet verfügbar sind die Daten danach nicht. Ausweislich der Datenschutzrichtlinie der Beklagten behält die Beklagte aber Daten so lange, wie sie benötigt werden, um die Produkte der Beklagten bereitzustellen, rechtliche Verpflichtungen zu erfüllen oder bestimmte Interessen zu schützen. Es ist damit – auch in zeitlicher Hinsicht – von einem erheblichen Kontrollverlust auszugehen. Weiter berücksichtigt wurde, welchen Zwecken die Verarbeitung der Daten nach der Datenschutzrichtlinie der Beklagten dient.

Im Falle der mehrtägigen Überwachung einer Privatperson durch eine Detektei hat das Bundesarbeitsgericht einen Schadensersatzbetrag in Höhe von 1.500 EUR für angemessen erachtet (BAG Urteil vom 25. Juli 2024 - 8 AZR 225/23 -, NJW 2025, 100). Im Fall des Ausspähens persönlicher Daten im Rahmen einer verdeckten "Recherche" hat das Oberlandesgericht Dresden einen Be-

trag von 5.000 EUR zuerkannt (OLG Dresden, Urteil vom 30. November 2021 - 4 U 1158/21 -, Juris). In den bereits entschiedenen Fällen, die mit dem hiesigen gleichgelagert waren, wurden Beträge zwischen 10.000 EUR (insb. LG Mainz, Urteil vom 27. Juni 2025 - 3 O 29/24, GRUR-RS 2025, 16871; LG Ellwangen Urt. v. 9.4.2025 – 2 O 266/24, GRUR-RS 2025, 16870) und 5.000 EUR zugesprochen (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264).

bb) Daran gemessen erachtet das Gericht hier einen Schadensersatzbetrag von 5.000 EUR für angemessen. Es handelt sich bei dem festgestellten Datenschutzverstoß um eine schwere Verletzung des Rechts auf informationelle Selbstbestimmung, da das gesamte, höchstpersönliche Internetnutzungsverhalten betroffen ist (vgl. oben). Dabei handelt es sich auch nicht nur um eine punktuelle, zeitlich begrenzte rechtswidrige Maßnahme der Beklagten, sondern um einen sich über einen großen, mehrjährigen Dauerverstoß gegen grundlegende Rechte nach der DSGVO. Dieser Verstoß betraf auch Daten, die einen hohen Marktwert haben (LG Lübeck, Urteil vom 27. November 2025 – 15 O 15/24 – Rn. 142-144, juris). Überzeugend führt hierzu das Landgericht Leipzig aus:

"(...) Für den Wert der Daten für die Beklagte hat das Gericht auf die Feststellungen des BKartA (Beschl. v. 2.5.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) zurückgegriffen. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der Werbeeinnahmen einen Anteil i.H.v. 97 % ausmachte (BKartA a.a.O., Rn. 7). Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O., Rn. 53). Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon überzeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studi-

en (siehe nur die Studie "Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?", Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz; Infografik "Preis, den Erwachsene in den USA für personenbezogene Daten aufrufen würden (in US-Dollar)", Statista mit Quelldaten von Morning ... Consult aus dem Jahr 2019, abgerufen unter https://cdn.statcdn.com/Infographic/images/normal/18449.jpeg). Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d.h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18b, beck-online)." (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264, Rn. 85)

Hinzu kommt, dass die Klägerseite von der Beklagtenseite keine praktikablen Wege aufgezeigt bekommt, die Kontrolle über die von der Beklagten erlangten Daten wiederzuerhalten. Die Beklagte stellt der Klägerseite schon keine aussagekräftigen Informationsmöglichkeiten zur Seite, mit der diese verlässliche Kenntnis davon erlangen könnte, welche konkreten Daten die Beklagte über sie gespeichert hat (vgl. oben), und ist auch ersichtlich nicht zur nachvollziehbaren Löschung dieser Daten bereit. Soweit im Übrigen in der veröffentlichten Rechtsprechung den Meta-Nutzerinnen bzw. -Nutzern immer wieder vorgehalten wird, sie könnten auf die Nutzung der Meta-Produkte verzichten, überzeugt das das Gericht nicht ansatzweise. Sinn und Zweck der DSGVO ist es gerade, allen europäischen Bürgern ein einheitliches und hohes Datenschutzniveau bezüglich aller auf dem europäischen Markt zugelassener Anwendungen, auch Social-Media-Produkten, zu gewährleisten. Die Argumentation, die Nutzer sollten eben auf diese Anwendungen verzichten, wenn dort Verletzungen des DSGVO stattfinden, führt diesen Regelungsabsatz ersichtlich ad absurdum (s. LG Lübeck, Urteil vom 27. November 2025 – 15 O 15/24 – Rn. 146, juris). Überzeugend führt hierzu auch das Landgericht Leipzig aus:

"Nicht anspruchsmindernd i.S.e. widersprüchlichen Verhaltens wirkt sich aus, dass der Kläger die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Die Beklagte nimmt im Bereich der Social-Media-Plattformen eine überragende marktübergreifende Stellung ein, welche bereits das Bundeskartellamt i.S.v. § 19a GWB festgestellt hat (BKartA, Beschl. v. 02.05.2022, Az. B6-27/21). Gerade für die Teilhabe am gesellschaftlichen Leben handelt es sich bei den Netzwerken der Beklagten mittlerweile um für den durchschnittlichen Bürger essenzielle Dienstleistungen (vgl. Erwägungsgründe Nr. 1, 3 zur VO 2022/2065), die faktisch nicht

durch ein alternatives Netzwerk ersetzt werden können (zusammenfassend zu den Hintergründen siehe Mohr, EuZW 2019, 265 unter Bezugnahme auf die F.-Entscheidung des Bundeskartellamts vom 06.02.2019). Auch wenn der Nutzer Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, ist es ihm deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass der Kläger ihre Netzwerke DSGVO-konform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt der Kläger zum Ausdruck, dass ihm die Datenschutzverstöße der Beklagten nicht egal sind, sondern er eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es dem Kläger hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, sein Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden (vgl. Paal, ZfDR 2023, 325)." (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264, Rn. 95)"

Auch diese Ausführungen macht sich das Gericht zu eigen.

Der vorliegende Fall ist mit dem der zitierten Entscheidung des Landgerichts Leipzig vom Niveau der erlittenen Beeinträchtigung vergleichbar: Der Kläger beschreibt - nicht substantiiert bestritten - ein eher datensparsames Nutzungsverhalten im Internet. Er macht kein Online-Banking, lehnt Cookies konsequent ab, sein Profil bei Facebook ist auf „privat“ gestellt. Trotz dieser Datensparsamkeit kann der Kläger bei durch seine DrittseitenNutzung (OnlineShops, Zahlungsdienst) über BusinessTools eine profilbildende, plattformübergreifende Erfassung nicht verhindern. Das steigert die Intensität des Eingriffs, der in einer umfassenden und vom Kläger nicht kontrollierten Zusammenführung seiner Daten liegt. Der Kläger hat durch seine konsequente Ablehnung von Cookies und private Profileinstellungen ein erhöhtes Schutzinteresse dokumentiert. Dass trotzdem Daten über die BusinessTools der Beklagten erfasst werden, verstärkt den empfundenen Kontrollverlust, der sich hier besonders in dem Widerspruch zwischen erkennbarer Schutzintention und faktischer Erfassung zeigt.

cc) Eine höhere immaterielle Entschädigung hätte die auf den Einzelfall bezogene Darlegung der Klagepartei erfordert, infolge der streitgegenständlichen Datenverarbeitung eine psychische Beeinträchtigung erlitten zu haben. Unabhängig vom Nachweis eines Kontrollverlusts reicht für einen Anspruch auf einen immateriellen Schadensersatz nämlich auch die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, um einen Schadensersatzanspruch zu begründen (vgl. EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 67 – MediaMarktSaturn;

vom 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 85 – Natsionalna agentsia za prihodite). Die Befürchtung samt ihren negativen Folgen muss dabei ordnungsgemäß nachgewiesen sein (vgl. EuGH, Urt. v. 20.07.2024 – C-590/22, DB 2024,1676 Rn. 36 – PS GbR; vom 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 75-86 – Natsionalna agentsia za prihodite). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (vgl. EuGH, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 35 – PS GbR; v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 68 – MediaMarktSaturn). Sind derartige psychische Beeinträchtigungen infolge einer Anhörung des Betroffenen nachgewiesen, ist der Entschädigungsbetrag in einer Höhe festzusetzen, die über dem im Falle eines bloßen Kontrollverlustes zuzusprechenden Betrag liegt (BGH, Urt. v. 18.11.2024 – Rn VIII 2 c) cc)). Zu einer solchen emotionalen Betroffenheit hat die Klagepartei jedoch keinerlei individualisierbare Anhaltspunkte vorgetragen; der Vortrag ihrer Prozessbevollmächtigten ist vielmehr identisch mit demjenigen in zahlreichen Parallelverfahren (vgl. auch OLG Dresden, Urteil vom 3. Februar 2026 – 4 U 292/25 –, juris Rn. 198).

e) Ein darüber hinausgehender 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.

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 (vgl. BGH, Urteil vom 12.03.2024 – VI ZR 1370/20).

Vorliegend ist jedoch mit der informationellen Selbstbestimmung ein besonderer (Teil-)Gehalt des allgemeinen Persönlichkeitsrechts betroffen. Zwar kann auch die Verletzung des Rechts auf informationelle Selbstbestimmung einen Entschädigungsanspruch begründen (so wohl auch BGH, Urteil vom 12.03.2024 – VI ZR 1370/20). Auch insoweit müsste aber ein schwerwiegender Eingriff in das allgemeine Persönlichkeitsrecht nachgewiesen sein und die Beeinträchtigung dürfte nicht in anderer Weise aufgefangen werden können.

Ein schwerwiegender Eingriff i. S. d. genannten Rechtsprechung wurde vorliegend von der Klagepartei jedoch nicht vorgetragen. Entscheidend ist dabei, dass die Klagepartei nicht im Kernbereich der Persönlichkeit betroffen ist und dass sie betreffende Daten nicht in die allgemeine Öffentlichkeit gelangt sind. Der Umfang der Datenverarbeitung allein und die Tatsache, dass von ei-

nem vorsätzlichen Verhalten auszugehen ist, begründen die notwendige besondere Schwere des Eingriffs nicht.

Hinzu kommt, dass Art. 82 DSGVO für Eingriffe in das Recht auf informationelle Selbstbestimmung gerade einen Schadensersatzanspruch bereithält. Durch die ihr zugesprochene Entschädigung für den erlittenen Kontrollverlust wird die von der Klagepartei erlittene Beeinträchtigung befriedigend aufgefangen.

f) Der Anspruch auf Zinsen seit Rechtshängigkeit ergibt sich aus §§ 291, 288 BGB. Bereits zuvor stehen dem Kläger Verzugszinsen aus §§ 286, 288 BGB zu, nachdem mit Schreiben des Prozessbevollmächtigten des Klägers (Anlage K7) der Beklagte eine Frist bis zum 25.03.2024 zur Zahlung des Schmerzensgeldes gesetzt wurde. Der Tenor wird durch den Antrag beschränkt.

6. Der Klagepartei steht schließlich ein Anspruch auf Ersatz vorgerichtlicher Anwaltskosten in tenorierter Höhe zu. Dieser beruht auf Art. 82 Abs. 1 DSGVO.

Das Gericht hat dabei einen berechtigten Gegenstandswert in Höhe von 6.000,00 € im Hinblick auf den Zahlungsanspruch und den Unterlassungsanspruch zugrunde gelegt (zum Streitwert s.u.).

Die Beklagte hat – wie ausgeführt – ihre Pflichten aus dem Vertragsverhältnis mit der Klageseite verletzt, sodass dieser ein Schadenersatzanspruch zusteht, der auch die Kosten der Mandatierung eines Rechtsanwalts umfasst. Dass dieser mandatiert wurde, ergibt sich jedenfalls aus dem Abmahnschreiben vom 04.03.2024 (vgl. Anlage K7).

Daher kann sich auch aus Art. 82 DSGVO unter diesen Voraussetzungen ein Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten ergeben (BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 79 f.). Es erscheint gerade im Hinblick darauf, dass zum Zeitpunkt des vorgerichtlichen Tätigwerdens eine Vielzahl von Rechtsfragen in Zusammenhang mit Art. 82 DSGVO noch ungeklärt waren, aus Sicht der Klagepartei höchst nachvollziehbar, sich zur Durchsetzung ihrer Ansprüche eines Rechtsanwalts zu bedienen (vgl. auch BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 80; s. Landgericht Berlin II, Urteil vom 11.04.2025, Az. 58 O 72/24, Anlage K9-4).

III.

Die Kostenentscheidung folgt aus § 92 Abs. 1 Satz 1 ZPO.

IV.

Die Entscheidung hinsichtlich der vorläufigen Vollstreckbarkeit beruht auf §§ 709 S. 1 ZPO.

V.

Der Streitwert beruht auf den Angaben der Parteien (vgl. §§ 3, 4, 5 ZPO).

Zur Festsetzung des Streitwertes sind die einzelnen Klageanträge orientiert am wirtschaftlichen Interesse der Klagepartei nach freiem Ermessen des festsetzenden Gerichts gemäß § 48 Abs. 1 Satz 1 GKG, § 3 ZPO zu bewerten und nach § 39 GKG sodann deren Einzelwerte aufzuaddieren.

Hierbei bilden die Parteiangaben ein gewichtiges Indiz. Allerdings besteht keine Bindung des Gerichts an die Parteiangaben (vgl. Hüßtege, in: Thomas/Putzo, ZPO, 46. Aufl. 2025, § 2 Rn. 24).

Das Unterlassungsbegehren ist mit 1.000,00 € zu bewerten. Der Streitwert der Unterlassungsanträge ist als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses der Klagepartei zu bestimmen, wobei gemäß § 48 Abs. 2 Satz 1 GKG alle Umstände des Einzelfalls zu beachten sind.

Der Auskunftsantrag soll die behauptete Ungewissheit beseitigen und ist daher wie der Unterlassungsantrag mit 1.000,00 € zu bewerten.

Der Löschungsantrag soll den behaupteten rechtswidrigen Zustand beseitigen. Er ist daher wie der Unterlassungsantrag mit 1.000,00 € zu bewerten.

Der Antrag auf Zahlung immateriellen Schadensersatzes ist mit dem bezifferten Mindestbetrag in Ansatz zu bringen (vgl. § 48 Abs. 1 Satz 1 GKG i. V. m. § 3 ZPO). Bei der Leistungsklage ist der formulierte Antrag wertbestimmend (vgl. Herget, in: Zöller ZPO, 36. Aufl. 2026, § 3 Rn. 16.112). Dieser Mindestbetrag beträgt ausweislich der Klageschrift 5.000,00 €.

Der Antrag auf Zahlung von vorgerichtlichen Anwaltskosten wirkt sich nicht streitwerterhöhend aus, § 43 I GKG.

Demnach ergibt sich ein Gesamtstreitwert in Höhe von 8.000,00 €.

VI.

Etwaiger neuer Tatsachenvortrag der Klagepartei in dem nicht nachgelassenen Schriftsatz vom 06.03.2026 war vorliegend nach § 296a ZPO verspätet und daher zurückzuweisen; rechtliche

Ausführungen wurden berücksichtigt.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht München I
Prielmayerstraße 7
80335 München

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem vierten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen
- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:
- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils

geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

[redacted]