Beglaubigte Abschrift

OBERLANDESGERICHT NAUMBURG

IM NAMEN DES VOLKES

URTEIL

9 U 20/25 OLG Naumburg
10 O 71/24 LG Magdeburg

verkündet am: 23. April 2026

[redacted] JOS
als Urkundsbeamter
der Geschäftsstelle

In dem Rechtsstreit

[redacted]

Kläger und Berufungskläger,

Prozessbevollmächtigte:
BK Automotive Rechtsanwaltsgesellschaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin,
Geschäftszeichen: DTS-008399-IUS

gegen

Meta Platforms Ireland Limited, vertreten durch Board of Directors,
Merrion Road Dublin 4, IRL D04 X2K5 Dublin // Ireland,

Beklagte und Berufungsbeklagte,

Prozessbevollmächtigte:
[redacted]

hat der 9. Zivilsenat des Oberlandesgerichts Naumburg auf die mündliche Verhandlung vom 24. März 2026 durch den Richter am Oberlandesgericht Becker, die Richterin am Oberlandesgericht Mederake und den Richter am Oberlandesgericht Nourney für Recht erkannt:

I. Auf die Berufung des Klägers wird das am 16. Januar 2025 verkündete Urteil des Landgerichts Magdeburg wie folgt abgeändert:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche personenbezogenen Daten sie seit dem 9. November 2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Instagram“ unter dem Benutzernamen „[redacted]“ des Klägers verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business-Tools“ sowie ob und wenn ja, welche konkreten Daten des Klägers die Beklagte seit dem 9. November 2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1. seit dem 9. November 2018 bereits gespeicherten personenbezogenen Daten des Klägers vollständig zu löschen.

3. Die Beklagte wird verurteilt, an den Kläger 1.500,00 EUR nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 07.02.2024 zu zahlen.

4. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von 453,87 EUR freizustellen.

5. Die weitergehende Klage wird abgewiesen.

II. Im Übrigen wird die Berufung zurückgewiesen.

III. Von den Kosten des Rechtsstreits erster Instanz trägt der Kläger 57 v. H. und die Beklagte 43 v. H. Von den Kosten des Berufungsverfahrens trägt der Kläger 15 v. H. und die Beklagte 85 v. H.

IV. Das Urteil ist vorläufig vollstreckbar.

Gründe:

I.

1.
Der Kläger (nf. „Klagepartei") macht Auskunfts-, Löschungs- und Schadenersatzansprüche aufgrund eines vermeintlich unerlaubten, fortlaufenden und unkontrollierten Datenabgriffs durch die Beklagte im Rahmen der Nutzung der Plattform „Instagram" geltend.

Die Beklagte betreibt die Social-Media-Plattform Instagram. Der Kläger ist seit dem 09.11.2018 dort Mitglied unter dem Namen „[redacted]".

Das Landgericht Magdeburg hat die Klage vollumfänglich abgewiesen. Hiergegen richtet sich die Berufung der Klagepartei, wobei sie bzgl. des Schadenersatzes nur noch eine Mindestsumme von 1.500,00 EUR statt wie erstinstanzlich 5.000,00 EUR beansprucht.

Von der weiteren Darstellung eines Sachverhalts wird nach §§ 540 Abs. 2, 313a Abs. 1 S. 1 ZPO, 544 Abs. 2 Nr. 1 ZPO abgesehen.

2.
Der Senat hat die Klagepartei in der Verhandlung am 24.03.2026 persönlich angehört. Er hat dort angegeben, 3-5 Stunden/Tag das Internet zu nutzen. Er recherchiere über Google, auch zu Krankheiten. Als sensible Seiten benannte er den Besuch von Pornoseiten und Onlinebanking. Bei Anmeldung – seinerzeit im Alter von 13 Jahren – habe er kein Bewusstsein über Datennutzung gehabt. Die Datenschutzerklärung habe er seinerzeit nicht gelesen. Er fühle sich machtlos und habe sein Surfverhalten angepasst. Auch habe er seine Browser gewechselt und eine Passwortsicherung installiert.

II.

Die Berufung der Klagepartei ist form- und fristgerecht eingelegt (§§ 517, 519 ZPO) und begründet (§ 520 ZPO) worden und auch im Übrigen zulässig. Der Klagepartei stehen gegen die Beklagte Ansprüche auf Auskunft, Löschung und Schadensersatz im tenorierten Umfang zu.

A.

Die deutschen Gerichte sind, wie das Landgericht rechtsfehlerfrei festgestellt hat, international zuständig.

1.

Die Klagepartei hat ihren gewöhnlichen Aufenthalt in der Bundesrepublik Deutschland, so dass die – auch unter der Geltung von § 513 Abs. 2 ZPO zu prüfende (vgl. z. B. BGH, Urteil vom 17. März 2025, VI ZR 11/14, Rn. 14, juris) – internationale Zuständigkeit deutscher Gerichte aus Art. 82 Abs. 6 i. V. m. Art. 79 Abs. 2, S. 2 DSGVO folgt (vgl. zuletzt: BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 12, juris). Ebenso ergibt sich die internationale Zuständigkeit aus Art. 17 Abs. 1 lit. c, 18 Abs. 1 Brüssel Ia-VO, da die Klagepartei als Verbraucherin gehandelt hat.

2.

Der sachliche, räumliche und zeitliche Anwendungsbereich der am 25. Mai 2018 in Kraft getretenen Datenschutzgrundverordnung ist eröffnet. Der sachliche Anwendungsbereich folgt aus Art. 2 Abs. 1 DSGVO, der für die automatisierte Verarbeitung personenbezogener Daten gilt. Da die Klagepartei bei der Beklagten einen Instagram-Account unterhält, verarbeitet die Beklagte folgerichtig auch die von der Klagepartei angegebenen und eingegebenen personenbezogenen Daten der Klagepartei. Die Eröffnung des räumlichen Anwendungsbereichs der DSGVO beruht auf ihrem Art. 3 Abs. 1, der auf die Verarbeitung personenbezogener Daten Anwendung findet, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen in der Europäischen Union erfolgt. Bei der Beklagten handelt es sich um ein Unternehmen nach dem Recht der Irischen Republik mit Sitz in Irland.

3.

Da die Beklagte das soziale Netzwerk Instagram für Nutzer in der Europäischen Union betreibt, ist sie auch Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO, und zwar auch und entgegen ihrer Ansicht, soweit über die streitgegenständlichen Business-Tools die Daten auch durch die Drittanbieter verarbeitet werden. Der Begriff „Verantwortlicher“ wird in Art. 4 Nr. 7 DSGVO weit definiert als die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, die Daten für sich verarbeitet oder für sich durch andere Personen oder Stellen verarbeiten lässt (Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DSGVO)/

Bundesdatenschutzgesetz (BDSG), Dezember 2025, Art. 4 EUV 2016/679, Rn. 145; EuGH, Urteil vom 2. Dezember 2025, C-492/23, Rn. 56, zuvor bereits Urteil vom 29. Juli 2019, Fashion ID, C-40/17, Rn. 74; juris).

a)
Der EuGH sieht eine weite Definition zur Verantwortlicheneigenschaft i.S.d. Art. 4 Abs. 7 DSGVO (Urteil vom 5. Dezember 2023, C-683/21, Rn. 29 und die dort angeführte Rechtsprechung, juris). Danach kann jede natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung solcher Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als für diese Verarbeitung Verantwortlicher angesehen werden (EuGH, a. a. O., Rn. 30, juris).

Zudem verweist der Begriff des „Verantwortlichen", da er sich, wie Art. 4 Nr. 7 DSGVO ausdrücklich vorsieht, auf die Stelle bezieht, die *„allein oder gemeinsam mit anderen"* über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, nicht zwingend auf eine einzige Stelle und kann mehrere an dieser Verarbeitung beteiligte Akteure betreffen, wobei dann jeder von ihnen den Datenschutzvorschriften unterliegt (vgl. in diesem Sinne noch zur RL 95/46/EG EuGH, Urteil vom 29. Juli 2019, C-40/17, Rn. 67, juris).

Art. 26 DSGVO, der sich in den begrifflichen Rahmen des „Verantwortlichen" nach Art. 4 Nr. 7 DSGVO einfügt, sieht im Wesentlichen vor, dass zwei oder mehr Verantwortliche, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, als *„gemeinsam Verantwortliche"* für diese Verarbeitung einzustufen sind.

Eine solche gemeinsame Verantwortlichkeit erfordert nicht notwendigerweise das Vorliegen gemeinsamer Entscheidungen über die Festlegung der Zwecke und Mittel der Verarbeitung der betreffenden personenbezogenen Daten. Der EuGH hat nämlich entschieden, dass die Mitwirkung an der Entscheidung über diese Zwecke und Mittel verschiedene Formen annehmen und sich sowohl aus einer gemeinsamen Entscheidung von zwei oder mehr Einrichtungen als auch aus übereinstimmenden Entscheidungen ergeben kann, die sich in einer Weise ergänzen, dass sich jede von ihnen konkret auf die Festlegung der Verarbeitungszwecke und -mittel auswirkt (vgl. in diesem Sinne Urteil vom 5. Dezember 2023, C-683/21, Rn. 43, juris).

Insoweit setzt die gemeinsame Verantwortlichkeit mehrerer Akteure für dieselbe Verarbeitung nach Art. 4 Nr. 7 DSGVO nicht voraus, dass jeder von ihnen Zugang zu den betreffenden personenbezogenen Daten hat (EuGH, Urteile vom 29. Juli 2019, Fashion ID, C-40/17, Rn. 69, vom 5. Dezember 2023, C-683/21, Rn. 42, juris).

In demselben Sinne hat der EuGH klargestellt, dass aus einer gemeinsamen Verantwortlichkeit nicht zwangsläufig folgt, dass die verschiedenen Akteure für dieselbe Verarbeitung personenbezogener Daten eine gleichwertige Verantwortlichkeit trifft. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist (EuGH, Urteile vom 10. Juli 2018, C-25/17, Rn. 66; vom 5. Dezember 2023, C-683/21, Rn. 42; vom 2. Dezember 2025, C-492/23, Rn. 57 - 63; OGH Wien, Urteil vom 26. November 2025, 6Ob189/24y, Rn. 84, 89, juris).

b)
Nach dieser Einschätzung ist die Beklagte als diejenige, die die Business-Tools den Drittwebseiten und Apps bereitstellt, auch als diejenige anzusehen, die über die Zwecke und Mittel der Verarbeitung dieser Daten hauptsächlich entschieden hat, und daher „Verantwortliche“ im Sinne von Art. 4 Nr. 7 DSGVO.

Die Beklagte trägt hierzu selbst vor, dass Drittunternehmen die von ihr entwickelten Business-Tools auf ihren Websites oder Apps integrieren und sich dazu entscheiden können, Kundendaten durch die von ihr bereitgestellte Software mit der Beklagten zu teilen, um bessere und interaktivere Inhalte und Werbeanzeigen zu erstellen und ein (größeres) Publikum für Werbekampagnen aufzubauen (z. B. Rn. 1 ff. Berufungserwiderung). Ob sich daraus für diese Unternehmen eigene Pflichten aus der DSGVO ergeben, kann hier dahinstehen, weil die von den Dritten erhobenen Daten jedenfalls zweckgerichtet mit der Beklagten in unterschiedlichem Umfang geteilt und von ihr sodann – wie sie in der mündlichen Verhandlung bestätigt hat – auch verarbeitet werden. Eine Verarbeitung liegt insbesondere auch dann vor, wenn die Beklagte die Daten, deren Nutzung durch das Setzen von Cookies untersagt wurde, sichtet, um sie zu löschen oder für weitere, von ihr definierte Verarbeitungszwecke zu behalten. Ob diese Daten dabei anonymisiert oder sonst verfremdet werden, kann dahinstehen. Im Ergebnis führt die Weitergabe zu einer Personalisierung der von den Drittanbietern gehashten Nutzerdaten bei der Beklagten und damit zu einer erneuten Nutzung dieser Daten durch die Beklagte. Die Kontrolle über die Programmierung und in der Folge über die Funktionalität des Tools verbleibt nach dem Konzept jedenfalls auch bei

der Beklagten. Diese entscheidet (mit), welche Daten erhoben und übermittelt werden. Dass eine „gemeinsame Verantwortlichkeit für die Datenverarbeitung mit dem jeweiligen Drittunternehmen gem. der DSGVO betreffend die Erhebung und Übermittlung zusätzlicher Daten an die Drittunternehmen über gewisse Business-Tools“ besteht, hat die Beklagte im Übrigen auch eingeräumt (vgl. die Nutzungsbedingungen für die Business-Tools in Anlage B5, dort S. 5; ebenso: EuGH, Urteil vom 13. Mai 2014, C-131/12, juris; OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25 e, Rn. 212, beck-online; OLG Dresden, Urteil vom 3. Februar 2026, 4 U 292/25, Rn. 169; OLG Jena, Urteil vom 2. März 2026, 3 U 31/25, Rn. 180, juris; OGH Österreich, Urteil vom 26. November 2025, 6 Ob 189/24, BeckRS 2025, 34948 Rn. 84, beck-online).

Dieser Umstand ist der Beklagten auch bewusst, da sie ihre Nutzer um eine entsprechende Einwilligung bei der Einstellung „*Informationen über Aktivitäten von Werbepartnern*“ bittet und gegen Gebühr auch eine werbefreie Nutzung von Instagram als werbefreies Abonnement anbietet.

Die Speicherung und (Weiter-)Verarbeitung nimmt die Beklagte auch nicht lediglich als Auftragsverarbeiterin im Sinne von Art. 28 DSGVO für Dritte wahr. Sie ist es selbst, die durch die Programmierung ihrer Tools allein über den Umfang der Möglichkeiten Dritter bestimmt, welche personenbezogenen Daten überhaupt erfasst werden können. Derartiges regelt die Beklagte zwar etwa in Ziff. 5 lit a. i. ihrer Nutzungsbedingungen, wonach sie gegenüber Dritten hinsichtlich bestimmter Zwecke nur als Auftragsverarbeiterin gesehen werden will (Anlage B 5). Eine solche Vertragsgestaltung im Innenverhältnis zwischen der Beklagten und Dritten ist aber nicht geeignet, über das insoweit zwingende Gesetzesrecht der Art. 4 Nr. 7 und Art. 28 DSGVO mit Wirkung für die Rechte Betroffener zu disponieren. Maßgeblich sind insoweit nicht die vertraglichen Bezeichnungen der Rollen, sondern die anhand der Regelungen der DSGVO zu bewertenden tatsächlichen Verhältnisse (Kühling/Buchner/Hartung, 4. Aufl. 2024, DSGVO Art. 28 Rn. 27). Diese ergeben eine umfassende und alleinige Entscheidungsbefugnis der Beklagten darüber, ob und wenn ja welche personenbezogenen Daten mittels ihrer Tools erfasst und an sie übermittelt werden können und sodann von ihr gespeichert und weiterverarbeitet werden. Entsprechend behält sich die Beklagte gegenüber Dritten auch das Recht vor, jederzeit deren Zugriff auf die „Business-Tools“ zu ändern, auszusetzen oder zu beenden (Ziff. 4 lit. a der Nutzungsbedingungen, Anlage B 5). Insbesondere eine solche Befugnis schließt es aus, sie lediglich als Auftragsverarbeiterin einzuordnen. Sie allein ist damit Herrin über das Mittel der Datenverarbeitung, wie sich auch aus Nr. 5 lit. a. ii ihrer Nutzungsbedingungen ergibt. Auch den Zweck

der Datenverarbeitung bestimmt im Wesentlichen sie, indem sie ihre „Business-Tools“ maßgeblich damit bewirbt, die Effizienz von Werbemaßnahmen Dritter auf ihren Plattformen steigern zu können, was zugleich dem eigennützigen Zweck dient, die Attraktivität dieser Plattformen als Werbemedium überhaupt zu fördern und damit die eigene Profitabilität (vgl. hierzu OLG Jena, Urteil vom 2. März 2026, 3 U 31/25, Rn. 182, juris).

4.
Auch der zeitliche Anwendungsbereich der DSGVO (Art. 99 Abs. 2 DSGVO) ist eröffnet, weil die hier in Rede stehenden Verstöße nach deren Inkrafttreten am 25. Mai 2018 erfolgt sind. Nur für diesen Zeitraum macht die Klagepartei Ansprüche geltend, weil sie erst danach der Plattform beigetreten ist.

5.
Neben der DSGVO ist auf das Rechtsverhältnis der Parteien gemäß Art. 3 Abs. 1, Art. 6 Abs. 2 Rom I-VO und nach den Nutzungsbedingungen der Beklagten deutsches Recht anwendbar. Die Anwendbarkeit deutschen Rechts ergibt sich im Übrigen auch aus Art. 6 Abs. 1 lit. b) Rom I-VO, weil ein Verbrauchervertrag vorliegt.

B. Klageantrag zu 1 (Auskunftsantrag)

Die Klagepartei hat einen Anspruch auf Auskunft gemäß Art. 15 Abs. 1 DSGVO im tenorierten Umfang.

1.
Der Klagepartei steht der geltend gemachte Auskunftsanspruch aus Art. 15 Abs. 1 DSGVO allerdings nicht mehr zu, soweit sie nach der Übertragung der Daten an Dritte (lit. a), b) und c) sowie zur automatisierten Entscheidungsfindung (Teil 3 des Antrags zu Ziff. 1) fragt. Die erste Frage hat die Beklagte bereits mit Schreiben vom 7. Juni 2024 (Anlage B 8, dort S. 9) dahin beantwortet, dass ihr auf der Grundlage ihrer verfügbaren Informationen keine Aufzeichnungen über individuelle Empfänger der personenbezogenen Daten der Klagepartei vorliegen. Die Beklagte hat weiter die Frage nach der automatisierten Verarbeitung gemäß § 22 DSGVO dahin beantwortet, dass sie keine Verarbeitung der personenbezogenen Daten der Klagepartei festgestellt habe, die in den Anwendungsbereich des Art. 22 Abs. 1 DSGVO fielen (Anlage B 8, dort S. 21). Insoweit ist daher Erfüllung eingetreten, § 362 Abs. 1 BGB.

2.
Nicht erfüllt und gegeben ist der Auskunftsanspruch, soweit die Klagepartei nach der Verarbeitung fragt („*welche personenbezogenen Daten die Beklagte seit dem 09.11.2018 verarbeitet*“ hat), was einen Teil des Auskunftsanspruchs ausmacht.

3.
Der Anspruch ist auch nicht etwa dadurch erfüllt worden (§ 362 Abs. 1 BGB), dass die Beklagte vorgerichtlich auf ihre sog. Selbsthilfetools verwiesen und der Klagepartei eine entsprechende Anleitung zur Verfügung gestellt hat (Anlage B 8).

a)
Eine Berufung auf die Erfüllung scheitert schon daran, dass die Klagepartei hierfür in die streitgegenständliche Datenverarbeitung einwilligen müsste (vgl. Schreiben der Beklagten vom 7. Juni 2024 (Anlage B 8)), was die Beklagte wegen der Reichweite der Datenverarbeitung gerade ablehnt.

b)
Ohnehin wäre der Anspruch auch nicht dadurch erfüllt worden (§ 362 Abs. 1 BGB), dass die Beklagte vorgerichtlich auf ihre sog. Selbsthilfetools verwiesen und der Klagepartei – unter der Bedingung, dass sie ihre Einwilligung erklärt – eine entsprechende Anleitung zur Verfügung gestellt hat. Selbst wenn die Klagepartei hierzu Zugang hätte, ist, wie die Beklagte aber selbst in ihrem Anschreiben an die Klagepartei (Anlage B 8), dort Seite 9, ausführt, ist schon nicht gewährleistet, dass die Nutzer die vollständige Information über alle von der Beklagten gespeicherten Daten erhalten, wenn sie das sog. Selbsthilfetool nutzen, denn die Beklagte führt in dem Schreiben lediglich Möglichkeiten an, die in dem Selbsthilfetool genannt werden. Soweit die Beklagte erklärt, sie übermittle keine personenbezogenen Daten an Werbetreibende (S. 8), kann dies dahingestellt bleiben, weil unstreitig ist, dass sie diese in gehashter Form zurückerhält. Welche Daten sie auf dieser Grundlage verarbeitet, hat sie nicht mitgeteilt. Die Auskunft verbleibt vielmehr im Ungefähren mit Formulierungen wie „*manchmal*“, „*zum Beispiel*“, „*können sehen*“, „*kann diese Personen bzw. dieses Unternehmen seine Nachricht lesen*“, „*beispielsweise*“, „*in einigen Fällen*“ usw..

Unstreitig erhält die Beklagte ausweislich ihrer eigenen Darstellung über ihre Business-Tools von den diese benutzenden Werbepartnern auch dann Informationen zur Klagepartei, wenn gerade keine Einwilligung in personalisierte Werbung durch die Klagepartei auf der Plattform vorliegt. Diese Daten werden zwar nicht mit dem Plattformkonto der Klagepartei

verknüpft, aber bei der Beklagten erfasst und gespeichert, folglich verarbeitet im Sinn der DSGVO, und könnten – über die IP-Adresse – der Klagepartei später einfach zugeordnet werden. Und diese Daten können schon nach dem eigenen Bekunden der Beklagten nicht über das sog. Selbsthilfetool abgerufen werden.

C. Klageantrag zu 2 (Löschung- und Anonymisierung)

1.
Der Klageantrag ist zulässig und auch teilweise begründet. Gegen die Zulässigkeit ergeben sich keine Bedenken.

Die Klagepartei kann aus Art. 17 Abs. 1 lit. d), 12 Abs. 3 DSGVO eine Löschung der von der Beklagten verarbeiteten personenbezogenen Daten verlangen.

a)
Dahinstehen kann, ob ein Löschungsanspruch gemäß Art. 17 Abs. 1 lit. b) DSGVO besteht, weil die von der Klagepartei eingeholte Einwilligung nicht wirksam war. Eine freiwillige Einwilligung zur Datenübermittlung an Drittwebseiten und -Apps i. S. d. Art. 4 Nr. 11 DSGVO liegt allerdings nicht vor (vgl. zu den Voraussetzungen im Einzelnen: Paschke/Berlit/Meyer/Kröner, Hamburger Kommentar Gesamtes Medienrecht, 77. Abschnitt: Grundregeln des medienrelevanten Datenschutzrechts, Rn. 27, beck-online). Die Beklagte kann sich nicht auf die eine Einwilligung der Klagepartei nach Art. 6 Abs. 1 lit. a), Art. 9 Abs. 2 lit. a) DSGVO berufen. Jedenfalls besteht ein Löschungsanspruch nach Abs. 1 lit. d) mit dem (konkludenten) Widerruf der Einwilligung durch die Klage (BeckOK DatenschutzR/Worms, 54. Ed. 01.11.2024, DSGVO Art. 17 Rn. 32, beck-online).

Die Datenübermittlung an Drittanbieter und zurück an die Beklagte, gleich ob durch die Cookie-Einstellungen der Klagepartei die Weiterverarbeitung gestattet war und ist oder nicht, war und ist nicht durch einen Erlaubnistatbestand Art. 6 Abs. 1 UAbs. 1 DSGVO gedeckt und daher rechtswidrig.

b)
Die Datenverarbeitung der Beklagten ist in drei Perioden einzuteilen: die Zeit vom 18.05.2018 bis zur Implementierung des Bezahl-Abonnements und der Cookie-Implementierung ab 3. November 2023 (lit. aa)), die Zeit vom 16. Juli 2020 bis 7. Oktober 2022 (lit. bb)), und die danach liegende Zeit bis heute (lit. cc)).

aa) Zwischen den Parteien ist unstreitig, dass vor dem 3. November 2023 die von den (Dritt-) Webseiten und Apps stammenden „Kontaktinformationen“ und/oder „Event-Daten“ ungefiltert und damit allgemein und unterschiedslos von der Beklagten verarbeitet wurden. Insoweit wird auf die Feststellungen des Bundeskartellamts, Beschluss vom 6. Februar 2019, B6-22/16, Bezug genommen. Dass die Beklagte vor dem 3. November 2023 Schranken gegen eine Übermittlung der Daten durch die Meta-Business-Tools eingebaut hätte, ist nicht ersichtlich.

bb) Die Datenübermittlung in die USA war darüber hinaus jedenfalls vom 16. Juli 2020 bis zum 7. Oktober 2022 nicht durch einen Erlaubnistatbestand der DSGVO gedeckt. Mit Urteil vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18, im Folgenden: Urteil Schrems II), erklärte der EuGH den Angemessenheitsbeschluss der EU-Kommission vom 12. Juli 2016 (ABl. 2016, L 207, S. 1, im Folgenden: Angemessenheitsbeschluss 2016) gemäß der Richtlinie 95/46 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes für ungültig. Der EuGH stellte fest, dass die bisher verwendeten Standardvertragsklauseln (SCC) in Bezug auf den Zugang der Geheimdienste zu Daten aufgrund von Bedenken gegenüber der massenhaften US-Datenüberwachung und fehlender Rechtsschutzmöglichkeiten für EU-Bürger nicht den EU-Datenschutzvorschriften entspreche (Eine ähnliche Problematik behandelt der indonesische Oberste Gerichtshof in seiner Entscheidung vom 19. Januar 2026, Case Number 137/PUU-XXIII/2025 für die dortige Rechtslage, ConflictofLaws.net.: Cross-Border Personal Data Transfers: The Remaining Issues Following the Indonesian Constitutional Court Decision, 25. Februar 2026.).

Die Beklagte hat für diesen Zeitraum die Hürde des Verbots von Datenübermittlungen in Drittstaaten gem. Art. 44 ff. DSGVO schuldhaft nicht überwunden. Gründe, die die Übermittlung der personenbezogenen Daten der Klagepartei in die USA im Zeitraum vom 7. Juli 2020 bis zum 7. Oktober 2022 rechtfertigen könnten und die sich aus den Erlaubnistatbeständen der Art. 45 bis 47 DSGVO ergeben könnten, sind nicht ersichtlich. Sie hat lediglich auf ihre Standardvertragsklauseln verwiesen, die die fehlende Rechtsschutzmöglichkeit in den USA nicht beheben konnten. Die Übermittlung war vielmehr weder nach Art. 46 Abs. 1 DSGVO aufgrund geeigneter Garantien für ein angemessenes Datenschutzniveau in den USA als Drittland noch aufgrund einer Einwilligung nach Art. 49 Abs. 1, S. 1 lit. a) DGSVO zulässig oder gemäß Art. 49 Abs. 1 lit. b) DSGVO erforderlich.

(1) Eine Einwilligung zur Datenübermittlung in die USA liegt nicht vor (vgl. zu den Voraussetzungen im Einzelnen: Paschke/Berlit/Meyer/Kröner, Hamburger Kommentar Gesamtes Medienrecht, 77. Abschnitt: Grundregeln des medienrelevanten Datenschutzrechts Rn. 27,

beck-online). Insbesondere ist in der Annahme der Facebook- bzw. Instagram-Nutzungsbedingungen keine wirksame Einwilligung zu einem Datentransfer in die USA im o. g. Zeitraum zu sehen, weil über die Frage des fehlenden individuellen Rechtsschutzes nicht aufgeklärt wurde.

(1.1.) Die Klagepartei wurde unstreitig weder über die konkreten Empfänger noch über die Risiken einer Datenübermittlung in die USA informiert. Eine solche Aufklärung ist gemäß Art. 49 Abs. 1 lit. a) DSGVO zwingend (Art. 7 und 4 Nr. 11 DSGVO). Der Betroffene muss jedoch über das konkrete Risiko der Datenübermittlung in ein Drittland ohne adäquates Schutzniveau aufgeklärt werden (Gola/Heckmann/Klug, 3. Aufl. 2022, DSGVO Art. 49 Rn. 6, beck-online).

(1.2.) Nach Art. 49 Abs. 1 lit. a) DSGVO ist eine Einwilligung zudem nur gültig, wenn die betroffene Person ausdrücklich und in Kenntnis der Sachlage zugestimmt hat. Die Beklagte kann nicht nachweisen, dass eine transparente Information über die Risiken der Drittstaatenübermittlung stattfand. Solches ist nicht ersichtlich.

(1.3.) Daraus folgt zugleich, dass die behauptete Einwilligung in die generelle Datenverarbeitung nicht freiwillig war (vgl. EWG 43 DSGVO; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 49 Rn. 16, beck-online).

(2) Auf Art. 49 Abs. 1 lit. b) und c) DSGVO (Erforderlichkeit der Datenübermittlung) kann die Beklagte die Datenübermittlung nicht stützen. Danach ist eine Datenübermittlung an ein Drittland zulässig, auch wenn weder ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO noch geeignete Garantien nach Art. 46 DSGVO bestehen, wenn die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist.

(2.1.) Wie EWG 111 DSGVO erhellt, setzt Art. 49 Abs. 1 lit. b) DSGVO dabei voraus, dass es sich lediglich um gelegentliche, also nicht um regelmäßige Datenübermittlungen handelt (vgl. auch Klug in: Gola/Heckmann, DSGVO, 3. Aufl., Art. 49, Rn. 7).

Die Beklagte führt jedoch selbst aus, dass die Übermittlung der Daten in die USA zum Funktionieren des sozialen Netzwerkes erforderlich sei, was keine bloß „*gelegentliche*“, sondern systematische Übermittlung darstellt.

(2.2.) Dies gilt hier umso mehr, als die Beklagte nicht darlegt, weshalb der Datentransfer in die USA erforderlich für die Vertragserfüllung und die gesamte Datenverarbeitung war. Denn es wäre ebenso gut möglich gewesen, den gesamten weltweiten Datenverkehr von Facebook oder Instagram in einem Staat zu verarbeiten, welcher über einen Angemessenheitsbeschluss mit der EU-Kommission verfügte oder auch in einem Mitgliedstaat der Europäischen Union. Anderenfalls hätte die Datenübertragung gänzlich unterbleiben müssen (EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 135, juris; Borges/Keil, Big Data/Duisberg, 1. Aufl. 2024, § 6 Rn. 315, beck-online). Dieser Schluss ergibt sich auch aus EWG 101, S. 6 DSGVO, wonach die Datenübermittlung nur stattfinden kann, wenn die Bestimmungen der DSGVO erfüllt werden.

(2.3.) Auch Art. 49 Abs. 1 lit. c) DSGVO betrifft lediglich Fälle, in denen gelegentlich stattfindende Übermittlungen zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde bzw. geschlossen werden soll, erforderlich sind. Der Betroffene selbst ist hierbei nicht Vertragspartner. In Betracht kommen etwa Verträge zugunsten Dritter i. S. v. § 328 BGB (Gola/Heckmann/Klug, 3. Aufl. 2022, DSGVO Art. 49 Rn. 8, beck-online). Ein solcher Fall liegt hier nicht vor.

(2.4.) Auch die übrigen Voraussetzungen des Art. 49 Abs. 1 lit. d) bis g) DSGVO liegen ersichtlich nicht vor.

(2.5.) Die Beklagte kann sich auch nicht auf Art. 49 DSGVO i. V. m. Art. 6 DSGVO berufen, insbesondere unter dem Argument, dass die Übermittlung zur Vertragsdurchführung erforderlich war, da sie andernfalls ihre Dienste nicht hätte anbieten können. Denn diese Vorschriften sind Ausnahmevorschriften und nur im Einzelfall anwendbar, dienen aber nicht als Grundlage *„massenhafter“* Übermittlungen (vgl. EWG 111 DSGVO).

(3) Für den Zeitraum vom 7. Juli 2020 bis zum 7. Oktober 2022 kann sich die Beklagte nicht auf die Rechtsgrundlage des Art. 45 Abs. 1 DSGVO berufen, weil der EuGH den Angemessenheitsbeschluss der EU-Kommission vom 12. Juli 2016 für unwirksam erklärt hat (EuGH, Urteil vom 16. Juli 2020, C-311/18, juris).

(4) Die Beklagte kann sich auch nicht auf die Standardvertragsklauseln mit der EU-Kommission und die darauf beruhenden Datenübermittlungsverträge gemäß Art. 46 Abs. 1 und Abs. 2 DSGVO und EWG 108 DSGVO berufen. Ausführungen hierzu fehlen gänzlich. Art. 46 DSGVO bildet ebenfalls keine Grundlage für die Datenübermittlung in die USA.

Ohnehin können durch die Standardvertragsklauseln nationale Gesetze nicht geändert werden (Thüsing in: Lutter/Bayer, Holding-Handbuch, 7. Auflage 2024, c) Verbindliche Unternehmensregelungen als Rechtfertigungsgrundlage, Art. 46 Abs. 2 lit. b, 47 DSGVO, Rn. 14_105). Damit steht auch außer Frage, dass Standardvertragsklauseln die Behörden eines Drittlands nicht binden können, da diese nicht Vertragspartei sind (EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 125, juris; Dehmel/Ossmann-Magiera/Weiss: Drittstaatentransfers nach Schrems II, MMR 2023, 17).

Daher ist für das gegebene Datenschutzniveau nicht allein auf die Standardvertragsklauseln, sondern auf die Rechtslage in den USA abzustellen.

Das einschlägige US-Recht und die einschlägigen US-amerikanischen Praktiken boten kein Schutzniveau, das dem im EU-Recht vorgesehenen gleichwertig ist. Dass die Standardvertragsklauseln eine ausreichende Lösung für einen derartigen Datentransfer geboten hätten, hat die Beklagte schon nicht näher dargelegt. Denn jedenfalls bestand für die Beklagte in den USA eine direkte Verpflichtung, den Zugriff auf die importierten Daten zu gewähren oder diese herauszugeben, die sich auch auf die kryptographischen Schlüssel erstrecken konnte (EDSA, Empfehlungen 01/2020, Rn. 81).

EU-Bürgern standen keine wirksamen Rechtsbehelfe gemäß Art. 47 GrCh zur Verfügung.

Der EuGH hat festgestellt, dass die Standardklauseln ihrer Wirksamkeit beraubt sind durch die Möglichkeit, dass us-amerikanische Behörden wegen Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder von Rechtsvorschriften der Vereinigten Staaten in die Grundrechte der Personen eingreifen können, deren personenbezogene Daten aus der Union in die Vereinigten Staaten übermittelt werden oder werden könnten, insbesondere nach § 702 FISA (§ 702 FISA - Foreign Intelligence Surveillance Act), der EO 12333 (Executive Order 12333 (EO 12333), https://www.archives.gov/federal-register/codification/executive-order/12333.html) und der PPD-28 (Presidential Policy Directive 28, PPD-28 vom 17. Januar 2014), weil insoweit keinerlei Einschränkungen oder Garantien für Nicht-US-Bürger bestünden (EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 165 und Rn. 180, juris). Insbesondere verleihe die EO 12333 keine Rechte, die gegenüber den amerikanischen Behörden gerichtlich durchgesetzt werden könnten (EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 182, juris). Es fehlte damit sowohl an der Rechtsschutzmöglichkeit (Rn. 192) als auch an der Verhältnismäßigkeit der Maßnahmen.

Der EuGH hat zusammenfassend in Rn. 184 ausgeführt:

„Folglich ist davon auszugehen, dass weder Section 702 des FISA noch die EO 12333 in Verbindung mit der PPD-28 den im Unionsrecht nach dem Grundsatz der Verhältnismäßigkeit bestehenden Mindestanforderungen genügen, so dass nicht angenommen werden kann, dass die auf diese Vorschriften gestützten Überwachungsprogramme auf das zwingend erforderliche Maß beschränkt sind."

Dieser Würdigung schließt sich der Senat nach eigener Prüfung der zugrunde liegenden Rechtsvorschriften an.

(5) Diese Einschätzung wird gestützt von dem Beschluss der irischen Datenschutzbehörde vom 13. April 2023 (https://www.edpb.europa.eu/system/files/2024-01/edpb_bindingdecision_202301_ie_sa_facebooktransfers_de.pdf), in dem diese in den Rn. 7.51 ff. festgestellt hat, dass ein Rechtsschutz für nachrichtendienstlich angeforderte Datenübermittlungen für EU-Bürger nicht bestehe und vielmehr die Beklagte verpflichtet sei, alle übertragenen Daten einschließlich der Kommunikation zugänglich zu machen.

(6) Dass die EO 12333 Eingrenzungen für diese Form der Überwachung vorsieht, ist nicht ersichtlich. EU-Bürger hatten keine Möglichkeit auf Rechtsschutz. Weitere Maßnahmen, die nach FISA in Bezug auf Daten, die aus der EU übertragen werden, ergriffen werden können, sind individualisierte elektronische Überwachung (§ 105 FISA), körperliche Durchsuchungen (§ 302 FISA), die Verwendung von Pen-Registern oder Trap-and-Trace-Geräten (§ 402 FISA) und die Sammlung von Geschäftsunterlagen bestimmter Unternehmen (öffentliche Verkehrsdienstleister, Unterkünfte, Fahrzeugvermietungen oder Lagerstätten, § 501 FISA). Nach Abschnitt 2.3 ist die ungehinderte Informationssammlung (sog. bulk collection) möglich, die die Beklagte ja auch selbst gerade vornimmt (vgl. Anlage K 11, Meta Playbook).

Der EGMR fordert im Falle einer Massenüberwachung von *Personen „Ende zu Ende Schutzmaßnahmen"* auf jeder Stufe des Überwachungsprozesses. Dies umfasst unter anderem die unabhängige vorherige Genehmigung einer Überwachungsmaßnahme (EGMR, Urteil vom 25. Mai 2021, 58170/13, 62322/14, 24960/15 (Big Brother Watch u. a./Vereinigtes Königreich), Rn. 350, juris). Hierzu hat sich die Beklagte nicht ansatzweise verhalten.

(7) Auch die Europäische Datenschutzbehörde hat in ihren Empfehlungen 1/2020 vom 18. Juni 2021 noch darauf hingewiesen, dass die Möglichkeit gerichtlicher Rechtsbehelfe,

das Vorhandensein eines umfassenden Datenschutzrechts und einer unabhängigen Datenschutzbehörde sowie auch die Einhaltung internationaler Übereinkommen über Datenschutzgarantien erforderlich sind (Rn. 37 und Rn. 40, 119) und unter Rn. 81 ausdrücklich auf die Zugriffsmöglichkeit amerikanischer Behörden hingewiesen.

(8) Dass die Standardvertragsklauseln diese Situation beheben konnten, hat die Beklagte zwar geltend gemacht, jedoch nicht vereinzelt. Die Standardvertragsklauseln im Anhang zum Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 erfüllen die Anforderungen nicht, weil nationale Gesetze damit nicht geändert werden können (Thüsing in: Lutter/Bayer, Holding-Handbuch, 7. Auflage 2024, c) Verbindliche Unternehmensregelungen als Rechtfertigungsgrundlage, Art. 46 Abs. 2 lit. b, 47 DSGVO, Rn. 14_105). Damit steht auch außer Frage, dass Standardvertragsklauseln die Behörden eines Drittlands nicht binden können, da diese nicht Vertragspartei sind (EuGH, Urteil vom 16. Juli 2020, C-311/18, Rn. 125, juris; Dehmel/Ossmann-Magiera/Weiss: Drittstaatentransfers nach Schrems II, MMR 2023, 17). Daher ist für das gegebene Datenschutzniveau nicht allein auf die Standardvertragsklauseln, sondern auf die Rechtslage in den USA abzustellen. Das EU-Datenschutzniveau ist frühestens mit der Executive Order EO 14086 und der damit verbundenen Beschränkung der Überwachungsbefugnisse der US-Nachrichtendienste und der Schaffung eines neuen Rechtsschutzmechanismus für EU-Bürger am 7. Oktober 2022 erreicht worden. Die EU-Kommission hat zu den mit der EO 14086 geschaffenen Mechanismen in dem Überprüfungsbericht vom 9. Oktober 2024 (Com (2024) 451) final ausgeführt:

„Based on the information gathered during this first review, the Commission concludes that the U. S. authorities have put in place the necessary structures and procedures to ensure that the Data Privacy Framework functions effectively." (S. 21).

Das EuG hat festgestellt, dass die in der EO 14086 vorgesehenen Garantien hinsichtlich der Funktionsweise und der Befugnisse des DPRC eine unabhängige und unparteiische Überprüfung der vom CLPO getroffenen Feststellungen ermöglichen und Bedenken gegen die Unabhängigkeit des PCLOB sowie des DPRC nicht bestehen (EuG, Urteil vom 3. September 2025, T-553/23, Rn. 49, 54, 63, juris). Bedenken bestünden auch nicht hinsichtlich der Errichtung (durch Gesetz i. S. d. Art. 47 GrCh) und der Funktionsweise (EuG, Urteil vom 3. September 2025, T-553/23, Rn. 73, beck-online). Die EO 14086 sehe auch eine Sammelerhebung (bulk collection) nur unter konkret beschriebenen Umständen vor. Außerdem sei eine gerichtliche Überprüfung vorgesehen (a. a. O., Rn. 106, 115).

(9) Auf diese Rechtslage hat der Senat in den Vorverfahren 9 U 44/25 und 9 U 125/24 in der mündlichen Verhandlung ausdrücklich hingewiesen.

cc) Auch für die Zeit nach dem 3. November 2023 verarbeitet die Beklagte trotz der Cookie-Einführung und der Möglichkeit, personalisierte Werbung nicht mehr anzeigen zu lassen, rechtswidrig Daten der Klagepartei.

(1) Auch ohne entsprechende Einwilligung über ihre oder die Cookies der Drittwebseiten nimmt die Beklagte Datenverknüpfungen vor, die über den vertraglich vereinbarten Zweck hinausgehen. Die Beklagte hat hierzu vorgetragen, sie nehme (1.) Datenverknüpfungen für das reibungslose Funktionieren der Meta-Dienste vor, (2.) verknüpfe Meta-Daten für die sog. Familiy-Analytics (Aufbereitung von Daten für Berichtspflichten und Nutzerstatistiken) und (3.) für ein höheres Sicherheitsniveau z. B. durch Sperrung von Konten bei Rechtsverstößen der Nutzer. Auch, wenn ein Nutzer Cookies auf den Drittwebseiten ablehnt, erhält die Beklagte zunächst diese Daten (vgl. Bundeskartellamt, Fallbericht vom 9. Oktober 2024, B6-22/16). Diese – aktuelle – Einschätzung des Bundeskartellamtes wird zunächst gestützt durch den Vortrag der Beklagten, in dem diese einräumt, Daten weiterhin für Sicherheits- und Integritätsinteressen und aus Gründen der Vorbeugung gegen Straftaten zu verarbeiten, wenn sie diese auch von den Drittwebseiten erhält. Die Conversions API aggregiert (gruppiert) hierfür die Eventdaten von Nutzern, die sich gegen die Nutzung ihrer Daten entschieden haben (vgl. S. 23 Meta Play Book). Die Anzeigen werden an die Testgruppe ausgeliefert und „*unter Wahrung der Privatsphäre verarbeitet*“ (vgl. S. 23 Meta PlayBook). Die Beklagte räumt im Meta Play Book (Anlage K 11; dort S. 23) ein, dass die Daten weiterverarbeitet werden, weil weiterhin verlässliche Berichte an die Drittunternehmen übermittelt werden sollen. In der von der Beklagten – unvollständig – vorgelegten Anlage B 12 (removing certain ad targeting options an expanding our ad controlls) erklärt sie selbst, dass sie beständig die „targeting options“ überprüft, was gedanklich voraussetzt, dass sie vorhanden sind.

(2) Eine solche Verarbeitung ist rechtswidrig, weil – wie EWG 26 DSGVO klarstellt – auch eine Pseudonymisierung (Abs. 5) keine Wirkung auf den Personenbezug der Daten hat, da es sich letztendlich lediglich um eine andere Form der Speicherung handelt, dem Verantwortlichen aber weiterhin der vollständige Informationsgehalt der Daten zur Verfügung steht und der individuelle Bezug jedes Informationselements ohne großen Aufwand hergestellt werden kann. Selbstverständlich beeinflusst auch eine Verschlüsselung von Daten deren Personenbezug in keiner Weise. Verschlüsselte Speicherung oder Übertragung ist eine Sicherheitsmaßnahme, die insbesondere unbefugte Kenntnisnahme der Daten erschwert,

aber berechtigten Personen weiterhin Zugang und Verarbeitungsmöglichkeit bietet (Ehmann/Selmayr/Klabunde/Horváth, 3. Aufl. 2024, DSGVO Art. 4 Rn. 19, beck-online).

c)
Die Datenverarbeitung durch die Beklagte ist durchgehend jedenfalls bis 3. November 2023 rechtswidrig, weil sie gegen den Grundsatz der Datenminimierung bei der Verarbeitung personenbezogener Daten, der in Art. 5 Abs. 1 lit. b), lit. c), Art. 25 Abs. 2, S. 1, 3 DSGVO verankert ist, verstoßen hat.

aa) Nach Art. 5 Abs. 1 lit. c), 25 Abs. 2 Satz 1 und 3 DSGVO muss die Datenverarbeitung gemäß § 4 Nr. 2 DSGVO dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß begrenzt sein. Ausnahmen und Einschränkungen des Grundsatzes des Schutzes solcher Daten sind auf das absolut Notwendige zu beschränken (Grundsatz der Datenminimierung; EuGH, Urteil vom 24. Februar 2024, C-175/20, Rn. 73; BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 87; juris).

Die Grundsätze des Art. 5 DSGVO werden durch konkrete Vorgaben zur technischen Ausgestaltung und insbesondere durch Vorgaben in Bezug auf datenschutzfreundliche Voreinstellungen in Art. 25 DSGVO konkretisiert (vgl. zum Verhältnis von Art. 5 und Art. 25 DSGVO: Heberlein in: Ehmann/Selmayr, DSGVO, 3. Aufl., Art. 5, Rn. 6 und 31; Schantz in: BeckOK DatenschutzR, 49. Ed. [Stand: 1. November 2021], Art. 5 DSGVO, Rn. 25; Herbst in: Kühling/Buchner, DSGVO - BDSG, 4. Aufl. 2024, Art. 5 DSGVO, Rn. 59 und Hartung in: Kühling/Buchner, DSGVO - BDSG, 4. Aufl. 2024, Art. 25 DSGVO, Rn. 25). Die datenschutzfreundlichste Voreinstellung ist zu wählen (BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 88, juris).

(1) Nach Art. 25 Abs. 2 DSGVO hat der Verantwortliche demnach geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Damit beinhaltet Art. 25 Abs. 2 Satz 3 DSGVO die ausdrückliche Verpflichtung zu Voreinstellungen, die verhindern, dass die Daten ohne Weiteres, also ohne bewusste persönliche Änderung der Voreinstellung, der Öffentlichkeit oder sonst einem unbestimmten

Adressatenkreis zugänglich gemacht werden (Heberlein in: Ehmann/Selmayr, DSGVO, 3. Aufl. 2024, Art. 5 Rn. 31; BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 86, 88; juris).

Die Vorgabe, die Daten nicht *„einer unbestimmten Zahl natürlicher Personen“* zugänglich zu machen, ist nach ihrem Zweck darauf ausgelegt, dass der Personenkreis derjenigen, die Zugriff auf die Daten des Betroffenen haben können, für diesen überschaubar sein soll. Die Regelung des Art. 25 Abs. 2 DSGVO hat dabei gerade die Voreinstellungen von sozialen Netzwerken im Blick (BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 89, juris).

(2) Diesen Anforderungen wurde bis November 2023 und wird das Vorgehen der Beklagten bis heute nicht gerecht. Dabei kann dahinstehen, ob die Oberfläche der Beklagten insoweit nutzerfreundlich gestaltet ist und – was die Klagepartei in ihrer mündlichen Anhörung verneint hat – eine bedienerfreundliche Leitung überhaupt möglich ist. Das genaue Gegenteil der Einstellungen der Beklagten wäre bis November 2023 dem Grundsatz der Datenminimierung gerecht geworden, nämlich die Voreinstellung, dass die Daten der Nutzer unter keinen Umständen bzw. nur bei entsprechender freiwilliger Einwilligung überhaupt weitergegeben werden. Zwischen den Parteien ist unstreitig, dass die von den (Dritt-) Webseiten und Apps stammenden „Kontaktinformationen“ und/oder „Event-Daten“ (Anlage B 5) ungefiltert und damit allgemein und unterschiedslos von der Beklagten verarbeitet wurden.

(3) Über die Business-Tools erhält die Beklagte Business-Tool-Daten, d. h. Kontaktinformationen, Standardinformationen und/oder Event-Daten (z. B. Besuche auf einer Webseite, Installation einer App, Kauf eines Produkts) von ihren Vertragspartnern, den Drittunternehmen. Bestimmte technische Standarddaten gelangen automatisch an die Beklagte, wenn der Nutzer eine Webseite aufruft, deren Anbieter die Business-Tools in seine Webseite eingebettet hat. Hierzu übermittelt der Browser dem Server des Drittanbieters die IP-Adresse des Rechners des Nutzers 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 Business-Tools-Nutzungsbedingungen verlangen in diesem Fall von dem Drittanbieter, die erforderlichen Angaben und Datenschutzbelehrungen zu erteilen und die notwendige Einwilligung einzuholen (Anlage B 5). Die Beklagte überprüft dies nicht. Sie verwehrt sich vielmehr nicht gegen die Tatsache, dass unter Zugrundelegung der Zuordenbarkeit qua „Digital Fingerprinting“ die von der Klagepartei erhobenen und verarbeiteten Daten als personenbezogene Daten im Sinne des

Art. 4 Nr. 1 DSGVO einzustufen sind, da ihr anhand der ihr vorliegenden Informationen insofern eine Individualisierung der Klagepartei möglich ist (vgl. EuGH, Urteil vom 19. Oktober 2016, Breyer, C-582/14, Rn. 49; EuGH, Urteil vom 17. Juni 2021, M. I. C. M., C-597/19, Rn. 102; auch BGH, Urteil vom 16. Mai 2017, VI ZR 135/13, Rn. 23; juris).

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

(4.1.) 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 Facebook-Konto anmelden und die dort erhobenen Daten werden nicht verwendet, um relevante Werbung zu zeigen. Sie werden aber in eingeschränktem Umfang genutzt, um für Sicherheit und Integrität zu sorgen und es kann sein, dass die Beklagte aggregierte Informationen zu Aktivitäten erhält, nicht aber die persönliche Cookie-Information des Nutzers (Anlage B 7, S. 41).

(4.2.) Entscheidet sich der Nutzer dafür, Werbung mithilfe der Informationen von Werbepartnern zu seinen Aktivitäten relevanter zu machen, erhält er stärker personalisierte Werbung. Seine Daten werden vollumfänglich verarbeitet.

bb) Der Senat sieht hierin – wie der EuGH (Urteil vom 4. Oktober 2024, C-446/21, Rn. 62 ff., juris) in einem die Beklagte betreffenden Fall – einen unverhältnismäßigen Eingriff in die durch Art. 7, 8 GrCh geschützten Rechte der Klagepartei auf Achtung des Privatlebens und auf Schutz ihrer personenbezogenen Daten. Der EuGH weist zurecht darauf hin, „*dass eine solche Verarbeitung besonders umfassend [ist], da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von … aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird*“ (EuGH, a. a. O, Rn. 62).

Diese Gefahr besteht auch mit den Änderungen der Cookie-Einstellungen fort. Aus dem Fallbericht des Bundeskartellamts vom 9. Oktober 2024 (B6-22/16) ergibt sich, dass noch am 9. Oktober 2024 und damit nach Implementierung der Cookies dem Nutzer noch nicht bewusst gemacht werde, dass die Akzeptanz der Cookies ein dauerhaftes Hinzufügen der Daten zu einem individuellen Profil bedeute und eine differenzierte Entscheidung nicht möglich sei. Zudem hat die EU-Kommission am 25. März 2024 ein Verfahren gegen das

werbungsfreie Abomodell eingeleitet, https://ec.europa.eu/commission/presscorner/detail/de/ip_24_3582.

In diesem Verstoß gegen die Vorschrift des Art. 5 Abs. 1 lit. c) DSGVO liegt zugleich eine konkrete unrechtmäßige Datenverarbeitung (EuGH, Urteil vom 4. Mai 2023, C-60/22, Rn. 54 - 57, juris).

d)
Die Datenverarbeitung ist auch nicht für die Vertragserfüllung nach Art. 6 Abs. 1 lit. b), Art. 9 Abs. 2 b) DSGVO erforderlich. Die Verarbeitung ist schließlich nicht durch überwiegende Interessen der Beklagten oder der Drittanbieter gegenüber den Interessen und Rechten der Klagepartei nach Art. 6 Abs. 1 f) DSGVO gerechtfertigt. Die Beklagte kann sich auch nicht auf die in ihrer Datenschutzrichtlinie (Anlage K 1) genannten Verarbeitungszwecke berufen.

aa) Art. 6 Abs. 1 lit. a) und Art. 9 Abs. 2 DSGVO
(1) Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO und Art. 9 Abs. 2 lit. a) DSGVO verlangen die Einwilligung der betroffenen Person im Hinblick auf die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke bzw. die Verarbeitung besonderer Kategorien von Daten gem. Art. 9 Abs. 1 DSGVO. Nach Art. 4 Nr. 11 DSGVO bezeichnet der Ausdruck „Einwilligung“ „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.

(2) Die Verarbeitung der personenbezogenen Daten lässt sich bis zum 3. November 2023 nicht über eine Einwilligung der Klagepartei gem. Art. 6 Abs. 1 lit. a DSGVO legitimieren (vgl. zur Einwilligung der Klagepartei Rn. 62 des Schriftsatzes vom 7. August 2024). Der EuGH geht davon aus, dass nach EWG 42 DSGVO die Einwilligung nicht als freiwillig erteilt angesehen werden kann, wenn die betroffene Person nicht über eine echte Wahlfreiheit verfügt oder nicht in der Lage ist, ihre Einwilligung zu verweigern oder zu widerrufen, ohne Nachteile zu erleiden. EWG 43 DSGVO verweist darauf, dass ein klares Ungleichgewicht zwischen den Beteiligten gegen die Freiwilligkeit der Einwilligung spreche und nach Art. 7 Abs. 4 DSGVO berücksichtigt werden müsse, ob die Einwilligung in eine Datenverarbeitung erfolge, die zur Vertragserfüllung nicht erforderlich sei (EuGH, Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./Bundeskartellamt), Rn. 143, 144 und 145; BGH, Beschluss vom 23. Juni 2020, KVR 69/19, Rn. 107; juris). Die Beklagte trägt für den Zeitraum

bis 3. November 2023 nicht einmal zu einer Einwilligung über Cookies vor. Denn erst für den Zeitraum danach hat die Beklagte die Alternative des werbefreien Abonnements bzw. der werbefreien Nutzung geschaffen.

(3) Aber auch für die Zeit nach dem 3. November 2023 liegt keine Einwilligung zur Datenverarbeitung über Business-Tools vor (vgl. Schriftsatz vom 22. Januar 2025). Wie die Beklagte selbst in ihrer Datenschutzrichtlinie einräumt, verarbeitet sie trotz fehlender Einwilligung Daten der Klagepartei (sogar, wenn jemand gar kein Konto bei der Beklagten hätte, vgl. S. 6 Datenschutzrichtlinie, Anlage K 1). Weiter heißt es auf S. 10: *„Wir verarbeiten bestimmte Informationen, die wir von Partnern als gemeinsam Verantwortlicher mit ihnen erhalten."* Die Beklagte räumt die Verwendung personenbezogener Daten letztlich auch ein, meint aber, sie dürfe diese aus Erforderlichkeitsgründen nutzen.

Mit dem verharmlosenden Hinweis auf aggregierte Informationen in den Cookie-Einstellungen (vgl. Rn. 38 Klageerwiderung vom 18. Juni 2024) wird auf die Tragweite der Verarbeitung, wie sie sich aus dem Meta Play Book ergibt, nicht ansatzweise hingewiesen, wenn die Klagepartei wie hier nach ihrer informatorischen Anhörung auf den Drittwebseiten die Cookies regelmäßig ablehnt. Denn auch aus dieser Gruppe heraus, in die ein Nutzer mit seiner randomnisierten ID eingruppiert wird, kann das Nutzerverhalten der Nutzer der Gruppe nachvollzogen werden, so dass letztlich auch Rückschlüsse auf das Nutzerverhalten der Klagepartei möglich sein können.

Aber auch die Einwilligung in die Anzeige von Werbung ist nicht vergleichbar mit dem systematischen Verarbeiten der Daten der Beklagten zum Zwecke der Datensammlung für ein individuelles Profil.

Folge der unfreiwilligen, weil unaufgeklärten Einwilligung ist deren Ungültigkeit (EWG 43 DSGVO; EDSA, Leitlinien 5/2020).

(4) Soweit sich die Beklagte auf die Nutzungsverträge mit den Drittanbietern beruft, die es ihnen untersagen sollen, die Daten an die Beklagte trotz Ablehnung der Cookies weiterzusenden, entlastet sie das nicht. Die Beklagte muss sich im Zeitpunkt der eigenen – nachfolgenden – Datenverarbeitung sicher sein, dass eine wirksame Einwilligung vorliegt. Das ist nach ihrem System gerade ausgeschlossen. Die Beklagte erhält von dem Drittanbieter erhobene Daten, auch wenn der Nutzer auf dessen Webseite die Cookies abgelehnt hat und jedenfalls bei Ablehnung der Cookies auf der Drittwebseite auch Standortdaten und Zugangsdaten, die bis zur Ablehnung der Cookies bereits erhoben wurden. Das folgt schon

daraus, dass die Beklagte, wie sie in der mündlichen Verhandlung vor dem Senat eingeräumt hat, auch Daten von Dritten erhält, die gar nicht auf ihrem Netzwerk angemeldet sind, weil der Drittwebseitenbetreiber nicht weiß, welcher Nutzer bei der Beklagten angemeldet ist und alle erhobenen Daten – soweit er sie nicht selbst über Cookies filtert – an die Beklagte zurücksendet (vgl. ebenfalls S. 6 Anlage K 1).

bb) Art. 6 Abs. 1 lit. b) DSGVO (Erforderlichkeit)
Die Datenverarbeitung über die Business-Tools war auch nicht erforderlich für die Vertragserfüllung. Im Grundsatz trägt die Beklagte als Verantwortliche die Darlegungs- und Beweislast für die Erforderlichkeit der von ihr vorgenommenen Datenverarbeitung (BGH, Urteil vom 18. Dezember 2025, I ZR 97/25, Rn. 45, juris).

(1) Eine Verarbeitung ist nur dann zur Vertragserfüllung „erforderlich", wenn diese objektiv für einen Zweck unerlässlich ist, der notwendiger Bestandteil des Vertrags – letztlich Hauptgegenstand des Vertrags – ist; eine bloße Nützlichkeit der Verarbeitung genügt nicht (EDSA, Leitlinien 2/2019, Version 2.0, Rn. 27 ff.). Der EuGH hat hierzu zu den streitgegenständlichen Tools ausgeführt:

„dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als im Sinne dieser Vorschrift für die Erfüllung eines Vertrags, dessen Vertragsparteien die betroffenen Personen sind, erforderlich angesehen werden kann, wenn diese Verarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte." (EuGH, Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./Bundeskartellamt), Rn. 125, juris).

In einem zweiten Schritt (vgl. unten lit. dd) ist weiter zu fragen, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch Art. 7 und 8 der EU-Grundrechte-charta gewährleisteten, eingreifen. Hierbei ist auch Art. 5 Abs. 1 lit. c DSGVO zu beachten (EuGH, Urteil vom 7. Dezember 2023, C-26/22, Rn. 77 f., juris).

Im Grundsatz trägt die Beklagte als Verantwortliche die Darlegungs- und Beweislast für die Erforderlichkeit der von ihr vorgenommenen Datenverarbeitung (BGH, Urteil vom 18. Dezember 2025, I ZR 97/25, Rn. 45; EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 98; juris).

(2) Weshalb die Übermittlung von Daten an Drittunternehmen u. a. zu Werbungs- und Targetingzwecken und sodann zurück an die Beklagte für die Erfüllung des Vertragszwecks eines Social Media Accounts erforderlich gewesen sein soll, ist nicht ersichtlich. Der Vertragszweck der Beklagten ist in ihren Nutzungsbedingungen formuliert als *„Technologien und Dienste, mit deren Hilfe sich Menschen miteinander vernetzen, Gemeinschaften bilden und ihre Unternehmen stärken können“* (vgl. Anlage B 5, S. 1). Dem Senat erschließt sich nicht, welcher rechtmäßige Zusammenhang zwischen dem Vertragszweck eines Social Media Accounts und der Verknüpfung der Daten der Klagepartei mit solchen von Drittunternehmen bestehen könnte, um diesen Werbung und der Beklagten ein Targeting zu ermöglichen, wie es die Mitteilung Propellant Media in Anlage B 4 verspricht.

Die Beklagte kann das Tatbestandsmerkmal der Erforderlichkeit auch nicht dadurch bestimmen, dass sie als marktbeherrschendes Unternehmen durch die Definition ihres Leistungsangebotes unter „Hintanstellung der Nutzerinteressen allein an ihrem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestands personenbezogener Daten seiner Nutzer auszurichten und über das für die Benutzung des sozialen Netzwerkes erforderliche Maß auszuweiten“, mithin die vertragscharakteristische Leistung willkürlich und einseitig ausweitet (BGH, Beschluss vom 23. Juni 2020, KVR 69/19, Rn. 110, juris).

Die Datenübertragung ist auch nicht zum Zwecke der Direktwerbung erforderlich (EWG 47 DSGVO). Denn die Klagepartei schließt eine solche durch Ablehnung der Cookies in der Regel und soweit möglich gerade aus. Die Beklagte bietet deshalb eine werbefreie Variante gerade an. Weshalb dann weitere Daten überhaupt erhoben werden müssen, erschließt sich angesichts der Bezahlvariante nicht.

(3) Die Beklagte kann sich auch nicht darauf berufen, es handele sich teilweise um Daten, die wegen der Eigenart des Internets erhoben werden. Soweit der EuGH auf die Notwendigkeit der Übermittlung von Browserdaten für bestimmte Zwecke verweist (EuGH, Urteil vom 29. Juli 2019, C-40/17 Rn. 26, Fashion ID, juris), ist der dortige Fall nicht vergleichbar. Es geht hier um einen Missbrauch der über das Social-Media-Versprechen der Vernetzung

von Freunden und Familie eingeholten Daten zu deren systematischer wirtschaftlicher Ausnutzung im vorrangigen Interesse der Beklagten und um aus der Funktionsweise des Internets Profit zu schlagen.

cc) Art. 6 Abs. 1 lit. c) bis e) DSGVO
Es besteht auch kein Rechtfertigungsgrund gemäß Art. 6 Abs. 1 lit. c) bis e) DSGVO.

(1) Gemäß lit. c) ist die Datenverarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung kraft Rechts der Union oder eines Mitgliedstaates zur Verfolgung eines gemäß Art. 6 Abs. 3 Satz 4 DSGVO im öffentlichen Interesse liegenden Ziels erforderlich ist (EuGH, Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./ Bundeskartellamt), Rn. 125, 133, juris; vgl. BeckOK DatenschutzR/Albers/Veit, 32. Ed., Art. 6 DSGVO Rn. 34; Heberlein in Ehmann/Selmayr, DSGVO, 2. Aufl., Art. 6 Rn. 16; Buchner/Petri in Kühling/Buchner, DSGVO, 2. Aufl., Art. 6 Rn. 77; vgl. Plath/Plath, DSGVO, 3. Aufl., Art. 6 Rn. 38 m. w. N.). Solches ist nicht ersichtlich. Der EuGH führt vielmehr aus, dass es hinsichtlich der Beklagten „*angesichts der Art und des im Wesentlichen wirtschaftlichen und kommerziellen Charakters der Tätigkeit dieses privaten Wirtschaftsteilnehmers allerdings wenig wahrscheinlich erscheint, dass ihm eine solche Aufgabe (zum Wohle der Gesellschaft oder die Förderung von Schutz, Integrität und Sicherheit – Einfügung durch den Senat) übertragen worden ist.*“ (EuGH, a. a. O., Rn. 133). Solches trägt die Beklagte auch nicht vor.

(2) Dasselbe folgt aus Art. 6 Abs. 1 lit. d) und e) DSGVO, der die Datenverarbeitung erlaubt, um lebenswichtige Interessen der betroffenen Personen oder anderer natürlicher Personen zu schützen.

Nach den Anforderungen des EuGH ist die streitgegenständliche Datenerhebung nicht erforderlich i. S. d. Art. 6 Abs. 1 lit. d) und e) (EuGH, Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./Bundeskartellamt), Rn. 130, 137, juris).

(3) Es ist auch nicht ersichtlich, dass die Datenverarbeitung für die Systeme und deren Arbeitsfähigkeit aus technischer Sicht erforderlich wäre. Die Beklagte behauptet zwar, die Datenerhebung sei aus Sicherheits- und Integritätsgründen erforderlich, vereinzelt ihren Vortrag hierzu aber nicht hinreichend. Es ist – außer mit Praktibilitätserwägungen der Beklagten – auch nicht nachvollziehbar, weshalb die Nutzerdaten aus Sicherheitsgründen erforderlich sein sollten. Die Beklagte verarbeitet hier Nutzerdaten, die sie gar nicht erhalten dürfte, so dass sie diese auch nicht zur Ertüchtigung ihrer eigenen Systeme verwenden

kann. Soweit sie zuletzt mit Schriftsatz vom 16. Februar 2026 hierzu vorgetragen hat, verhilft dieser Vortrag nicht zur Bejahung der Berechtigung der verarbeiteten Daten.

Das folgt zunächst schon daraus, dass die Beklagte wiederum keine genauen Angaben macht („möglicherweise", „verstoßen könnten"). Der Umstand, dass kriminelle Aktivitäten aufgedeckt werden könnten, wird nicht in Verbindung gebracht mit den individuellen Nutzerdaten und der Notwendigkeit von deren Verarbeitung. Soweit die Datenverarbeitung für die Verarbeitung „einiger" Business-Tool-Daten erforderlich sei, wird dieser Vortrag zwar durch Beispiele unterlegt, weshalb aber die personenbezogenen Daten der Klagepartei hierfür erforderlich sein sollen, ist nicht ersichtlich. Es ist auch nicht vereinzelt, weshalb die Daten der Klagepartei, die Nachrichten- und Shoppingseiten besucht, zur Abwehr feindlicher Akteure erforderlich sein sollen.

(4) Die Beklagte kann die Daten auch nicht aus Gründen der Strafverfolgung verarbeiten (lit. ee)). Die Beklagte ist ein Wirtschaftsunternehmen und keine Strafverfolgungsbehörde. Sollen kriminelle Handlungen unterbunden werden, muss mit den Strafverfolgungsbehörden zusammengearbeitet werden, die dann über die Berechtigung und den Umfang der Verarbeitung entscheiden können. Die Begründung der rechtlichen Verpflichtung kann sich nur aus einer Rechtsgrundlage der Union oder eines Mitgliedstaates nach Abs. 3, S. 1 ergeben. Diese Rechtsgrundlage muss ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel stehen (Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 6 Abs. 1 Rn. 53, beck-online; EuGH (Große Kammer), Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./BKartA), Rn. 138, juris). Hierfür ist – insbesondere vor dem Hintergrund des Art. 6 Abs. 3 DSGVO – nichts ersichtlich. Pflichten aus Rechtsvorschriften anderer Staaten können nur als rechtliche Pflichten i. S. d. Vorschrift angesehen werden, wenn die Union oder der Mitgliedstaat sie in die eigene Rechtsordnung übernommen hat. Auch hierfür gibt es keinerlei Anhaltspunkte. Außerdem muss „*diese Verarbeitung innerhalb der Grenzen des unbedingt Notwendigen*" erfolgen. Diese Grenzen hat die Beklagte nicht erläutert.

dd) Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen)

Die Datenverarbeitung über die Business-Tools ist auch nicht zur Wahrung der berechtigten Interessen der Beklagten oder Dritter erforderlich. Danach ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener

Daten erfordern, überwiegen. Die Beklagte hat sich insoweit auf ihre Berufsausübungsfreiheit als berechtigtes Interesse berufen, die sie durch die Einhaltung der Vorschriften der DSGVO bedroht sieht. Ferner diene sie Mess- und Analysezwecken, der Nutzer- und Netzwerksicherheit, Forschungszwecken sowie der Möglichkeit, auf rechtliche Anfragen antworten zu können.

(1) Dabei dient die Verarbeitung über die Business-Tools *„nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich im Sinne dieser Vorschrift …, wenn der fragliche Betreiber den Nutzern, bei denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses unbedingt notwendig ist und wenn sich aus einer Abwägung der einander gegenüberstehenden Interessen unter Würdigung aller relevanten Umstände ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten dieser Nutzer gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.*“ (EuGH, Urteil vom 4. Juli 2023, C-252/21 (Meta Platforms Inc. u. a./Bundeskartellamt), Rn. 126, juris; BeckOK DatenschutzR/Veit/Albers, 54. Ed. 01.08.2025, DSGVO Art. 6 Rn. 66, beck-online). Hieran fehlt es noch immer.

(2) Zudem muss dieses Interesse zusätzlich zu den wirtschaftlichen Interessen der Beklagten bestehen (OLG München, Beschluss vom 19. November 2024, 27 U 2473/24 e, Rn. 14, beck-online; BeckOK DatenschutzR/Veit/Albers, 54. Ed. 01.08.2025, DSGVO Art. 6 Rn. 68 m. w. N., beck-online). Ein solches überschießendes Interesse ist nicht ersichtlich.

(3) Zwar kann die Verarbeitung von Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden (EWG 47 Satz 7 und Art. 21 Abs. 3 DSGVO), gegen eine Interessenabwägung gem. Art. 6 Abs. 1 lit. f DSGVO spricht aber hier, dass die bezweckte Informationsgewinnung zur Planung weiterer Werbemaßnahmen auch für weitere, über die bloße Direktwerbung hinausgehende Werbeaktivitäten durch Anlegung eines digitalen Fingerabdrucks genutzt wird und die Direktwerbung gerade ausgeschaltet werden kann. Insofern müsste der Drittanbieter die Klagepartei bei Datenerhebung darüber informieren, dass diese Daten an die Beklagte zur Erkennung ihrer Nutzereigenschaft übermittelt und dann für weitere Targetingmaßnahmen genutzt werden. Genau dieser Umstand spricht für eine eingriffsintensive Verarbeitung und überwiegende Interessen der Nutzer und damit der Klagepartei. Denn damit wird der Kunde zum Objekt der Zuordnung zu bestimmten Gruppen im rein wirtschaftlichen Interesse der Beklagten. In

keinem Fall hat die Klagepartei ihre personenbezogenen Daten für derartige Zwecke angegeben, so dass ihre Interessen, Grundrechte und Grundfreiheiten gegenüber dem berechtigten Interesse der Beklagten überwiegen (Boymanns/Schönbrunn: Customer-Matching mit Kundenlisten: Lösungswege für Unternehmen, ZD 2025, 674, beck-online; EDSA-Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Version 2.0, Rn. 65).

(4) Vor diesem Hintergrund überwiegt das Interesse der Klagepartei auf informationelle Selbstbestimmung das Interesse der Beklagten auf Verarbeitung personenbezogener Daten zum Zweck des Targeting, Fingerprintings und der Eingruppierung in bestimmte Themengruppen. Es liegt fern, dass die Beklagte ihr Netzwerk nicht betreiben könnte und daher ihr Grundrecht auf Berufsausübung eingeschränkt wäre, wenn sie – wie sie durch die Nutzungsbedingungen oberflächlich gesehen vermittelt – die Daten gegen Werbung weitergeben würde oder auf diese Weitergabe im Abonnement verzichtet. Zwar steht der Wirksamkeit der Einwilligung nicht entgegen, dass die Bereitstellung der personenbezogenen Daten durch eine Vertragspartei selbst zum Gegenstand der Hauptleistungspflicht i. S. v. „Daten gegen Leistung“ gemacht wurde (OLG Frankfurt, Urteil vom 27. Juni 2019, 6 U 6/19, juris). Allerdings ist in diesen Fällen auf einen angemessenen Interessenausgleich der Vertragsparteien zu achten, wenn für den gewünschten Vertragsschluss wegen der marktbeherrschenden Stellung der Beklagten keine zumutbaren Alternativen zur Verfügung stehen (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 154, juris). Diesen Interessenausgleich nimmt die Beklagte nicht ansatzweise vor, wie sich aus Anlagen K 5 und K 6 ergibt. Für sie sind vielmehr ihre eigenen wirtschaftlichen Interessen alleiniges Maß. Das Recht der Klagepartei auf informationelle Selbstbestimmung wird von ihr nur nicht in ihre Überlegungen einbezogen, sie wischt dieses als störend weg, so dass sie schon vom Ansatz nicht über zumutbare Alternativen nachdenkt oder zu diesen vorträgt. Ein Grundrecht auf maximalen Profit ist mit der Berufungsausübungsfreiheit jedoch nicht verbunden, schon gar nicht schrankenlos.

(5) Entgegen der Ansicht der Beklagten handelt es sich bei den erhobenen Daten auch nicht um einen Abgleich der Nutzer mit der Kundenliste zur Informationseinholung für die Vorbereitung von Werbemaßnahmen inner- oder außerhalb der Plattform. Eine Erforderlichkeit wäre womöglich anzunehmen, wenn die Beklagte ihren Nutzern ein mit dem Tool-Einsatz verfolgtes berechtigtes Interesse mitgeteilt haben und dieser Abgleich von Nutzerdaten innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses unbedingt notwendig ist (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 126,

juris). Das ist mit dem digitalen Fingerprinting und der Eingruppierung im Falle der Cookie-Ablehnung gerade nicht der Fall.

(6) Dem Vortrag der Beklagten steht zudem bereits entgegen, dass er ihren eigenen Nutzerinformationen widerspricht, die eine Verarbeitung auch zu *„weiteren eigenen Zwecke wie Messungen und Verbesserung unserer Werbesysteme“* zulassen. 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.

(7) Darüber hinaus folgt aus dem Zweckbindungsgrundsatz, dass der Umfang der Datenverarbeitung, auf die sich die Einwilligung bezieht, für den Einwilligenden erkennbar sein muss, Art. 4 Nr. 11 DSGVO. Das Wissenselement umfasst daher die Kenntnis über alle mit der Datenverarbeitung zusammenhängenden relevanten Umstände, also Reichweite, Dauer, Umfang und Zweck der Datenverarbeitung und muss hinreichend bestimmt sein, Art. 5 Abs. 1 lit. b, Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 4 Nr. 11 DSGVO, EWG 32 DSGVO. Darüber hinaus folgt aus Art. 7 Abs. 2, S. 1 DSGVO das Transparenzgebot. Zu einer vollständigen Einwilligung hat die Beklagte gerade nicht vorgetragen. Die Reichweite der Datenverarbeitung, wie sie sich aus dem Meta Play Book und Anlage K 6 ergibt, ist nicht ansatzweise von der Cookie-Beschreibung auf Bl. 77 Bd. I d. A. umfasst.

ee) Einwilligung gemäß Artikel 9 DSGVO

Im vorliegenden Einzelfall sind unter den verarbeiteten Daten auch solche, die dem besonderen Schutz des Art. 9 DSGVO unterliegen („sensible Daten“) in Form von Daten über ihre politischen Meinungen. Damit muss die Verarbeitung des gesamten Datensatzes an Art. 9 Abs. 2 DSGVO gemessen werden (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 89, juris), wobei die Beklagte zum Umfang und der Art und Weise der Datenverarbeitung nicht konkret vorgetragen hat.

Eine wirksame Einwilligung scheitert an der fehlenden ausdrücklichen freiwilligen Einwilligung in die Verarbeitung von besonderen Datenkategorien nach Art. 9 Abs. 1 lit. a DSGVO.

b)
Die Klagepartei hat daher einen Löschungsanspruch wegen der unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten (lit. d). Die personenbezogenen Daten der Klagepartei wurden durch die Beklagte durch die Verwendung der Business-Tools unrechtmäßig verarbeitet. Dies geschah ohne Einwilligung oder sonstige Rechtfertigung. Insbesondere der Nutzungsvertrag zwischen den beiden Parteien gestattet die Verarbeitung der personenbezogenen Daten seit dem 24. November 2019 nicht. Die dem Urteil zugrunde zu legenden Datenverarbeitungsvorgänge sind nicht von einer Einwilligung der Klagepartei abgedeckt. Die Beklagte kann sich insbesondere nicht auf eine Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO berufen, auch wenn die Klagepartei die Abo-Variante nicht angenommen hat.

cc) Die Beklagte verarbeitet unstreitig personenbezogene Daten der Klagepartei, Art. 4 Nr. 1 DSGVO.

b)
Das Löschungsrecht der Klagepartei ist auch nicht gemäß Art. 17 Abs. 3 DSGVO eingeschränkt. Nach Abs. 3 besteht kein Löschungsanspruch nach Abs. 1, soweit die Verarbeitung aus den nachfolgend aufgezählten Gründen erforderlich ist. Greift einer der Ausnahmetatbestände, soll eine weitere Verarbeitung der personenbezogenen Daten rechtmäßig sein (Erwägungsgrund 65; BeckOK DatenschutzR/Worms, 54. Ed. 01.11.2024, DSGVO Art. 17 Rn. 78, beck-online). Keiner der in Abs. 3 genannten Fälle liegt hier vor.

c)
Einen Anspruch auf Anonymisierung kennt die DSGVO demgegenüber nicht, ein solcher ist auch kein ‚Minus' zur Löschung, nachdem er mit erheblichem Aufwand verbunden sein kann (ebenso Senat, Urteil vom 5. Februar 2026, 9 U 44/25 und 9 U 124/24, unv.; OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25, Rn. 261, beck-online; a. A.: OLG Dresden, Urteil vom 3. Februar 2026, 4 U 292/25, Rn. 75, beck-online). Art. 32 DSGVO gibt keinen Individualanspruch (BeckOK IT-Recht/Borges, 20. Ed. 01.04.2025, DSGVO Art. 32, beck-online), sondern einen Schadenersatzanspruch bei Verletzung der Pflicht zu Anonymisierung gemäß Art. 82 Abs. 1 DSGVO (Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 31 f., beck-online). Zwar kann die betroffene Person den Umfang ihres Löschungsrechts selbst bestimmen, zum Beispiel durch Beschränkung ihres Antrags auf bestimmte Daten, Datenarten aber auch auf bestimmte Formen, Zwecke oder Teile der Verarbeitung (BGH, Beschluss vom 4. Juni 2024, II ZB 10/23, Rn. 19, juris), dass

aber hieraus eine Verpflichtung zu einem womöglich aufwendigen Tun folgen könnte, ist nicht ersichtlich.

d)
Auch ein vertraglicher Anspruch aus einer wirksamen Abrede über eine alternative Erfüllungsmodalität i. S. einer Wahlschuld gemäß § 262 BGB besteht nicht. Die Beklagte hat vorliegend das klägerische Angebot (anstelle einer Löschung die Daten zu anonymisieren) unmissverständlich zurückgewiesen und damit abgelehnt.

e)
Der klägerische Anspruch auf Löschung ist des Weiteren nicht bereits durch die Zurverfügungstellung des Self-Service-Tools der Beklagten erfüllt. Zwar ist der Beklagten die Verwendung von automatisierten Verfahrensweisen zur Löschung bzw. Anonymisierung der Nutzerdaten grundsätzlich zuzubilligen (vgl. Paal/Pauly/Paal, 3. Aufl. 2021, DSGVO Art. 17 Rn. 29), jedoch hat die Beklagte nicht hinreichend dazu vorgetragen, dass die von ihr zur Verfügung gestellten Tools eine vollständige Löschung sämtlicher Daten, insbesondere der unter Antrag Ziff. 1 genannten, ermöglichen. Denn die Klagepartei kann in ihren Datenschutzeinstellungen zwar die Löschung durch Auswahl der Optionen „Frühere Aktivitäten löschen“ bzw. „Künftige Aktivitäten trennen“ vornehmen. Hierdurch werden die Off-Site-Daten jedoch lediglich vom Account der Klagepartei getrennt, nicht hingegen gelöscht (vgl. etwa ebenfalls: LG Stuttgart, Urteil vom 5. Februar 2025, 27 O 190/23, Rn. 27, juris). Nach dem Vortrag der Klagepartei, dem die Beklagte nicht hinreichend entgegengetreten ist, bedeutet die Trennung lediglich eine Pseudonymisierung der Daten, die letztlich umkehrbar ist (s. Art. 4 Nr. 5 DSGVO). Dies ist gerade nicht ausreichend.

f)
Schließlich muss sich die Klagepartei nicht auf eine eigene Löschung ihres Nutzerprofils verweisen lassen. 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, Beschluss vom 2. Mai 2022, B6-27/21). Gerade für die Teilhabe am gesellschaftlichen Leben handelt es sich bei den Netzwerken der Beklagten mittlerweile um eine für den durchschnittlichen Bürger essenzielle Dienstleistung (vgl. Erwägungsgründe Nr. 1, 3 zur VO (EU) vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, Gesetz über digitale Dienste), die faktisch nicht durch ein alternatives Netzwerk ersetzt werden kann (zusammenfassend zu den Hintergründen siehe Mohr, Kartellrechtlicher Konditionenmissbrauch durch datenschutzwidrige Allgemeine Geschäftsbedingungen, EuZW 2019, 265 unter Bezugnahme auf

die Facebook-Entscheidung des Bundeskartellamts vom 6. Februar 2019). Der Klagepartei ist es deshalb nicht zuzumuten, dass sie sämtliche Profile bei der Beklagten löscht und ihre Nutzung beendet. Vielmehr muss ihr die Möglichkeit eröffnet bleiben, das Netzwerk der Beklagten zu nutzen, ohne dass die streitgegenständliche Datenverarbeitung über die Business-Tools stattfindet.

ff) Einwilligung gegenüber den Drittanbietern

Es kann dahinstehen, ob die Klagepartei auch Drittwebseiten eine wirksame Einwilligung zur Verarbeitung der dort angefallenen Daten erteilt hat. Entgegen der Ansicht der Beklagten oblag auch nicht den Drittanbietern allein die Einholung der Einwilligung in die Datenverarbeitung über die Business-Tools. Vielmehr ist die Beklagte auch Verantwortliche für die Verarbeitung der Daten im Sinne des Art. 28 DSGVO (EuGH, Urteil vom 29. Juli 2019, C-40/17, Rn. 106, juris; vgl. Abschnitt B. 3. c) bb)).

gg) Entgegen der Ansicht der Beklagten scheidet der Anspruch der Klagepartei auch nicht deshalb aus, weil sie sich nicht für das kostenpflichtige Abonnement entschieden hat. Der EuGH hat hierzu festgestellt, dass „diese Nutzer die Freiheit haben (müssen), im Zuge des Vertragsabschlusses die Einwilligung in bestimmte Datenverarbeitungsvorgänge, die für die Erfüllung des Vertrags nicht erforderlich sind, einzeln zu verweigern, ohne dazu gezwungen zu sein, auf die Nutzung des vom Betreiber des sozialen Online-Netzwerks angebotenen Dienstes vollständig zu verzichten, was bedingt, dass ihnen, gegebenenfalls gegen ein angemessenes Entgelt, eine gleichwertige Alternative angeboten wird, die nicht mit solchen Datenverarbeitungsvorgängen einhergeht“ (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 150, juris). Ob in der Abo-Variante bzw. dem kostenlosen Angebot ohne Werbung eine gleichwertige Alternative liegt, kann dahinstehen, weil die Daten der Nutzer trotzdem an die Beklagte übertragen werden, wie sich aus Anlage K 11 ergibt.

D. Klageantrag zu 3 (Schadensersatz)

Angesichts der rechtswidrigen Datenverarbeitung steht der Klagepartei zumindest gemäß Art. 82 Abs. 1 DSGVO ein Schadensersatzanspruch in Höhe von 1.500,00 EUR gegen die Beklagte zu. Insofern handelt es sich um einen einheitlichen Anspruch, der – vergleichbar mit den sog. Scraping-Vorfällen – in einem einheitlichen Geschehen wurzelt, das hinsichtlich der damit verbundenen Folgen nicht in einzelne Datenschutzverstöße aufgespalten werden kann (BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 18; OLG Jena, aaO, Rn. 223, juris)

1.

Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen im Sinne von § 4 Nr. 7 DSGVO. Voraussetzungen dieses Anspruchs sind also ein Verstoß des Verantwortlichen gegen die DSGVO und ein kausal auf diese Pflichtverletzung zurückzuführender materieller oder immaterieller Schaden des Betroffenen (EuGH, Urteil vom 4. Mai 2023, C-300/21 Rn. 32, juris), der für diese Anspruchsvoraussetzungen die Beweislast trägt (EuGH, Urteil vom 24. Januar 2024, C-687/21, Rn. 61, juris). Dabei hat derjenige, der geltend macht, von negativen Folgen eines Verstoßes gegen die DSGVO betroffen zu sein, nachzuweisen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen. Beruft er sich auf die Befürchtung, seine personenbezogenen Daten könnten aufgrund des Verstoßes missbräuchlich verwendet werden, hat das nationale Gericht zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (EuGH, Urteil vom 14. Dezember 2023, C-340/21, Rn. 84 f., juris).

2.

Die Beklagte verarbeitet rechtswidrig unter Verstoß gegen Vorschriften der DSGVO personenbezogene Daten der Klagepartei. Auf die Ausführungen unter Abschnitt C. wird insoweit Bezug genommen.

3.

Die Klagepartei hat einen immateriellen Schaden erlitten.

a)

Die Auslegung des Schadensbegriffs erfolgt unionsrechtlich, so dass iRd Haftungsbegründung nicht auf das nationale Verständnis des immateriellen Schadens zurückgegriffen werden kann (BeckOK DatenschutzR/Quaas, 53. Ed. 1.8.2025, DS-GVO Art. 82 Rn. 23c; EuGH, Urteil vom 25. Januar 2024, C-687/21, Rn. 64, juris). Maßgebliche Grundlage ist EWG 146 S. 3 DSGVO, der ausdrücklich fordert, dass der Begriff des Schadens „weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht“ (Kühling/Buchner, DS-GVO BDSG/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 17; Taeger/Gabel, DSGVO – BDSG – TTDSG/Moos/Schefzig, 4. Aufl. 2022, DSGVO Art. 82 Rn. 27). Daneben enthalten EWG 75 und 85 DSGVO eine nicht abschließende Aufzählung potenzieller ersatzfähiger Schadensformen. Dort wird u. a. der Verlust

der Kontrolle über personenbezogene Daten als beispielhafte Ausprägung eines immateriellen Schadens benannt.

Der EuGH hat den Schadensersatzanspruch des Art. 82 Abs. 1 DSGVO in mehreren Entscheidungen präzisiert und betont, dass für dessen Geltendmachung drei kumulative Voraussetzungen erfüllt sein müssen:
- ein Verstoß gegen die Bestimmungen der DSGVO,
- ein entstandener materieller oder immaterieller Schaden sowie
- ein Kausalzusammenhang zwischen Schaden und Verstoß (BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 40 m. zahlr. w. N., juris).

Bereits *„ein zeitlich begrenzter Verlust der Kontrolle der betroffenen Person über ihre personenbezogenen Daten (kann)… ausreichen…, um einen immateriellen Schaden' zu verursachen*", sofern nachgewiesen werde, inwiefern die betroffene Person tatsächlich einen solchen Schaden erlitten habe (zuletzt: EuGH, Urteil vom 4. Oktober 2024, C-200/23, Rn. 140, 150, 156; BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 25, juris). Dabei braucht der Kontrollverlust nicht sicher festzustehen. Vielmehr reicht aus, dass die durch einen Verstoß gegen die DSGVO ausgelöste Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten von Dritten missbräuchlich verwendet werden, für sich genommen einen „immateriellen Schaden" im Sinne von Art. 82 Abs. 1 darstellen kann (vgl. in diesem Sinne EuGH, Urteile vom 14. Dezember 2023, C-340/21, Rn. 79 bis 86; vom 25. Januar 2024, MediaMarktSaturn, C-687/21, EU:C:2024:72, Rn. 65; vom 20. Juni 2024, C-590/22, Rn. 32; BGH, Urteil vom 13. Mai 2025, VI ZR 186/22, Rn. 34; BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 40, juris).

Entscheidend ist, ob die betroffene Person die tatsächliche Kontrolle über ihre Daten nicht (mehr) ausüben kann und eine weitere Verbreitung realistisch nicht mehr einzudämmen ist (ebenso: Boole: Kontrollverlust als Schaden, ZD 2026, 17) oder eine Befürchtung hierfür realistischerweise besteht. Ein wahrgenommener Kontrollverlust kann sich im Einzelfall in anhaltendem Stress, Angstzuständen, einem Gefühl erhöhter Verletzlichkeit, Schlafstörungen oder vermeidendem Kommunikationsverhalten – und damit in einem anhaltenden Gefühl des Unwohlseins – niederschlagen (Ikezuruora, Mind Matters: Investigating the Impact of Data Breaches on Mental Health, 2024, abrufbar unter: https://www.privacyend.com/impact-data-breaches-mental-health; Sustainability Directory, Why Is Digital Privacy Essential for Mental Health?, 2025, abrufbar unter: https://lifestyle.sustainability-directory.com/question/why-is-digital-privacy-essential-for-mental-health). Mit dem Verlust der Kontrolle über

personenbezogene Daten wird das grundlegende Bedürfnis nach Sicherheit und Vorhersehbarkeit unterminiert. Zugleich schwindet das Gefühl informationeller Selbstbestimmung sowie die Möglichkeit, Datenflüsse zu überblicken. Der Verlust der Datenhoheit geht regelmäßig mit Reichweiten-, Verknüpfungs- und Irreversibilitätsrisiken und -gefühlen einher. Demzufolge bezeichnet EWG 85 DSGVO ausdrücklich die „Einschränkung von Rechten" als Schaden. Aus EWG 75 DSGVO folgt, dass ein Identitätsdiebstahl und die Aufhebung der Pseudonymisierung einen Schaden darstellen können und wenn Daten genutzt werden, um persönliche Profile zu erstellen oder die Verarbeitung eine große Menge personenbezogener Daten umfasst. Ebenso wenig wie beim Kontrollverlust ist es für eine Befürchtung erforderlich, dass es zu einer missbräuchlichen Verwendung der Daten tatsächlich kommt. Die mit der begründeten Befürchtung einer missbräuchlichen Datenverwendung verbundenen negativen Folgen können auch negative Gefühle wie Sorge und Ärger sein, auch wenn diese Teil des allgemeinen Lebensrisikos sein können. Die Anforderungen an die Darlegung der Befürchtung eines Datenmissbrauchs dürfen nicht überspannt werden (vgl. EuGH, Urteil vom 4. September 2025, C-655/23, Rn. 62, 64; BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 37, juris). Je plausibler die Befürchtung eines Datenmissbrauchs im konkreten Fall erscheint, desto geringere Anforderungen sind an ihre Darlegung zu stellen (BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 38, juris).

b)

aa) Für die Zeit bis zum 3. November 2023 stellt der Senat einen Kontrollverlust der Daten der Klagepartei fest, die sich mindestens auf die im Antrag zu Ziff. 1 benannten Daten beziehen und in einer nicht genau feststellbaren, jedoch sehr hohen Quantität an Daten und die bis Oktober 2022 darüber hinaus in einem unsicheren Drittland verarbeitet wurden, ohne dass die hierfür erforderliche Einwilligung vorlag oder sonstige Rechtfertigungsgründe vorlagen. Der Senat sieht es in der Zusammenschau mit den Anlagen K 2, K 13 und K 14 und dem Ergebnis der informatorischen Anhörung der Klagepartei im Termin der mündlichen Verhandlung als erwiesen an, dass die Klagepartei einige der in den Anlagen K 2, K 13 bis 14 aufgeführten Webseiten im Rahmen ihres Surfverhaltens mehrfach besucht hat, auch wenn sie genaue Zeitpunkte und Dauer nicht mehr benennen kann. Denn sie hat in ihrer informatorischen Anhörung ausgeführt, regelmäßig und täglich (3-5 Stunden) das Internet zu nutzen, was der Senat für glaubhaft hält. Dabei handelt es sich auch um Finanz-, Gesundheits- und Erotikseiten und damit auch um sensible Daten i.S.d. 9 Abs. 1 DSGVO. Bei den aufgeführten Webseiten handelt es sich um ca. 40 v.H. der in Deutschland regelmäßig aufgesuchten Webseiten. Der Senat ist nach Prüfung der Webseiten in den Anlagen K 2, K 13 bis K 14 der Überzeugung, dass es sich hierbei um die gängigen Webseiten in

Deutschland handelt, die der deutsche Nutzer wie die Klagepartei regelmäßig und überwiegend aufruft. Dass es nach dem Vortrag in der Berufungserwiderung über 2 Mrd. Webseiten weltweit geben mag, lässt die Befürchtung nicht entfallen. Denn die Klagepartei hat in ihrer Anhörung neben der Senatsbekanntheit der Beliebtheit der in den Anlagen K 2, K 13 bis K 15 aufgeführten Webseiten auch zu den von ihr regelmäßig besuchten Webseiten, die mit den in den Anlagen benannten übereinstimmen, vorgetragen. Es erfolgte daher eine Verknüpfung mit dem Benutzerkonto der Klagepartei und eine Verwendung seiner sensiblen Daten.

Dass die Beklagte in einem Schriftsatz darauf verweist, dass es weltweit mehrere Millionen Webseiten gibt, ändert daran nichts, weil die Klagepartei vorgetragen hat, dass sie die deutschsprachigen Webseiten aufruft und nutzt.

Die Schilderung der Klagepartei zu den besuchten Webseiten ist auch nicht verspätet. Es kann dahinstehen, ob die Klagepartei in erster Instanz bereits hinreichend detailliert zu den besuchten Webseiten vorgetragen hat. Soweit dies zu verneinen wäre, handelte es sich bei dem Vorbringen in der mündlichen Verhandlung vor dem Senat zwar um neuen Vortrag gemäß § 531 Abs. 2 ZPO. Ob ein in zweiter Instanz konkretisiertes Vorbringen neu ist, hängt davon ab, wie allgemein es in erster Instanz gehalten war. Wenn es einen sehr allgemein gehaltenen Vortrag der ersten Instanz konkretisiert oder erstmals substantiiert, ist es neu, nicht aber dann, wenn ein bereits schlüssiges Vorbringen aus erster Instanz durch weitere Tatsachenbehauptungen zusätzlich konkretisiert, verdeutlicht oder erläutert wird (vgl. BGH, Urteil vom 14. Juli 2004, VIII ZR 367/03, Rn. 21, juris). Jedenfalls hat die Zulassung des neuen klägerischen Vortrages nach § 531 Abs. 2 Ziff. 2 ZPO zu erfolgen, weil das Landgericht die Klagepartei verfahrensfehlerhaft nicht auf die mangelnde Substanz ihres diesbezüglichen Vortrages hingewiesen hat. Zudem hat die Klagepartei sowohl in der Klage als auch in der Replik um einen gerichtlichen Hinweis gebeten, sollte weiterer Vortrag zur Substantiierung erforderlich sein. Sie hat hierzu ihren Rechtsstandpunkt zur Darlegungslast vorgetragen. Die Rechtsprechung des Bundesgerichtshofes zur Hinweispflicht des Gerichts ist streng. Danach hat das Gericht die Pflicht, auf die Komplettierung und Konkretisierung des Streitstoffes und seine prozessgerechte Aufbereitung hinzuwirken (vgl. zum Ganzen: Zöller-Greger, ZPO, 36. Aufl., § 139 ZPO, Rn. 2 ff.), anderenfalls muss das Berufungsgericht den Hinweis erneut erteilen und den daraufhin ergangenen Vortrag zulassen.

bb) Einen Kontrollverlust durch Abfassen ihrer Daten ab dem 3. November 2023 hat und konnte die Klagepartei mangels eigener Kenntnis weder darlegen noch beweisen, weil sie

zwar auf den Drittwebseiten nach Möglichkeit die Cookies ablehnt, aber eine solche Einstellung nicht auf Instagram vorgenommen hat. Damit aber können die Drittwebseiten Daten an die Beklagte übersenden, ohne dass die Klagepartei auch nur ansatzweise überblicken kann, welche Dimension diese Datenverarbeitung hat. Gerade dieser Umstand verstärkt das subjektive Gefühl des Ausgeliefertseins und führt dazu, dass die Befürchtung der Klagepartei vor einem Kontrollverlust ihrer Daten einem hier nicht feststellbaren tatsächlichen Kontrollverlust gleichzustellen ist. Diese Befürchtung ist auch begründet. Die Klagepartei hat umfassend dargelegt, wie sie diese Ungewissheit der Verwendung ihrer Daten belaste, sie kein Vertrauen mehr in die Datenübermittlung habe. Diese Umstände reichen für einen Kontrollverlust aus.

Die Einholung eines Sachverständigengutachtens zur Frage der genauen Datenübermittlung über die Conversions API war daher nicht erforderlich. Denn wie die Beklagte im Meta Play Book (dort S. 23) und in Anlage *Redesigning our systems to provide more control over Off-Facebook Activity*, dort S. 3 und 4, einräumt, werden die Daten weiterverarbeitet, weil weiterhin verlässliche Berichte an die Drittunternehmen übermittelt werden sollen. Daraus ergibt sich, dass die Beklagte weiterhin die Daten der Klagepartei – lediglich in einem Bündel mit den Daten anderer Nutzer – nutzt, auch wenn die Klagepartei einer Nutzung ihrer Daten für Werbezwecke widersprochen hat. Die Befürchtung ist hier daher auch nicht rein hypothetisch.

In ihrer informatorischen Vernehmung vor dem Senat hat die Klagepartei überzeugend und plausibel dargelegt, dass sie aufgrund der systematischen und von ihr ungewollten Datenabfassung einen Identitätsdiebstahl befürchtet. Sie fragt sich, welche Daten weitergegeben werden und wer bei ihr mitliest. Die Befürchtung eines Kontrollverlusts liegt nach ihrer Aussage in der ständigen und sich kontinuierlich wiederholenden Verletzung datenschutzrechtlicher Vorschriften in Verbindung mit der Infiltrierung hunderter Webseiten mit Business-Tools, die sie regelmäßig aufruft und über die sie letztlich keine Kenntnis hat (vgl. Anlagen K 2, K 13 und K 14).

cc) Verschulden

(1) Ferner ist erforderlich, dass dieser rechtswidrige Umgang mit den Daten schuldhaft, dh gem. § 276 BGB vorsätzlich oder fahrlässig erfolgte, wobei Art. 82 Abs. 3 DSGVO hinsichtlich des Nachweises des Verschuldens eine Umkehr der Beweislast vorsieht, indem zunächst ein schuldhaftes Verhalten vermutet wird, von dem sich der Verantwortliche oder der Auftragsverarbeiter entlasten kann, wenn er nachweist, dass er in keinerlei Hinsicht für

den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DSGVO Art. 82 Rn. 24, beck-online).

(2) Dass die beständige und praktisch täglich neue Zuwiderhandlung seit 16. Juli 2020 bis zum 3. November 2023 als auch darüber hinaus einen vorsätzlichen Charakter hatte, folgt aus dem Umstand, dass die Beklagte gegen die DSGVO verstoßen hat, obwohl die Beklagte seit dem Jahr 2016 wusste, dass die Übermittlungen an Drittanbieter einen Verstoß gegen die DSGVO auslösen würden. Das Bundeskartellamt hat auf ein im März 2016 eingeleitetes Verfahren mit Beschluss vom 6. Februar 2019 der Beklagten auf der Grundlage von § 19 Abs. 1 GWB untersagt, Konditionen zu verwenden, die die Nutzung von Facebook durch private Nutzer davon abhängig machen, dass Facebook Daten, die bei dem Besuch von Webseiten oder bei der Nutzung mobiler Apps dritter Anbieter über Programmierstellen („Facebook Business-Tools") erfasst werden, ohne Einwilligung der Nutzer mit den unter den „Facebook-Konten" gespeicherten Daten verknüpfen und verwenden kann und eine wirksame Einwilligung nur dann vorliegt, wenn die Bereitstellung des Dienstes Facebook.com nicht von der Erteilung der Einwilligung abhängig gemacht wird (Bundeskartellamt, Beschluss vom 6. Februar 2019, B6-22/16, juris). Der EuGH hat mit Urteil vom 16. Juli 2020, Facebook Ireland und Schrems (C-311/18) die Datenübermittlung in die USA als rechtswidrig erkannt. Spätestens seit diesem Zeitpunkt, für die USA-Datenübermittlung bis Oktober 2022, hat die Beklagte daher vorsätzlich oder zumindest mit dolus eventualis gehandelt. Diese Datenübertragung gilt auch für Instagram.

Aus Art. 25 Abs. 1 DSGVO geht eindeutig hervor, dass der für die Verarbeitung Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst verpflichtet ist, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Grundsätze des Datenschutzes wirksam umzusetzen und die erforderlichen Garantien in die Verarbeitung einzubeziehen, damit die Anforderungen der DSGVO erfüllt und die Rechte der betroffenen Personen geschützt werden. Auch aus dem Fallbericht des Bundeskartellamts vom 9. Oktober 2024 (B6-22/16) ergibt sich, dass noch am 9. Oktober 2024 und damit nach Implementierung der Cookies dem Nutzer noch nicht bewusst gemacht werde, dass die Akzeptanz der Cookies ein dauerhaftes Hinzufügen der Daten zu einem individuellen Profil bedeute und eine differenzierte Entscheidung nicht möglich sei. Zudem hat die EU-Kommission am 25. März 2024 ein Verfahren gegen das werbungsfreie Abomodell eingeleitet (https://ec.europa.eu/commission/presscorner/detail/de/ip_24_3582). Für Verstöße durch das sog. „Consent or Pay-Modell" der Beklagten, weil Verbraucher keinen Dienst wählen

konnten, bei dem weniger personenbezogene Daten verwendet werden, hat die Europäische Kommission gegen die Beklagte am 23. April 2025 eine Geldbuße von 200 Mio. EUR verhängt.

Art. 82 DSGVO ist zudem dahin auszulegen, dass das Verschulden vermutet wird, wenn der Verantwortliche nicht nachweist, dass die Handlung, die den Schaden verursacht hat, ihm nicht zurechenbar ist (EuGH, Urteil vom 4. Oktober 2024, C-507/23, juris Rn. 24; EuGH, Urteil vom 21. Dezember 2023, C-667/21, Rn. 103; Senat, Urteil vom 26. Juni 2025, 9 U 88/23, Rn. 36, juris). Das ist der Beklagten nicht gelungen.

dd) Kausalität
Die Verwendung der Business-Tools ist kausal zu dem von der Klagepartei empfundenen Kontrollverlust und der Befürchtung eines solchen. Hierfür ist es ausreichend, dass feststeht, dass die Beklagte ständig personenbezogene, sensible Daten über das Internetnutzungsverhalten innerhalb oder außerhalb ihres Netzwerkes erhoben hat und erheben kann und sich daraus das Wissen bzw. die Befürchtung der Klagepartei ergibt, bei der Nutzung des Internets und damit bei einem großen Teil seines Lebens in dystopischer Weise – weil sowohl das Ausmaß als auch die Art und Weise der Verarbeitung nebst den damit verbundenen Folgen nicht mehr nachverfolgbar oder auch nur ansatzweise nachvollziehbar ist – überwacht zu werden.

c) Höhe
aa) Art. 82 DSGVO enthält keine eigenen Bemessungsregeln für die Höhe des Schadenersatzes. Nach EWG 146 DSGVO ist ein vollständiger und wirksamer Schadenersatz erforderlich.

Daher sind „insbesondere die Festlegung der Kriterien für die Ermittlung des Umfangs des geschuldeten Schadensersatzes in Ermangelung einschlägiger unionsrechtlicher Vorschriften Aufgabe des Rechts des einzelnen Mitgliedstaats, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten“ (EuGH, Urteil vom 4. Mai 2023, C-300/21, Rn. 54, juris), so dass § 287 ZPO anwendbar ist. Darüber hinaus erkennt der EuGH eine Ausgleichsfunktion des Schadensersatzes an. Der erlittene Schaden ist „vollständig und wirksam“ auszugleichen. Eine strafende oder abschreckende Funktion kommt Art. 82 DSGVO ausdrücklich nicht zu. Ziel ist ein Ausgleich ohne symbolische Unterkompensation und ohne überkompensierende Strafwirkung (EuGH, Urteil vom 4. Mai 2023, C-300/21, Rn. 58; EuGH, Urteil vom 25. Januar 2024, C-687/21, Rn. 60; EuGH, Urteil vom 20. Juni 2024, C-182/22 und C-189/22, Rn. 45 f.; EuGH, Urteil vom 4. Oktober 2024, C-200/23, Rn. 141; BGH, Urteil

vom 18. November 2024, VI ZR 10/24, Rn. 97; juris). Der BGH geht in ständiger Rechtsprechung davon aus, dass, wenn die Haftung dem Grunde nach besteht, ein Anspruch nicht allein deshalb abgewiesen werden darf, weil Anhaltspunkte für eine Schätzung des gesamten Schadens fehlen. In diesen Fällen ist vielmehr zu prüfen, ob sich aus dem Sachverhalt nicht ein in jedem Fall gegebener Mindestschaden ergibt. Die Anforderungen an die Substantiierung sind i. R. d. § 287 ZPO niedriger als für die anspruchs-begründenden Tatsachen (BGH, Urteil vom 24. September 2014, VIII ZR 394/12, Rn. 73, juris). Nur wenn mangels greifbarer Anhaltspunkte eine Grundlage für das Urteil nicht zu gewinnen ist und das richterliche Ermessen vollends in der Luft hängen würde, wenn also eine Schätzung nicht möglich ist, bleibt es bei der Regel, dass den Kläger die Beweislast für die klagebegründenden Tatsachen trifft und deren Nichterweislichkeit ihm schadet (BGH, Urteil vom 6. Dezember 2012, VII ZR 84/10, Rn. 23, juris).

Die Modalitäten der Schadensermittlung dürfen bei einem – wie im Streitfall – unter das Unionsrecht fallenden Sachverhalt nicht ungünstiger sein als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz). Auch dürfen sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz), (vgl. EuGH, Urteile vom 4. Oktober 2024, C-507/23, Rn. 31; vom 20. Juni 2024, C-182/22 und C-189/22, Rn. 32; vom 4. Mai 2023, C-300/21, Rn. 53; BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 95, juris).

bb) Sofern ein Schaden allein im Kontrollverlust besteht, sind die Sensibilität der konkret betroffenen personenbezogenen Daten, auch aus Art. 9 DSGVO (EWG 75 DSGVO), deren typischerweise zweckgemäße Verwendung, die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle etwa durch Entfernung einer Veröffentlichung aus dem Internet oder Änderung des personenbezogenen Datums, z. B. in Form eines Rufnummernwechsels oder einer neuen Kreditkartennummer zu berücksichtigen (BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 99, juris).

Zu berücksichtigen ist weiter, dass der Eingriff seit knapp acht Jahren kontinuierlich erfolgt und nur die Beklagte als „Spion“ im Hintergrund weiß, welche Daten in welchem Umfang tatsächlich verarbeitet wurden, die Klagepartei mithin im Ungewissen ist, über welche Daten die Beklagte verfügt und wie sie diese verarbeitet und an wen sie sie weitergibt. Diese Unwissenheit schafft Unsicherheit.

cc) Im Kern geht es also um den Schutz der Verhaltensfreiheit des Einzelnen und damit um eine Vorverlagerung des Freiheitsschutzes auf die Stufe der Persönlichkeitsrechtsgefährdung. Wenn der Einzelne damit rechnen und befürchten muss, dass sein Handeln registriert wird, wird er davon Abstand nehmen – erst recht, wenn er negative Folgen hierdurch befürchtet und vom Schlimmsten ausgehen muss. Es kommt zu einem Einschüchterungseffekt; gewissermaßen setzt beim Einzelnen die „Schere im Kopf" an. Dies gilt aber nicht nur, wenn ihm unmittelbar Nachteile drohen. Wenn andere sich aufgrund von Informationen bereits ein festes Bild über den Einzelnen gemacht haben, ist der Einzelne in seiner Fähigkeit eingeschränkt, selbst zu entscheiden, wie er sich anderen gegenüber darstellen möchte und seine Selbstdarstellung gegenüber Dritten vielleicht im Leben auch einmal vollständig neu zu konstruieren. Damit ist keine Garantie verbunden, dass ihm eine Selbstdarstellung so gelingt, wie er es möchte; die Rahmenbedingungen müssen ihm aber zumindest die Chance geben.

In dieser Situation befindet sich die Klagepartei, was sie in ihrer informatorischen Anhörung vor dem Senat bestätigt hat.

dd) Für die Zeit nach dem 3. November 2023 ist die Befürchtung des Kontrollverlustes zu berücksichtigen. Ab dieser Zeit kann die Klagepartei noch nicht einmal abschätzen, was die Beklagte über ihn weiß und wie sie die Daten verwenden wird, was das Gefühl ausgelöst hat, ihr Privatleben kontinuierlich überwacht (ebenso EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 118 f., juris).

Hierbei ist zu berücksichtigen, dass die Klagepartei davon ausgehen muss, dass die Beklagte sehr viel über ihn weiß und sämtliche Daten gegen ihn verwenden wird. Die von der Klagepartei in der mündlichen Verhandlung vor dem Senat beschriebene Folge war die Anpassung seines Verhaltens, um nicht mehr Daten zu liefern.

Hieraus folgt: die Dimension des Datenschutzverstoßes liegt auf sämtlichen Ebenen des Lebens der Klagepartei und beeinträchtigt die Entfaltung ihrer Persönlichkeit für sich und in Beziehung zur Gesellschaft bis hin zum vorsichtigen und damit limitierten Agieren im Internet.

Zu berücksichtigen ist ferner die Erhebung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO.

ee) Für die Höhe des angemessenen Schadenersatzes bei Kontrollverlust bzw. dessen Befürchtung wegen Datenschutzverstößen zieht der Senat vergleichsweise das Urteil des

EuG vom 8. Januar 2025, T-354/22 (400 EUR); das Urteil des BGH vom 18. November 2024, VI ZR 10/24 (100 EUR); das Urteil des Landesarbeitsgerichts Mecklenburg-Vorpommern, Urteil vom 24. Mai 2019, 2 Sa 214/18 (2.000 EUR), das Urteil des OLG Koblenz vom 18. Mai 2022, 5 U 2141/21 (500 EUR), das Urteil des OLG Dresden vom 30. November 2021, 4 U 1158/21 (5.000 EUR), das Urteil des OLG Hamburg vom 10. Januar 2024, 13 U 70/23 (4.000 EUR) sowie die Urteile des OLG München vom 18. Dezember 2025, 14 U 1314/25 e (500 EUR), 14 U 2300/25 e (750 EUR), 14 U 1068/25 e (750 EUR) und 14 U 881/25 e (250 EUR) heran. In ihren neuesten Entscheidungen sind das OLG München von einem angemessenen Schadenersatz i. H. v. 500 EUR (OLG München, Urteil vom 18. Dezember 2025, 14 U 1314/25, Rn. 189, beck-online), das OLG Dresden i. H. v. 1.500 EUR (OLG Dresden, Urteil vom 3. Februar 2026, 4 U 292/25, Rn. 192, juris) und das OLG Jena i. H. v. 3.000 EUR (OLG Jena, Urteil vom 2. März 2026, 3 U 31/25, Rn. 232, juris).

Der Senat hält in diesem individuellen Fall ein Schmerzensgeld von 1.500,00 EUR für angemessen. Die Beeinträchtigungen sind primär höchstpersönlicher Natur und kommen körperlichen Beeinträchtigungen nicht nahe. Der Senat berücksichtigt dabei die Zeitdauer der ungehinderten Datensammlung, auch in den USA ohne angemessenes Rechtsschutzniveau, bis zur Implementierung des Abonnements und der Möglichkeit, Werbung über Cookies abzulehnen. Für diesen Zeitraum bis November 2023 hat die Beklagte sämtliche Daten einschließlich sensibler Daten, die die Klagepartei mit Drittwebseiten, die die Meta Pixel implementiert hatten, ungehindert und ungefiltert und ohne Zustimmung der Klagepartei in nicht gekannter Menge verarbeitet, obwohl ein Rechtfertigungsgrund nach Art. 6 DSGVO nicht vorlag. Eine Kontrolle über die eigenen Daten hatte die Klagepartei nicht mehr.

Für den Zeitraum ab dem November 2023 lässt sich – worauf die Beklagte zu Recht verweist – ein konkreter Kontrollverlust nicht nachweisen. Denn mit den Cookies war es, worauf das Bundeskartellamt mit der Fallstudie vom 9. Oktober 2024 hinweist (dort S. 2 ff, B6-22/16), möglich, Nutzungsdaten separat zu halten und die Nutzer zu befähigen, über den Menü-Punkt „Cookies verwalten“ einzustellen, dass ihre Daten bei Nutzung eines Dienstes der Beklagten nicht zusammengeführt werden. Außerdem ist nicht konkret feststellbar, in welchen Fällen die Klagepartei tatsächlich Cookies abgelehnt oder aus Zeit- und Bequemlichkeitsgründen, wie sie in der mündlichen Anhörung vor dem Senat eingeräumt hat, angenommen hat. Nichtsdestotrotz verbleibt die Befürchtung eines Kontrollverlustes. Die Klagepartei hat in ihrer informatorischen Anhörung hierzu ausgeführt, sie wisse nicht, was mit ihren Daten passiere. Es sei für sie undurchschaubar, in welchem System ihre

Daten landen würden, weshalb sie bewusst auf einige Seiten nicht mehr gehe und deutlich selektiere, aus Sorge, ihre Daten würden missbraucht.

Insgesamt rechtfertigt sich für den umfassenden, über fünfeinhalb Jahre andauernden, umfassenden Kontrollverlust und die mehr als zweijährige Befürchtung eines umfassenden Kontrollverlusts unter Berücksichtigung der Tatsache, dass die Klagepartei Anfangs erst 13 Jahre alt war und auch Seiten mit hohem Diskretionsinteresse besucht (Pornoseiten), ein individuelles Schmerzensgeld i. H. v. 1.500,00 EUR.

d)
Ob im Weiteren auch ein Anspruch gem. § 823 Abs. 1 BGB i. V. m. Art. 1, 2 GG aufgrund der Verletzung des Persönlichkeitsrechts besteht, wie die Klagepartei meint, kann dahinstehen, da dieser jedenfalls keinen höheren Schadensersatzanspruch begründet. Grundsätzlich haben die von der DSGVO zur Verfügung gestellten Rechtsbehelfe abschließenden Charakter, wie sich insbesondere aus den EWG 9 und 10 DSGVO ergibt. Dies gilt jedoch in Anbetracht des EWG 146 S. 4 nicht für Art. 82 DSGVO. Dementsprechend können konkurrierende Ansprüche aus §§ 823 ff. BGB ebenso wie aus quasivertraglichen oder vertraglichen Sonderverbindungen (§ 280 Abs. 1 BGB) bestehen (Sydow/Marsch DSGVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 27, beck-online).

aa) Ein Anspruch aus § 823 Abs. 1 BGB in Verbindung mit Art. 2 Abs. 1, Art. 1 Abs. 1 GG erfordert eine hinreichend schwerwiegende Persönlichkeitsverletzung oder Verletzung des Rechts auf informationelle Selbstbestimmung, deren Ausgleich eine Geldzahlung rechtfertigt (BGH, Urteil vom 12. März 2024, VI ZR 1370/20, Rn. 70; OLG Hamm, Urteil vom 29. November 2024, I-25 U 12/24, Rn. 32, juris). Ob eine solche vorliegt, kann hier dahinstehen, weil eine solche jedenfalls keinen höheren immateriellen Schadenersatz rechtfertigen würde (so auch OLG Jena, a. a. O., Rn. 244).

bb) Ein Anspruch aus § 7 BDSG a. F. oder § 823 Abs. 1 BGB in Verbindung mit Art. 2 Abs. 1, Art. 1 Abs. 1 GG wegen einer Persönlichkeitsrechtsverletzung kommt nicht in Betracht (vgl. OLG Hamm, Urteil vom 15. August 2023, 7 U 19/23, Rn. 202 - 204, juris). Während § 7 BDSG a. F. nur den Ersatz eines materiellen Schadens vorsieht (BGH, Urteil vom 29. November 2016, VI ZR 530/15, Rn. 11 ff.; OLG Köln, Urteil vom 16. Dezember 2022, 7 U 184/21, Rn. 11 ff., juris), setzt ein Anspruch aus § 823 Abs. 1 BGB in Verbindung mit Art. 2 Abs. 1, Art. 1 Abs. 1 GG regelmäßig ebenfalls eine schwerwiegende Persönlichkeitsrechtsverletzung voraus, die hier jedenfalls zu keinem höheren Schadenersatz führen würde.

cc) Die Voraussetzungen eines Anspruchs aus § 280 Abs. 1 BGB und § 823 Abs. 2 BGB bedürfen keiner weiteren Erörterung, weil sich aus diesen Rechtsgrundlagen – ihre Voraussetzungen unterstellt – kein Anspruch auf einen über 1.500,00 EUR hinausgehenden Schadensbetrag ergeben würden. Die für die Bemessung der Schadenshöhe im Rahmen des Anspruchs gemäß Art. 82 DSGVO maßgeblichen Gesichtspunkte sind für die Schadensbemessung im Rahmen der vorstehenden Anspruchslagen ebenfalls maßgeblich. Die unionsrechtlichen Beschränkungen bewirken im vorliegenden Fall keine Beschränkung des Schadens, so dass dieser unter alleiniger Anwendung nationalen Rechts auch unter Berücksichtigung des gravierenden Verschuldens der Beklagten nicht höher zu bemessen wäre.

dd) Ein Anspruch auf Schadensersatz folgt auch nicht aus § 280 Abs. 1, § 241 Abs. 2 BGB (vgl. zum Nutzungsvertrag auch BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 83 m. w. N., Rn. 50, juris), da es bereits an einem immateriellen Schaden der Klagepartei mangelt und insoweit im Rahmen von § 253 Abs. 2 BGB die Erheblichkeits- / Bagatellgrenze für den Ersatz immateriellen Schadens nicht überschritten ist (vgl. zur Gesundheitsverletzung: BGH, Urteil vom 6. Dezember 2022, VI ZR 168/21, Rn. 18, juris).

4.
Der Zinsanspruch folgt aus §§ 288 Abs. 1, 291, 187 Abs. 1 analog BGB mit Zustellung am 19. Dezember 2023.

E. Klageantrag zu 4 (außergerichtliche Rechtsanwaltskosten)

Der Klagepartei steht gegen die Beklagte infolge des von der Beklagten begangenen Datenschutzverstoßes aus Art. 82 Abs. 1 DSGVO i. V. m. § 257 BGB schließlich ein auf Freistellung von vorgerichtlichen Rechtsanwaltskosten gerichteter Anspruch in der aus dem Tenor ersichtlichen Höhe zu.

1.
Die Kosten der Rechtsverfolgung und deshalb auch die Kosten eines mit der Sache befassten Rechtsanwalts gehören, soweit sie zur Wahrnehmung der Rechte erforderlich und zweckmäßig waren, grundsätzlich zu dem wegen einer unerlaubten Handlung zu ersetzenden Schaden. Dabei ist maßgeblich, wie sich die voraussichtliche Abwicklung des Schadensfalls aus der Sicht des Geschädigten darstellt. Ist die Verantwortung für den Schaden und damit die Haftung von vornherein nach Grund und Höhe derart klar, dass aus der Sicht des Geschädigten kein vernünftiger Zweifel daran bestehen kann, dass der Schädiger ohne

Weiteres seiner Ersatzpflicht nachkommen werde, so wird es grundsätzlich nicht erforderlich sein, schon für die erstmalige Geltendmachung des Schadens gegenüber dem Schädiger einen Rechtsanwalt hinzuzuziehen. In derart einfach gelagerten Fällen kann der Geschädigte den Schaden grundsätzlich selbst geltend machen, so dass sich die sofortige Einschaltung eines Rechtsanwalts nur unter besonderen Voraussetzungen als erforderlich erweisen kann (BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 79, juris).

2.
Nach diesen Maßstäben sind der Klagepartei die Rechtsanwaltskosten zu ersetzen, die auf die außergerichtliche Geltendmachung der begründeten Ansprüche, denen der Senat einen Wert von 3.500,00 EUR zumisst, entfallen.

Nach den Umständen, insbesondere wegen der für sie unübersichtlichen Rechtslage und aus Gründen des Sachzusammenhangs, durfte die Klagepartei aufgrund des Datenschutzverstoßes der Beklagten eine Beauftragung seines Prozessbevollmächtigten auch für erforderlich und zweckmäßig halten.

Auf der Grundlage des Gegenstandswertes der begründeten Ansprüche in Höhe von 3.500,00 EUR für die außergerichtliche Tätigkeit ergeben sich zu erstattende Kosten von 453,87 EUR (1,3 Geschäftsgebühr Nr. 2300 VV RVG in der Fassung vom 15. März 2022: 361,40 EUR, Auslagen Nr. 7001 und 7002 VV RVG: 20,00 EUR und 19 v. H. Umsatzsteuer Nr. 7008 RVG).

H. Kosten, Streitwert und Revision

1.
Die prozessualen Nebenentscheidungen beruhen auf §§ 92 Abs. 1, 708 Nr. 10, 713 ZPO.

2.
Die Streitwertfestsetzung beruht auf § 3 ZPO, §§ 39 Abs. 1, 47 Abs. 1, 48 Abs. 1 GKG.

Für die Fälle nichtvermögensrechtlicher Streitigkeiten bestimmt § 48 Abs. 2 S. 1 GKG, dass der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen zu bestimmen ist. Im Grundsatz kann in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei einer nichtvermögensrechtlichen Streitigkeit und mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Wert von

5.000,00 EUR ausgegangen werden (vgl. etwa BGH, Beschluss vom 17. November 2015, II ZB 8/14, Rn. 13, juris). Bei der Bemessung darf ferner das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (vgl. BGH, Beschluss vom 28. Januar 2021, III ZR 162/20, Rn. 9 m. w. N.).

Hieran gemessen hat der Senat den Streitwert auf insgesamt bis zu 3.500,00 EUR festgesetzt.

Den Auskunfts- und Löschungsantrag hat der Senat mit je 1.000,00 EUR bewertet. Der Antrag zu 3. betrifft eine vermögensrechtliche Streitigkeit; der Streitwert ergibt sich aus dem von der Klagepartei vorgestellten immateriellen (Mindest-) Ersatzbetrag in Höhe von 1.500,00 EUR. Der Antrag auf Zahlung außergerichtlicher Kosten war im Rahmen der Streitwertfestsetzung nicht zu berücksichtigen, da dieser den Gebührenstreitwert gem. § 43 Abs. 1 GKG (auch über § 48 Abs. 1 S. 1 GKG i. V. m. § 4 Abs. 1 S. 1 ZPO) nicht beeinflusst.

3.
Der Senat lässt die Revision nicht zu, weil ein Fall des § 543 Abs. 2 ZPO nicht vorliegt.

Grundsätzliche Bedeutung i. S. d. § 543 Abs. 2 Nr. 1 ZPO kommt einer Rechtssache zu, wenn sie eine entscheidungserhebliche, klärungsbedürftige und klärungsfähige Rechtsfrage aufwirft, die sich in einer unbestimmten Vielzahl von Fällen stellen kann und deswegen das abstrakte Interesse der Allgemeinheit an der einheitlichen Entwicklung und Handhabung des Rechts berührt. Klärungsbedürftig ist eine Rechtsfrage dann, wenn sie zweifelhaft ist, also über Umfang und Bedeutung einer Rechtsvorschrift Unklarheiten bestehen. Derartige Unklarheiten bestehen unter anderem dann, wenn die Rechtsfrage vom Bundesgerichtshof bisher nicht entschieden ist und von einigen Oberlandesgerichten unterschiedlich beantwortet wird, oder wenn in der Literatur unterschiedliche Meinungen vertreten werden (vgl. etwa BGH, Beschluss vom 17. Dezember 2024, VIII ZR 213/23, Rn. 20 m. w. N., juris). Zwar ist allgemein bekannt, dass schon jetzt eine hohe fünfstellige Zahl vergleichbarer Verfahren geführt wird. Die wirtschaftliche Bedeutung für die Beklagte (und andere Anbieter vergleichbarer Dienstleistungen) liegt vor diesem Hintergrund auf der Hand. Auch Rechtsschutzversicherer und Gerichte wird man zu den beteiligten Verkehrskreisen zählen können. Der Umstand, dass eine einheitliche Entscheidung des Bundesgerichtshofes in mehreren denselben Sachverhaltskomplex betreffenden Parallelverfahren angestrebt wird, gibt der Sache keine allgemeine, mithin grundsätzliche Bedeutung. Dies gilt auch dann, wenn es sich zwar um eine Vielzahl von Einzelverfahren handelt, es aber nicht ersichtlich

ist, dass deren tatsächliches oder wirtschaftliches Gewicht Allgemeininteressen in besonderem Maße berührt (BGH, Beschluss vom 21. November 2018, VII ZR 232/17, Rn. 14, juris).

Zudem wirft dieses Urteil keine entscheidungserhebliche, klärungsbedürftige und klärungsfähige Rechtsfrage auf, die noch nicht entschieden wäre. Der Senat wendet sämtliche EuGH-Rechtsprechung und die Rechtsprechung des Bundesgerichtshofes auf diesen Fall an. Offene Fragen hinsichtlich der Auslegung der DSGVO, für die gegebenenfalls gemäß Art. 267 Abs. 2 AEUV der EuGH anzurufen wäre, haben sich nicht ergeben. Entgegen der Auffassung der Beklagten wird auch die Darlegungs- und Beweislast nicht zu ihren Ungunsten verschoben. Vielmehr stützt sich der Senat allein auf unstreitiges Vorbringen. Lediglich soweit Anlagen K 2, K 13 und 14 zur Grundlage genommen werden, sieht er in Übereinstimmung mit der höchstrichterlichen Rechtsprechung eine sekundäre Beweislast bei der Beklagten. Eine sekundäre Darlegungslast kommt insbesondere dann in Betracht, wenn die beweisbelastete Partei außerhalb des von ihr vorzutragenden Geschehensablaufs steht und keine nähere Kenntnis der maßgebenden Tatsachen besitzt, während der Gegner zumutbar nähere Angaben machen kann (zuletzt (BGH, Urteil vom 21. Oktober 2025, EnZR 68/23, Rn. 26 m. zahlr. w. N., juris). Dieser Fall liegt hier vor und ist nicht klärungsbedürftig. Die Zumessung des Schadenersatzes ist gemäß § 287 ZPO anhand der festgestellten Tatsachen vorzunehmen und eine Tatsachen- und keine Rechtsfrage.

Zur Fortbildung des Rechts i. S. d. § 543 Abs. 2 Nr. 2 Alt. 1 ZPO ist das Verfahren ebenfalls nicht geeignet. Das Urteil weicht in keinem Punkt von der bisherigen höchstrichterlichen und EuGH-Rechtsprechung oder der gängigen Kommentarliteratur ab, sondern wendet die Vorschriften der DSGVO entsprechend der Rechtsprechung an. Der Zulassungsgrund der Sicherung einer einheitlichen Rechtsprechung (§ 543 Abs. 2 Satz 1 Nr. 2 Alt. 2 ZPO) ist ebenfalls nicht gegeben. Der Senat setzt sich nicht in Widerspruch zur höchstrichterlichen Rechtsprechung und hat keine abweichenden Auslegungsgrundsätze herangezogen. Die Auslegung der Vorschriften der DSGVO ist – soweit eine Entscheidung ergeht – höchstrichterlich geklärt (im Ganzen ebenso: OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25 e, Rn. 212, beck-online; OLG Dresden, Urteil vom 3. Februar 2026, 4 U 292/25, Rn. 169; OLG Jena, Urteil vom 2. März 2026, 3 U 31/25, Rn. 180, juris; OGH Österreich, Urteil vom 26. November 2025, 6 Ob 189/24, BeckRS 2025, 34948 Rn. 84, beck-online).

[redacted]
Richter am Oberlandesgericht

[redacted]
Richterin am Oberlandesgericht

[redacted]
Richter am Oberlandesgericht