Beglaubigte Abschrift

OBERLANDESGERICHT NAUMBURG

IM NAMEN DES VOLKES

URTEIL

9 U 44/25 OLG Naumburg
10 O 368/24 LG Magdeburg

Verkündet am: 5. Februar 2026
[redacted]
als Urkundsbeamtin der Geschäftsstelle

In dem Rechtsstreit

[redacted]

Kläger und Berufungskläger,

Prozessbevollmächtigte:
Anwaltsgesellschaft BK Automotive Rechtsanwaltsgesell-schaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin, Geschäftszeichen: DTS-007235-IU

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 13. Januar 2026 durch die Richterin am Oberlandesgericht [redacted] die Richterin am Oberlandesgericht [redacted] und den Richter am Oberlandesgericht [redacted] für Recht erkannt:

I. Auf die Berufung der Klagepartei wird das am 27. Februar 2025 verkündete Urteil der 10. Zivilkammer des Landgerichts Magdeburg – Einzelrichter – abgeändert:

1. Es wird festgestellt, dass zur Nutzung des Netzwerks „Instagram" unter dem Benutzernamen „[redacted]" die Verarbeitung von folgenden personenbezogenen Daten der Klagepartei mit Hilfe der Meta Business Tools durch die Beklagte in folgendem Umfang seit dem 25. Mai 2018 nicht zulässig war:
a) auf Dritt-Webseiten und -Apps die personenbezogenen Daten der Klagepartei, ob direkt oder in gehashter Form übertragen, d. h.
- E-Mail der Klagepartei
- Telefonnummer der Klagepartei
- Vorname der Klagepartei
- Nachname der Klagepartei
- Geburtsdatum der Klagepartei
- Geschlecht der Klagepartei
- Aufenthaltsort der Klagepartei
- Externe IDs besuchter Webseiten (von der Beklagten „external_ID" genannt)
- IP-Adresse des Clients
- User-Agent des Clients (d. h. gesammelte Browserinformationen)
- interne Klick-ID der Beklagten
- interne Browser-ID der Beklagten
- Abonnement-ID
- Lead-ID
- anon_id
- die Advertising ID des Betriebssystems Android (von der Beklagten „madid" genannt) sowie
b) auf durch die Klagepartei besuchten Dritt-Webseiten
- die URLs der Webseiten samt ihrer Unterseiten
- der Zeitpunkt des Besuchs
- der „Referrer" (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),
- die von der Klagepartei auf der Webseite angeklickten Buttons sowie
- weitere von der Beklagten „Events" genannte Daten, die die Interaktionen der Klagepartei auf der jeweiligen Webseite dokumentieren

c) in den durch die Klagepartei genutzten mobilen Dritt-Apps
- der Name der App sowie
- der Zeitpunkt des Besuchs
- die von der Klagepartei in der App angeklickten Buttons sowie
- die von der Beklagten „Events“ genannte Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren.

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps außerhalb der Netzwerke der Beklagten die in Ziff. 1 genannten personenbezogenen Daten der Klagepartei mit Hilfe einer Software wie Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verarbeiten, sofern die Beklagte die Verarbeitung der personenbezogenen Daten nicht auf eine informierte Einwilligung i.S.d. Art. 6 Abs. 1 Satz 1 lit. a) DSGVO oder einen Rechtfertigungsgrund nach Art. 6 Abs. 1 Satz 1 lit. b) bis f) oder Art. 9 Abs. 2 DSGVO stützen kann.

3. Die Beklagte wird verurteilt, eine über die aktuelle Speicherung hinausgehende Verarbeitung gemäß Art. 4 Nr. 2 DSGVO der unter Ziffer I.1. aufgeführten seit dem 25. Mai 2018 bereits verarbeiteten personenbezogenen Daten der Klagepartei gemäß Ziffer I.1. bei Meidung eines für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000 EUR, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, bis zur Erfüllung des Löschungsanspruchs gemäß Ziff. 4 zu unterlassen, insbesondere diese nicht an Dritte zu übermitteln, sofern die Beklagte die Verarbeitung der personenbezogenen Daten nicht auf eine informierte Einwilligung i.S.d. Art. 6 Abs. 1 Satz 1 lit. a) DSGVO oder einen Rechtfertigungsgrund nach Art. 6 Abs. 1 Satz 1 lit. b) bis f) oder Art. 9 Abs. 2 DSGVO stützen kann.

4. Die Beklagte wird verurteilt, sämtliche vorstehend unter Ziffer I.1. aufgeführten seit dem 25. Mai 2018 bereits gespeicherten personenbezogenen Daten der Klagepartei einen Monat nach rechtskräftigem Abschluss des Verfahrens hin vollständig zu löschen und der Klagepartei die Löschung zu bestätigen.

5. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz in Höhe von 1.250,00 EUR nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 29. April 2024 zu zahlen.

6. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten in Höhe von 887,30 EUR freizustellen.

7. Im Übrigen wird die Klage abgewiesen.

II. Die weitergehende Berufung wird zurückgewiesen.

III. Von den Kosten des Rechtsstreits einschließlich des Berufungsverfahrens trägt die Klagepartei 30 v.H. und die Beklagte 70 v.H.

IV. Das Urteil ist ohne Sicherheitsleistung vorläufig vollstreckbar.

Und beschlossen:

Der Streitwert beträgt bis 13.000 EUR.

Gründe:

I.

Die Parteien streiten über Löschungs-, Unterlassungs- und Schadensersatzansprüche im Zusammenhang mit der Verarbeitung personenbezogener Daten der Klagepartei durch sog. Business Tools der Beklagten.

Die Klagepartei nutzt als Privatperson seit dem 2. November 2009 mit unter dem Benutzernamen „[redacted]“ das Angebot der Beklagten bei dem sozialen Netzwerk Instagram, über ein Apple-Iphone. Sie nutzt in der Regel den Browser Chrome und verbringt nach ihrer Behauptung ca. 3 h täglich und ca. 42 h je Monat im Internet. Seit ca. 1 Jahr nutzt sie Instagram nicht mehr. Sie macht Ansprüche aus der behaupteten Praxis der Beklagten geltend, diese missachte das europäische Datenschutzrecht, indem sie die Nutzer überwache, deren persönliche und höchstpersönliche Daten rechtswidrig erhebe, in unsichere Drittstaaten übertrage, dort unbefristet speichere, diese in unbekanntem Maße auswerte und an Dritte weitergebe, ohne den betroffenen Nutzer hiervon zu informieren.

Die Beklagte, geschäftsansässig in Irland, bietet mit dem Social Media Dienst Instagram Dienste an, die täglich weltweit ca. 3,48 Milliarden privaten Nutzern bis zum 3. November 2023 kostenlos zur Verfügung gestellt wurden. Seit dem 4. November 2023 sind diese Dienste nur noch für die Nutzer kostenlos, die zugestimmt haben, dass ihre personenbezogenen Daten erhoben und verwendet werden, um personalisierte Werbung an sie zu richten, wobei die Nutzer die Möglichkeit haben, ein kostenpflichtiges Abonnement abzuschließen, um Zugang zu einer Version dieser Dienste ohne zielgerichtete Werbung zu erhalten. Dieses Angebot hat die Klagepartei nicht angenommen.

Das Geschäftsmodell des sozialen Online-Netzwerks Instagram beruht auf der Finanzierung durch Onlinewerbung, die sich gezielt an den individuellen Nutzer des sozialen Netzwerks insbesondere nach Maßgabe seines Konsumverhaltens, seiner Interessen und seiner Lebenssituation richtet. Diese Art der Werbung wird technisch ermöglicht, indem automatisiert detaillierte Profile der Nutzer erstellt werden.

Dafür nutzt und verarbeitet die Beklagte verschiedene Daten, die sie in ihrer Datenschutzrichtlinie (Anlage K 1, S. 5 ff.) aufführt und auf die sie bei der Registrierung ebenso hinweist wie auf die Cookie-Richtlinie. Zu diesen Daten gehören neben den persönlichen Informationen, die der Nutzer bei der Registrierung angibt, wie Name, E-Mail-Adresse und Telefonnummer (vgl. Nutzungsbedingungen S. 1, Anlage B 2), das Nutzungsverhalten des jeweiligen Nutzers in Produkten der Beklagten (= sog. On-Site-Daten), Informationen über Freunde und Follower des Nutzers und deren Nutzungsverhalten in Produkten der Beklagten sowie Informationen über die technischen Geräte, mit deren Hilfe der Nutzer die Produkte der Beklagten nutzt. Zudem sammelt die Beklagte sog. Eventdaten, die sie bezeichnet als „*Informationen von Partnern über Handlungen, die du sowohl innerhalb als auch außerhalb unserer Produkte durchführst. Dazu können z.B. andere von dir besuchte Websites, von dir verwendete Apps oder von dir gespielte Online-Spiele gehören.*“ Weiter heißt es: „*Partner teilen auch Informationen wie deine E-Mail-Adresse, Cookies und deine Geräte-ID für Werbezwecke mit uns. … Wir erhalten diese Informationen unabhängig davon, ob du bei unseren Produkten angemeldet bist bzw. ein Konto auf ihnen hast oder nicht. Partner geben außerdem ihre Kommunikation mit dir an uns weiter, wenn sie uns anweisen, Dienstleistungen für ihr Unternehmen zu erbringen, wie Unterstützung bei der Verwaltung ihrer Kommunikation […] … Partner nutzen unsere Tools, Integrationen und … Audience Network-Technologien, um Informationen mit uns zu teilen. Diese Partner erheben deine Informationen, wenn du ihre Website oder App besuchst oder ihre Dienste nutzt…“.* (vgl. im Einzelnen auch S. 9 der Anlage K 1). Bei Letzteren handelt es sich um sog. Off-Site-Daten. Die Daten werden „gehasht“ (verschlüsselt) übersandt, wobei die gleichen Daten über den gleichen Schlüssel zur gleichen Verschlüsselung führen, so dass jeweils gleichartige „Hashs“ zusammengeführt und

sodann dem Nutzer zugeordnet werden können (vgl. S. 9, 10, Anlage K 1 – Datenschutzrichtlinie und S. 2 Anlage K 8 – Parameter für KundInneninformation).

Die Beklagte bietet Drittunternehmen (sog. Partnern) für die Erhebung der Off-Site-Daten Softwareprogramme zur Einbindung in das Meta-System an, die sog. Meta Business Tools. Dazu gehören die Tools „Meta Pixel", „App Events über Facebook SDK" (bzw. „Facebook SDK" für mobile Apps), „Conversion API" und „App Events API" (folgend: Business Tools). Die Beklagte schließt mit den Drittanbietern Nutzungsverträge, in die sie ihre Datenschutzrichtlinie einbezieht (Anlage K 1 und B 9). In Ziff. 3. lit. d) der Nutzungsbedingungen (Stand 25. April 2023, Anlage B 5) mit den Drittwebseitenbetreibern werden diese verpflichtet, die „erforderlichen Einwilligungen" der Endnutzer vor Nutzung der Business Tools einzuholen.

Genereller Zweck der Business Tools ist es unter anderem, die Effektivität von Werbeanzeigen von Drittunternehmen auf den von der Beklagten angebotenen Plattformen wie Instagram oder Facebook zu erhöhen und zu messen. Hierzu können von den Business Tools Daten an die Beklagte übermittelt werden. Im Einzelnen unterscheiden sich dabei die technischen Abläufe nach der Art der eingebundenen Tools und der Zustimmung/Ablehnung der Nutzer.

Die Business Tools ermöglichen allgemein gefasst folgende Datenerhebung:
Sobald ein Nutzer die Webadresse oder URL eines Drittanbieters, der die Business Tools nutzt, eingegeben hat, kommuniziert der Browser des Nutzers mit dem Server des Drittanbieters, um die Inhalte der Seite zu laden (sog. HTTP-Anfrage) und darüber hinaus über Cookies mit den Servern der Beklagten, um diese eingebetteten Inhalte mittels einer weiteren http-Anfrage anzufragen. Hierzu heißt es in den „*Parametern für Kund*innen-Information" an die Drittunternehmen*" (Anlage K 8):

*„Du kannst mit den Meta-Business-Tools Parameter für Kund*innen-Informationen an Meta senden. Dabei handelt es sich um eine Reihe von Identifizierungsmerkmalen wie Namen und E-Mail-Adressen von Nutzer*innen, die du zusammen mit deinen Event-Daten teilst."*

Über die sog. Klick-ID, die von den Cookies _fbp und _fbc bei einer Nutzeraktivität, dem sog. Event, ausgelesen wird, die First Party Cookies und die Cookies der Drittwebseiten, erhält die Beklagte Nutzerdaten. Ob diese Daten auch zurückfließen, wenn der Nutzer die sog. Third Party Cookies, über die die Informationen an die Beklagte zurückfließen, nicht zugelassen hat, ist streitig.

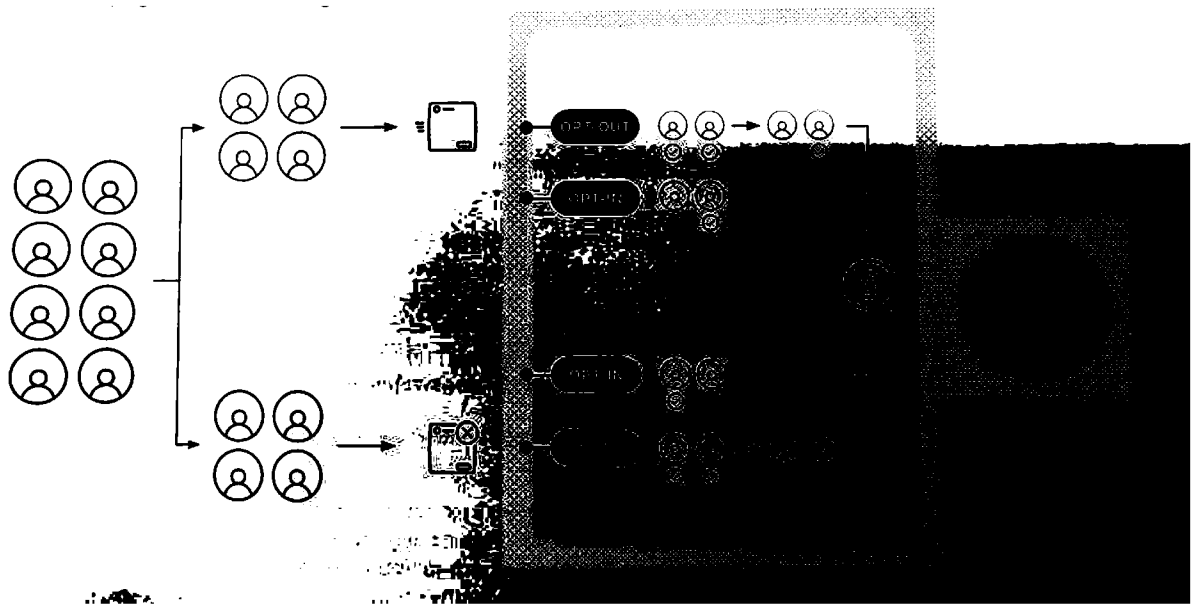
Der Meta Pixel nutzt die first party cookies der Webseite, um seine Daten abzulegen, wieder auszulesen, zusammenzuführen und an die Beklagte zu übersenden, ohne dass der Nutzer dies bemerkt (vgl. Anlage K 10, S. 2). In der Beschreibung der Top 11 Pixel in Anlage B 4 heißt es:

„This pixel is loaded when a user visits a website or opens an email and is used to track users activities… Once added to your site, these … pixel graphics gather user behaviour and collect other insights that allow you to measure the impact an ROI of your ads.“

Als Teil der http-Anfrage des Nutzers werden die technischen Standarddaten vom Gerät des Nutzers an die Beklagte gesendet. Dabei handelt es sich um Geräteinformationen, die der Beklagten mit einer Wahrscheinlichkeit von über 99 v.H. eine Nutzeridentifikation ermöglichen (vgl. BKartA, Beschluss vom 6. Februar 2019, Az. B6-22/16, Rn. 580, BeckRS 2019, 4895, beckonline). Technische Standarddaten in diesem Sinne sind etwa die mit dem Nutzergerät verknüpfte IP-Adresse, das Betriebssystem des Geräts, die Art des verwendeten Browsers (z. B. Chrome, Firefox, Safari, usw.), dessen Softwareversion, die vom Kunden verwendete Sprache, ob das Gerät des Kunden einen Touchscreen hat und die Parameter dieses Touchscreens. Im weiteren Verlauf kann dann das derart aktivierte „Business-Tool“ unter im Einzelnen streitigen Umständen weitere Daten (im Folgenden „weitere personenbezogene Daten“), insbesondere zur aktuellen und zurückliegenden Aktivität auf der Homepage wie etwa Klicks auf einzelne Artikel oder Buttons, Tastatureingaben, Formulareingaben etc. (sog. „*event data*“) an Meta übertragen, wobei Art und Umfang der übermittelten Daten davon abhängen, welches der vorgenannten Business Tools das Drittunternehmen integriert hat und wie es dieses Tool im Einzelnen einsetzt.

Ist auf der von der Nutzerin oder dem Nutzer besuchten Seite hingegen das Business Tool „Conversions API” bzw. auf der App das Business Tool „App Events API” (im folgenden: „API-Tools“) eingebunden, erfolgt keine weitere direkte http-Abfrage an die Beklagte. Vielmehr wird das Business-Tool im Folgenden und unter im Einzelnen streitigen Umständen direkt auf dem Server des Drittanbieters aktiv und kann von dort die vorgenannten technischen Standarddaten sowie „weitere personenbezogene Daten“ an die Beklagte übermitteln. Mit der Conversion API können „*Marketingdaten direkt und zuverlässig von deinem Server* [= dem Server des Drittunternehmens*] an die Meta-Systeme übermittelt (*werden*), die deine Werbeanzeigen ausliefern*“ (Meta Playbook, S. 4 und 23, Anlage K 11, Anlagenband).

Die Daten werden auch weitergeleitet, wenn sich die Nutzer gegen die Nutzung ihrer Daten entschieden haben. Wegen des Datentransfers bei der Conversions API wird auf das Schaubild in Anlage K 11, Meta Playbook, dort S. 23, Bezug genommen:



Hierzu heißt es:

*„Die ConversionsAPI ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben."*

Und weiter in Fußnote 12:
*„Opt-out-Nutzer*innen sind Personen, die der Tracking-Einwilligung von Facebook/Instagram auf Mobilgeräten ab iOS 14.5 nicht zugestimmt haben."*

Da die ConversionsAPI nicht in den Browser des Nutzers geladen werden muss, kann der Nutzer sie nicht abschalten. Die entsprechenden Systeme nutzt die Beklagte auch bei Nutzern, die die Schaltflächen *„Optionale Cookies erlauben"* und „Informationen über Aktivitäten von Werbepartnern" nicht aktiviert haben (vgl. Beispiel einer Nutzung von spiegel.de, Replik S. 25 bis 33). Die Drittunternehmen werden ermuntert, Meta Pixel und die Conversion App zu verbinden, weil das *„Optimierungsmöglichkeiten für die Kampagnen-Performance"* biete (vgl. S. 11, Anlage K 11).

Hierzu heißt es in dem Leitfaden der Beklagten *„Redesigning our systems to provide more control over Off-Facebook Activity"* (S. 4, Anlage K 11):

„We needed to respect people´s desire to disconnect off-site activity from their account and still provide reliable measurement reports to businesses – even if many people choose to disconnect this data from their account….When a person chooses to disconnect his or her off-site activity, we remove the mapping between the MID and the UID and generate a new random MID for that person. This prevents system from connecting the off-site activity data

to that persons UID…. The bucketed MID does not represent an individual user. We can aggregate that observation with others who viewed the same ad – without determining exactly which person within the bucket took that action.“

Außerdem verarbeitet die Beklagte Daten für Sicherheitsuntersuchungen (vgl. S. 4, Anlage K 11).

Der Nutzer kann nicht verhindern, dass die Beklagte die über Dritte generierten Daten erhält. Drittunternehmen können wählen, ob sie die Event-Daten und Kontaktinformationen über die streitgegenständlichen Business Tools mit der Beklagten teilen (vgl. Meta Developer Page „*General Data Protection Regulation*“, Anlage B 15; „*Ressource zur Cookie-Einwilligung*“, Anlage B 16).

Für die Verarbeitung der personenbezogenen Daten der Nutzer des sozialen Netzwerks Instagram stützt sich die Beklagte auf den Nutzungsvertrag, den die Nutzer durch Betätigung der Schaltfläche „*Registrieren*“ abschließen und mit dem sie den von der Beklagten festgelegten allgemeinen Nutzungsbedingungen zustimmen. Zugleich wird auf die Datenschutzrichtlinie (Anlage K 1) verwiesen. Der Nutzer kann *„mithilfe verschiedener Einstelloptionen kontrollieren, welche Arten von Werbeanzeigen und Werbetreibenden“* er sieht (S. 2, Anlage B 2, Nutzungsbedingungen).

Bevor die Nutzer auf der Website der Beklagten zur Einstellung „*Informationen von Werbepartnern zu deinen Aktivitäten*“ gelangen, erklärt die Beklagte sowohl die Art der gesammelten und verwendeten Daten (d. h. Daten, die erfasst werden, „*wenn du die Website [oder] App eines Werbepartners besuchst“) als auch den Verarbeitungszweck, für den die Einwilligung eingeholt wird (d. h. um „dir die besten Anzeigen zu zeigen*“). Die Einstellung „*Informationen von Werbepartnern zu deinen Aktivitäten“* informiert die Nutzer: *„Du kannst deine Auswahl jederzeit ändern“*. Weiter heißt es:

„Wenn wir wissen, was dir gefällt, können wir dir relevantere Werbung für neue Dinge zeigen. Wenn du Webseiten oder Apps von Werbepartnern besuchst oder in ihren Geschäften etwas kaufst, senden diese möglicherweise Informationen zu deiner Aktivität und worin diese bestand. […] So können wir dir eher Werbung zeigen, die relevant für dich ist und genauso interessant wie dein regulärer Content. Wir tun dies aber nur dann zu diesem Zweck, wenn du das möchtest. Du kannst entscheiden, ob wir diese Informationen nutzen können, um passende Werbung für dich anzuzeigen.“

Unter der Unterüberschrift „*Was ist unsere Rechtsgrundlage*“ erklärt die Beklagte:
„*Wir stützen uns bei der Verarbeitung deiner Informationen für die in dieser Datenschutzrichtlinie beschriebenen Zwecke auf verschiedene Rechtsgrundlagen. Je nach den Umständen stützen wir uns auf unterschiedliche Rechtsgrundlagen, wenn wir dieselben Informationen für verschiedene Zwecke verarbeiten. Für jede der nachstehend aufgeführten Rechtsgrundlagen erläutern wir, warum wir deine Informationen verarbeiten…* […]“ „*Wir verarbeiten Informationen für die folgenden Rechtsgrundlagen:…*“

Der Nutzer hat für die Verarbeitung seiner Daten die Möglichkeit, zwischen zwei Einstellungen zu wählen:

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

Beim Öffnen einer Drittwebsite erscheint seit dem 3. November 2023 für den Nutzer eine zusätzliche Schaltfläche, auf welcher der Nutzer eine Einstellung für Cookies betreffend die weitere Nutzung der Drittwebsite treffen kann. Der Nutzer hat seitdem die Wahl zwischen einer weiteren entgeltfreien Nutzung mit Werbung und Tracking oder einer entgeltlichen Weiternutzung, ohne dass seine Daten an Werbetreibende weitergegeben werden (s. Screenshot auf Seite 24, 25 der Klageerwiderung vom 31. Juli 2024, Bl. 97 Bd. I d. A.). Darüber hinaus können die Nutzer optionale Cookies auf anderen Apps und Webseiten erlauben, andernfalls eine Abmeldung von den Apps und Webseiten erfolgt. Außerdem heißt es weiter: „*Wenn du diese Cookies nicht erlaubst, kann es sein, dass wir weiterhin aggregierte Informationen zu Aktivitäten auf diesen Websites erhalten.*“ (Screenshot, Klageerwiderung vom 31. Juli 2024, Bl. 98 Bd. I d. A.).

Nutzer können die Anzeige von Werbung über optionale Cookies steuern. Zu optionalen Cookies heißt es auf den Seiten der Beklagten:

„Unsere Cookies in anderen Apps und auf anderen Websites:
Wir verwenden Cookies in Apps und auf Websites von anderen Unternehmen, die Meta-Technologien nutzen. Mithilfe dieser Cookies können andere Unternehmen Informationen über deine Aktivitäten in ihren Apps und auf ihren Websites mit uns teilen.“

Wegen der weiteren Einzelheiten der Informationen wird auf den Text auf S. 97 Bd. I d. A. Bezug genommen.

Die Drittanbieter teilen mit der Beklagten Kontaktinformationen und sog. Event-Daten (Aktivitäten) der Nutzer, *„über Personen und ihre Handlungen …., die sie auf deinen Websites und in deinen Apps oder Shops vornehmen“* (Business-Tools Nutzungsbedingungen“, Anlage B 5, Seite 1), die von der Beklagten u.a. für Messlösungen und Analysedienste über Nutzer und ihre Nutzung der Apps, Webseiten, Produkte und Dienstleistungen genutzt werden, die sog. Targeting (Ausrichtung von Werbekampagnen auf Personen) zu ermöglichen und die diese bis zu zwei Jahre lang speichert (vgl. S. 2 bis 4 der Nutzungsbedingungen für Business Tools, Anlage B 5). Gemäß Ziff. 3.d) ist der Drittunternehmer verpflichtet, die erforderlichen Einwilligungen der Nutzer einzuholen (Anlage B5, S. 4). Eine Kontrolle durch die Beklagte sehen die Nutzungsbedingungen nicht vor. Hierzu heißt es im Business Tool-Hilfebereich für Unternehmen, Anlage B 6, S. 1:
„Metas Systeme sind zwar darauf ausgelegt, potenziell unzulässige Informationen herauszufiltern, die sie erkennen können, aber letztendlich bist du für die Daten verantwortlich, die du mit Meta teilst“.

Zu den berechtigten Interessen der Beklagten zu dieser Datenverarbeitung heißt es in der Datenschutzrichtlinie (S. 62 Anlage K 1):

„Wir verarbeiten deine Informationen so, wie es für unsere berechtigten Interessen bzw. die von anderen erforderlich ist. Zu unseren Interessen zählen u.a. die Bereitstellung eines innovativen, personalisierten, sicheren und profitablen Dienstes für unsere Nutzer und Partner ….“

Die Beklagte hat eine formelle Art. 26 DSGVO-Vereinbarung mit Drittunternehmen getroffen. Nach den Nutzungsbedingungen für die Business Tools ist der Drittanbieter verpflichtet, auf die Pixel der Beklagten hinzuweisen (vergleiche Anl. B 5, Anlagenband Beklagte, Rn. 27, Klageerwiderung).

Die Business-Tools sind in zahlreiche Webseiten und Apps in Deutschland im Hintergrund eingebunden. Hierzu gehören

- zahlreiche große Nachrichtenseiten und -Apps (z.B. spiegel.de, bild.de, welt.de, faz.net, stern.de),
- großen Reiseseiten und -Apps (z.B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de, momondo.de),
- Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shopapotheke.de, docmorris.de, aerzte.de, heliosgesundheit.de, jameda.de),
- Dating- und Erotikseiten (parship.de, amorelie.de, orion.de, lovescout24.de),

- Seiten mit Inhalten aus der Intimsphäre (krebshilfe.de, tfpfertility.com, niewieder-alkohol.de, nvve.nl).

Nach klägerischer Darstellung sind in Deutschland exemplarisch etwa die weiteren in Anlagen K 13 und K 14, auf die wegen der Einzelheiten Bezug genommen wird, gelisteten großen Webseiten Partner der Beklagten.

Die angefallenen Daten sendet die Beklagte weltweit in Drittstaaten, insbesondere die USA, und gibt sie auch an Dritte sowie an Behörden weiter (vgl. S. 72 Datenschutzrichtlinie, Anlage K 1).

Die Einstellung „*Deine Aktivitäten außerhalb der Meta-Technologien*“ erlaubt es den Nutzern, eine Zusammenfassung der mit ihren Konten verknüpften Informationen über die Aktivitäten des Nutzers auf Apps und/oder Websites, die von Drittunternehmen mit der Beklagten geteilt wurden, zu kontrollieren und abzurufen („*Von Drittunternehmen geteilte Informationen über Aktivitäten*“). Zusätzlich zu der Möglichkeit für Nutzer, über die Einstellung „*Deine Aktivitäten außerhalb von Meta-Technologien*“ eine Zusammenfassung ihrer „*Neueste Aktivitäten*“ abzurufen, können die Nutzer die von Drittunternehmen geteilten Informationen über Aktivitäten von dem Instagram-Konto „trennen“ lassen und/oder die künftigen Verknüpfungen zwischen Instagram-Konto und den von Drittunternehmen geteilten Informationen über Aktivitäten ausschalten. Die Beklagte stellt ihren Nutzern dabei keine Möglichkeit zur Verfügung, die Löschung der unter dem Tenor Ziff. 1 aufgeführten Off-Site-Daten herbeizuführen. Über das Tool werden nur Daten bzgl. solcher Drittwebsites oder -Apps angezeigt, die besucht wurden, währenddessen der Nutzer auf dem gleichen Gerät im Netzwerk der Beklagten eingeloggt war. Die innerhalb des Tools zu findenden Informationen teilen nicht mit, an welche konkrete Empfänger die Daten weitergegeben wurden. Zudem sind die Informationen auf einen Zeitraum von wenigen Monaten begrenzt.

Die Klagepartei begehrte mit Schreiben vom 8. November 2023 Auskunft über die Nutzung von Daten durch Einbindung der Business Tools (Anlage K3, Anlagenband). Die Beklagte erteilte am 27. Dezember 2024 Auskunft lediglich durch Hinweis auf ihre Self-Service-Tools (Anlagenband Beklagte, Anlage B 10).

Die Klagepartei hat im ersten Rechtszuge die Ansicht vertreten, ihre Zustimmung zu den Nutzungsbedingungen der digitalen Plattform der Beklagten erfülle nicht die Voraussetzungen von Art. 6 Abs. 1 und Art. 7 DS-GVO. Zudem verarbeite die Beklagte, die als verantwortliche Verarbeiterin auch der von den Drittseiten verarbeiteten Daten anzusehen sei, sensible Daten der Klagepartei i.S.v. Art. 9 DSGVO ohne die hierfür erforderliche Einwilligung nach

Art. 7 DSGVO. Die Beklagte sei Verantwortliche i.S.d. Art. 28 DSGVO auch für die Drittwebseiten, weil diese die von der Beklagten bereitgestellten Tools anwendeten.

Sie hat zur Funktionsweise der ConversionsAPI behauptet, die Cookies _fbp und _fbc enthielten eine vom Meta-Pixel generierte ID, die den jeweiligen Browser identifiziert, der einen ggf. blockierten Third Party Cookie umgehen kann und die Daten von Webseitenbesuchen an die Beklagte übermitteln kann.

Die Klagepartei hat die Auffassung vertreten, die Datenverarbeitung durch die Beklagte verstoße auch gegen § 42 Abs. 2 BDSG.

Sie, die Klagepartei, habe mangels entsprechender Aufklärung nicht freiwillig und wirksam in die streitgegenständliche Datenverarbeitung eingewilligt, weder auf den Seiten der Beklagten noch auf den Seiten der Drittanbieter. Jedenfalls aber habe sie mit der Einreichung dieser Klage ihre Zustimmung zur Verarbeitung ihrer Business Tool-Daten durch die Beklagte widerrufen. Zudem habe die Beklagte nicht ihren gesetzlichen Informationspflichten mit dem Hinweis auf optionale Cookies genügt, weil jedenfalls nicht auf das streitgegenständliche Fingerprinting hingewiesen werde. Zumindest habe die Beklagte gegen das Kopplungsverbot in Art. 7 Abs. 4 DSGVO verstoßen, weil die Einwilligung nicht den Exzess der Datenverarbeitung durch die Beklagte decke. Ihrer Ansicht nach erfüllte das Tool „*Informationen unserer Werbepartner zu deinen Aktivitäten*“ nicht die Anforderungen an Art. 15 DSGVO.

Ihrer Ansicht nach sei die streitgegenständliche Datenerhebung für die Erfüllung der Hauptleistung, d.h. die Zurverfügungstellung des Netzwerkes der Beklagten, nicht erforderlich. Auch mit der Abonnement-Variante habe die Beklagte die Nutzung der Daten nicht ausgeschlossen, sondern zeige die entsprechende Werbung lediglich nicht mehr an.

Aus Anlage K 11 ergebe sich, dass die Beklagte auch sensible Daten i.S.d. Art. 9 DSGVO erhebe. Sie, die Klagepartei, beschäftige sich im Internet ca. 42 h/Monat mit sensiblen Daten, u.a. finanziellen Themen, Steuern, Altersvorsorge und Vermögensmehrung. Ca. 2 h je Monat recherchiere sie zu Gesundheitsthemen wie Schwangerschaft und Familienplanung, 30 h je Monat zu politischen Themen wie Migration, Klimawandel, Genderthemen und Kriege. Wegen des Ausmaßes der Verwendung der Business Tools auf diesen Webseiten nehme sie Bezug auf die am 30. April 2023 veröffentlichte Studie „*The Hitchhiker's Guide to Facebook Web Tracking with Invisible Pixels and Click IDs*“ (Anlage K 7).

Ihrer Ansicht nach sei die Datenübermittlung in die USA vom 25. Mai 2018 bis zum Angemessenheitsbeschluss der Europäischen Kommission am 9. Juli 2023 rechtswidrig gewesen,

nachdem der EuGH das Abkommen zur Datenübermittlung „Privacy Shield“ zwischen der EU und den USA für ungültig erklärt habe.

Ihr Anspruch auf künftige Löschung folge aus Art. 17 DSGVO i.V.m. § 259 ZPO. Derzeit würden die Daten lediglich über das Off-Activity-Tool pseudonymisiert, was ihrer Ansicht nach gemäß EWG 26 DSGVO nicht mit einer Mischung aller Nutzerdaten gleichzusetzen sei. Der Anspruch aus dem Klagantrag zu Ziff. 3 ergebe sich aus Art. 18 Abs. 1 lit. b) DSGVO sowie als Nebenpflicht des Art. 15 DSGVO und als vertragliche Nebenpflicht gemäß § 242 BGB, da die Beklagte kein Recht zur weiteren Verarbeitung der streitgegenständlichen Daten habe.

Es liege ein schwerer Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung vor, weil sie keinerlei Zugriff auf die Verarbeitung ihrer Daten mehr habe.

Die Klagepartei hat hinsichtlich der Folgen behauptet, sie habe ein vollständiges Überwachungsgefühl und fühle sich der Beklagten aufgrund ihrer Marktmacht ausgeliefert. Sie habe nicht gewusst, dass sie auch nach einem Logout aus Instagram nachverfolgt werde, auch auf anderen Webseiten und Apps. Diese Erkenntnis habe sie schockiert. Sie befürchte den Verlust sozialer Kontakte, wenn sie auf die Nutzung der Apps der Beklagten verzichte. Infolge des Fingerprintings habe sie Sorge über die Verwendung ihrer Daten und der Daten der Familienmitglieder. Andererseits gehöre die Internetnutzung für sie zum Leben. In der modernen Welt könne sie nicht darauf verzichten. Sie habe auch die Produkte der Beklagten geschätzt. Sie sei sehr verunsichert, weil sie keinerlei Kenntnis über Quantität und Qualität der Datensammlung habe. Normalerweise lehne sie Cookies ab und nutze den sog. Inkognito-Modus. Allerdings sei dieser für sie nicht standardmäßig darstellbar. Wegen der Datenübermittlung in die USA habe sie Angst, dass sie die Kontrolle über ihre Daten nie wiedererlangen werde. Sie empfinde einen vollständigen Kontrollverlust. Diese Sorge wirke sich auf ihr Internetverhalten dahin aus, dass sie Sorge habe, sie werde beständig von der Beklagten getrackt. Sie fürchte, die Datenkontrolle für immer verloren zu haben. Sie schlafe schlecht. Ihren Schadenersatzanspruch hat sie mit mindestens 5.000 EUR als angemessen bezeichnet.

Die Beklagte hat im ersten Rechtszuge die Unzulässigkeit des Klageantrages zu 1. mangels für den Feststellungsantrag erforderlichen Rechtsschutzinteresses gerügt. Außerdem sei der Klageantrag zu unbestimmt. Zudem habe die Klagepartei nicht dargelegt, dass sie Dritt-Webseiten oder Apps Dritter besucht oder verwendet habe. Die Bezugnahme auf Anlagen K 13 und 14 sei ihrer Ansicht nach nicht ausreichend. Höchstpersönliche Daten würden ohnehin nicht offengelegt.

Die Beklagte hat weiter die Auffassung vertreten, sie könne sich auf eine Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO stützen. Die Klagepartei habe auch ausdrücklich in die streitgegenständliche Datenverarbeitung eingewilligt.

Die Beklagte hat behauptet, im Kontext des Einsatzes der Business Tools „Meta Pixel“ bzw. „App Events“ sei die Erhebung und Übertragung der technischen Standarddaten an die Beklagte per HTTP-Abfrage der zeitgemäßen Nutzung des Internets immanent. Die Drittanbieter könnten zudem die Übermittlung der technischen Standarddaten per HTTP-Anfrage an die Beklagte „pausieren“ bis die Nutzer über Cookie-Banner ihre Einwilligung hierzu erteilt hätten. Im Hinblick auf alle eingesetzten Business-Tools hat die Beklagte behauptet, dass die Frage, welche Daten („*technische Standarddaten*“ und „*weitere personenbezogene Daten*“) durch die Business-Tools selbst an sie übermittelt würden, davon abhänge, ob die Nutzer vorab zugestimmt hätten sowie von der Konfiguration der Einstellungen der Business-Tools bei den Drittanbietern. Die Drittfirmen hätten sich verpflichtet, diese Datenübertragungsfunktionen der Business Tools nur dann zu aktivieren, wenn sie zuvor eine Zustimmung der Nutzer eingeholt hätten. Eine Kontrolle dahingehend, ob dies von den Drittfirmen auch umgesetzt worden sei, finde nicht statt. Es werde von der Beklagten jedoch überprüft, ob die übermittelten Daten besonders geschützte personenbezogene Daten enthielten.

Dem Drittunternehmen obliege es, zeitnahe Offenlegungen gegenüber den Besuchern seiner eigenen Webseite oder App vorzunehmen. Sie sei weder Inhaberin noch Verwalterin oder Betreiberin der in den Anlagen der Klagepartei genannten Drittwebseiten oder -Apps und daher nicht in der Lage, den Nutzern direkt Informationen über die Datenverarbeitungsaktivitäten zur Verfügung zu stellen. Es obliege den Drittunternehmen die erforderliche Einwilligung von den Besuchern der Website einzuholen. Wie sich aus ihren Meta Business Tool Nutzungsbedingungen ergebe, sei das Drittunternehmen und nicht sie Verantwortliche i.S.d. Art. 26 DSGVO (Business Tool-Bedingungen, Anlage B 5, Ziff. 5).

Ihrer Ansicht nach habe die Klagepartei wie alle Nutzer über ihre Einstellungen auf Instagram eine echte Wahl und Kontrolle über die Verarbeitung von Business Tools Daten zur Bereitstellung personalisierter Werbung.

Soweit die Klagepartei eine Webseite oder App besucht habe, die eines der streitgegenständlichen Business Tools verwendet habe, habe die Klagepartei über das Cookie-Banner der Webseite oder App die Einstellungen über Cookies wählen können. Die Einwilligung zur Verarbeitung von Business Tools Daten zur Bereitstellung personalisierter Werbung gemäß Art. 7 DSGVO sei freiwillig und wirksam erfolgt. Die Klagepartei habe – insoweit unstreitig –

„optionale Cookies“ erlaubt bzw. diese bei „*Informationen über Aktivitäten von Werbepartnern*“ aktiviert.

Hinsichtlich der Ansicht der Klagepartei, sie habe mit der Klage ihre Einwilligung widerrufen, vertritt sie die Auffassung, diese sei gemäß Art. 7 Abs. 3 DSGVO unwirksam.

Hinsichtlich der Datenübertragung in die USA, die für das Funktionieren des Netzwerkes unerlässlich sei, stütze sie sich auf die Angemessenheitsbeschlüsse der EU-Kommission und die Standardvertragsklauseln.

Sie hat die Ansicht vertreten ein Unterlassungsanspruch folge nicht aus der DSGVO, insbesondere nicht aus Art. 17 DSGVO.

Der Klageantrag zu 3. sei ihrer Ansicht nach unzulässig, weil Art. 18 Abs. 1 lit. b) DSGVO den betroffenen Personen kein Recht auf Unterlassung gewähre.

Der Klagantrag zu 4 (künftige Löschung und Anonymisierung) sei unzulässig, weil er unter einer unzulässigen außerprozessualen Bedingung stehe. Jedenfalls sei er unbestimmt. Entgegen der Auffassung der Klageseite sehe die DSGVO außerdem kein Recht auf Anonymisierung vor.

Hinsichtlich des Schadensersatzanspruches hat die Beklagte die Ansicht vertreten, weder sei ein solcher schlüssig vorgetragen, noch nachgewiesen.

Wegen des weiteren Sach- und Streitstandes im ersten Rechtszug einschließlich der dort ergangenen Entscheidung wird auf das angefochtene Urteil (Leseabschrift Bl. 65 bis 82 Bd. III d. A.) Bezug genommen (§ 540 Abs. 1 Nr. 1 ZPO).

Das Landgericht hat die Klage abgewiesen und zur Begründung ausgeführt, der Feststellungsantrag (Klageantrag zu 1) sei mangels Feststellungsinteresses und fehlenden Rechtsschutzinteresses unzulässig. Im Übrigen wäre der Antrag auch unbegründet, weil nicht ersichtlich sei, wie die Beklagte die Klagepartei ausgeforscht habe. Der Unterlassungsantrag (Klageantrag zu 2) sei mangels Bestimmtheit unzulässig, weil keine konkreten Daten aufgeführt würden. Außerdem sei der Antrag nicht mehr vom Schutzumfang des Art. 17 DSGVO umfasst. Gemäß Art. 17 DSGVO könne auch kein Unterlassungsanspruch, sondern nur Löschungsansprüche geltend gemacht werden. Gleiches gelte für den Klageantrag zu 3). Eine Anspruchsgrundlage für den Klageantrag zu 4 (Anonymisierung und Löschung der Daten) ergebe sich nicht aus Art. 17 DSGVO, weil die Anonymisierung kein Minus zum

Löschungsantrag darstelle. Die Klagepartei habe auch keinen Anspruch auf Schadenersatz gemäß Art. 82 DSGVO (Klageantrag zu 5). Die Klagepartei habe ihren Anspruch schon deshalb nicht schlüssig dargelegt, weil es an der genauen Angabe der verarbeiteten Daten fehle. Dass die Beklagte einer rechtswidrigen geheimdienstlichen Spionagepraxis nachgehe, die auf sie erhebliche Auswirkungen habe, habe die Klagepartei nicht schlüssig dargelegt oder bewiesen. Anhaltspunkte für einen Schaden gesundheitlicher Art fehlten zudem. Im Übrigen verhalte sich die Klagepartei widersprüchlich, weil sie die von der Beklagten ab 3. November 2023 genutzte Einwilligungsoption nicht gewählt habe.

Mit der hiergegen gerichteten Berufung verfolgt die Klagepartei ihr erstinstanzliches Klagebegehren weiter. Sie vertritt die Auffassung, sie habe ein schutzwürdiges Interesse an der Feststellung des streitigen Rechtsverhältnisses, hilfsweise jedenfalls als Zwischenfeststellungsantrag gemäß § 256 Abs. 2 ZPO. Der Unterlassungsantrag in Ziff. 2 sei hinreichend bestimmt. Entgegen der Auffassung des Landgerichts sei es unerheblich, welche Daten sie hinterlegt habe, weil es ausschließlich um die Unterlassung der Verarbeitung durch die Software Business Tools über Drittseiten und Apps, wie sie es am Beispiel der User-ID, des User Agent, der Klick-ID und der Browser-ID dargestellt habe, gehe. Der Antrag sei auch begründet, weil eine Einwilligung und damit ein Rechtfertigungsgrund nicht vorliege. Der Unterlassungsantrag zu 3. sei zulässig gemäß Art. 18 Abs. 1 DSGVO. Folge der Einschränkung nach Art. 18 Abs. 1 DSGVO sei, dass nur die Speicherung der jeweiligen Daten erfolgen könne, jedoch keine Weiterverarbeitung. Das Rechtsschutzbedürfnis entfalle auch nicht durch die Selbstlöschungsmöglichkeit. Entgegen der landgerichtlichen Auffassung folge ein Anspruch auf Unterlassung der weiteren Verarbeitung u. a. aus Art. 18 Abs. 1 lit. b) DSGVO. Der Anspruch könne im Rahmen einer Unterlassungsklage geltend gemacht werden.

Dem Klageantrag zu 4 (Verpflichtung zur Löschung) fehle nicht das Rechtsschutzbedürfnis. Vielmehr verletze das Verhalten der Beklagten ihr Recht auf informationelle Selbstbestimmung, weil die Daten bei der Beklagten trotz getrennter Systeme mit kontrolliertem Zugang weiterhin zuordenbar vorlägen. Außerdem stelle die Anonymisierung eine anteilige Löschung im Sinne des Art. 17 DSGVO dar.

Sie habe auch einen Anspruch auf Schadenersatz, der im umfassenden Kontrollverlust aufgrund des Verstoßes gegen Art. 5 Abs. 1, 25 DSGVO bestehe.

Sie verhalte sich auch nicht widersprüchlich, wenn sie das Abomodell nicht annehme, weil durch dieses die Datenverarbeitung nicht wesentlich verändert werde und die Erfassung, Weiterleitung, Speicherung und Weiterverarbeitung unverändert stattfinde.

Die Klagepartei beantragt,

das erstinstanzliche Urteil des Landgericht Magdeburg vom 27.02.2025 abzuändern und neu zu fassen wie folgt:

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks "Instagram" unter dem Benutzernamen „[redacted]" der Beklagten die Erfassung mit Hilfe der Meta Business Tools, die Weiterleitung an die Server der Beklagten, die dortige Speicherung und anschließende Verwendung von folgenden personenbezogenen Daten nicht gestattet:

a) auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der Klagepartei, ob direkt oder in gehashter Form übertragen, d. h.

- E-Mail der Klagepartei
- Telefonnummer der Klagepartei
- Vorname der Klagepartei
- Nachname der Klagepartei
- Geburtsdatum der Klagepartei
- Geschlecht der Klagepartei
- Ort der Klagepartei
- Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID" genannt)
- IP-Adresse des Clients
- User-Agent des Clients (d. h. gesammelte Browserinformationen)
- interne Klick-ID der Beklagten
- interne Browser-ID der Beklagten
- Abonnement-ID
- Lead-ID
- anon_id
- die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid" genannt)

sowie folgende personenbezogene Daten der Klagepartei

b) auf Webseiten

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

c) in mobilen Dritt-Apps

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

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten der Klagepartei gem. dem Antrag zu 1. mit Hilfe der Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden.

3. Die Beklagte wird verurteilt, die über die aktuelle Speicherung hinausgehende Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO sämtlicher unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits von der Beklagten verarbeiteten personenbezogenen Daten bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, bis zur Erfüllung des Löschungsanspruchs nach rechtskräftigem Abschluss des Verfahrens zu unterlassen, insbesondere diese nicht an Dritte zu übermitteln.

4. Die Beklagte wird verpflichtet, sämtliche gem. dem Antrag zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten der Klagepartei einen Monat nach rechtskräftigem Abschluss des Verfahrens vollständig zu löschen und der Klagepartei die Löschung zu bestätigen sowie sämtliche gem. dem Antrag zu 1 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.

5. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über

dem Basiszinssatz seit dem 07.12.2023, zu zahlen.

6. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 1.295,43 Euro freizustellen.

Die Beklagte beantragt,

die Berufung zurückzuweisen.

Die Beklagte verteidigt unter Wiederholung und Vertiefung ihres erstinstanzlichen Vortrages die angegriffene Entscheidung. Ihrer Ansicht nach scheitere der Anspruch im Wesentlichen daran, dass die Klagepartei nicht vorgetragen habe, welche Websites oder Apps von Drittanbietern und wann sie diese besucht habe, ob diese Website oder App zum Zeitpunkt des Besuchs der Klagepartei eines der streitgegenständlichen Business Tools verwendet habe; ob die Klagepartei ihre Zustimmung über das Cookie-Banner auf dieser Website oder App erteilt habe und welche Daten die Website oder App über die streitgegenständlichen Business Tools an die Beklagte übermittelt habe. Die Verarbeitung dieser Daten diene gezielt der Erkennung und Prävention von Sicherheitsbedrohungen sowie der Aufrechterhaltung der Integrität der Plattform.

Unter Bezugnahme auf Anlage B 15 macht sie geltend, bei Meta Pixel würde vor einer Einwilligung des Nutzers keine http-Anfrage gestellt. Bei der Integration von Conversions API könne ein Drittunternehmen eine serverseitige Einwilligungslogik implementieren, um sicherzustellen, dass Daten nur dann über die Conversions API an die Beklagte gesendet würden, wenn der Nutzer seine Einwilligung erteilt habe (Anlagen B 16 und B 17).

Hinsichtlich des Unterlassungsantrages macht die Beklagte geltend, ihr Grundrecht auf Berufsfreiheit gemäß Art. 12 GG überwiege das Interesse der Nutzer an einer Unterlassung der Verarbeitung über Business Tool-Daten. Mit den Klageanträgen würden sie und die Drittunternehmen ihrer Ansicht nach daran gehindert, die streitgegenständlichen Business Tools im Allgemeinen zu nutzen. Dies sei unzulässig. Sofern die Klagepartei ihre Einwilligung widerrufe, bestehe keine Wiederholungsgefahr der Datennutzung.

Der Senat hat am 13. Januar 2026 mündlich verhandelt und die Klagepartei informatorisch angehört. Auf die Schriftsätze der Parteien samt Anlagen, auch die der ersten Instanz, das landgerichtliche Urteil sowie das Protokoll der mündlichen Verhandlung auch in erster Instanz wird ergänzend Bezug genommen.

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 die tenorierten Ansprüche auf Feststellung, Unterlassung, Löschung und Schadensersatz in dem 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.

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.

Die Zuständigkeit folgt auch aus Art. 79 Abs. 2 DSGVO. Gemäß § 79 Abs. 2 DSGVO sind für Klagen gegen einen Verantwortlichen die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Nach S. 2 der Vorschrift können solche Klagen wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich – was vorliegend nicht der Fall ist – bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Die Klagepartei hat ihren gewöhnlichen Aufenthalt in Deutschland (vgl. zuletzt: BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 12, juris).

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. Dass die Beklagte personenbezogene Daten der Klagepartei verarbeitet hat, ist zwischen den Parteien unstreitig. 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 (DS-GVO)/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 führt zur Verantwortlicheneigenschaft i.S.d. Art. 4 Abs. 7 DSGVO aus:
„Durch diese weite Definition soll im Einklang mit dem Ziel der DSGVO ein wirksamer Schutz der Grundfreiheiten und Grundrechte natürlicher Personen und insbesondere ein hohes Schutzniveau für das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten gewährleistet werden." (Urteil vom 5. Dezember 2023, Nacionalinis visuomenės sveikatos centras, C-683/21, Rn. 29 und die dort angeführte Rechtsprechung, juris).

Somit 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, Urteil vom 5. Dezember 2023, C-683/21, 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 EuGH, Urteil vom 29. Juli 2019, Fashion ID, 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).

Im selben Sinne hat der Gerichtshof 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, 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 (Schriftsatz der Beklagten vom 27. Dezember 2024, Rn. 43, Bl. 29 Bd. III f. d. A.; vgl. auch die Nutzungsbedingungen für die Business Tools in Anlage B 5, 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, beckonline).

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.

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.

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 (Feststellungsantrag)

1. Zulässigkeit

Der Klagantrag zu 1. ist als Zwischenfeststellungsklage gemäß § 256 Abs. 2 ZPO zulässig.

Soweit die Klagepartei die Feststellung begehrt, wonach der zwischen den Parteien bestehende „Nutzungsvertrag“ es der Beklagten verwehrt, bestimmte – hinreichend genau bezeichnete – personenbezogene Daten von Dritt-Webseiten und Dritt-Apps zu erheben, weiterzugeben, zu speichern und zu verwenden (Antrag zu 1.), ergibt sich die Zulässigkeit der Klage aus § 256 Abs. 2 ZPO.

a)
Allerdings folgt die Zulässigkeit nicht aus § 256 Abs. 1 ZPO, weil es am Feststellungsinteresse fehlt.

aa) Ein Feststellungsinteresse i.S.v. § 256 Abs. 1 ZPO besteht, wenn dem subjektiven Recht der Klagepartei eine gegenwärtige Gefahr der Unsicherheit dadurch droht, dass die Beklagtenseite es ernstlich bestreitet oder sie sich eines Rechts gegen die Klagepartei berühmt, und wenn das erstrebte Urteil infolge seiner Rechtskraft geeignet ist, diese Gefahr zu beseitigen. Dieses Erfordernis beruht darauf, dass es nicht zu den Aufgaben der Gerichte gehört, einem Beteiligten zu bescheinigen, ob er im Recht war oder nicht (BGH, Urteil vom 17. Juni 2016, V ZR 272/15, Rn. 13, juris). Ist der Klagepartei eine Klage auf Leistung möglich und zumutbar und erschöpft sie das Rechtsschutzziel. Es fehlt grundsätzlich das Feststellungsinteresse, weil die Klagepartei im Sinne einer besseren Rechtsschutzmöglichkeit den Streitstoff in einem Prozess klären kann (Zöller-Greger, ZPO, 36. Auflage, § 256 ZPO, Rn. 14).

bb) Die bereits gestellten Leistungsanträge auf Löschung, Unterlassung und Schadenersatz erschöpfen das Rechtsschutzziel der Klagepartei dadurch, dass ihr Schadenersatz aufgrund der vergangenen Datenverarbeitung gezahlt und die streitgegenständliche Datenerhebung unterlassen werden soll (zu den Anforderungen: MüKoZPO/Becker-Eberhard, 7. Aufl. 2025, ZPO § 256 Rn. 47; Stein/Roth, 24. Aufl. 2024, ZPO, § 256 Rn. 76, beck-online). Diese lassen das Feststellungsinteresse entfallen, wenn sich – wie hier – das Rechtsschutzziel hierin erschöpft. Soweit die Klagepartei sich gegen die weitere Verwendung der Daten wendet, ist ihr Rechtsschutzziel in den Anträgen zu Ziff. 2 bis 5. abgebildet (OLG München, Urteil vom 18. Februar 2020, 18 U 3465/19, Rn. 45, juris).

b)
Der Antrag zu Ziff. 1 ist als Zwischenfeststellungsklage nach § 256 Abs. 2 ZPO zulässig, was von Amts wegen zu prüfen ist (BGH, Urteil vom 25. Oktober 2007, VII ZR 27/06, Rn. 10 mwN, juris).

aa) Gegenstand einer Zwischenfeststellungsklage kann das Bestehen oder Nichtbestehen eines Rechtsverhältnisses sein, also die aus einem konkreten Lebenssachverhalt entstandenen Rechtsbeziehungen von Personen zu Personen oder von Personen zu Sachen. Ein Rechtsverhältnis ist eine aus dem vorgetragenen Sachverhalt abgeleitete rechtliche Beziehung von Personen untereinander oder zu einem Gegenstand, die ein subjektives Recht enthält oder aus der ein solches Recht entspringen kann (zuletzt: BGH, Urteil vom 13. November 2025, IX ZR 127/24, Rn. 27, juris).

Darunter fallen auch einzelne Folgen von Rechtsbeziehungen, wozu der Senat auch die Frage zählt, ob ein Rechtsverhältnis – wie hier von der Klagepartei behauptet – rechtswidrig ausgestaltet wird (vgl. BGH, Urteil vom 6. April 2016, VIII ZR 79/15, Rn. 44, juris). Auf die Feststellung der Unzulässigkeit des Verhaltens der Beklagten zielt der Feststellungsantrag ab, mithin auf das Nichtbestehen eines Rechtsverhältnisses.

Vorliegend verbindet die Parteien unstreitig ein Vertrag zur Nutzung der Social Media Plattform Instagram. Nach dem Verständnis des Senats begehrt die Klagepartei die Feststellung, dass der Beklagten ein von ihr aus diesem Vertrag hergeleitetes und in Anspruch genommenes Recht nicht zusteht.

bb) Die begehrte Feststellung muss sich allerdings grundsätzlich auf einen Gegenstand beziehen, der über den der Rechtskraft fähigen Gegenstand des Hauptsachebegehrens hinausgeht. Die danach erforderliche Vorgreiflichkeit für die Entscheidung in der Hauptsache, also die Möglichkeit, dass das inzidenter ohnehin zu klärende Rechtsverhältnis zwischen den Parteien noch über den gegenwärtigen Streitgegenstand hinaus Bedeutung hat oder gewinnen kann (BGH, Urteil vom 5. November 2024, II ZR 35/23, Rn. 17, juris), durch die zugleich das sonst nach § 256 Abs. 1 ZPO erforderliche berechtigte Interesse an der begehrten Feststellung ersetzt wird, liegt hier vor.

(1) Präjudiziell (im strengen Sinne) ist das Rechtsverhältnis, wenn es für den in der Hauptentscheidung enthaltenen Subsumtionsschluss ein notwendiges Element ist und die Feststellung über den gegenwärtigen Streitgegenstand hinaus Bedeutung hat oder gewinnen kann. Bei der Zwischenfeststellungsklage genügt grundsätzlich hierfür schon die bloße Möglichkeit (MüKoZPO/Becker-Eberhard, 7. Aufl. 2025, ZPO § 256 Rn. 85, beck-online; BeckOK

ZPO/Bacher, 58. Ed. 1.9.2025, ZPO § 256 Rn. 43, beck-online; Zöller-Greger, ZPO, 36. Aufl., § 256, Rn. 35; BGH, Urteil vom 28. Januar 2020, Rn. 16, juris; OLG Dresden, Beschluss vom 13. Februar 2024, 4 U 1325/23, Rn. 9; beckonline).

(2) Diese weitergehende Bedeutung liegt vor, weil sich – vom Vortrag der Parteien ausgehend – nicht ausschließen lässt, dass die von Drittanbietern stammenden und der begehrten Feststellung unterliegenden Daten der Klagepartei in die Hände Nichtberechtigter geraten (z.B. durch die in der Datenschutzerklärung der Beklagte angesprochenen „Angriffsversuche auf Meta-Server“) und dass hieraus neuerlich Ansprüche der Klagepartei entstehen. Die Folgen eines derartigen Angriffs gingen über den Unterlassungsantrag hinaus. Die Klagepartei hat zudem bislang auch noch keinen Auskunftsanspruch rechtshängig gemacht, für den die Frage der Rechtmäßigkeit ebenfalls eine Rolle spielen könnte. Ein Ausspruch über den Zwischenfeststellungsantrag der Klagepartei könnte daher weitergehende rechtliche Bedeutung haben (OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25 e, Rn. 178, beckonline).

2. Begründetheit

Der Antrag zu Ziff. 1 ist auch begründet.

a)
Die Beklagte verarbeitet personenbezogene Daten der Klagepartei. Bei den im Klageantrag zu 1. genannten Daten handelt es sich um personenbezogene Daten.

aa) Gemäß Art. 4 Nr. 1 DSGVO bezeichnet der Ausdruck „*personenbezogene Daten*“ im Sinne der DSGVO. Hierunter sind nach der Begriffsbestimmung dieser Vorschrift alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei klargestellt wird, dass „als identifizierbar eine natürliche Person angesehen wird, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (zuletzt: EuGH, Urteil vom 2. Dezember 2025, C-492/23, Rn. 48 mwN; BGH, EuGH-Vorlage vom 28. August 2025, VI ZR 258/24, Rn. 23; Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl., Art. 4 Nr. 1 DSGVO Rn. 6; Klar/Kühling in Kühling/Buchner, DSGVO BDSG, 4. Aufl., Art. 4 Nr. 1 DSGVO Rn. 2; Klabunde/Horváth in Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl., Art. 4 Rn. 8; Ziebarth in Sydow/Marsch, DSGVO/ BDSG, 3. Aufl., Art. 4 DSGVO Rn. 7). Er umfasst

auch alle Informationen, die erst aus einer Verarbeitung zuvor vorhandener personenbezogener Daten resultieren (Ehmann/Selmayr/Ehmann, 3. Aufl. 2024, DS-GVO, Art. 15 Rn. 34, beck-online; EuGH, Urteil vom 4. Mai 2023, C 487/21, Rn. 26, juris).

bb) Unzweifelhaft sind danach die E-Mail der Klagepartei, ihre Telefonnummer, ihr Vor- und Nachname, ihr Geburtsdatum, ihr Geschlecht und der Ort, an dem sie sich befindet, personenbezogene Daten. Ebenso handelt es sich bei der IP-Adresse des genutzten Clients um ein personenbezogenes Datum (Ehmann/Selmayr/Klabunde/Horváth, 3. Aufl. 2024, DS-GVO Art. 4 Rn. 18, beck-online).

Ferner handelt es sich auch bei der internen Klick-ID sowie der internen Browser-ID der Beklagten um personenbezogene Daten. Mit diesen Daten können die Aufrufe der Drittwebseite und die Aktionen darauf eindeutig einem bestimmten Instagram-Konto zugeordnet werden, in diesem Fall dem Konto der Klagepartei.

Auch die URLs der besuchten Webseiten samt ihrer Unterseiten, der Zeitpunkt des Besuchs, der „Referrer“ (d.h. die Webseite, über die der Nutzer zur aktuellen Webseite gekommen ist), die von der Klagepartei angeklickten Buttons sowie die weiteren, von der Beklagten „Events“ genannten Daten, die die Interaktion der Klagepartei auf der jeweiligen Webseite dokumentieren sind personenbezogene Daten, da sie jeweils in Verbindung mit weiteren Informationen der Klagepartei zugeordnet werden können und dadurch Informationen über diese beinhalten. So kann dadurch ermittelt werden, welche Webseiten die Klagepartei besuchte, wann dies geschah, von welcher Webseite sie dort hingelangte, sowie welche Aktionen sie dort durchgeführt hat, beispielsweise, ob sie bestimmte Artikel gekauft hat.

Aus den gleichen Gründen handelt es sich schließlich bei dem Namen der App, sowie dem Zeitpunkt des Besuchs, den von der Klagepartei in der App angeklickten Buttons, sowie den von der Beklagten „Events“ genannten Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren, um personenbezogene Daten.

Die Daten zum User-Agent des Clients, welche ausweislich des klägerischen Vortrags, welchem die Beklagte nicht entgegengetreten ist, die für das Digital Fingerprinting nutzbaren Daten darstellen, stellen somit ebenfalls personenbezogene Daten dar.

Schließlich sind auch die Lead-ID, die Abonnement-ID, die anon_id sowie die externe ID besuchter Webseiten (external ID) personenbezogene Daten. Denn als „ID“ stellen sie Identitätsdokumente bzw. Kennungen der Klagepartei bezüglich ihrer Aktionen/Kontakte im Internet als potenzieller Kunde („Lead“), als Abonnent sowie die Kennung der Klagepartei bei

anderen Werbetreibenden dar (Ehmann/Selmayr/Klabunde/Horváth, 3. Aufl. 2024, DS-GVO Art. 4 Rn. 17, beck-online).

b)
Die Datenverarbeitung der Beklagten ist in drei Perioden einzuteilen: die Zeit vom 25. Mai 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 der danach liegenden 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. Hiergegen wendet sich die Beklagte auch nicht substantiiert.

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.

Die Beklagte hat für diesen Zeitraum die Hürde des Verbots von Datenübermittlungen in Drittstaaten gem. Art. 44 ff. DS-GVO schuldhaft nicht überwunden. Gründe, die die Übermittlung der personenbezogenen Daten der Klagepartei in die USA im Zeitraum vom 16. Juli 2020 bis zum 7. Oktober 2022 rechtfertigen könnten und die sich aus den Erlaubnistatbeständen der Art. 45 bis 47 DSGVO ergeben könnten, hat die Beklagte nicht hinreichend dargetan. Sie hat hierzu gar keinen weiteren detaillierten Vortrag gehalten und lediglich auf ihre Standardvertragsklauseln verwiesen. Die Übermittlung war jedoch 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) DSGVO 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 Instagram-Nutzungsbedingungen (Anlagen B 2 und B 3) keine wirksame Einwilligung zu einem Datentransfer in die USA im o.g. Zeitraum zu sehen.

(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 über das konkrete Risiko der Datenübermittlung in ein Drittland ohne adäquates Schutzniveau aufgeklärt werden (Gola/Heckmann/Klug, 3. Aufl. 2022, DS-GVO 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. Hierzu fehlt jeglicher Vortrag.

(1.3.) Daraus folgt zugleich, dass die behauptete Einwilligung nicht freiwillig war (vgl. EWG 43 DSGVO; Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO 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“ Übermittlung darstellt.

(2.2.) Die 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 iSv § 328 BGB (Gola/Heckmann/Klug, 3. Aufl. 2022, DS-GVO 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 ganz bestimmt nicht als Grundlage „massenhafter“ Übermittlungen (vgl. EWG 111 DSGVO).

(3) Für den Zeitraum vom 16. 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 DS-GVO, 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 Suveillance 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 sind die ungehinderte Informationssammlung (sog. bulk collection) möglich, die die Beklagte ja auch selbst gerade vornimmt (vgl. Anlage K 11 und K 126).

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 ua/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 Daten-

schutzgarantien 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 DS-GVO, 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 (aaO, Rn. 106, 115).

(9) Auf diese Rechtslage hat der Senat 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 Nutzer und der Klagepartei.

(1) Die Klagepartei hat in ihrer informatorischen Anhörung vor dem Senat ausgeführt, sie lehne auf den Drittwebseiten Cookies nach Möglichkeit ab, wenn sie dies nach den auf dem Bildschirm erscheinenden Einstellungen tun könne. Nur selten, aus Zeit- oder Bequemlichkeitsgründen, nehme sie ausnahmeweise Cookies an. Dagegen habe sie nach ihrer Kenntnis keine Möglichkeit, auf der Instagram-Seite der Weitergabe der Daten an Dritte oder der Datenverarbeitung durch Instagram zuzustimmen oder diese abzulehnen. Denn man könne nach ihrer Erfahrung nur zustimmen, andernfalls könne man die Seite nicht mehr nutzen, wenn man alles abwähle. Der Senat geht aufgrund dieser Aussage davon aus, dass die Klagepartei die Cookies auf der Website der Beklagten nicht abgewählt und auch die Abonnement-Variante nicht angenommen hat. Auch die durch eine Cookie-Einwilligung oder Abwahl der Abonnement-Variante durchgeführte Datenverarbeitung ist rechtswidrig. Sie verstößt sowohl gegen den Grundsatz der Datenminimierung (vgl. Ziff. 3) und ist mangels Rechtfertigungsgrundes aus Art. 6 DSGVO (vgl. Ziff. 4) rechtswidrig.

(2) Aber 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 ConversionsAPI 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). Aus Anlage K 17 (*Redesigning our systems*, dort S. 4) folgt ebenfalls, dass im Fall der Trennung der Off-Site-Aktivitäten eine zufällige Measurement ID gebildet und die Nutzerdaten weiterhin in einer Gruppe verarbeitet werden. Außerdem erhält der Nutzer eine ASID zugeordnet, der es bei Trennung des Nutzeraccounts ermöglicht, die mit dem Nutzer verbundenen Daten zu erhalten (S. 5, Anlage K 6). Die Beklagte räumt im Meta Playbook (Anlage K 11; dort S. 23)

und in Anlage K 17 (*Redesigning our systems to provide more control over Off-Facebook Activity*, dort S. 3 und 4), ein, dass die Daten weiterverarbeitet werden, weil weiterhin verlässliche Berichte an die Drittunternehmen übermittelt werden sollen. Daher wird eine neue – zufällige – Measurement ID für den Nutzer geschaffen, die zwar keinen individuellen Nutzer mehr repräsentiert, aber gleichwohl die Daten des jeweiligen Nutzers in einem Bündel verarbeitet („*Instead, it is assigned to many users.*"). Mit dieser Methode nutzt die Beklagte weiterhin die – pseudonymisierten – Nutzerdaten für ihre eigenen Analysezwecke („*We can conclude that one pf the people in the bucket saw an ad and then visited the target website.*"). Daraus ergibt sich, dass die Beklagte weiterhin die Daten der Klagepartei – lediglich in einem Bündel mit den Daten anderer Nutzer – nutzt, obwohl die Klagepartei einer Nutzung ihrer Daten für Werbezwecke widersprochen hat.

(3) Eine solche Verarbeitung ist rechtswidrig, weil – wie EWG 26 DSGVO klarstellt, hat auch eine Pseudonymisierung (Abs. 5) keine Wirkung auf den Personenbezug der Daten, 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, DS-GVO Art. 4 Rn. 19, beck-online).

c)
Die Datenverarbeitung durch die Beklagte ist durchgehend ab dem 25. Mai 2018 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 B5) 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 B5). 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 Instagram-Konto anmelden und die dort erhobenen Daten werden nicht verwendet, um relevante Werbung zu zeigen. Sie werden aber in eingeschränktem Umfang genutzt, um für Sicherheit und Integrität zu sorgen und es kann sein, dass die Beklagte aggregierte Informationen zu Aktivitäten erhält, nicht aber die persönliche Cookie-Information des Nutzers (Anlage 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, aaO, Rn. 62). Diese Gefahr besteht auch mit den Änderungen der Cookie-Einstellungen fort.

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 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. Eine freiwillige Einwilligung zur Datenübermittlung an Drittwebseiten und -Apps i.S.d. Art. 4 Nr. 11 DSGVO 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). Die Beklagte kann sich nicht auf eine Einwilligung der Klagepartei nach Art. 6 Abs. 1 lit. a), Art. 9 Abs. 2 lit. a) DSGVO berufen.

Nach Art. 7 Abs. 1, EWG 42 DSGVO trägt die Beklagte in Fällen, in denen die Verarbeitung auf einer Einwilligung beruht, die Beweislast dafür, dass die Klagepartei in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 152, juris).

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 DS-GVO

(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. ua/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 geschaffen. Soweit die Beklagte meint, darin, dass die Klagepartei „optionale Cookies“ erlaubt bzw. diese bei „Informationen über Aktivitäten von Werbepartnern“ aktiviert habe, liege eine wirksame Einwilligung, geht diese Auffassung fehl.

(3) Aber auch für die Zeit nach dem 3. November 2023 liegt in der unter Rn. 84 des Schriftsatzes vom 29. Juli 2024 dargestellten Einwilligung keine Einwilligung zur Datenverarbeitung über Business Tools. Denn, dass die Informationen der Drittanbieter nicht auch an die Beklagte gesandt und praktisch ungefiltert für alle Zwecke verwendet werden und die Klagepartei hierin eingewilligt hat, ergibt sich hieraus gerade nicht. Vielmehr heißt es nur, dass die Nutzer wählen können, ob die Werbung angezeigt werden soll. Die darüber hinausgehende Rückinformation der Drittanbieter, und sei es auch – wie die Beklagte vorträgt, unter Verstoß gegen deren vertragliche Pflichten – an die Beklagte und weitere Verarbeitungsvorgänge

sind nicht erwähnt. Allenfalls bezog sich die Einwilligung der Klagepartei allein auf die Verarbeitung ihrer personenbezogenen Daten zu Werbezwecken, nicht aber auf die exzessive Verarbeitung über die Business Tools. Mit dem verharmlosenden Hinweis auf aggregierte Informationen in den Cookie-Einstellungen (vgl. Rn. 33 Schriftsatz vom 12. Februar 2024) wird auf die Tragweite der Verarbeitung, wie sie sich aus dem Meta Playbook und Anlage K 11 ergibt, nicht ansatzweise hingewiesen, wenn die Klagepartei wie hier nach ihrer informatorischen Anhörung auf den Drittwebseiten die Cookies ablehnt. Denn auch aus dieser Gruppe heraus, in die ein Nutzer mit seiner randomisierten 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. Außerdem besteht für die Beklagte weiterhin die Möglichkeit, individualisierte Informationen zurückzuhalten (vgl. S. 4 Anlage K 11 – „*we can retain a limited set of flagged activity for a longer time*“). Denklogisch müssen die Nutzerdaten für die Beklagte nutzbar bleiben, bevor böswillige Akteure handeln. Daraus folgt, dass eine nicht näher bezeichnete Datenmenge über einen unbekannten Zeitraum (möglicherweise bis zu 2 Jahre) über jeden Nutzer gespeichert wird, um die Nutzung von eventuellen böswilligen Akteuren zu verhindern.

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, Rn. ff.).

(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.

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. ua/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-Grundrechtecharta 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, 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 ansatzweise 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 2, 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 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 eklatanten 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, was die Beklagte in Rn. 154 ihrer Berufungserwiderung zwar der Klagepartei vorwirft, sich aber durch ihre systematische Datenausbeutung und -verwendung allein auf ihrer Seite zeigt. Sie selbst führt dazu in Anlage K 17 (dort S. 5). aus, sie müsse weiterhin sicherstellen, dass die Messberichtserstattung und die Integrität ihrer Plattform wie bisher funktionieren.

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. ua/ 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 mwN). 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, aaO, 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. ua/Bundeskartellamt) Rn. 130, 137, juris).

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. Es ist – außer 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.

Die Beklagte kann die Daten auch nicht aus Gründen der Strafverfolgung verarbeiten (lit. ee)). Die Beklagte ist ein Wirtschaftsunternehmen und keine Strafverfolgungsbehörde. 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, DS-GVO Art. 6 Abs. 1 Rn. 53, beck-online; EuGH (Große Kammer), Urteil vom 4. Juli

2023, C-252/21 (Meta Platforms Inc. ua/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 iSd 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. ua/Bundeskartellamt) Rn. 126, juris; BeckOK DatenschutzR/Veit/Albers, 54. Ed. 1.8.2025, DS-GVO 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, beckonline; BeckOK DatenschutzR/Veit/Albers, 54. Ed. 1.8.2025, DS-GVO Art. 6 Rn. 68 mwN, 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 Nutzer-Eigenschaft 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 das berechtigte 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).

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 11 und K 17 ergibt. Für sie sind vielmehr ihre eigenen wirtschaftlichen Interessen alleiniges Maß. Das Recht der Klagepartei auf informationelle Selbstbestimmung wird von ihr nicht 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.

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.

(4) 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 Playbook und Anlage K 17 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 Gesundheitsdaten. 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.

Die Klagepartei hat in ihrer informatorischen Anhörung vor dem Senat erläutert, dass sie Finanz- und Aktienseiten, aber auch Gesundheitsseiten wie die Shopapotheke.de besuche. Die Beklagte hat diesen Vortrag mit Nichtwissen bestritten. Der Senat folgt der Aussage der Klagepartei. Die Klagepartei war gut vorbereitet und ihr besonderes Interesse am Datenschutz mit ihrer Tätigkeit für die Bundeswehr und dort besonders sensiblen Bereichen wie Auslandseinsätzen begründet. Ihr sei das Ausmaß der Datenverarbeitung zunächst nicht

bewusst gewesen und sei nun entsetzt, welche Daten gesammelt werden könnten, was für ihre Berufsausübung bei der Bundeswehr durchaus problematisch werden könnte, insbesondere hinsichtlich der Gesundheitsdaten. Der Senat folgt der Aussage der Klagepartei in ihrer informatorischen Anhörung vor dem Senat und legt sie seiner Entscheidung zugrunde. Die Klagepartei hat ausgeführt, sie surfe aufgrund ihres Alters und ihrer beruflichen Anforderungen häufig nach Gesundheitsfragen im Internet, insbesondere auf Apothekenseiten wie shopapotheke.de (vgl. Anlagen K 13 und K 14 zur Implementierung der Business Tools auf dieser Seite).

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 eine gleichwertige Alternative liegt, kann dahinstehen, weil die Daten der Nutzer trotzdem an die Beklagte übertragen werden, wie sich aus Anlagen K 11 und K 17 ergibt.

C. Unterlassungsantrag (Klagantrag zu 2.)

Die Klagepartei hat künftig einen Anspruch auf Unterlassung der Datenverarbeitung auf Drittseiten und -Apps gemäß §§ 1004 Abs. 1 analog, 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 GG, Art. 1 Abs. 1 GG, ihres Rechts auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh und dem Nutzungsvertrag (BGH, Urteil vom 11. November 2025, VI ZR 396/24, Rn. 43, juris). Anspruchsgrundlagen aus der DSGVO ergeben sich nicht (EuGH, Urteil vom 4. September 2025, C-655/23, Rn. 43, juris).

1.
Der Unterlassungsantrag ist im tenorierten Umfang zulässig, insbesondere entgegen der Ansicht der Beklagten hinreichend bestimmt.

a)
Ein Klageantrag ist hinreichend bestimmt, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt. Ein Unterlassungsantrag darf vor diesem Hintergrund nicht derartig undeutlich gefasst sein, dass die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (st. Rspr., vgl. z. B. BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 52 mwN, juris). Erforderlich ist eine Bezugnahme auf die konkrete Verletzungsform und dass der Klageantrag zumindest unter Heranziehung des Klagevortrags unzweideutig erkennen lässt, in welchen Merkmalen des angegriffenen Verhaltens die Grundlage und der Anknüpfungspunkt für den Rechtsverstoß und damit das Unterlassungsgebot liegen soll (BGH, aaO, Rn. 53, juris).

b)
Der Antrag ist hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Denn er lässt sich unter Heranziehung des Klagevorbringens dahingehend auslegen, dass die Klagepartei ein Unterlassen jeglicher Verarbeitung ihrer personenbezogenen Daten i.S.d. Art. 4 Nr. 1 DSGVO, welche sie genau benannt hat, außerhalb der Netzwerke der Beklagten durch Dritte verlangt. Durch die genaue Auflistung der Daten wird der Beklagten ohne Weiteres deutlich, für welche Zwecke sie die personenbezogenen Daten der Klagepartei noch verarbeiten darf und für welche die Klagepartei die Unterlassung der Datenverarbeitung begehrt. Der Unterlassungsantrag konkretisiert darüber hinaus die inkriminierte Verletzungshandlung, nämlich die behauptete unrechtmäßige Verarbeitung ihrer Daten durch die Business Tools auf Grundlage einer unwirksamen Einwilligung. Auf eine Spezifizierung der Drittwebseiten und Apps kommt es nicht an, weil die Einbeziehung der Business Tools in der aktuellen Funktionsweise grundsätzlich untersagt werden soll. Mit anderen Worten: Der Beklagten sollen alle Verarbeitungsvorgänge, die sie über Drittwebseiten durch die Business Tools vornimmt, untersagt werden, wenn die genannten Datenpunkte bezeichnet sind. Dass sich die Klagepartei an den – durch Rechtsprechung und Literatur deutlich konturierten – Begriffen des Art. 4 Nr. 2 DSGVO orientiert, sorgt entgegen der Ansicht der Beklagten für mehr und nicht für weniger Klarheit.

Dass denkbare Ausnahmetatbestände – insbesondere eine etwaige Einwilligung und ein Rechtsfertigungsgrund gemäß Art. 6 Abs. 1 lit. b) bis e) DSGVO – enthalten sind (vgl. hierzu zuletzt etwa BGH, Urteil vom 18. Oktober 2025, IV ZR 431/24, Rn. 28 ff. für sog. „Schufa-Verfahren“, juris), führt zur Zulässigkeit des Antrages, weil anderenfalls im Vollstreckungsverfahren nicht erkennbar wäre, welche konkreten Handlungen von dem Verbot ausgenommen werden sollen (BGH, Urteil vom 18. Oktober 2012, I ZR 137/11, Rn. 21, juris). Der Senat erachtet es daher für prozessual überzeugend, für diese Fragen im Falle der Vollstreckung aus dem vorliegenden Urteil trotz eventuellem Vorliegens einer Einwilligung den Weg einer Vollstreckungsgegenklage zu beschreiten (wie hier: OLG Düsseldorf, Urteil vom 23. Oktober 2025, I-16 U 47/25, Rn. 31 mwN, juris).

c)
Der Klagepartei fehlt für den solchermaßen zu verstehenden Antrag auch nicht das Rechtsschutzbedürfnis.

aa) Das Rechtsschutzbedürfnis fehlt, wenn eine Klage oder ein Antrag objektiv schlechthin sinnlos ist, wenn also der Kläger unter keinen Umständen mit seinem prozessualen Begehren irgendeinen schutzwürdigen Vorteil erlangen kann. Das ist etwa der Fall, wenn ein einfacherer oder billigerer Weg zur Erreichung des Rechtsschutzziels besteht oder der Antragsteller kein berechtigtes Interesse an der beantragten Entscheidung hat. Dafür gelten jedoch strenge Maßstäbe (vgl. BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 67, juris). Für einen den Komplex der Scraping-Fälle im Datenarchiv der Beklagten betreffenden Unterlassungsantrag hat der Bundesgerichtshof bereits entschieden, dass die dem Nutzer mögliche Löschung der Mobiltelefonnummer aus seinem Nutzerprofil bei der Beklagten kein einfacherer und billigerer Weg ist, um die geforderte Unterlassung zu erreichen, weil sich der Nutzer damit der Sicherheitsvorteile einer Zwei-Faktor-Authentifizierung begebe (BGH, Urteil vom 18. November 2024, Rn. 69, juris). Daraus folgt, dass ein Rechtsschutzbedürfnis für den Unterlassungsantrag nicht zu verneinen ist, weil die Klagepartei ihr Instagram-Konto löschen könnte. Dadurch würde sich die Klagepartei der gesamten Nutzungsmöglichkeit begeben. Die Klagepartei hat insoweit in ihrer informatorischen Anhörung vor dem Senat ausgeführt, sie sei zwar nicht mehr so viel wie früher auf Instagram aktiv, nutze ihren Account aber noch als privates Tagebuch, für den sie wegen der vielen privaten Daten auch einen Schutz begehre. Eine Löschung ihres Accounts komme daher für sie nicht in Betracht.

bb) Die Beklagte kann die Klagepartei nicht darauf verweisen, dass sie über die Einstellung „*Informationen von Werbepartnern zu deinen Aktivitäten*“ mit technischen Möglichkeiten des Internet-Browsers die Datenweitergabe verhindern könnte. Die Beklagte verweist selbst zu

Recht darauf, dass sich die Klagepartei nicht gegen einzelne konkrete Datenverarbeitungen der Beklagten wendet. Sie wendet sich vielmehr gegen die systematische, grundsätzliche Anwendung der Business Tools auf sie als Person und die hierdurch verwirklichte allgegenwärtige Gefährdung ihrer informationellen Selbstbestimmung.

cc) Der Unterlassungsantrag überschreitet auch nicht in unzulässiger Weise den Rahmen eines deutschen Zivilprozesses, weil die Stattgabe des Antrags zur Einstellung des Betriebs der Business Tools in der aktuellen Funktionsweise führen würde (Rn. 110 Berufungserwiderung). Der Senat hat hier nicht zu entscheiden, ob die Verarbeitung von Daten über die Business Tools generell rechtswidrig ist, sondern ob sich aus einer Anspruchsgrundlage im deutschen oder EU-Recht ein Anspruch der Klagepartei auf Unterlassung der Datenverarbeitung ihrer personenbezogenen Daten ergibt. Soweit die Datenverarbeitungsvorgänge betreffend die Klagepartei mit weiteren Datenverarbeitungsvorgängen anderer Nutzer so verknüpft sind, dass eine individuelle Trennung der Datenverarbeitungsvorgänge technisch nicht möglich ist, steht dieser Umstand dem individuellen Rechtsschutz für die Klagepartei nicht entgegen. Gegebenenfalls muss die Beklagte ihre Datenverarbeitung dann den rechtlichen Erfordernissen anpassen, wenn sie die Datenverarbeitung über die Business Tools für die weiteren Nutzer weiter bereitstellen will.

Das Bundesverfassungsgericht hat zum Recht auf informationelle Selbstbestimmung ausgeführt:

„Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG)

verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83, Rn. 148, juris).

Hieraus folgt, dass ein Individualrechtsschutz zu gewährleisten ist.

d)
Der so verstandene Unterlassungsantrag enthält entgegen der Ansicht der Beklagten auch kein im Sinne des § 890 Abs. 2 ZPO unzulässiges Antragsbegehren bzw. ist nicht auf ein zukünftiges aktives Tun gerichtet. Die Klagepartei begehrt die Unterlassung der Verarbeitung ihrer personenbezogenen Daten auf Drittwebseiten.

Die Beklagte kann sich auch nicht darauf berufen, die Drittanbieter entschieden, ob sie die streitgegenständlichen Business Tools nutzen, um Daten an sie zu senden, weil diese Frage nicht streitgegenständlich ist.

e)
Dass die Beklagte – z.B. durch eine entsprechende Gestaltung der Business-Tools – (aktiv) handeln muss, um den Unterlassungsanspruch erfüllen zu können, hindert die Unterlassungsanordnung nicht (st. Rspr., z.B. BGH, Urteil vom 15. August 2013, I ZR 80/12, Rn. 21; BGH, Urteil vom 26. Juli 2018, I ZR 64/17, Rn. 57, juris). Unter die von der Beklagten vorzunehmenden Handlungen kann auch die Einwirkung auf Dritte fallen (vgl. BGH, Urteil vom 14. März 2017, VI ZR 721/15, Rn. 35, juris).

2.
Der Unterlassungsantrag ist im tenorierten Umfang auch begründet. Die Klagepartei kann verlangen, dass die Beklagte es unterlässt, ihre personenbezogenen Daten anlässlich eines Besuchs auf Drittwebseiten und -Apps zu verheben. Allerdings ergibt sich ein Unterlassungsanspruch nicht aus der DSGVO (EuGH, Urteil vom 4. September 2025, C-65/23, Rn. 43, juris). Er ergibt sich wegen der Verletzung von Vertragspflichten gemäß § 280 Abs. 1, § 241 Abs. 2 BGB aus dem mit der Beklagten geschlossenen Nutzungsvertrag selbst und zum anderen aus §§ 1004 Abs. 1 S. 2 analog, 823 Abs. 1 BGB, wenn, ebenso wie bei einem gesetzlichen Unterlassungsanspruch nach § 823 Abs. 1 BGB i.V.m. § 1004 Abs. 1 Satz 2 BGB analog, eine Erstbegehungs- beziehungsweise Wiederholungsgefahr besteht (vgl. BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 83, mit Verweis auf BGH, Urteile vom

2. Mai 2024, I ZR 12/23, Rn. 14, vom 29. Juli 2021, III ZR 179/20, Rn. 102 f., und vom 8. November 2022, II ZR 91/21, Rn. 64, juris; BeckOK DatenschutzR/Albers/Veit, 54. Ed. 1.8.2025, DS-GVO Art. 6 Rn. 115, beck-online). Dabei begründet ein einmal erfolgter Vertragsverstoß die tatsächliche Vermutung für seine Wiederholung, nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urteil vom 29. Juli 2021, III ZR 192/20, Rn. 115-116; Urteil vom 20. Juni 2013, I ZR 55/12, Rn. 18; Beschluss vom 3. April 2014, I ZB 42/11, Rn. 12; mwN, juris).

Der nicht erforderliche und auch nicht durch eine Einwilligung gedeckte Verstoß gegen den Grundsatz der Datenminimierung und die rechtswidrige Datenverarbeitung mangels Rechtfertigungsgrundes hat die Klagepartei in ihrem allgemeinen Persönlichkeitsrecht verletzt, das sie gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten schützt (Recht auf informationelle Selbstbestimmung, vgl. hierzu Art. 7, 8 GRCh; Art. 8 EMRK; BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83, insb. Rn. 148, juris).

Die Beklagte darf anders als in ihren AGB aufgeführt „App-, Browser- und Geräteinformationen“ und „Informationen von Partnern, Anbietern und Dritten“ nicht dauerhaft und uneingeschränkt ohne eine gesonderte Einwilligung zur „Erfüllung eines Vertrages”, zur „Erfüllung einer rechtlichen Verpflichtung”, zum Schutz „wesentlicher Interessen”, zur „Wahrung öffentlicher Interessen” oder für die „berechtigten Interessen” der Beklagten verarbeiten, wenn hierfür keine Einwilligung vorliegt. Im Einzelnen:

a)
Die Beklagte verarbeitet personenbezogene Daten der Klagepartei. Bei den im Klageantrag zu 1) genannten Daten handelt es sich um personenbezogene Daten (vgl. B.2.b) und c).

aa) Der Senat geht auch davon aus, dass die Klagepartei von der Datenerhebungspraxis der Beklagten über Drittwebseiten betroffen war, ohne dass es entgegen der Ansicht der Beklagten weiteren Vortrages zum Aufrufen der Seiten bedarf. Die Beklagte bestreitet schon nicht, grundsätzlich mittels der Business Tools personenbezogene Daten über die Klagepartei zu erfassen. Eine substantiierte Darlegung, wann die Klagepartei welche Webseite besuchte oder welche Applikation nutzte, ist nicht geboten. Die Beklagte bedarf dieser Information schon nicht, weil die erforderlichen Daten auf ihr zugänglichen Servern hinterlegt sind.

(1) Das Maß der Substantiierung ist individuell zu bestimmen. Eine Partei hat grundsätzlich auf Erklärungen des Prozessgegners substantiiert mit näheren positiven Angaben zu erwidern und darzulegen, von welchem Sachverhalt sie selbst ausgeht (vgl. BGH, Beschluss

vom 20. Mai 2015, IV ZR 127/14, Rn. 17; BGH, Urteil vom 26. Januar 2023, I ZR 15/22, Rn. 18; BGH, Urteil vom 12. Juli 2023, VIII ZR 60/22, Rn. 26, juris). Je detaillierter der Vortrag der Gegenseite, desto weiter reicht auch die eigene Substantiierungspflicht (vgl. BGH, Urteil vom 12. Juli 2023, VIII ZR 60/22, Rn. 26; BGH, Beschluss vom 17. April 2024, XII ZR 56/23, Rn. 12; BGH, Urteil vom 18. April 2024, IX ZR 129/22, Rn. 23, juris). So ist etwa einfaches Bestreiten dabei grundsätzlich nur dann ausreichend, wenn und soweit es der betreffenden Partei entweder an der erforderlichen Tatsachenkenntnis fehlt oder der Vortrag der Gegenseite seinerseits nur pauschal erfolgt (vgl. BeckOK ZPO/von Selle, 53. Ed. 01.07.2024, ZPO § 138 Rn. 15; Musielak/Voit/Stadler, 21. Aufl. 2024, ZPO § 138 Rn. 10; MüKoZPO/Fritsche, 6. Aufl. 2020, ZPO § 138 Rn. 22).

(2) Der Vortrag der Klagepartei hierzu ist – auch im Zusammenhang mit den von der Beklagten vorgelegten Unterlagen – hinreichend. Die Partei genügt ihrer Darlegungslast, wenn sie Tatsachen vorträgt, die in Verbindung mit einem Rechtssatz geeignet sind, das geltend gemachte Recht in ihrer Person entstanden erscheinen zu lassen; die Angabe näherer Einzelheiten ist nicht erforderlich, wenn sie für die Rechtsfolge nicht erforderlich sind. Das Gericht muss nur in die Lage versetzt werden, aufgrund des tatsächlichen Vorbringens der Partei zu entscheiden, ob die gesetzlichen Voraussetzungen für das Bestehen des geltend gemachten Rechts vorliegen (Anders/Gehle/Anders, 84. Aufl. 2026, ZPO § 138 Rn. 22, beck-online; BGH, Beschluss vom 11. Februar 2025, VI ZR 185/24, Rn. 10, juris).

Von einer Klagepartei, die Unterlassung einer Datenverarbeitung auf Dritt-Webseiten über ihren Social-Media-Account verlangt, kann keine genaue Kenntnis der betroffenen Drittwebseiten und der Datenverarbeitung durch die Beklagte verlangt werden. Sie ist daher nicht verpflichtet, vorzutragen, mit welchen Werbepartnern die Beklagte entsprechende Verträge abgeschlossen hat und ob sie Daten von diesen über die Klagepartei erhalten hat. Die Beklagte stellt dies, insbesondere Anlagen K 13 und K 14, auch nicht streitig, sondern verweist explizit darauf, keine Verpflichtung zu haben, eine entsprechende Übersicht zur Verfügung zu stellen und auch keine anderen Unternehmen zu kennen, die sich entsprechend verhielten.

Es reicht aus, wenn die Klagepartei, die gerade keine eigene Kenntnis davon hat, auf welchen Webseiten und in welche Applikationen die streitgegenständlichen Business Tools tatsächlich integriert sind, sämtliche Indizien dafür vorträgt, dass sie während ihrer täglichen Internetnutzung als Instagram-Nutzer mit erheblicher Wahrscheinlichkeit von den oben beschriebenen Überwachungsmaßnahmen durch die eingesetzten Business-Tools betroffen war. Für die Wahrscheinlichkeit der Betroffenheit spricht schon die Tatsache der praktisch umfassenden Kontraktierung aller gängigen Medien und Shopping-Möglichkeiten. Es ist

nach Ansicht des Senates bei realistischer Betrachtung praktisch ausgeschlossen, bei regelmäßiger Internetnutzung die in Anlagen K 13 und K 14 aufgeführten Seiten, die Business Tools verwenden, zu umgehen. Betroffen sind alle bedeutenden Informationsmedien, alle gängigen Shopping-Websites, zahlreiche Gesundheitsseiten und auch Seiten, die das Sexualleben betreffen. Dass die Klagepartei über Jahre ihre tägliche Nutzung der Dritt-Homepages insoweit nachvollzieht, kann nicht erwartet werden, zumal sie die Nutzung von Business Tools durch die Drittwebseiten nur vermuten kann. Dass sie Verlaufsprotokolle vorhält, aus denen sie diese Informationen ziehen könnte, hat die Klagepartei nicht vorgetragen. Darüber hinaus hat sie geltend gemacht, dass auch sensible Daten gemäß Art. 9 DSGVO betroffen sein könnten. Der Senat hält es angesichts der Anzahl der von der Beklagten verpflichteten Unternehmen praktisch für ausgeschlossen, dass die Klagepartei bei normaler Internetnutzung nicht zumindest gelegentlich eine der Websites aufruft. Soweit die Beklagte die klägerseits genannte Prozentzahl von 30 % bis 40 % für nicht nachvollziehbar hält, trägt sie hierzu selbst keine gegenteiligen Tatsachen vor.

(3) Diese Tatsachen rechtfertigen den ausreichenden Schluss, dass die Klagepartei mit hinreichender Wahrscheinlichkeit auch konkret von der Datenverarbeitung durch die Business Tools betroffen ist. Die Erwägungen des Bundesverfassungsgerichts zur Begründung der Möglichkeit einer eigenen und gegenwärtigen Betroffenheit durch heimliche Maßnahmen, erachtet der Senat insofern für übertragbar: Ausreichend ist, dass der Betroffene mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt wird, weil sie mit einiger – überwiegender – Wahrscheinlichkeit von der angegriffenen Datenverarbeitung betroffen ist (§ 138 Abs. 3 und 4 ZPO; vgl. BVerfG, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 38; BVerfG, Urteil vom 01. Oktober 2024, 1 BvR 1160/19, Rn. 61; BVerfG, Beschluss vom 08. Oktober 2024, 1 BvR 1743/16, Rn. 89, juris). Es ist daher ausreichend, wenn sich die Klagepartei auf Vermutungen stützt (BGH, Beschluss vom 20. Mai 2015, IV ZR 127/14, Rn. 17, beck-online). Denn hier findet eine Überwachung der Nutzer derart statt, dass diese bei dem Besuch von Drittseiten nicht nachvollziehen können, ob und welche sie betreffende Daten an die Beklagte gelangen und was dort mit diesen Daten geschieht. Zudem weisen die Maßnahmen unstreitig eine sehr große Streubreite auf, zielen nicht auf einen begrenzten Personenkreis ab und erfassen potentiell und zufällig eine sehr große Zahl an Personen.

Die Beklagte, die diese Daten ohnehin zur Erfüllung ihrer Auskunftspflicht gemäß Art. 15 DSGVO vorzuhalten hat, kann demgegenüber die von ihr verarbeiteten Daten aus ihren Systemen ersehen und vortragen, ob und in welcher Weise die Klagepartei betroffen war (zur sekundären Beweislast: BGH, Urteil vom 25. Mai 2020, VI ZR 252/19, Rn. 42, juris). Dabei kann auch dahinstehen, ob die Klagepartei über die Selbstauskunftstools der Beklagten sich

die notwendigen Informationen selbst hätte beschaffen können.

Gem. § 138 Abs. 3 und 4 ZPO ist daher der vollständige klägerische Vortrag zum Vorgehen der Beklagten in Bezug auf die Datenerhebung und -verarbeitung – insbesondere zur Funktionsweise der Business Tools, der Übertragung der personenbezogenen Daten und der Erstellung von Nutzerprofilen – dem Urteil als unstreitig zugrunde zu legen. Die Beklagte ist dem klägerischen Vortrag in nicht erheblicher Weise entgegengetreten. Der Vortrag der Beklagtenseite erschöpft sich im Wesentlichen darin, dass sie mangels Einwilligung der Klagepartei keine Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung vornehme. Darüber hinaus gesteht die Beklagte zu, dass sie die Daten, welche ihr über die Business Tools übermittelt werden, für andere Zwecke wie beispielsweise „Schutz und Integrität“ nutzt (siehe u.a. S. 12 Datenschutzrichtlinie, Anlage K 1).

Insoweit ist es nach den oben skizzierten Anforderungen an einen substantiierten Vortrag auch ausreichend, wenn sich die Klagepartei zur Plausibilisierung der Erhebung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO auf den „*Hitchhikers Guide to Facebook Web Tracking with Invisible Pixels and Click-IDs*“ (Anlage K 7) bezieht, aus dem sich ergibt, dass zwischen 5,3 und 16,9 v.H. aller betroffenen sensiblen Websites Business Tools verwenden. Der Senat hat nach der informatorischen Anhörung der Klagepartei die Überzeugung gewonnen, dass diese auch auf sensiblen Webseiten, wie Gesundheitsseiten, digital unterwegs war. Die Klagepartei hat hierzu ausgeführt, sie sei auf Jameda und Apothekenseiten unterwegs gewesen. Der Senat hat nach der informatorischen Anhörung der Klagepartei keinen Zweifel, dass die insoweit überzeugende Klagepartei auf diesen Seiten unterwegs war. Die Klagepartei hat zunächst mitgeteilt, sie wolle sich nicht zu sensiblen Seiten äußern, weil sie sich nicht soweit offenbaren wolle. Im Verlauf der Anhörung, in der sie zusehends offener wurde, hat sie dann mitgeteilt, sie sei auf den Gesundheitsseiten gesurft. Außerdem geht der Senat aufgrund der Aussage der Klagepartei davon aus, dass weitere sensible Daten i.S.d. Art. 9 DSGVO betroffen waren, weil sich die Klagepartei dahin eingelassen hat, „*was ich da mache, möchte ich nicht mit meiner Frau teilen*“. Daraus schließt der Senat, dass die Klagepartei auch sehr persönliche Seiten aufgerufen hat. Diese Schlussfolgerung wird gestützt durch die weitere Mitteilung der Klagepartei, sie nutze nun Foren, um sich zu informieren und hoffe, dass diese Seiten nicht auch infiltriert seien.

(4) Die Praxis der Beklagten, über die streitgegenständlichen Tools personenbezogenen Daten auch der Klagepartei zu erheben, betrifft diese in ihrem Recht auf informationelle Selbstbestimmung als Teilbereich des Selbstbestimmungsrechts. Unter Berücksichtigung der modernen Bedingungen der Datenverarbeitung gewährleistet es den Schutz des Einzelnen

gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Damit soll erreicht werden, dass jeder aus eigener Selbstbestimmung heraus frei planen und entscheiden kann, und zwar ohne Zweifel darüber, welche der ihn betreffenden Informationen seiner sozialen Umwelt oder seinen Kommunikationspartnern bekannt sind (Fezer/Büscher/Obergfell/Prinz, 3. Aufl. 2016, Rn. 81, beck-online). Dieses unter den Bedingungen der modernen und von digitalen Systemen zutiefst geprägten Massengesellschaft essentielle Grundrecht schützt die Grundrechtsträger auch gegenüber Privaten in ihrem Recht, selbst zu entscheiden, welche Daten an Dritte herausgegeben werden und welche nicht. „*Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.*“ (BVerfG, Beschluss vom 6. November 2019, 1 BvR 16/13, juris).

bb) Die Datenverarbeitung der Beklagte ist auch rechtswidrig. Wegen der Einzelheiten wird auf Abschnitt B.1. Bezug genommen.

b)
Für die für den Unterlassungsanspruch notwendige Wiederholungsgefahr spricht nach der von der Beklagten begangenen Pflichtverletzung eine tatsächliche Vermutung (vgl. BGH, Urteil vom 29. Juli 2021, III ZR 179/20, Rn. 103, juris). Dabei begründet die Verletzung einer Vertragspflicht die Vermutung für eine Wiederholungsgefahr nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urteil vom 29. Juli 2021, III ZR 192/20, Rn. 116 m.w.N., juris). Für eine Widerlegung dieser Vermutung ausreichende Anhaltspunkte, an die strenge Anforderungen zu stellen sind, hat die Beklagte nicht vorgetragen. Es ist nach den Erklärungen der Beklagten davon auszugehen, dass sie ihr System der Business Tools aufrechterhält. Sie verteidigt ihr System und meint, ihr sei als Beteiligte im Wirtschaftsleben die Nutzung ihrer Business Tools erlaubt. Sie nutzt ihre Tools – soweit ersichtlich – weiterhin und beabsichtigt keine Unterlassung. Das rechtswidrige Verhalten dauert an, eine Wiederholungsgefahr ist damit indiziert. Anhaltspunkte für eine Widerlegung der Vermutung sind weder vorgetragen noch ersichtlich.

c)
Zu Recht verweist die Beklagte darauf, dass bestimmte Datenverarbeitungsvorgänge gerechtfertigt sein können, insbesondere nach Art. 6 Abs. 1 (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 137, juris) und 9 Abs. 1 und 2 DSGVO oder wenn die Klagepartei eine Einwilligung nach Art. 4 Nr. 11 DSGVO erteilt (EuGH, Urteil vom 4. Juli 2023, C-252/21, Rn. 91 f.,

juris).

Der Senat erachtet – wie auch das Oberlandesgericht München (OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25 e, Rn. 258, juris) – die mit dem Verweis auf die Ausnahmetatbestände der Art. 6, 9 DSGVO einhergehende Unbestimmtheit im vorliegenden Fall für das Vollstreckungsverfahren als noch akzeptabel, um den Anspruch auf effektiven negatorischen Rechtsschutz nicht unzulässig zu verkürzen (vgl. Roth, in Stein, § 253 ZPO Rn. 37 mwN.; Thüringer Oberlandesgericht, Urteil vom 17. Juli 2002, 2 U 59/02, juris). Zu berücksichtigen ist, dass die fehlende weitergehende Präzisierung der konkreten Verletzungshandlungen maßgeblich auf dem prozessualen Vorgehen der Beklagten beruht. Zudem sind die Ausnahmetatbestände der Art. 6 und 9 DSGVO hinreichend konkretisiert und bestimmt, wie sich auch aus den z.T. durchaus vergleichbaren Sachverhalten aus der Rechtsprechung des EuGH ergibt (s. nur EuGH, Urteil vom 4. Juli 2023, C-252/21[Facebook Ireland] und EuGH, Urteil vom 4. Oktober 2024, C-446/21, juris). Mit Blick auf die Vollstreckung wird hinreichend deutlich, welches Verhalten untersagt wird. Der Senat konnte deshalb im Tenor auf diese gesetzlichen Regelungen Bezug nehmen.

Entscheidend ist dabei, dass es der Klagepartei mangels substantiierten Vortrages der Beklagten zur Datenverarbeitung gar nicht möglich und auch nicht zumutbar ist, den Unterlassungsantrag auf konkrete Verletzungsformen zu beschränken (vgl. allgemein BGH, Urteil vom 29. April 2010, I ZR 202/07, Rn. 32, juris). Würde die Beklagte offenlegen, welche Daten der Klagepartei sie in der Vergangenheit zu welchem Zweck verarbeitet hat, wäre ihr eine Beschränkung des Unterlassungsantrages auf konkrete Verletzungshandlungen möglich und ggf. zumutbar. Anderenfalls würde das von der DSGVO vorgegebene hohe Datenschutzniveau unter dem Grundsatz der Datenminimierung in Art. 5 DSGVO auch nicht erreicht werden können.

D. Klagantrag zu 3.

Der Klagantrag zu 3. ist zulässig und begründet.

1.

Wegen der Frage der Bestimmtheit des Klageantrages wird zunächst auf die Anforderungen, wie sie in Abschnitt D.1. dargelegt sind, Bezug genommen.

Dass die Beklagte – z.B. durch eine entsprechende Gestaltung der Business Tools – (aktiv) handeln muss, um den Unterlassungsanspruch erfüllen zu können, hindert die Unterlassungsanordnung nicht (st. Rspr., z.B. BGH, Urteil vom 15. August 2013, I ZR 80/12, Rn. 21;

BGH, Urteil vom 26. Juli 2018, I ZR 64/17, Rn. 57, juris). Unter die von der Beklagten vorzunehmenden Handlungen kann auch die Einwirkung auf Dritte fallen (vgl. BGH, Urteil vom 14. März 2017, VI ZR 721/15, Rn. 35).

2.
Im Hinblick auf bereits erhobene Daten beantragt die Klagepartei das Unterlassen einer weiteren Verarbeitung bis zur Löschung der Daten. Es kann dahinstehen, ob Art. 17 Abs. 1 DSGVO jedenfalls in dieser Konstellation einen Unterlassungsanspruch gewährt (so BGH GRUR 2023, 1724 Rn. 20 unter Hinweis auf EuGH GRUR 2023, 184), weil der entsprechende Anspruch sich andernfalls wiederum aus nationalen Vorschriften ergibt, zum einen unmittelbar aus dem Nutzungsvertrag der Parteien und zum anderen aus einer entsprechenden Anwendung der §§ 1004 Abs. 1 S. 2, 823 Abs. 1 BGB. Bei der Verletzung von Vertragspflichten ergibt sich jedenfalls dann ein Unterlassungsanspruch aus dem Vertrag, wenn bereits einmal Pflichten aus dem – fortbestehenden – Vertragsverhältnis verletzt wurden und die Vertragsverletzung noch andauert (so i.E. BGH NJW 2021, 3179, der diesen Anspruch aus § 280 Abs. 1 BGB ableitet). Genau so liegt der Fall hier: Durch die rechtswidrige Datenverarbeitung (s.o., I.1) hat die Beklagte gegen eine (Haupt- oder Neben-) Pflicht des Nutzungsvertrages verstoßen und sie tut es – soweit ersichtlich – weiterhin. Die – auch insoweit nötige (BGH a.a.O.) – Wiederholungsgefahr wird damit indiziert. Anhaltspunkte für eine Widerlegung der Vermutung sind weder vorgetragen noch ersichtlich.

Als Folge der Einschränkung darf nach Art. 18 Abs. 2 DSGVO grundsätzlich nur die Speicherung der jeweiligen Daten erfolgen, es sei denn, dass sich die Beklagte als verarbeitende Person auf die dort aufgeführten Ausnahmen bezieht. Für das Vorliegen der Ausnahmetatbestände trägt der Verantwortliche die Darlegungs- und Beweislast (vgl. Ehmann/Selmayr/Kamann/Braun, 3. Aufl. 2024, DS-GVO Art. 18 Rn. 30, beckonline).
Der Anspruch kann im Rahmen einer Unterlassungsklage geltend gemacht werden (Ehmann/Selmayr/Kamann/Braun, 3. Aufl. 2024, DS-GVO Art. 18 Rn. 37, beck-online).

3.
Der Anspruch folgt auch aus § 1004 Abs. 1 BGB analog i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG und aus §§ 280 Abs. 1, 241 Abs. 2, 242 BGB. Der nicht erforderliche und auch nicht durch eine Einwilligung gedeckte Verstoß gegen den Grundsatz der Datenminimierung (s.o., I.) hat den Kläger in seinem allgemeinen Persönlichkeitsrecht verletzt, das er gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten schützt (Recht auf informationelle Selbstbestimmung, vgl. hierzu Art. 7, 8 GRCh; Art. 8 EMRK; Rspr des EuGH seit 29/69 Rs. Stauder; Rspr des BVerfG zu Art. 2 Abs. 1, 1 Abs. 1 GG seit BVerfG NJW 1984, 419 – Volkszählungsurteil). Das rechtswidrige Verhalten dauert

an, eine Wiederholungsgefahr ist damit indiziert. Anhaltspunkte für eine Widerlegung der Vermutung sind weder vorgetragen noch ersichtlich.

Wegen der Einschränkung wird auf Abschnitt C.2.d) Bezug genommen.

E. Löschungs- und Anonymisierungsantrag (Klagantrag zu 4.)

Der Antrag der Klagepartei, die Beklagte zur zukünftigen Löschung sämtlicher im streitgegenständlichen Zeitraum erhobenen Daten zu verpflichten, ist zulässig und begründet. Gem. Art. 17 Abs. 1 lit. d) DSGVO i.V.m. § 259 ZPO kann die betroffene Person vom Verantwortlichen der Datenverarbeitung die Löschung der Daten verlangen, wenn die personenbezogenen Daten nicht rechtmäßig verarbeitet wurden.

1.
Anhaltspunkte dafür, dass die Klagepartei entgegen § 260 ZPO („dieselbe Prozessart“) eine einstweilige Regelung dahingehend anstrebt, es der Beklagten bis einen Monat nach Rechtskraft zu untersagen, den bestehenden Löschungsanspruch zu erfüllen, sieht der Senat angesichts der Formulierung des Antrages nicht. Die Frage der Realisierung des Anspruchs im Zeitraum bis zur Rechtskraft des Urteils (im Falle einer stattgebenden Entscheidung) richtet sich vielmehr nach den Vorschriften über die vorläufige Vollstreckbarkeit (§§ 708 ff. ZPO) (OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25, Rn. 182, beck-online).

2.
Der Antrag ist auch zulässig.

Soweit die Klagepartei von der Beklagten verlangt, bestimmte Daten „vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen“, erweist sich der Antrag zu 4. als hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 a.E. ZPO. Durch die Einräumung einer Wahlmöglichkeit wird keine Unsicherheit von außen in den Prozess hineingetragen, die Beklagte wird durch das ihr eingeräumte Wahlrecht nicht beschwert (vgl. OLG Düsseldorf, Urteil vom 21. September 2023, VI-5 U 4/22 (Kart), Rn. 68, juris; s. auch Roth, in: Stein, § 260 ZPO, aaO, Rn. 10). Dass es prozessual möglich sein muss, der Beklagten ein Wahlrecht einzuräumen, beweist § 264 Abs. 1 BGB, der unmittelbar den – hier nicht einschlägigen – Fall der Wahlschuld betrifft.

Es handelt sich prozessual dabei auch nicht um einen grundsätzlich unzulässigen, weil zu unbestimmten alternativen Klageantrag. Denn es soll anders als bei einem alternativen Klageantrag nicht dem Gericht, sondern der Beklagten überlassen bleiben, ob sie löscht oder stattdessen anonymisiert, so dass sich für die Beklagte keine unzumutbare Unbestimmtheit ergäbe (s. zu der Unterscheidung nur MüKoZPO/Becker-Eberhard, 7. Aufl. 2025, ZPO § 260 Rn. 23).

Die Anonymisierung ist daher als Unterfall der Löschung zu begreifen und kein Aliud (vgl. Kühling/Buchner/Herbst, 4. Aufl. 2024, DS-GVO Art. 17 Rn. 39, beckonline). Die Pflicht, Daten zu löschen, kann somit auch durch die Aufhebung des Personenbezugs mittels Anonymisierung erfüllt werden (Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/ Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), 11. Ergänzungslieferung 2024, Art. 17 EUV 2016/679, Rn. 57a).

2.
Der Klagantrag ist auch teilweise begründet.

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

aa) Ein Löschungsanspruch gemäß lit. b) besteht nicht, weil die von der Klagepartei eingeholte Einwilligung nicht wirksam war. Auf die Ausführungen unter B.2.d).wird Bezug genommen. Die betroffene Person muss jedoch ursprünglich eine wirksame Einwilligung nach Art. 6 Abs. 1 lit. a) oder Art. 9 Abs. 2 lit. a) abgegeben haben. Liegt keine wirksame Einwilligung vor, so besteht ein Löschungsanspruch nach Abs. 1 lit. d) (BeckOK DatenschutzR/Worms, 54. Ed. 1.11.2024, DS-GVO Art. 17 Rn. 32, beck-online).

bb) Die Klagepartei hat einen Anspruch wegen der unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten (lit. d). Die in Antrag Ziff. 1 aufgeführten 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 25. Mai 2018 nicht. Die dem Urteil zugrunde zulegenden 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 (vgl. Abschnitt B.2.d)aa)). Sonstige Rechtfertigungsgründe nach Art. 6 und 9 DSGVO hat die

Beklagte nicht hinreichend vorgetragen. Auf die Ausführungen unter Abschnitt B. wird Bezug genommen.

Ein Fall einer rechtmäßigen Datenverarbeitung, die unter einen der in Art. 6 Abs. 1 UAbs. 1 DSGVO vorgesehenen Fälle subsumierbar wäre, liegt nicht vor.

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. 1.11.2024, DS-GVO 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 OLG München, Endurteil vom 18. Dezember 2025, 14 U 1314/25, Rn. 261, beck-online). Art. 32 DSGVO gibt keinen Individualanspruch (BeckOK IT-Recht/Borges, 20. Ed. 1.4.2025, DS-GVO Art. 32, beck-online), sondern einen Schadenersatzanspruch bei Verletzung der Pflicht zu Anonymisierung gemäß Art. 82 Abs. 1 DSGVO (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 31 f., beck-online).

d)
Auch ein vertraglicher Anspruch aus einer wirksamen Abrede über eine alternative Erfüllungsmodalität besteht nicht.

Zwar hat die Klagepartei der Beklagten teilweise ein Erfüllungssurrogat angeboten (s. Antrag zu 4.: nach Wahl der Beklagten Anonymisierung statt Löschung). Eine solche Abrede ist aufgrund der Vertragsfreiheit grundsätzlich zulässig. Dem steht auch nicht etwa entgegen, dass die DSGVO keinen Anspruch auf Anonymisierung gewährt. Vielmehr steht es dem Gläubiger grundsätzlich frei, sich mit einem Aliud als Erfüllungssurrogat zufriedenzugeben und das Erlöschen seines Anspruchs hinzunehmen. Es bleibt den Parteien eines Schuldverhältnisses also unbenommen, eine gesonderte Vereinbarung darüber zu treffen, dass die Schuld durch eine andere als die zunächst versprochene Leistung erfüllt werden soll (s. nur Schmidt, in: Münchener Kommentar zum BGB, 10. Auflage 2025, § 364, Rn. 2).

Wie der Inhalt dieses Angebots der Klagepartei auf eine wahlweise Erfüllung durch Anonymisierung materiellrechtlich genau einzuordnen ist, ob eine Wahlschuld im Sinne von § 262 BGB intendiert ist oder hingegen eine – nach h.M. (s. nur BeckOGK/Krafka, 1.10.2025, BGB § 262, Rn. 5 m.w.N.) wegen des kaum passenden gesetzlichen Wahlschuldregimes davon zu unterscheidende – Ersetzungsbefugnis, braucht vorliegend ebenso wenig entschieden zu werden wie die Frage, ob eine wirksam vereinbarte alternative Erfüllungsmodalität entgegen der wohl h.A. (s. nur MüKoZPO/Becker-Eberhard, 7. Aufl. 2025, ZPO § 260 Rn. 24 m.w.N.) in den Tenor einer Verurteilung zur Löschung aufzunehmen wäre, weil sie den Anspruch auf Löschung gleichsam qualitativ verkürzt und ein Kläger, der eine solche Wahlmöglichkeit materiellrechtlich wirksam vereinbart hat, dementsprechend „zu viel“ beantragt, wenn er dennoch uneingeschränkte Verurteilung zur Leistung beantragt.

Denn die Beklagte hat vorliegend das klägerische Angebot, anstatt zu löschen zu anonymisieren, unmissverständlich zurückgewiesen und damit abgelehnt (OLG München, Endurteil v. 18.12.2025 – 14 U 1314/25, GRUR-RS 2025, 36455 Rn. 260-265, beck-online).

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, DS-GVO 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 Teil-

habe 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. Dies gilt hier umso mehr, als die Klagepartei in der mündlichen Verhandlung vor dem Senat glaubhaft versichert hat, der Instagram-Account stelle für sie eine Art Tagebuch dar, über welches sie für sie wichtige Ereignisse nachvollziehen und sich erinnern könne.

F. Schadenersatz (Klagantrag zu 5.)

Angesichts der rechtswidrigen Datenverarbeitung steht der Klagepartei zumindest gemäß Art. 82 Abs. 1 DSGVO ein Schadensersatzanspruch in Höhe von 1.200 EUR gegen die Beklagte zu.

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 B. wird 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 DS-GVO 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, Natsionalna agentsia za prihodite, 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 dies 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 Anlagen K 13 und K 14 und dem Ergebnis der informatorischen Anhörung der Klagepartei im Termin der mündlichen Verhandlung vom 13. Januar 2026 als erwiesen an, dass die Klagepartei die in Anlagen K 13 und K 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, sie surfe täglich mehrere Stunden im Netz, was der Senat für glaubhaft hält. Dabei handelt es sich insbesondere um Apotheken-, Baumarkt- und Shoppingseiten, und damit auch um sensible Daten i.S.d. Art. 9 Abs. 1 DSGVO (Gesundheitsdaten). 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 Anlagen K 13 und 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 und diese mit den von der Klagepartei nach ihrer Aussage aufgerufenen Seiten übereinstimmen. 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 Anlagen K 13 und K 14 aufgeführten Webseiten auch zu den von ihr regelmäßig besuchten Webseiten, die mit den in Anlagen K 13 und K 14 benannten übereinstimmen, vorgetragen.

Dass die Beklagte mit ihrer Berufungsbegründung 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.

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 einem hier nicht feststellbaren Kontrollverlust gleichzustellen ist. Die Einholung eines Sachverständigengutachtens zur Frage der genauen Datenübermittlung über die Conversions API

war daher nicht erforderlich. Denn wie die Beklagte im Meta Playbook (Anlage K 11; dort S. 23) und in Anlage K 17 (*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 am 13. Januar 2026 hat die Klagepartei überzeugend und plausibel dargelegt, dass sie aufgrund der systematischen und von ihr ungewollten Datenabfassung einen Identitätsdiebstahl befürchtet. Dies gelte für sie umso mehr, als sie beruflich im Hochrisikobereich für kritische Infrastruktur arbeite und sich ein Kontrollverlust auch beruflich für sie auswirken könne. 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 aufgerufen hat (vgl. Anlagen K 13 und K 14). Sie fühle sich vollkommen schutzlos, wenn aufgrund der Daten ein von ihr nicht beeinflussbares, möglicherweise verfälschtes Bild zusammengesetzt werde, auch über Themen, die sie so nicht preisgeben möchte und gerade die Anonymität des Internets gesucht habe. Sie sei seit einem Jahr nicht mehr bei Instagram und halte ihre Kontakte meist analog nunmehr aufrecht und telefoniere viel. Sie bedaure, dass die doch recht erfolgreiche Kommunikation über Instagram wegen der Überwachung nicht mehr aufrecht zu erhalten sei. Sie fühle sich hilflos und beobachtet. Sie fühle „eine Schere im Kopf“. Er empfinde es als „ein Unding“, dass er trotz der klaren Regelungen in der DSGVO gezwungen sei, seine Rechte im Prozesswege geltend zu machen. Dieser Weg sei aber notwendig, um das Gefühl der ständigen Beobachtung wieder loszuwerden.

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, DS-GVO Art. 82 Rn. 24, beck-online).

(2) Dass die beständige und praktisch täglich neue Zuwiderhandlung seit dem 25. Mai 2018 sowohl 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 Instagram durch private Nutzer davon abhängig machen, dass die Beklagte Daten, die bei dem Besuch von Webseiten oder bei der Nutzung mobiler Apps dritter Anbieter über Programmierstellen („Business Tools“) erfasst werden, ohne Einwilligung der Nutzer mit den unter den „Instagram-Konten“ gespeicherten Daten verknüpfen und verwenden kann und eine wirksame Einwilligung nur dann vorliegt, wenn die Bereitstellung des Dienstes Instagram 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.

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, dass 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).

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, auch 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 iRd § 287 ZPO niedriger als für die anspruchsbegründenden 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, zB 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. In ihrer informatorischen Anhörung vor dem Senat hat sie angegeben, ihr Nutzungsverhalten wegen der von ihr relativ spät erkannten Datenverarbeitung stark geändert zu haben, sehr vorsichtig im Internet zu agieren und nur noch Seiten aufzuschlagen, von denen sie glaubt, diese seien vertrauenswürdig. Dabei sei ihr allerdings klar, dass sie sich über die Vertrauenswürdigkeit irren könne, was bei ihr umso größere Verunsicherung hervorrufe. Für sie sei Datenschutz angesichts dessen, dass sie im Hochrisikobereich für kritische Infrastruktur arbeite und besonders vulnerabel sehr hoch angesiedelt, zumal sie auch nicht wissen könne, ob und wie sich die gesammelten Daten auf ihr Berufsleben auswirken könnten. Sie müsse sich schlichtweg auf die Einhaltung des Datenschutzes verlassen können.

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 sie weiß und wie sie die Daten verwenden wird, was das Gefühl ausgelöst hat, ihr Privatleben werde 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 sie weiß und sämtliche Daten gegen sie verwenden wird. Die von der Klagepartei in der mündlichen Verhandlung vor dem Senat beschriebene Folge war die Anpassung ihres 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 und seiner beruflichen Tätigkeit bis hin zum vorsichtigen und damit limitierten Agieren im Internet.

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.

Der Senat hält in diesem individuellen Fall ein Schmerzensgeld von 1.250 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 – mehr als fünf Jahre seit Inkrafttreten der DSGVO – 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 3. 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 er 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 bereits ihr Surfverhalten umgestellt habe und häufig analoge Kontaktaufnahme vorziehe oder nur – vermeintlich – sichere Seiten oder Foren nutze.

Insgesamt rechtfertigt sich für den umfassenden, über fünf Jahre andauernden, umfassenden Kontrollverlust und die mehr als zweijährige Befürchtung eines umfassenden Kontrollverlusts angesichts der beruflichen Tätigkeit der Klagepartei im Hochrisikobereich ein individuelles Schmerzensgeld i.H.v. 1.250 EUR.

d)
Ob im Weiteren auch ein Anspruch gem. § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG besteht, 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 DS-GVO/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). Daran fehlt es im vorliegenden Fall im Hinblick auf den bloßen Kontrollverlust und dessen Befürchtung und auch unter Zugrundelegung der der Klagepartei geschilderten Auswirkungen auf ihr Vertrauen und ihr Surfverhalten.

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 offensichtlich nicht gegeben ist.

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 1.200 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 Anspruchsgrundlagen 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. Da sich die Zustellung nicht feststellen lässt, ist erster Fälligkeitstag der Tag der Verteidigungsanzeige am 29. April 2024.

F. Außergerichtliche Rechtsanwaltskosten (Klagantrag zu 6.)

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 9.250 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 ihres Prozessbevollmächtigten auch für erforderlich und zweckmäßig halten.

Auf der Grundlage des festzusetzenden Gegenstandswertes von 9.250 EUR für die außergerichtliche Tätigkeit ergeben sich zu erstattende Kosten von 887,30 EUR (1,3 Geschäftsgebühr Nr. 2300 VV RVG in der Fassung vom 15. März 2022: 725,40 EUR, Auslagen Nr. 7001 u. 7002 VV RVG: 20 EUR und 19 v.H. Umsatzsteuer Nr. 7008 RVG).

G.
Über den gestellten Schriftsatznachlassantrag der Beklagten war nicht mehr zu entscheiden, nachdem sie selbst erneut mit Schriftsatz vom 28. Januar 2026 zur Funktionsweise der Business Tools vorgetragen hat. Der Schriftsatz vom 28. Januar 2026 gab auch keinen Anlass zur Wiedereröffnung der mündlichen Verhandlung, weil er keinen neuen, entscheidungserheblichen Sachvortrag enthält. Im Übrigen wäre dem Antrag nicht stattzugeben gewesen, weil die für die Entscheidung des Senats zugrunde gelegte Funktionsweise der Conversions API unstreitig ist.

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 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, GRUR-RS 2021, 2286 Rn. 9 m.w.N.).

Hieran gemessen hat der Senat den Streitwert auf insgesamt 13.000 EUR festgesetzt.

Hinsichtlich der Zwischenfeststellungsklage gemäß § 256 Abs. 2 ZPO zu Ziff. 1 gilt: Maßgebend für den Streitwert ist das Feststellungsinteresse der Klagepartei (vgl. OLG Karlsruhe, Urteil vom 22. Januar 1997, 13 U 9/95, Rn. 111, juris), welches sich gemäß § 47 Abs. 1 GKG

am Interesse der Klagepartei an der begehrten Abänderung entsprechend dem Rechtsschutzziel bemisst (vgl. Herget in: Zöller, ZPO, 35. Auflage 2024, § 3 ZPO, Rn. 16_39). Eine Zwischenfeststellungsklage ermöglicht den rechtskräftigen Ausspruch über die für die Hauptklage vorgreiflichen Rechtsverhältnisse (vgl. Zöller-Greger, ZPO, 35. Auflage 2024, § 256 ZPO, Rn. 35). Dabei bemisst sich der Streitwert einer Zwischenfeststellungsklage nach denselben Kriterien wie der einer Feststellungsklage i.S.d. § 256 Abs. 1 ZPO (vgl. MüKoZPO/ Becker-Eberhard, 7. Aufl. 2025, ZPO § 256 Rn. 96, beck-online).
Gemessen an diesen Grundsätzen bewertet der Senat das Rechtsschutzziel mit 1.000 EUR.

Der als Antrag zu 2. gestellte Antrag auf Unterlassung betrifft eine nichtvermögensrechtliche Streitigkeit. Der Senat hat für diesen Unterlassungsantrag einen Gebührenstreitwert von 5.000 EUR festgesetzt. Dabei ist der Streitwert des Unterlassungsantrags als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses zu ermitteln, unter Berücksichtigung der jeweiligen Umstände des Einzelfalls, § 48 Abs. 2 S. 1 GKG.

Für den Löschungsanspruch setzt das Gericht einen Gebührenstreitwert von 1.000 EUR an und berücksichtigt, dass es sich um Daten des Nutzers aus der Kategorie des Art. 9 Abs. 1 DSGVO handelt, an dessen Löschung der Nutzer ein erhebliches Interesse hat, weil er dann die Kontrolle über die eigenen, jedoch bereits erhobenen Daten wiedererlangt.

Der Antrag zu 5. betrifft eine vermögensrechtliche Streitigkeit; der Streitwert ergibt sich aus dem von der Klagepartei vorgestellten immateriellen (Mindest-)Ersatzbetrag in Höhe von 5.000,00 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.

Vorliegend besteht das vorgreifliche Rechtsverhältnis in dem unentgeltlichen Nutzungsvertrag und ist daher mit einem Wert im unteren Bereich zu bewerten.

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 mwN, 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 Anlage K 13 und K 14 zur Grundlage genommen wird, 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.

[redacted] [redacted] [redacted]

Vorstehende Abschrift stimmt mit
dem mir in Urschrift vorliegenden Schriftstück
überein und wird hiermit beglaubigt.
Naumburg, 13. Februar 2026

(elektronisch signiert)
[redacted]ustizbeschäftigte
als Urkundsbeamtin der Geschäftsstelle