Oberlandesgericht Dresden

Zivilsenat

Aktenzeichen: **4 U 292/25**
Landgericht Dresden, 3 O 2035/23

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

[redacted] - Kläger und Berufungskläger -

Prozessbevollmächtigte:
BK Baumeister & Kollegen Verbraucherkanzlei, Viktoria-Luise-Platz 7, 10777 Berlin,
Gz.: DTS-003419-IUS

gegen

Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Irland
vertreten durch d. Director

- Beklagte und Berufungsbeklagte -

Prozessbevollmächtigte:
Rechtsanwälte [redacted]

wegen illegaler Datenverarbeitung

hat der 4. Zivilsenat des Oberlandesgerichts Dresden durch

Vorsitzenden Richter am Oberlandesgericht [redacted]
Richterin am Oberlandesgericht [redacted] und
Richterin am Oberlandesgericht [redacted]

aufgrund der mündlichen Verhandlung vom 09.12.2025 am 03.02.2026

für Recht erkannt:

I. Auf die Berufung des Klägers wird das Urteil des Landgerichts Dresden vom 04.02.2025, Az 3 O 2035/23, unter Zurückweisung der Berufung im Übrigen, teilweise abgeändert.

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

a) auf Dritt-Webseiten und -Apps entstehen und direkt oder in gehashter Form übertragen werden, d. h.

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

sowie 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 Ltd. „Events" genannten 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 Ltd. „Events“ genannten Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren.

3. Die Beklagte wird verpflichtet, sämtliche unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits verarbeiteten personenbezogenen Daten der Klagepartei ab sofort unverändert am gespeicherten Ort zu belassen, d. h. insbesondere diese erst einen Monat nach rechtskräftigem Abschluss des Verfahrens zu löschen, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden, und 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.

2. Die Beklagte wird verurteilt, an die Klagepartei als Ausgleich für Datenschutzverstöße durch Verwendung von Meta Business Tools einen immateriellen Schadenersatz in Höhe von 1.500,- EUR nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 08.09.2023, zu zahlen.

3. Im Übrigen wird die Klage abgewiesen.

II. Die weitergehende Berufung wird zurückgewiesen.

III. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

IV. Das Urteil ist vorläufig vollstreckbar.

V. Die Revision wird nicht zugelassen.

Beschluss:

Der Streitwert wird für beide Instanzen auf 9.000,00 EUR festgesetzt.

Gründe

I.

Der Kläger macht im Zusammenhang mit der Verwendung und Bereitstellung sog. „Meta Business Tools“ durch die Beklagte wegen behaupteter rechtswidriger Verarbeitung personenbezogener Daten Feststellungs-, Unterlassungs- und Schadensersatzansprüche geltend und verlangt daneben, bis zum rechtskräftigen Verfahrensabschluss bereits erhobene Daten unverändert zu belassen und nicht weiterzugeben sowie danach die bereits gespeicherten Daten zu anonymisieren oder nach Wahl der Beklagten zu löschen.

Die Beklagte ist Betreiberin u.a. des sozialen Netzwerks „Instagram“, das vom Kläger seit dem 01.11.2013 unter dem Benutzernamen [redacted] ausschließlich privat genutzt wird.

A.

Die Beklagte, deren Geschäftsmodell es ist, gegen Entgelt werbetreibenden Kunden zielgerichtete personalisierte Werbung zu ermöglichen, bietet dafür im geschäftlichen Verkehr mit den „Meta Business-Tools“ Technologien an (u.a. Meta Pixel, Conversions API, App Events über Facebook-SDK, Offline-Conversions und App Events API, vgl. B3), die von den Geschäftspartnern der Beklagten auf zahlreichen und teilweise reichweitenstarken Webseiten, Servern oder Apps eingebunden werden und deren Verwendung u.a. den Nutzungs- und Datenverarbeitungsbedingungen der Beklagten unterliegen (vgl. Anl. B5, Stand 25.04.2023, B6 - Abruf v. 12.1.2024 -, B9 - Stand 3.7.2024 -, Anl. Kl. „Parameter für Kund*innen- Informationen“ Abruf v. 25.04.2024, Bl. 229 eA LG, Anl. 2 Bekl. z. SS. v. 12.01.2026, Bl. 935 eA). Die Business-Tools dienen dazu, personenbezogene Daten zu sammeln, die diese Unternehmen aus online und offline erfolgten Kunden-Interaktionen gewinnen; hierzu gehören sog. „Kontaktinformationen“ und sog. „Event-Daten“ (vgl. Anl. B5). Diese Daten leiten die Unternehmen mittels Business-Tools an die Beklagte weiter (sog. „teilen“). Im Einzelnen unterscheiden sich dabei die technischen Abläufe nach der Art der eingebundenen Technologien.

In den unternehmensbezogenen Nutzungsbedingungen für Meta Business-Tools (hier zit. n. Stand 25.04.2023, Anl. B5, weitere Fassungen v. 31.08.2020, v. 23.08.2025, v. 03.11.2025, vgl. Anl.-Konvolut B23; im folgenden NB-MBT) heißt es dazu:

> „1. Teilen von Business-Tool-Daten mit Meta
>
> a. Du kannst die Meta-Business-Tools nutzen, um uns eine oder beide der folgenden Arten von personenbezogenen Informationen („Business-Tool-Daten“) für die in Abschnitt 2 beschriebenen Zwecke zu senden:
>
> i. „Kontaktinformationen“ sind Informationen, mit denen Einzelpersonen identifiziert werden können, wie Namen, E-Mail-Adressen und Telefonnummern. Diese verwenden wir nur für Abgleichzwecke. Wir hashen vor der Übermittlung die Kontaktinformationen, die du uns über ein Meta-JavaScript-Pixel für Abgleichzwecke sendest. Wenn du oder dein Dienstanbieter ein Meta-Image-Pixel oder andere Meta-Business-Tools nutzt, musst du bzw. muss dein Dienstanbieter vor der Übermittlung die Kontaktinformationen auf eine von uns vorgegebene Art und Weise hashen.
>
> ii. „Event-Daten“ sind sonstige Informationen, die du über Personen und ihre Handlungen teilst, die sie auf deinen Websites und in deinen Apps oder Shops vornehmen, wie z. B. Besuche auf deinen Websites, Installationen deiner Apps und Käufe deiner Produkte. ...
>
> b. Vorbehaltlich von Abschnitt 1.d teilen wir keine Business-Tool-Daten, die du uns be-

reitstellst, mit Dritten (einschließlich Werbetreibenden), sofern du uns nicht mitteilst, dass uns dies gestattet ist, oder wir von Rechts wegen dazu verpflichtet sind.

c. Wir implementieren Prozesse und Verfahren zum Schutz der Vertraulichkeit und Sicherheit der Business-Tool-Daten wie u. a. mittels geeigneter organisatorischer, technischer und physischer Sicherheitsvorkehrungen, die darauf ausgelegt sind, (a) die Sicherheit und Integrität der Business-Tool-Daten zu schützen, während sie sich in unseren Systemen befinden, und (b) die Business-Tool-Daten gegen den zufälligen oder unberechtigten Zugriff bzw. gegen die versehentliche oder unberechtigte Verwendung, Änderung oder Offenlegung innerhalb unserer Systeme zu schützen. Diese Prozesse und Verfahren umfassen die Maßnahmen, die in den Datensicherheitsbedingungen von Meta aufgeführt sind, die ausdrücklich Bestandteil dieser Nutzungsbedingungen für Business-Tools sind. ...
d. Du erklärst dich damit einverstanden, dass Meta einer bestimmten Person auf deren Antrag hin den Zugriff auf die Event-Daten zu ihrer Person und/oder eine Kopie davon bereitstellen kann.
e. Du sicherst zu und gewährleistest, dass du (unter Einhaltung sämtlicher geltender Gesetze, Vorschriften und Branchenrichtlinien) über alle erforderlichen Rechte und Berechtigungen sowie über eine Rechtsgrundlage für die Offenlegung und Verwendung der Business-Tool-Daten verfügst (und dass jeder möglicherweise von dir eingesetzte Datenanbieter hierüber verfügt).
h. Du sicherst zu und gewährleistest, dass du keine Business-Tool-Daten mit uns teilst, von denen du weißt bzw. angemessenerweise wissen solltest, dass sie von Kindern unter 13 Jahren stammen bzw. diese thematisieren oder dass sie Informationen zu Gesundheit, Finanzen oder andere Kategorien vertraulicher Informationen enthalten (einschließlich jeglicher Informationen, die gemäß geltenden Gesetzen, Vorschriften bzw. Branchenrichtlinien als vertraulich gelten).

Die von Unternehmen über die Meta-Business-Tools an die Beklagte übermittelten personenbezogenen Daten können von dieser für verschiedene - auch eigene - Zwecke genutzt werden, u.a. für Analysen, zur Messung, Effizienzsteigerung und Targeting von Werbung, unabhängig davon, ob die Daten einen Nutzer ihrer sozialen Netzwerke betreffen. Die Nutzungsbedingungen bestimmen hierzu:

„2. Verwendung von Business-Tool-Daten

a. Wir können Business-Tool-Daten für folgende Zwecke verwenden:

i. Kontaktinformationen für den Abgleich
1. Du beauftragst uns, die Kontaktinformationen ausschließlich dafür zu verarbeiten, sie mit Nutzer-IDs abzugleichen („Abgeglichene Nutzer-IDs“) und diese Nutzer-IDs mit entsprechenden Event-Daten zu kombinieren. Wir löschen Kontaktinformationen nach dem Abgleichprozess.

ii. Event-Daten für Messlösungen und Analysedienste
1. Du kannst uns beauftragen, Event-Daten zu verarbeiten, um Mess- und Analysedienste und -produkte bereitzustellen, ...

iii. Event-Daten für das Targeting deiner Werbeanzeigen
...Meta verarbeitet Event-Daten, um solche Zielgruppen für dich zu erstellen....

iv. Event-Daten für die Zustellung kommerzieller und transaktionsbezogener Nachrichten
1. Wir können die abgeglichenen Nutzer-IDs und zugehörigen Event-Daten verwenden, um dich dabei zu unterstützen, Personen mit transaktionsbezogenen und sonstigen kommerziellen Nachrichten im Messenger und in anderen Meta-Produkten zu erreichen....

v. Event-Daten zur Verbesserung der Anzeigenauslieferung, zur Personalisierung von Funktionen und Inhalten sowie zur Verbesserung, Bereitstellung und Sicherung der Meta Produkte
1. Im Zusammenhang mit dem Anzeigen-Targeting und der Anzeigenauslieferung tun wir Folgendes:
(i) Wir verwenden deine Event-Daten nur dann zur Anzeigenauslieferung, nachdem wir sie mit anderen Daten, die von anderen Werbekunden oder auf andere Weise auf Meta-Produkten erfasst wurden, aggregiert haben;...
2. Wir können Event-Daten in Beziehung zu Personen setzen, die Meta-Produkte nutzen, um die Ziele deiner Werbekampagne zu unterstützen, die Wirksamkeit der Anzeigenauslieferung zu verbessern und die Relevanz von Werbeanzeigen für Nutzer zu ermitteln. Wir können Event-Daten verwenden, um die Funktionen und Inhalte (einschließlich Werbeanzeigen und Empfehlungen) zu personalisieren, die wir Personen auf und außerhalb von unseren Meta-Produkten zeigen.
3. Um das Erlebnis für Nutzer von Meta-Produkten zu verbessern, können wir Event-Daten auch verwenden, um den Schutz und die Sicherheit auf und außerhalb von Meta Produkten zu fördern, sowie für Forschungs- und Entwicklungszwecke und für den Erhalt der Integrität der Meta-Produkte sowie für deren Bereitstellung und Verbesserung.
...
4. Änderung, Beendigung und Speicherung:

a. Wir können deinen Zugriff auf die Meta-Business-Tools jederzeit ändern, aussetzen oder beenden oder ihre Verfügbarkeit einstellen. Du kannst deine Nutzung der Meta-Business-Tools jederzeit beenden.
b. Nach Maßgabe dieser Nutzungsbedingungen für Business-Tools dürfen wir die Event-Daten maximal zwei Jahre lang speichern. Wir können jegliche von dir unter Verwendung der Event Daten erstellten Zielgruppen so lange speichern, bis du sie über deine Konto-Tools löschst. ...
c. Wir behalten uns das Recht vor, deine Einhaltung dieser Nutzungsbedingungen für Business-Tools zu überwachen bzw. zu überprüfen.
...

5. Zusätzliche Bedingungen für die Verarbeitung personenbezogener Informationen

a. DSGVO.
Sofern die Business-Tool-Daten personenbezogene Informationen enthalten, die du gemäß der Datenschutz-Grundverordnung...verarbeitest, gelten folgende Bedingungen:
i. Die Parteien erkennen an und vereinbaren, dass du der Verantwortliche bist hinsichtlich der Verarbeitung von in Business-Tool-Daten enthaltenen personenbezogenen Informationen für die in den Abschnitten 2.a.i und 2.a.ii oben beschriebenen Zwecke der Bereitstellung von Abgleich-, Messungs- und Analysediensten (z. B. um dir Analysen und Kampagnenberichte bereitzustellen), und dass du Meta Platforms Ireland...beauftragst, solche personenbezogenen Informationen für diese Zwecke in deinem Auftrag als dein Auftragsverarbeiter gemäß diesen Nutzungsbedingungen für Business-Tools und den Meta Datenverarbeitungsbedingungen zu verarbeiten. Die Datenverarbeitungs-

bedingungen werden durch Bezugnahme ausdrücklich Bestandteil dieser Nutzungsbedingungen. Sie gelten zwischen dir und Meta Ireland zusammen mit diesen Nutzungsbedingungen für Business-Tools.
ii. In Bezug auf personenbezogene Informationen in Event-Daten, die im Zusammenhang stehen mit Handlungen von Personen auf deinen Websites und in deinen Apps mit integrierten Meta-Business-Tools, für deren Verarbeitung du gemeinsam mit Meta Ireland die Mittel und Zwecke festlegst, erkennen du und Meta Ireland an und stimmen zu, gemeinsam Verantwortliche gemäß Artikel 26 DSGVO zu sein. Die gemeinsame Verantwortlichkeit umfasst die Erhebung solcher personenbezogenen Informationen über die Meta-Business-Tools und ihre anschließende Übermittlung an Meta Ireland, um sie für die oben in den Abschnitten 2.a.iii bis 2.a.v.1 („Gemeinsame Verarbeitung") dargelegten Zwecke zu verwenden. ...Die gemeinsame Verarbeitung unterliegt dem Zusatz für Verantwortliche, der durch Bezugnahme ausdrücklich Bestandteil dieser Nutzungsbedingungen wird, und gilt zwischen dir und Meta Ireland zusammen mit diesen Nutzungsbedingungen für Business-Tools. Meta Ireland bleibt für jegliche Verarbeitung dieser Daten nach deren Übermittlung an Meta Ireland ein unabhängiger Verantwortlicher gemäß Artikel 4 (7) DSGVO.
iii. Du bleibst bzw. Meta Ireland bleibt für jegliche Verarbeitung von in Business-Tool-Daten enthaltenen personenbezogenen Informationen gemäß DSGVO, die nicht den Abschnitten 5.a.i und 5.a.ii unterliegt, unabhängiger Verantwortlicher gemäß Artikel 4 (7) DSGVO. ...
Hinweis:
ii. Im Sinne der Nutzungsbedingungen für Meta-Business-Tools gilt für Bezugnahmen in bestehenden Nutzungsbedingungen oder Vereinbarungen Folgendes: (i) „Umsatzdaten" sind nun Business-Tool-Daten, (ii) „Nutzerinformationen" heißen jetzt Kontaktinformationen, (iii) Verkaufstransaktionsdaten" sind jetzt Event-Daten, (iv) „Abgeglichene Daten" bezeichnen jetzt Event-Daten, die mit abgeglichenen Nutzer-IDs kombiniert wurden, (v) „Nicht abgeglichene Daten" sind jetzt Event-Daten, die nicht mit abgeglichenen Nutzer-IDs kombiniert wurden,"

In „Parameter für Kund*innen-Informationen" wird zu den über Business-Tools übermittelten Informationen weiter ausgeführt:

„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. Mithilfe von Parametern für Kund*innen-Informationen kann Meta Events einfacher Nutzer*innen-Konten in den Meta-Technologien zuordnen. So kannst du leichter messen, wie effektiv deine Anzeigen sind, und deine Anzeigen an Personen ausliefern, die diese wahrscheinlich relevant finden.
Einige Parameter für Kund*innen Informationen müssen zunächst gehasht werden, bevor sie an Meta gesendet werden. Dies wird in den Nutzungsbedingungen für Meta-Business-Tools und Metas Entwicklungsdokumentation festgelegt. Meta setzt hierfür die Hashing-Methode SHA-256 voraus, ein kryptografischer sicherer Hashing-Algorithmus, der den Branchenstandards entspricht. Die Parameter für Kund*innen-Informationen müssen, falls erforderlich, gehasht und mit den zugewiesenen Parameter-Namen gesendet werden. Falls diese Voraussetzung nicht erfüllt wird, ist das sowohl ein Verstoß gegen unsere Nutzungsbedingungen als auch nicht hilfreich für deine Anzeigen Performance.
Manche Arten von Informationen sind unzulässig und dürfen nicht an Meta gesendet werden. Dazu gehören z.B. Gesundheits- oder Finanzdaten über Personen, Informationen von oder über Kinder(n) unter 13, Parameter für Kund*innen-Informationen, die nicht so gehasht sind, wie von Meta vorausgesetzt, und IDs, die wir nicht zulassen, wie

etwa Sozialversicherungsnummern und Kreditkartennummern. ..."

und weiter:

> „Die Parameter für Kund*innen-Informationen sind eine Reihe von Nutzer-IDs, die du zusammen mit deinen Event-Informationen freigibst. ...
> Im Leitfaden zu Datenschutz und Datennutzung von Meta findest du weitere Informationen dazu, welche Daten bei Verwendung der Conversions API gesendet werden.
>
> Unsere Systeme sind so konzipiert, dass sie keine Kund*innen-Informationen akzeptieren, die nicht gehashte Kontaktinformationen sind, sofern dies nicht nachfolgend angegeben ist. Kontaktinformationen sind Informationen, mit denen Einzelpersonen identifiziert werden können, wie Namen, E-Mail-Adressen und Telefonnummern. Diese verwenden wir nur für Abgleichzwecke. Wenn du das Meta Business-SDK verwendest, erfolgt das Hashen automatisch. ..."

Eine weitere, an Verwender der Business-Tools der Beklagten gerichtete Richtlinie betrifft das Teilen von unzulässigen Informationen (vgl. Anl. B6). Hier heißt es u.a.:

> „Identifizieren von potenziell unzulässigen Informationen und entsprechende Benachrichtigungen
> Du wirst z. B. möglicherweise per E-Mail, im Meta Events Manager oder im Meta Werbeanzeigenmanager benachrichtigt, wenn Metas System in den von dir geteilten Daten potenziell unzulässige Informationen entdeckt und daraus entfernt. ...
> 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. Du kannst am besten gewährleisten, dass deine Integration keine vertraulichen oder unzulässigen Informationen an Meta sendet. Metas Systeme sollen deine eigenen Mechanismen zur Einhaltung dieser Regeln lediglich ergänzen. ..."

Hat die Beklagte Kontakt- oder Event-Daten von Drittunternehmen über die streitgegenständlichen Business-Tools erhalten, erfolgt ein Abgleich zur Feststellung, ob die übermittelten Daten einem registrierten Nutzer ihrer sozialen Netzwerke zuzuordnen sind. Nach dieser Verarbeitung entscheidet die Beklagte, welche weiteren Maßnahmen in Bezug auf diese spezifischen Daten ergriffen werden, abhängig von den Einstellungen des Nutzers. Sofern die Daten keinem registrierten Nutzer zuzuordnen sind, speichert sie diese Daten nicht mit Ausnahme bestimmter Daten, die für begrenzte Zwecke wie Sicherheit und Integrität verwendet werden können.

B.

Mit der Registrierung bei einem von der Beklagten betriebenen sozialen Netzwerk (Instagram und/oder Facebook) stimmen Nutzer - so auch die Klagepartei - diesbezüglichen Nutzungsbedingungen zu (Anl. B2, Fassung vom 15.01.2024), die wiederum auf eine Datenschutzrichtlinie (Anl. B10, aktualisierte Fassung vom 26.06.2024) und eine sog. Cookie-Richtlinie (nicht

vorgelegt) verweisen.

In Bezug auf die Verarbeitung von personenbezogenen Daten auf den genannten sozialen Netzwerken durch die Beklagte zum Zweck der Bereitstellung von personalisierter Werbung nutzt diese u.a. optionale Cookies und andere, ähnliche Technologien. Diese definiert die Beklagte wie folgt:

> „Cookies sind eine Art von Technologie und bestehen normalerweise aus kleinen Textstücken, die verwendet werden können, um Informationen auf dem Computer, Mobilgerät oder sonstigen elektronischen Geräten eines Nutzers zu speichern bzw. darauf zuzugreifen. Cookies lassen sich für verschiedene Zwecke verwenden, beispielsweise, um sich die Einstellungen oder Präferenzen eines Nutzers auf einer Website zu merken, die Nutzeranmeldung zu unterstützen oder den Traffic auf einer Website zu analysieren. Sonstige Technologien, einschließlich der auf Webbrowsern oder Geräten gespeicherten Daten, der mit einem Gerät verknüpften Kennungen sowie sonstiger Software, können auch für ähnliche Zwecke genutzt werden. Wir bezeichnen alle diese Technologien als Cookies."

Nutzer müssen die Berechtigung zur Verwendung optionaler Cookies der Beklagten in anderen Apps und auf Websites von anderen Unternehmen positiv erteilen, indem sie über die „Einstellungen und Privatsphäre"-Seite und in der „Kontenübersicht" die „Meta Cookies in anderen Apps und auf anderen Websites"- Einstellung verwenden (im folgenden auszugsweise zitiert, zu den weiteren Einzelheiten vgl. Anl. B7 unter IV.). Zur Erläuterung führt die Beklagte hier u.a. aus:

> „So verwenden wir diese Cookies
> Wenn du diese Apps und Websites besuchst, verwenden wir Informationen, die wir erhalten, für folgendes:
> Um dein Nutzungserlebnis in Meta-Produkten unter anderem dadurch zu personalisieren, dass wir dir Werbeanzeigen zeigen, die eher dem entspricht, was du gerne sehen möchtest...
> Um Meta-Produkte noch besser zu machen, weil wir nachvollziehen können, ob die Produkte ordnungsgemäß funktionieren oder besser auf die Bedürfnisse unserer Nutzer zugeschnitten werden müssen
> Um Unternehmen, die unsere Tools verwenden bei Analysen und Messungen ihrer Anzeigen Performance zu unterstützen"
>
> Wenn du diese Cookies erlaubst
> ...
> Verwenden wir deine individuellen Cookie-Informationen, um dir relevante Werbung zu zeigen …
>
> Wenn du diese Cookies nicht erlaubst:
> ...
> Verwenden wir Informationen in eingeschränktem Umfang, um für Sicherheit und Integrität zu sorgen. Hierzu gehört auch die Überwachung von Angriffsversuchen auf unsere Systeme, beispielsweise eine gezielte Überlastung unserer Website durch zu viele Anfragen,

Verwenden wir diese Informationen nicht, um dir relevante Werbung zu zeigen, Kann es sein, dass wir weiterhin aggregierte Informationen zu Aktivitäten in diesen Apps und auf diesen Websites erhalten. Deine persönlichen Cookie-Informationen sind darin jedoch nicht enthalten“

Die Kontenübersicht enthält ferner eine Einstellung „Deine Aktivitäten außerhalb von Meta-Technologien“ betreffend Informationen zu Interaktionen, die von Dritt-Unternehmen mittels Business-Tools an die Beklagte übermittelt wurden oder werden (sog. off-site Aktivitäten oder „Third-Party Activity Data“), über die Nutzer folgendes auswählen können:

„Erfahre mehr über Aktivitäten außerhalb von Meta-Technologien“
„Neueste Aktivitäten ansehen“
„Bestimmte Aktivitäten trennen“
„Frühere Aktivitäten löschen“
„Künftige Aktivitäten verwalten“

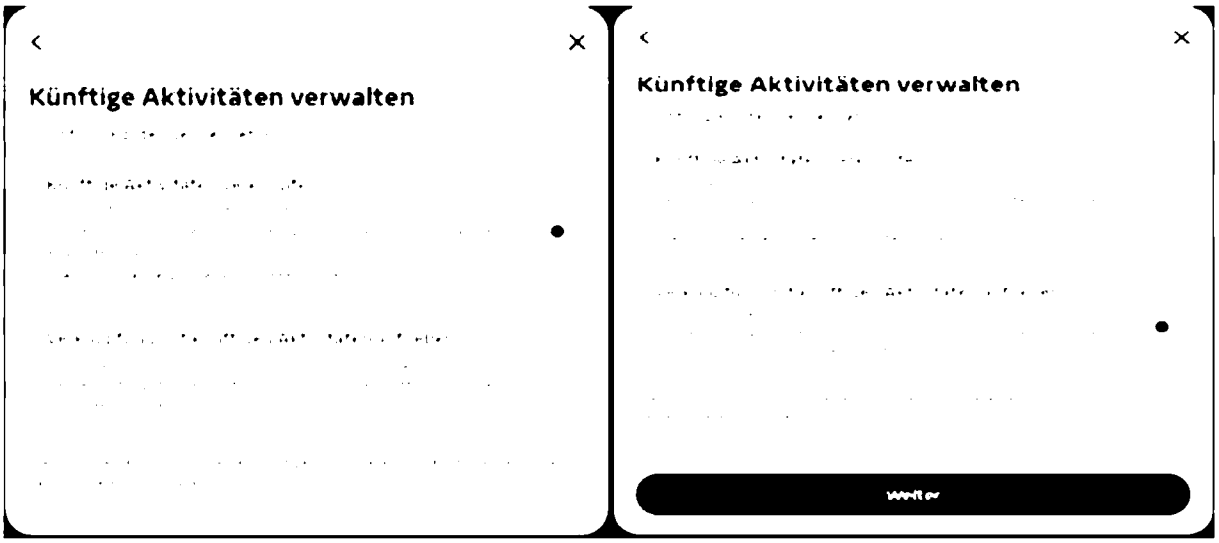
Nach Auswahl „Bestimmte Aktivitäten trennen“ erscheint die Mitteilung:

„...Aktivitäten von den ausgewählten Apps und Websites werden nicht mehr in deinen Konten gespeichert....“

Nach Auswahl „Frühere Aktivitäten löschen“ wird ausgeführt:

„...Dein Aktivitätenverlauf wird von deinen Konten getrennt. ...“

Nach Auswahl von „Künftige Aktivitäten verwalten“ erscheinen folgende Auswahl-Menüpunkte:

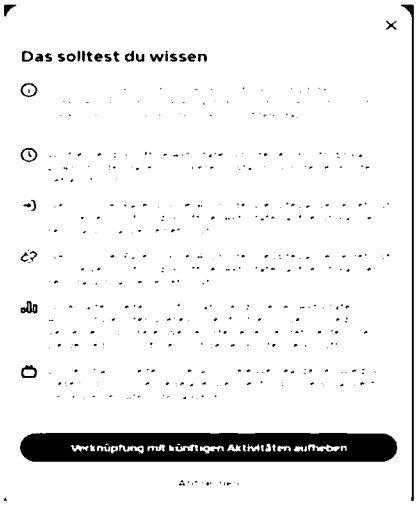


„Künftige Aktivitäten verknüpfen (hier Voreinstellung: aktiv; vgl aber auch Bl. 345 eA LG)
Informationen, die Unternehmen und Organisationen zu deinen Interaktionen mit Ihnen an uns übermitteln, werden zukünftig verknüpft.

Verknüpfung mit künftigen Aktivitäten aufheben
Informationen, die Unternehmen und Organisationen zu deinen Interaktionen mit Ihnen an uns übermitteln, werden zukünftig nicht mehr verknüpft.

Wenn du die Verknüpfung deiner künftigen Aktivitäten aufhebst, löschen wir auch deine früheren Aktivitäten..."

Nach Betätigen der Schaltfläche „weiter" erscheint eine „Das solltest du wissen"- Seite:



(„...Wir trennen zukünftige Aktivitäten von deinem Konto. …
Wir erhalten weiterhin Informationen zu deinen Aktivitäten von Apps und Websites. Diese können für Messungen sowie zur Verbesserung unserer Werbesysteme verwendet werden. Sie werden jedoch nicht mehr mit deinem Konto verknüpft. Du siehst auch weiterhin genausoviele Werbeanzeigen wie zuvor, diese werden jedoch nicht mehr mit deinen Konten verknüpft.....")

Ferner bietet die Beklagte den Nutzern ihrer sozialen Netzwerke „Kontoverlauf"- und „Deine Informationen herunterladen"-Tools an, welche es ihnen ermöglichen sollen, ihre Instagram-Profilinformationen anzusehen und von ihnen eine Kopie herunterzuladen, einschließlich Informationen zu den Aktivitäten, die Meta von Drittunternehmen auf den sozialen Netzwerken erhält (vgl. zu den Einzelheiten Anl. B7).

Die Klagepartei willigte in die Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung entsprechend der Einstellung „Informationen von Werbepartnern über deine Aktivitäten" bzw. „Werbepräferenzen" nicht ein.

C.

Sie wendet sich gegen die Verarbeitung ihrer personenbezogenen Daten, die an die Beklagte über auf Drittseiten, -Servern und -Apps implementierten Business-Tools gelangen (Bl. 263 eA). Insbesondere beanstandet sie, dass nach Übertragung der (auch gehashten) Daten an die Beklagte mittels Business Tools, die auf dem Rechner des Nutzers oder den Servern von Webseiten- und App-Betreibern laufen, ein Abgleich erfolge, durch den die Beklagte ermitteln könne, wessen personenbezogene Daten sie durch Business Tools gesammelt, an ihre Ser-

ver übertragen lassen und bereits verarbeitet habe. Die Daten der Klagepartei verarbeite die Beklagten automatisch ohne jede Unterscheidung genauso wie die Daten aller anderen Nutzer auch. Die Beklagte gebe der Klagepartei keine Möglichkeit, diese Datenverarbeitung zu beenden, die stets stattfinde und nicht berücksichtige, ob die Klagepartei hierin eingewilligt habe oder nicht oder ob sie ihren Instagram- oder Facebook-Account weiterbetreibe oder lösche. Die Beklagte, welche die Darlegungs- und Beweislast bzgl. einer Rechtfertigung und Einwilligung nach Art. 6 DSGVO trage, habe bisher nur Screenshots von Schaltflächen zur „Einwilligung in die Verarbeitung für personenbezogene Werbung" vorlegt und auf unbenannte „Dritte" verwiesen, mit denen sie angeblich Verträge abgeschlossen habe, die diese Dritten dazu verpflichte, wirksame Einwilligungen bei dem Nutzer einzuholen. Dieser Vortrag sei unsubstantiiert und nicht einlassungsfähig. Weitere konkrete Rechtfertigungsgründe könne sie nicht für sich in Anspruch nehmen. Soweit sie Sicherheitsaspekte anführe, bleibe ihr Vortrag vage. Zudem sei sie spätestens bei der Verarbeitung auf ihren eigenen Servern (nach der Übertragung durch Business Tools) nicht mehr „gemeinsam Verantwortliche" i.S.d Art. 26 DSGVO mit Drittbetreibern und könne sich auf eine diesen erteilte Einwilligung nicht berufen.

Der Kläger beantragt,

das erstinstanzliche Urteil des Landgerichts Dresden vom 04.02.2025 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 Erhebung mit Hilfe der Meta Business Tools, die Weitergabe 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.

a) **E-Mail der Klagepartei**
b) **Telefonnummer der Klagepartei**
c) **Vorname der Klagepartei**
d) **Nachname der Klagepartei**
e) **Geburtsdatum der Klagepartei**
f) **Geschlecht der Klagepartei**
g) **Ort der Klagepartei**
h) **Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID" genannt)**
i) **IP-Adresse des Clients**
j) **User-Agent des Clients (d. h. gesammelte Browserinformationen)**
k) **interne Klick-ID der Meta Ltd.**
l) **interne Browser-ID der Meta Ltd.**
m) **Abonnement-ID**

n) **Lead-ID**
o) **anon_id**

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

3. Die Beklagte wird verpflichtet, sämtliche unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits verarbeiteten personenbezogenen Daten der Klagepartei ab sofort unverändert am gespeicherten Ort zu belassen, d. h. insbesondere diese erst einen Monat nach rechtskräftigem Abschluss des Verfahrens zu löschen, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden, und 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 08.09.2023, 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.

Sie ist der Auffassung, streitgegenständlich sei allein die Datenverarbeitung zur Bereitstellung personalisierter Werbung gemäß Art. 6 Abs. 1 lit. a DSGVO. In diese müsse der Nutzer über die Schaltfläche „Informationen über Aktivitäten von Werbepartnern" einwilligen, die auf eine Datenquelle beschränkt sei, nämlich auf die von Werbepartnern übermittelten Aktivitäten eines Nutzers außerhalb der Plattform Instagram. Eine Datenverarbeitung zur Bereitstellung personalisierter Werbung erfolge nur, wenn ein Nutzer eine solche Einstellung erteilt habe. Anderenfalls könne eine solche Datenverarbeitung nicht erfolgen, was die Beklagte nach erfolgtem Abgleich zur Feststellung, ob der Nutzer in ihren sozialen Netzwerken registriert sei, ermittle. Dies gelte auch für die Klagepartei, die eine solche Einwilligung nicht erteilt habe. Wenn ein Nutzer über Einstellmöglichkeiten innerhalb der Metasysteme optionale „Meta-Cookies auf anderen Apps und Webseiten" nicht erlaube, werde keine Datenverarbeitung zur Bereitstellung personalisierter Werbung für diesen Nutzer vorgenommen bzw. würden - wie an anderer Stelle ausgeführt wird - „für bestimmte Verarbeitungsvorgänge" keine über Cookies und ähnliche Technologien erhobenen Daten, einschließlich der streitgegenständlichen Datenverarbeitung verwendet. In diesem Fall nutze sie nur eingeschränkt Daten, die über Cookies und ähnliche Technologien erhoben wurden, und zwar für eingeschränkte Zwecke, wie Sicherheits- und Integritätszwecke, einschließlich Zwecke der Überwachung von versuchten Angriffen auf die Systeme der Beklagten, wie z.B. durch die forcierte Überlastung ihrer Webseite. Die Beklagte stütze sich nicht für jeden Verarbeitungszweck auf eine Einwilligung, da dies auch gesetzlich nicht erforderlich sei. Mangels konkreter Darlegung, welchen Verarbeitungszweck die Klagepartei angreifen möchte, könne sie hierauf auch nicht konkret erwidern.

Ferner übermittelten Drittunternehmen Daten über die Aktivitäten einer Person auf ihrer Webseite oder App über die streitgegenständlichen Business-Tools nur dann an die Beklagte, wenn diese Person tatsächlich mit einem Drittunternehmen interagiere, das eines der streitgegenständlichen Business-Tools nutze. Diese Drittunternehmen seien über die Nutzungsbedingungen für Business Tools verpflichtet, alle Offenlegungen vorzunehmen sowie Rechte und Genehmigungen einzuholen, bevor sie Business-Tools Daten an die Beklagte weitergäben. Die Beklagte habe darüber hinaus eine formelle Art. 26 DSGVO-Vereinbarung mit Drittunter-

nehmen getroffen (der „Vertragszusatz“ vgl. Anl. B9), die diese verpflichte, eine Einwilligung hinsichtlich der Platzierung nicht notwendiger Cookies einzuholen. Die Implementierung von „Cookie-Bannern“ und die Einholung der Einwilligungen liege daher in erster Linie in der Verantwortung der Drittunternehmen. Hinsichtlich der gerügten Übermittlung von sog. technischen Standarddaten z.B. über HTTP-Anfragen, würden von Drittunternehmen sowohl bei Meta Pixel als auch bei der Conversions-API Technologien eingesetzt, die sicherstellen sollen, dass keine Daten an die Beklagte übertragen werden, bis eine Einwilligung eingeholt worden sei; hierüber habe die Beklagte auch informiert (vgl. Anl. B16, B17, B18, Schaubild Anl. 2). Mangels Zugriffs auf die Drittwebseiten und -Apps kontrolliere die Beklagte zwar nicht, ob die Business-Tools richtig installiert seien, dies stünde aber allein in der Verantwortung der Drittunternehmen. Nur diese hätten die Möglichkeit, ihren Code dementsprechend zu konfigurieren und sicherzustellen, dass der Browser der Person oder der Server des Drittunternehmens eine HTTP-Anfrage erst dann ausführe, wenn die Person ihre Einwilligung zu nicht notwendigen Cookies erteilt habe. Um den Schutz besonders sensibler Daten zu gewährleisten, habe die Beklagte Maßnahmen implementiert, die dazu dienen sollen, den Erhalt und die Nutzung potentiell sensibler Daten zu verhindern. Hierzu gehöre die Kategorisierung der Datenquellen mit erweiterten Datenbeschränkungen und die automatisierte Blockierung und Filterung vor oder bei Empfang der Ereignisdaten bevor diese Daten in den Werbesystemen von Meta gespeichert oder verwendet werden. Der Klagepartei hätte es daher oblegen, konkret darzulegen welche Webseiten sie besucht habe (zB durch den Browserverlauf) und unter Beweis zu stellen, dass über diese Webseiten Daten an die Beklagte übermittelt würde, ohne dass zuvor die Einwilligung der Klagepartei eingeholt worden sei. Auf eine etwaige Beweisnot, auch mit Blick auf die angebliche Unzumutbarkeit, den gesamten Browserverlauf öffentlich zu machen, könne sich die Klagepartei nicht berufen. Auch die von ihr vorgelegte Liste der angeblich meistbesuchten Webseiten genüge nicht. Vielmehr habe die Beklagte einige der Webseiten dieser Liste überprüft, die zum Zeitpunkt der Überprüfung keine Business-Tools verwendet hätten.

Soweit Datenverarbeitungsvorgänge betroffen seien, die bis zu drei Jahre vor Klageerhebung liegen, hat die Beklagte die Verjährungseinrede erhoben.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen und auf das Protokoll der mündlichen Verhandlung ergänzend Bezug genommen.

II.

Die zulässige Berufung hat in dem aus dem Tenor ersichtlichen Umfang Erfolg.

A.

Die internationale Zuständigkeit deutscher Gerichte ist gemäß Art. 18 Abs. 1 EuGVVO sowie gemäß Art. 79 Abs. 2, Satz 2 DSGVO gegeben, denn die Klagepartei hat ihren gewöhnlichen Aufenthalt in Deutschland. Der sachliche, räumliche und zeitliche Anwendungsbereich der am 25.05.2018 in Kraft getretenen Datenschutzgrundverordnung ist eröffnet.

B.

1.

Der auf die Feststellung gerichtete Antrag, dass das zwischen den Parteien bestehende Nutzungsverhältnis die Speicherung und Verwendung von über Business Tools erhobenen personenbezogenen Daten nicht gestatte, ist unzulässig. Er beinhaltet kein feststellungsfähiges Rechtsverhältnis im Sinne des § 256 ZPO (a). Zudem liegt das für den Antrag erforderliche Feststellungsinteresse nicht vor (b).

a)

Nach ständiger Rechtsprechung können bloße Elemente oder Vorfragen eines Rechtsverhältnisses, reine Tatsachen oder etwa die Wirksamkeit von Willenserklärungen oder die Rechtswidrigkeit eines Verhaltens nicht Gegenstand einer Feststellungsklage sein (vgl. BGH, Versäumnisurteil vom 27.03.2015 – V ZR 296/13 - NJW-RR 2015, 915, Tz 7 - juris; vgl. Urt. v. 20.04.2018 - V ZR 106/17 - NJW 2018, 3441, Tz 13; vgl. LG Stuttgart, Urt. v. 05.02.2025 - 27 O 190/23 - juris; vgl. LG Braunschweig, Urt. v. 04.06.2025 - 9 O 2615/23 - juris). Für die Zwischenfeststellungsklage gemäß § 256 Abs. 2 ZPO gilt nichts anderes. Auch sie kann nicht auf die Feststellung der Rechtswidrigkeit bzw. Unzulässigkeit eines Verhaltens gerichtet werden (vgl. BGH, Urt. v. 20.04.2018 - V ZR 106/17 - a.a.O.). Entgegen der Auffassung der Klagepartei richtet sich der Feststellungsantrag vorliegend indes gerade nicht auf die Feststellung des Bestehens oder Nichtbestehens des zugrundeliegenden Vertrags über die Nutzung des sozialen Netzwerks der Beklagten, sondern beschränkt sich auf die Feststellung der Rechtswidrigkeit ("… nicht gestattet") eines Verhaltens der Beklagten, nämlich der im Einzelnen aufgeführten Datenverarbeitungsvorgänge (a.A. allerdings ohne nähere Begründung OLG München, Urt. v. 18.12.2025 - 14 U 1068/25e, n.v., Anlage der Klagepartei im Berufungsverfahren). Der Feststellungsantrag ist überdies auch nicht hinreichend bestimmt, weil in das Feststellungsbegehren eine Vielzahl weiterer Rechtsverhältnisse zwischen der Beklagten und Dritten einbezogen werden, da als Anknüpfungspunkt die „Erhebung mit Hilfe der Meta Business-Tools“ und „Weitergabe an die Server der Beklagten“ dienen soll. Die Erhebung und Weitergabe erfolgt aber nach dem unstreitigen Parteivortrag allein bei Drittunternehmen, die Business-Tools einset-

zen. Eine generelle Feststellung der Rechtswidrigkeit all dieser jeweiligen Datenerhebungen und -weitergaben ist schon wegen der letztlich unbekannten Anzahl dieser Dritten und wegen der Möglichkeit von jeweils abweichenden Cookie- und Einwilligungsvereinbarungen, auch in Bezug auf die Klagepartei, unmöglich.

b)

Unabhängig hiervon liegt für den Antrag auch kein Feststellungsinteresse i.S.v. § 256 Abs. 1 ZPO vor. Voraussetzung hierfür ist, dass dem subjektiven Recht der Klägerseite eine gegenwärtige Gefahr der Unsicherheit dadurch droht, dass die Beklagtenseite es ernstlich bestreitet oder sie sich eines Rechts gegen die Klägerseite berühmt, und dass das erstrebte Urteil infolge seiner Rechtskraft geeignet ist, diese Gefahr zu beseitigen. Ist der Klägerseite eine Klage auf Leistung möglich und zumutbar und erschöpft sie das Rechtsschutzziel, fehlt grundsätzlich das Feststellungsinteresse, weil die Klägerseite im Sinne einer besseren Rechtsschutzmöglichkeit den Streitstoff in einem Prozess klären kann (vgl. Greger in: Zöller, Zivilprozessordnung, 36. Auflage 2026, § 256, Rn 14 ZPO). Dies ist hier der Fall. Soweit es der Klagepartei darum geht, für künftige Ansprüche Klarheit über die Pflichtverletzungen der Beklagten zu schaffen, erschöpft sich ihr Rechtsschutzziel in dem ebenfalls gestellten Antrag auf Unterlassung der Verarbeitung. Auf eine noch nicht abgeschlossene Schadensentwicklung, mit der sie ihr Interesse an der Feststellung begründen will, kann sich die Klagepartei schon deswegen nicht berufen, weil ihr Antrag nicht auf die Feststellung einer Schadensersatzpflicht der Beklagten zielt, sondern auf die Vorfrage, ob deren Geschäftsverhalten rechtswidrig ist (vgl. OLG Hamm, Beschluss vom 10.09.2025 – I-28 U 63/25 –, Rn. 56 - 59, juris).

2.

a)

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

Ein Klageantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens der Klagepartei nicht durch vermeidbare Ungenauigkeit auf die Beklagtenseite abwälzt und eine Zwangsvollstreckung aus

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

An diesen Anforderungen gemessen ist der Antrag der Klagepartei, die Beklagte solle es unterlassen, personenbezogene Daten der Klägerseite zu erheben, an ihre Server weiterzuleiten, zu speichern und zu verwenden, die außerhalb ihrer Netzwerke mittels der von ihr vertriebenen Business-Tools auf Drittseiten und -Apps erhoben und an sie übertragen werden, hinreichend bestimmt. Er lässt sich unter Heranziehung des Klagevorbringens sinngemäß dahingehend auslegen, dass die Klagepartei sich dagegen wendet, dass ihre (sämtliche) personenbezogenen Daten über eine auf Drittwebseiten bzw. -Apps implementierte Software an die Beklagte gelangen und dort von ihr für eigene Zwecke genutzt werden. Entsprechend dem in den sog. Scraping-Fällen als hinreichend bestimmt angesehenen Unterlassungsbegehren begehrt sie eine Unterlassung jeglicher Verarbeitung ihrer durch Business-Tools erhobenen Daten durch die Beklagte. Dies gilt auch für Daten, die von Drittunternehmen übermittelt werden, die hierfür zuvor eine Einwilligung der Klagepartei eingeholt haben. Dem zur Auslegung des Antrags heranzuziehenden Vorbringen der Klagepartei ist deutlich zu entnehmen, dass sie auch für diesen Fall von einer rechtswidrigen Verarbeitung ausgeht.

Die Klagepartei ist zur Konkretisierung ihres Antrags auch nicht gehalten, einzelne Webseiten oder Apps zu benennen, deren Nutzung die Datenübertragung an die betroffene Plattform infolge eines von der Beklagten zur Verfügung gestellten Trackingtools ausgelöst haben könnte.

Die Beklagte bestreitet nicht, dass zahlreiche Webseiten (aus dem Bereich Nachrichten, Medien, Shopping) ihre Business-Tools implementiert haben. Für einen regelmäßigen Nutzer des Internets, der online einkauft, Reisen bucht und sich über Nachrichten, Wetter, Politik oder/ und Gesundheitsfragen informiert, ist es schlechterdings nicht möglich, nur Webseiten aufzusuchen, die Business-Tools nicht verwenden. Von der Klagepartei kann nicht verlangt werden vorzutragen, welche Werbetreibende die Business-Tools der Beklagten implementiert haben, denn dies ist mangels Kenntnis nicht möglich (vgl. hierzu LG Berlin II, Urt. v. 04.04.2024 - 39 O 67/24, Rn 79 - juris; vgl. OLG München, Urt. v. 18.12.2025, a.a.O.). Der Klagepartei ist es auch grundsätzlich nicht zumutbar, näher zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten und mit diesen Tools versehenen Homepages vorzutragen. Zum einen kann schon naturgemäß niemand mit vertretbarem Aufwand rekonstruieren, welche Homepages zu welchem Zeitpunkt er in der Vergangenheit besucht hat; auch ist niemand verpflichtet, entsprechende Verlaufsprotokolle in seinen Rechnern vorzuhalten (vgl. LG Braunschweig, Urt. v. 04.06.2025 - 9 O 2615/23, Rn 95 - juris). Zum anderen wäre der Klagepartei aber auch selbst dann, wenn dieses Wissen vorhanden wäre, kein weitergehend substantiierter Vortrag möglich, da sie keinen vollständigen Überblick darüber hat, auf welchen Homepages zu welchem Zeitpunkt welche Business-Tools der Beklagten aktiv waren und welche Daten hierüber an die Beklagte übermittelt wurden. Faktisch wäre die Klagepartei entsprechend gezwungen, ihr gesamtes Internetnutzungsverhalten offen zu legen, was ersichtlich im eklatanten Widerspruch zum Normzweck der DSGVO stünde (vgl. LG Braunschweig, a.a.O., Rn 95 - juris). Für die Zulässigkeit des Unterlassungsantrags ist es angesichts dessen ausreichend, wenn mit einiger Wahrscheinlichkeit jedenfalls feststeht, dass die Klagepartei als Internetnutzerin von der streitigen Datenverarbeitung erfasst wurde und wird (so auch LG Braunschweig, a.a.O., Rn. 90, - juris).

Dies ist hier mit Blick auf die oben zitierten (Dritt-)Nutzungsbedingungen der Beklagten ausreichend bestimmt dargelegt. Der Unterlassungsantrag konkretisiert die inkriminierte Verletzungshandlung, nämlich die behauptete unrechtmäßige Verarbeitung von an die Beklagte mittels Business-Tools gelangter Daten trotz fehlender Einwilligung der Klagepartei bzw. auf Grundlage einer unwirksamen Einwilligung (soweit Dritte Daten an die Beklagte übertragen). Ob Daten an die Beklagte zumindest teilweise unabhängig von ihrer Auswahlentscheidung auf Webseiten von Drittunternehmen oder auch bei fehlender Einwilligung zum Zweck der Bereitstellung personalisierter Werbung auf der Plattform der Beklagten übertragen werden, ist für die Zulässigkeit des Unterlassungsbegehrens unerheblich, genauso wie die Frage, ob eine solche Datenverarbeitung für die Funktionsweise der Webseiten erforderlich ist und/oder hierfür rechtfertigende Gründe vorliegen (i.d.S. auch OGH Österreich, Urt. v. 26.11.2025 - 6 Ob

189/24y, Rn. 78 ff, Rn. 82, BeckRS 2025, 34948; a.A. OLG München, a.a.O., S. 23). So verstanden gibt es auch keine Auslegungsprobleme im Vollstreckungsverfahren, da die Klagepartei die Datenverarbeitung durch die Beklagte mittels Daten, die über Business Tools an sie gelangen, in Gänze unterlassen wissen will.

Entgegen der Auffassung der Beklagten besteht für einen solchen Antrag auch ein Rechtsschutzbedürfnis. Zwar kann die Klagepartei ihr Konto bei der Beklagten ohne weiteres selbst löschen, indem sie die Löschung ihres Kontos initiiert. Allerdings ist das Rechtsschutzziel – die Untersagung einer unrechtmäßigen Verarbeitung ihrer Daten – mit dem dann erreichten Ergebnis nicht identisch. Dieses Rechtsschutzziel ist auch besonders schützenswert, weil die DSGVO allen europäischen Bürgern ein einheitliches und hohes Datenschutzniveau bezüglich aller auf dem europäischen Markt zugelassener Anwendungen – und somit auch Social-Media-Plattformen – gewährleisten soll. Würde man die Klagepartei auf das Löschen ihres Nutzerprofils verweisen, so würde man zugleich diese Regelungsabsicht ad absurdum führen (LG Aschaffenburg, Urt. v. 20.10.2025 - 31 O 98/24, S. 28, Anlagen K zum Schriftsatz vom 21.01.2026; LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, GRUR-RS 2025, 32563, Rn. 99). Auch der Verweis auf die Möglichkeit der Klagepartei, über die Schaltfläche „Deine Aktivitäten außerhalb der Meta Technologien“ selbst die Verarbeitung einzuschränken, verfängt nicht: Zwar führen die Einstellungen „Bestimmte Aktivitäten trennen“ dazu, dass Aktivitäten von Apps und Websites, die der Nutzer auswählen muss, nicht mehr in seinen Konten gespeichert werden; „Frühere Aktivitäten löschen“ dazu, dass die von Drittunternehmen geteilten Informationen über Aktivitäten vom Konto des Nutzers getrennt werden und „Verknüpfung mit künftigen Aktivitäten aufheben“ dazu, dass Informationen, die Unternehmen und Organisationen zu Interaktionen mit dem Nutzer an die Beklagte übermitteln, zukünftig nicht mehr verknüpft werden. Der Transfer personenbezogener Daten von Drittunternehmen an die Beklagte bleibt davon aber unberührt.

b)

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

aa) Zwar ergibt sich der Anspruch nicht unmittelbar aus den Vorschriften der DSGVO (EuGH, Urt. v. 04. 09. 2025 – C-655/23 –, LS 1 und Rz. 52, - juris; vgl. Senat, Urt. v. 14.12.2021 - 4 U 1278/21, Rn 46 - juris). Der Rückgriff auf nationale Vorschriften ist insoweit aber möglich (EuGH, a.a.O) und ergibt sich nach deutschem Recht wegen der Verletzung des allgemeinen Persönlichkeitsrechts der Klagepartei aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 Art. 1 Abs. 2 GG; § 823 Abs. 2 BGB i.V.m. Art. 6 DSGVO, jeweils i.V.m. § 1004 Abs. 1 S. 2 BGB analog.

Der Unterlassungsanspruch setzt voraus, dass eine konkrete (Erstbegehungs- oder Wiederholungs-)Gefahr dafür besteht, dass die Beklagte gegenwärtig über die Meta Business-Tools gesammelte personenbezogene Daten der Klagepartei verarbeitet, die Beklagte Verantwortliche für diese Verarbeitung ist und sie eine Rechtfertigung gem. Art. 6 DSGVO für diese Datenverarbeitung nicht darlegt und beweist. Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr wird durch das festgestellte rechtsverletzende Verhalten indiziert (vgl. Senat, Beschl. v. 24.06.2024 – 4 U 168/24 –, Rn. 18, m.w.N., -juris).

Da es sich bei diesen Verarbeitungsvorgängen um interne Abläufe in den Systemen der Beklagten handelt, trifft sie dabei eine sekundäre Darlegungslast zu den Datenverarbeitungsvorgängen bei der Erhebung und Verarbeitung personenbezogener Daten mittels Business-Tools. Die Klagepartei hat demgegenüber nicht darzulegen, welche konkreten Webseiten sie aufgesucht hat und auf welchen dieser Webseiten Business-Tools zum Einsatz kommen (s.o. 2. a)). Schon aus diesem Grund kann von ihr – anders als die Beklagte meint – auch nicht verlangt werden, darzulegen und zu beweisen, dass sie auf diesen Webseiten die Einwilligung in die Datenerhebung über Business-Tools verweigert hat. Zwingende Voraussetzung für eine Datenübermittlung an die Beklagte ist die Cookie-Einwilligung des Nutzers auf Drittwebseiten ohnehin nicht, weil unstreitig die Implementierung der Business-Tools auf zahlreichen Drittwebseiten fehlerhaft ist, so dass dort Daten auch dann an die Beklagte weitergeleitet werden, wenn der Nutzer eine solche Einwilligung nicht erteilt hat. Nachdem unstreitig ist, dass die Klagepartei bei der Beklagten als Nutzer registriert ist und dass auf einer erheblichen Anzahl namhafter und reichweitenstarker Webseiten in Deutschland die Business-Tools der Beklagten in ihren verschiedenen Ausprägungen zum Einsatz kommen, ist vielmehr davon auszugehen, dass auch von der Klagepartei Business-Tool-Daten erhoben werden. Soweit sich die Beklagte darauf beruft, dass dies ausnahmsweise nicht der Fall ist, trägt sie auch hierfür die Darlegungslast (vgl. hierzu auch Senat, Urt. v. 11.02.2025 – 4 U 1283/24 –, juris, und mit überzeugender Begründung: LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, Rn. 88-92 m.w.N., -juris).

bb) Bei Anwendung dieser Maßstäbe hat die Beklagte die Behauptung, die ihr seitens ihrer Geschäftspartner über Business-Tools übermittelten personenbezogenen Daten der Klagepartei verarbeite sie auch bei fehlender Einwilligung des Nutzers, nicht substantiiert bestritten. Hierfür ist nicht entscheidend, ob sie die von Drittunternehmern übermittelten Daten verarbeitet, um der Klagepartei personalisierte Werbung zu zeigen. Entscheidend ist vielmehr, dass sie diese Daten auf ihrer Plattform jedenfalls vorübergehend speichert und mit den sog. on-site-Daten der Klagepartei zusammenführt, bevor diese in einem weiteren Schritt durch Zu-

weisung von Ad-IDs, Hash-Werten und Cookie-IDs pseudonymisiert werden. Diese Zusammenfassung in für die Beklagte auswertbaren individuellen Nutzerprofilen stellt ein Verknüpfen i.S.d.Art. 4 Nr. 2 DSGVO dar, weil hiermit eine inhaltliche Umgestaltung erfolgt und die verknüpften Daten einen neuen Aussagewert erhalten (vgl. hierzu Schaffland/Holthaus in: Schaffland/Wiltfang, DS-GVO/BDSG, 6. Erglfg. 2025, Art. 4 EUV 2016/679, Rn. 116). Die hiermit einhergehende Bildung individueller Nutzerprofile stellt zugleich ein Profiling der Nutzer im Sinne von Art. 4 Nr. 4 DSGVO dar, weil die mit der o.a Verknüpfung verbundene Erstellung eines Profils einer Person durch Auswertung von Daten und Bewertungen aufgrund von Algorithmen zur Erstellung eines Persönlichkeits-, Verhaltens- oder Bewegungsprofils durch Sammlung von Daten, unter anderem durch (im Internet) hinterlassene (Cookies), getätigte und veröffentlichte Informationen z. B. zu sozialen Kontakten, politischer Einstellung, persönlichem Weltbild, persönlichen Vorlieben, finanziellen Verhältnissen, gesundheitlicher Situation und weiteren Angaben ein modellhaftes, auf Algorithmen beruhendes Gesamtbild der individuellen Persönlichkeit ergeben (vgl. auch insoweit Schaffland/Wiltfang, aaO, Art. 4 EUV 2016/679, Rn. 125). Dies steht zur Überzeugung des Senats aufgrund des Sachvortrags der Parteien und in Würdigung der vorgelegten NB-MBT sowie der Nutzungsbedingungen für Plattform-Nutzer (im Folgenden NB-PN) fest.

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

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

Nach den NB-MBT (vgl. dort Ziff. 2 a) kann die Beklagte sämtliche Business-Tools-Daten für eine Reihe von Zwecken verwenden, insbesondere auch die übermittelten Kontaktinformationen mit von ihr selbst vergebenen Nutzer-IDs abgleichen und mit den Event-Daten kombinieren. Entsprechend dem Hinweis unter Ziff. iv am Ende ihrer Nutzungsbedingungen definiert die

Beklagte als „abgeglichene Daten“ Event-Daten, die mit abgeglichenen Nutzer-IDs kombiniert wurden. Somit kann sie den betreffenden Nutzer eindeutig identifizieren und ihm sämtliche Interaktionen zuordnen. Im Anschluss an diesen Abgleichprozess werden - lediglich - die von Dritten übermittelten Kontaktinformationen von ihr gelöscht (vgl. Ziff. 2 a i.1. Satz 2 NB-MBT), was nach dem Verständnis des Senats jedoch keine Auswirkungen auf die zuvor von der Beklagten in ihren Systemen erfolgte Identifizierung und Zuordnung zu einem bestimmten Nutzer wie der Klagepartei hat. Dies wird auch durch Ziff. 2. a. bestätigt, insbesondere unter v. der NB-MBT. Dabei verarbeitet die Beklagte die ihr von Dritten übermittelten Daten auch nicht ausschließlich für drittbezogene (Werbe-)Zwecke. Aus der Regelung unter Ziff. 2. a. v. 2. NB-MBT ergibt sich vielmehr, dass sie die übermittelten Event-Daten verwenden kann, „um die Funktionen und Inhalte (einschließlich Werbeanzeigen und Empfehlungen) zu personalisieren, die wir Personen auf und außerhalb von unseren Meta-Produkten zeigen.“ Nach Ziff. 2. a. v. 3. NB-MBT ist die Beklagte ferner berechtigt, „um das Erlebnis für Nutzer von Meta-Produkten zu verbessern“, Event-Daten zu verwenden, „um den Schutz und die Sicherheit auf und außerhalb von Meta-Produkten zu fördern, sowie für Forschungs- und Entwicklungszwecke und für den Erhalt der Integrität der Meta-Produkte sowie für deren Bereitstellung und Verbesserung.“

(2) Auch die in den Nutzungsvertrag mit der Klagepartei (NB-PN) einbezogenen Erläuterungen zur „Deine Aktivitäten außerhalb von Meta-Technologien“- Einstellung („Off-site Aktivitäten“ bzw.„Third-Party Activity Data“) bestätigen eine fortlaufende Verarbeitung der ihr übermittelten Business-Tools Daten, unabhängig von der Einwilligung eines Nutzers. Entsprechend den Ausführungen unter Ziff. IV und den Informationen in der abgebildeten Infobox (vgl. Anl. B7) verwendet die Beklagte über ihre optionalen Cookies in anderen Apps und Websites geteilte Informationen des Nutzers zur Verbesserung des Nutzungserlebnisses in Meta-Produkten mittels personalisierter Werbeanzeigen, zur Erbringung von Diensten außerhalb der Meta-Plattformen, zur Verbesserung von Meta-Produkten und zur Unterstützung der Business-Tools-Verwender bei Analysen und Messungen ihrer Anzeigenperformance. Bei einem Nutzer, der optionale Cookies auf Dritt-Apps und -Websites erlaubt, verwendet die Beklagte die individuellen Cookie-Informationen zur Anzeige von relevanter Werbung. Die Einstellungen des Nutzers für Werbung und seine Werbepräferenzen werden dabei „berücksichtigt“, ohne dass die Beklagte näher erläutert, in welcher Form dies geschieht. Ein Nutzer, der - wie die Klagepartei - Cookies der Beklagten über die Plattform-Einstellungen nicht erlaubt, wird zwar bei den Dritt-Websites und -Apps von seinen Plattform-Konten abgemeldet. Selbst nach dem Beklagtenvorbringen folgt hieraus indes nicht zwingend, dass die Beklagte über ihre Business-Tools keine personenbezogenen Daten dieses Nutzers mehr erhält. Denn sie bestätigt,

dass sie die Informationen in eingeschränktem Umfang für „Sicherheit und Integrität", und nicht für die Anzeige von für den Nutzer relevanter Werbung verwendet. Darüber hinaus könne sie aber auch weiterhin „aggregierte" Informationen zu Aktivitäten in diesen Apps und auf diesen Websites erhalten, während (nur) „persönliche" Cookie-Informationen darin nicht enthalten sein sollen. Zudem wird in den NB-PN ausdrücklich darauf hingewiesen, dass die Beklagte im Fall einer Kontentrennung, und zwar bezogen auf zukünftige und vergangene Aktivitäten, auch weiterhin Informationen zu den Aktivitäten von Apps und Websites erhalte, die sie für Messungen sowie zur Verbesserung ihrer Werbesysteme verwenden könne (vgl. Infobox: „Das solltest du wissen").

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

> „Wir bestätigen Werbetreibenden außerdem, welche Werbeanzeigen du gesehen hast, die dich zu einer Handlung veranlasst haben, beispielsweise zum Herunterladen der App eines Werbetreibenden. Wir teilen mit diesen Werbetreibenden und ihren Anbietern jedoch keine Informationen, die für sich genommen dazu verwendet werden können, dich zu kontaktieren oder identifizieren (wie z. B. dein Name oder deine E-Mail-Adresse), es sei denn, du gibst uns deine Einwilligung dazu. ..." (vgl. S. 48)

lässt darauf schließen, dass auch ohne Einwilligung des Nutzers bestimmte nutzerbezogene Datenkategorien an Geschäftspartner der Beklagten weitergegeben werden, wenn auch nicht solche, die seine eindeutige direkte Identifizierung ermöglichen.

(3) Die Beklagte kann sich nicht mit Erfolg darauf berufen, die Privatsphäre der Nutzer sei gewahrt, da sie personenbezogene Daten aggregiere, also einzelne Datenpunkte zu Gruppen zusammenfasse, so dass Erkenntnisse aus den gesammelten Informationen mehrerer Personen und nicht aus denen einer einzelnen Person gewonnen werden. Dagegen steht, dass schon wegen der Vielzahl der durch Off-site Aktivitäten bzw. Third-Party Activity Data gewonnenen Datenpunkte und Informationen es zumindest nicht ausgeschlossen erscheint, dass einzelne Nutzer und/oder ihm zugeordnete Events identifizierbar bleiben. Welche Daten kon-

kret aggregiert und von der Beklagten genutzt werden, sei es für eigene Zwecke, sei es, indem sie sie weiterleitet bzw. teilt, wird durch die Datenschutzbedingungen nur beispielhaft und damit unzureichend erläutert wie folgt:

> „Partner, die unsere Analysedienste nutzen
> Menschen setzen auf unsere Produkte, wie Unternehmenskonten, professionelle Tools und Facebook-Seiten, um ihre Unternehmen zu betreiben und zu bewerben. Unternehmen nutzen unsere Analysedienste, um mehr darüber zu erfahren, wie Personen ihre Inhalte, Features, Produkte und Dienste verwenden. Wir verwenden die von uns erfassten Informationen über dich, um diese Dienste bereitzustellen. Wir geben diese Informationen in zusammengefassten Berichten an Partner weiter, die ihnen Aufschluss darüber geben, wie gut ihre Inhalte, Features, Produkte und Dienste abschneiden. So können sie die Erfahrung der Nutzer mit diesen Inhalten, Produkten und Diensten besser verstehen. Diese Berichte aggregieren z. B. folgende Informationen:
> Wie viele Personen mit den Inhalten, Produkten oder Diensten unserer Partner interagiert haben
> Allgemeine demografische Daten und Interessen der Personen, die mit ihnen interagiert haben
> Wie Personen die Produkte und Dienste unserer Partner nutzen, um sich mit Meta-Produkten zu verbinden, und ihre Verbindungs- und Netzwerkleistung
>
> Werbetreibende erhalten auch andere Informationen. ...“

Dass sämtliche nutzerbezogene Informationen aggregiert werden, wird von der Beklagten auch nicht hinreichend substantiiert in Abrede gestellt, da sie hierzu in der Datenschutzerklärung unter „Wie verwenden wir deine Informationen?“ in wesentlichen Punkten unklar und einschränkend mitteilt, „um weniger Informationen zu verwenden, die mit einzelnen Nutzern verknüpft“ seien, diese „in einigen Fällen de-identifiziert, zusammenfasst oder anonymisiert, so dass der Nutzer damit nicht mehr identifizierbar“ sei. Soweit sie in diesem Zusammenhang zur Klarstellung darauf hinweist, dass sie die über Cookies und ähnliche Technologien gesammelten Daten einer Person nicht zur Anzeige von Werbung verwende, wenn diese Person „Meta-Cookies in anderen Apps und auf anderen Websites“ nicht ausdrücklich zulasse (Bl. 210 eA), bezieht sie sich ausschließlich auf (eigene) Werbe- und nicht auf andere, in ihren Nutzungsbedingungen genannten Zwecke, die hierüber hinausgehen.

(4) Schließlich ist auch das Hashen (Verschlüsseln) der von Partnern der Beklagten übermittelten Daten nicht geeignet, ihre Behauptung zu stützen, sie verarbeitete bei fehlender Einwilligung ihrer Nutzer keine personenbezogenen Daten, die ihr mittels Business Tools übermittelt werden. Drittunternehmen übermitteln der Beklagten zwar Kontakt- und Eventdaten ihrer Kunden in gehashter Form bei Vorliegen einer „Cookie-Einwilligung“. Den NB-MBT und den Parametern für Kund:innen Informationen lässt sich aber entnehmen, dass die Beklagte, die ihren Geschäftspartnern die für die Verschlüsselung dieser Daten zu verwendende Technologie im

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

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

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

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

(7) Dies gilt auch hinsichtlich der besonderen Kategorien personenbezogener Daten (im folgenden BKD) i.S.d. Art 9 Abs. 1 DSGVO, da die Datenverarbeitung über die Business-Tools der Beklagten insofern nicht zwischen „einfachen“ und „sensiblen“ personenbezogenen Daten unterscheidet, als sie nicht extrahiert, ob Daten sensibel sind oder nicht (vgl. OGH Wien, a.a.O., Rn. 98 und 99, EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 71, 73; - juris). Zwar untersagt die Beklagte den Verwendern ihrer Business-Tools die Übermittlung von BKD wie Gesundheits- oder Finanzdaten, Informationen von oder über Kindern unter 13 sowie nicht zugelassene IDs wie etwa Sozialversicherungs- oder Kreditkartennummern (vgl. NB-MBT, Abschnitt 1. h., Richtlinie Unzulässige Informationen, „Parameter für Kund*innen-Informationen“). Bei Verstößen hiergegen steht jedoch zumindest für den Zeitraum bis zu den vorstehend zitierten Entscheidungen fest, dass die automatisiert ablaufende Datenverarbeitung der Beklagten sen-

sible Daten objektiv umfasste und der gesamte Verarbeitungsvorgang als "Verarbeitung besonderer Kategorien personenbezogener Daten" zu beurteilen ist (vgl. OGH, a.a.O., EuGH, a.a.O.), was eine für ein Unterlassungsbegehren ausreichende Erstbegehungs-, aber auch eine Wiederholungsgefahr indiziert. Im Übrigen ist kaum vorstellbar, dass bei der Übermittlung von diesen Drittwebseiten an die Beklagte keine sensiblen Daten enthalten sind. Denn schon allein das Aufsuchen oder Registrieren auf entsprechenden Drittwebseiten sowie die dort getätigten Aktionen, wie z.B. Online-Bestellungen, können Rückschlüsse auf Gesundheit, sexuelle Orientierung, Finanzen und Weltanschauung eines Nutzers zulassen.

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

cc) Die Beklagte ist als Verantwortliche i.S.d. Art. 4 Ziff. 7 DSGVO für die Erhebung von über Business-Tools auf Drittseiten erlangten Daten und deren anschließende Weiterverarbeitung passivlegitimiert. Gemäß Art. 4 Ziff. 7 DSGVO ist Verantwortlicher diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine gemeinsame Verantwortung besteht nach Art. 26 Ziff. 1 Satz 1 DSGVO, wenn zwei

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

Diese Verantwortlichkeit kann sie weder durch vertragliche Vereinbarungen mit den Drittanbietern auf diese abwälzen, noch kann sie sich durch etwaige Belehrungen der Drittanbieter im Hinblick auf deren datenschutzrechtlichen Pflichten von der eigenen Verantwortlichkeit freizeichnen, schon weil sie selbst gegenüber ihren Business-tools-Kunden die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO feststellt (“...--Tools Nutzungsbedingungen, Anlage B 5 Seite 5 unter 5 a. ii.). Aus denselben Gründen kann sich die Beklagte daher auch nicht darauf berufen, entsprechend ihren NB-MBT unter Ziff. 5. hinsichtlich bestimmter Verarbeitungszwecke (Abgleich-, Messung- und Analysedienste) lediglich als Auftragsverarbeiter i.S.d. Art. 4 Nr. 9 DSGVO der Drittunternehmer tätig zu werden. Nimmt eine Stelle - wie hier die Beklagte - aus Eigeninteresse auf die Verarbeitung Einfluss und wirkt auf diese Weise neben einem anderen Beteiligten an der Entscheidung über Zweck und Mittel der Verarbeitung mit, führt dies regelmäßig zu einer (gemeinsamen) Verantwortlichkeit (EuGH, Urt. v. 29.7.2019, a.a.O.; Simitis/Hornung/ Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 26 Rn. 25, Art. 4 Nr. 7, Rn. 24, m.w.N., beck-online; BeckOK DatenschutzR/Spoerr, 54. Ed. 01.11.2025, DS-GVO Art. 26 Rn. 18-22, m.w.N. beck-online).

dd) Bei den von der Klagepartei aufgezählten und unstreitig von der Beklagten auch verarbeite-

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

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

(1) Damit der Rechtfertigungsgrund einer Einwilligung der Klagepartei als betroffene Person greift, muss die Beklagte nachweisen, dass die Weitergabe von Daten der Klagepartei an sie von einer auf konkrete Zwecke bezogenen freiwilligen Einwilligung gedeckt ist, vgl. Art. 6, Art 7 Ziff. 2 und 4 DSGVO. Dieser Nachweis ist ihr nicht gelungen. Dies betrifft die im Unterlassungsantrag genannten Verarbeitungsvorgänge der Datenerhebung mittels Business-Tools bei den Drittunternehmen, der Weitergabe an die Server der Beklagten, die Speicherung und die anschließende Verwendung. Unstreitig hat die Klagepartei der Beklagten weder über die "Meta-Cookies in anderen Apps und auf anderen Webseiten" noch über die Schaltfläche "Informationen über deine Aktivitäten" eine Einwilligung zur Nutzung von Business-Tool-Daten erteilt. Eine solche Einwilligung nimmt die Beklagte auch nicht für sich in Anspruch, sie beruft

sich auch nicht auf eine vor dem 25.05.2018 erklärte Einwilligung, die ohnehin unter der Geltung der DSGVO keine rechtfertigende Wirkung mehr entfalten könnte (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 114 - juris). Die Beklagte kann sich auch nicht auf eine etwaig erteilte Einwilligung der Klagepartei auf Drittwebseiten und -Apps berufen, da sich diese nur auf Datenverarbeitungszwecke des Webseiten- bzw. App-Betreibers als Business-Tools Verwender, aber nicht auf diejenigen des Anbieters dieser Technologien bezieht (vgl. EuGH, Urt. v. 29.7.2019 – C-40/17 (Fashion ID) a.a.O., Rn. 97). Es obliegt somit nicht den Drittunternehmen, eine Einwilligung des Nutzers für eine Verarbeitung von Daten für Zwecke der Beklagten einzuholen. Ob die Klagepartei die (Nicht-)Erteilung einer Einwilligung hierin auf Drittseiten substantiiert dargelegt hat, ist daher nicht entscheidend.

(2) Die Beklagte kann sich auch nicht mit Erfolg darauf berufen, sie verarbeite Business-Tools Daten als für die Erfüllung der Verträge mit geschäftsfähigen Nutzern erforderlich gemäß Art. 6 Ziff. 1 lit. b DSGVO. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 98, - juris). Entscheidend ist dabei, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen. Zudem ist bei einem Vertrag, der mehrere Dienstleistungen oder mehrere eigenständige Elemente einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit des Rechtfertigungstatbestandes für jede dieser Dienstleistungen gesondert zu beurteilen (vgl. EuGH, a.a.O., Rn. 100). Dass die Verwendung der Business-Tools und die Verarbeitung der durch sie gewonnenen personenbezogenen Daten zur Nutzung der sozialen Plattform unerlässlich wäre, lässt sich nicht feststellen. Der Betrieb und die Nutzung der streitgegenständlichen Plattform sind vielmehr ohne Einbindung der Business-Tools möglich, was nicht zuletzt die Einführung des Bezahlmodells seit dem 03.11.2023 verdeutlicht. Für fernliegend hält der Senat die Annahme, die Verarbeitung von Business-Tools-Daten sei aus Sicherheits- und Integritätszwecke geboten. Insoweit fehlt es aber schon an nachvollziehbaren, hinreichend konkreten Sachvortrag, dass der Hauptgegenstand des Vertrags, der hier in der Nutzung der Social-media-Plattform der Beklagten liegt, ohne die zusätzliche und außerhalb des eigentlichen Vertragszwecks liegende,

umfassende Verarbeitung von Off-site Daten ihrer Geschäftspartner nicht erfüllt werden könnte, diese also objektiv unerlässlich für den mit der Klagepartei bestehenden Nutzungsvertrag sind.

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

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

(b) Soweit die Beklagte auch insoweit geltend macht, die Speicherung der Off-Site-Daten sei zu Sicherheits- und Integritätszwecken notwendig, trägt dies den Rechtfertigungsgrund des berechtigten Interesses nicht. Denn sie bezieht sich auch in diesem Zusammenhang auf die Datenerhebung mittels Business-Tools, die wiederum als „Einfallstor“ für kriminelle Aktivitäten bzw. Ausnutzung der Systeme diene und der sie durch eine Speicherung/Auswertung dieser Daten begegnen müsse. Diese Begründung ist nicht geeignet, die Verarbeitung von individualisierten und/oder individualisierbaren Nutzerdaten auf ihrer Plattform zu rechtfertigen (so auch LG Stuttgart, Urt. v. 05.02.2025 - 27 O 190/23 -, Rn. 85, -juris; LG Lübeck, Urt. v. 10.01.2025 - 15 O 269/23 -, Rn. 130, -juris). Im Übrigen widerspricht der Vortrag der Beklagten, dass die Daten nur zu Sicherheits- und Integritätszwecken genutzt werden ihren eigenen Informationen (Anlage K 7, Abb.26, Abb. 32), in denen sie mitteilt, dass sie trotz „Trennung“ und/oder „Verknüpfung mit künftigen Aktivitäten aufheben“ weiterhin Informationen zu den Aktivitäten erhält

und diese für „Messungen sowie zur Verbesserung ihrer Werbesysteme“ verwendet. Schließlich steht dieser Vortrag auch nicht im Einklang mit den Informationen, die die Beklagte ihren Nutzern erteilt. Dort heißt es u.a.:

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

Sicherheits- und Integritätszwecke finden hier keine Erwähnung.

(c) Bei der gebotenen Gesamtabwägung nach Art 6 Abs. 1 lit f) DSGVO ist zudem zu berücksichtigten, dass die von der Beklagten angegebene Speicherpraxis mit wesentlichen Grundgedanken der DSGVO nicht im Einklang steht. Die auch nach Vortrag der Beklagten bestehende längerfristige Speicherung von abgeglichenen Daten, also Nutzer-IDs und Event-Daten, begründet sie mit Sicherheits- und Integritätsprozessen, für die sie nach ihrem Sachvortrag „aufgrund deren Komplexität und Feinheiten“ keinen „konkreten Zeitrahmen“ angeben könne, da sie sicherstellen müsse, dass „schwerwiegende oder böswillige Aktivitäten keine negativen Auswirkungen auf die Nutzer, Produkte oder Systeme von Meta haben“. Die „maximalen Aufbewahrungsfristen“ lege sie im Rahmen eines umfassenden, funktionsübergreifenden Überprüfungsprozesses fest, Daten werden „in der Regel bis zu 90 Tage aufbewahrt“, u.U. auch länger. Eine solche Speicherpraxis verstößt gegen Art. 5 Ziff. 1 lit. e DSGVO. In EG 39 S. 8 wird gefordert, „dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt“. Dass die Speicherung sämtlicher zunächst zu Zwecken wie Verbesserung des Erlebnisses für Nutzer von Meta-Produkten, Förderung von Schutz und die Sicherheit auf und außerhalb von Meta-Produkten, für Forschungs- und Entwicklungszwecke, Erhalt der Integrität der Meta-Produkte, für deren Bereitstellung und Verbesserung übermittelter personenbezogener Daten für einen unbestimmten Zeitraum nunmehr mit Sicherheits- und Integritätsprozessen und -interessen begründet wird, ist nicht nachvollziehbar und für den Senat nicht überzeugend.

(d) Schließlich verstößt die streitgegenständliche Datenverarbeitung auch gegen den Grundsatz der Datenminimierung, Art. 5 Ziff 1 lit. c DSGVO, der verlangt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung

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

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

3.

Der Klagepartei steht nach Art. 18 Ziff. 1 lit. b) DSGVO ein Anspruch darauf zu, dass die Beklagte ihre personenbezogenen Daten ab sofort unverändert am gespeicherten Ort belässt, sie nur mit ihrer Einwilligung weiterverarbeitet und erst nach Abschluss des Verfahrens auf ihre Aufforderung hin löscht. Der Antrag ist aufgrund des erkennbaren Rechtsschutzziels, die

Verarbeitung der gespeicherten Daten bis zum Abschluss des Verfahrens zu unterbinden, dahingehend auszulegen, dass damit eine Einschränkung der Verarbeitung i.S.d. Art 18 Ziff. 1 lit. b DSGVO statt der sofortigen Löschung verlangt werden soll und dass sich der Antrag nur auf Daten bezieht, die derzeit bei der Beklagten noch vorhanden sind und die sie nicht bereits z.B. aufgrund Ablaufs interner Speicherfristen gelöscht hat.

Das Recht auf Einschränkung der Verarbeitung kann von der betroffenen Person im Fall einer rechtswidrigen Verarbeitung personenbezogener Daten (lit. b) auch im Zusammenhang mit einem Löschungsverlangen geltend gemacht werden. Die Vorschrift räumt der betroffenen Person ein echtes Wahlrecht ein, denn diese kann in Fällen der rechtswidrigen Verarbeitung statt der Löschung die Einschränkung der Verarbeitung verlangen, denn die betroffene Person hat ein schützenswertes Interesse daran, dass der Verantwortliche die fraglichen Daten nicht unbeschränkt weiterverarbeitet, während er prüft, ob ein Anspruch auf Löschung tatsächlich besteht. Es kann auch auf eine längerfristige oder dauerhafte Einschränkung gerichtet sein, von der vorliegend angesichts der absehbar längeren Verfahrensdauer auszugehen ist (Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 18 Rn. 3, 6, beck-online). Ausdrücklich heißt es in Erwägungsgrund 67, dass in automatisierten Dateisystemen die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen soll. Sichergestellt werden soll hierdurch, dass die personenbezogenen Daten „in keiner Weise weiter verarbeitet und nicht verändert werden können". Hierbei soll auf die Beschränkung in dem System unmissverständlich hingewiesen werden (BeckOK DatenschutzR/Worms, 54. Ed. 1.11.2024, DS-GVO Art. 18 Rn. 15, beck-online).

Die Voraussetzungen der Vorschrift liegen vor, da die Verarbeitung der personenbezogenen Daten der Klagepartei, die die Beklagte gespeichert hat, rechtswidrig war (s.o.).

4.

Der Antrag auf Löschung der unter Ziffer 1 a) und auf Anonymisierung der unter Ziffern 1 b) und 1 c) genannten personenbezogenen Daten ist zulässig und begründet.

a)

Es fehlt insbesondere nicht an einer hinreichenden Bestimmtheit i.S.d. § 253 Abs.2 Nr.2 ZPO. Ein Klageantrag ist hinreichend bestimmt, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens der Klagepartei nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fort-

setzung des Streits im Vollstreckungsverfahren erwarten lässt (vgl. BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn 52 - juris). Vorliegend hat die Klagepartei die zu löschenden und die zu anonymisierenden Daten hinreichend genau bezeichnet. Dass die Beklagte verpflichtet werden soll, die Löschung erst nach Aufforderung durch die Klagepartei durchzuführen, was von einer einseitigen ausserprozessualen Erklärung der Klagepartei abhängt, führt nicht zur Unbestimmtheit des Löschungsantrags. Es handelt sich insoweit um eine aufschiebende Bedingung, deren Eintritt gemäß §§ 726, 731 ZPO bei Beginn der Vollstreckung im Klauselerteilungsverfahren zu prüfen ist (vgl. BGH, Urt. v. 14.12.1998 - II ZR 330/97 - juris). Der dort festgelegte Löschungszeitpunkt spätestens sechs Monate nach rechtskräftigem Abschluss des Verfahrens lässt sich im Vollstreckungsverfahren ohne weiteres ermitteln.

An dem erforderlichen Rechtsschutzinteresse fehlt es nicht deshalb, weil der Klagepartei die Möglichkeit zusteht, die Löschung durch Auswahl in den Datenschutzeinstellungen bei den Optionen "Frühere Aktivitäten Löschen" bzw. "Künftige Aktivitäten trennen" selbst durchzuführen. Denn es ist nicht ersichtlich, dass die Klagepartei hierdurch die Off-Site-Daten nicht lediglich von ihrem Account trennen, sondern die von der Beklagten gespeicherten Daten insgesamt löschen kann. Unter Löschung ist die endgültige Unbrauchbarmachung der Daten zu verstehen. Es muss irreversibel sichergestellt sein, dass die entsprechenden personenbezogenen Daten nicht mehr Gegenstand der (produktiven) Datenverarbeitung sein können (vgl. Kamlah in Plath, Kommentar zur DSGVO, 4. Aufl, Art. 17, Rn 2 - juris). Die Beklagte hat in der mündlichen Verhandlung vor dem Senat (im Parallelverfahren 4 U 296/25) eingeräumt, dass die Trennung nicht die dauerhafte Löschung bedeute, sondern nur die Trennung zum Nutzerkonto.

b)

Der Klagepartei steht entsprechend den Ausführungen unter Ziff. 2 dieser Entscheidung ein Anspruch auf Löschung ihrer in Ziffer 1. a) des Antrages aufgeführten personengebundenen Daten gemäß Art. 17 Abs. 1 b), d) DSGVO zu. Die personenbezogenen Daten der Klagepartei werden unrechtmäßig verarbeitet gemäß Art. 17 Abs.1 d) DSGVO (s.o unter 2.). Die Beklagte hat keine ausreichenden Rechtfertigungsgründe gem. Art. 6 Ziff. 1 Unterabs. 1 DSGVO dargelegt und bewiesen (ebd.). Des Weiteren hat die Beklagte nicht nachvollziehbar dargelegt, wie sie mit von Drittwebseiten übermittelten sensiblen Daten im Sinne von Art. 9 Abs.1 DSGVO verfährt (ebd.). Die Verarbeitung dieser personenbezogenen Daten ist grundsätzlich untersagt.

c)

Der Klagepartei steht auch ein Anspruch auf Anonymisierung der in Ziffer 1 b) und c) aufgeführten Daten zu, Art. 17 DSGVO. Die DSGVO sieht zwar kein ausdrückliches Recht auf Anonymisierung vor, jedoch ist diese ein Minus zur Löschung und damit von Art. 17 DSGVO umfasst. Der Löschpflicht kann auch durch entsprechende Anonymisierung der Daten entsprochen werden (vgl. Meents/Hinzpeter in Traeger/Gabel (Hrsg.) Kommentar zur DSGVO, 2022, § Art. 17, Rn 75; Schaffland/Holthaus in Schaffland/Wiltfang, Kommentar DSGVO 2025, Art. 17, Rn 57a - juris), wenn die betroffene Person die Anonymisierung verlangt. Schließlich kann die betroffene Person den Umfang ihres Löschungsrechts selbst bestimmen, zum Beispiel durch Beschränkung ihres Antrags auf bestimmte Daten, Datenarten aber auch auf bestimmte Formen, Zwecke oder Teile der Verarbeitung (vgl. BGH, Beschl. v. 04.06.2024 - II ZB 10/23, Rn 19 - juris). Im Übrigen wird auch insoweit auf die Ausführungen unter 2. Bezug genommen.

5.

Der Klagepartei steht wegen der streitgegenständlichen Datenverarbeitung ein immaterieller Schadenersatz in aus dem Tenor ersichtlicher Höhe gemäß Art. 82 Ziff. 1 DSGVO zu.

Nach ständiger Rechtsprechung des EuGH erfordert ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DSGVO einen Verstoß gegen Vorschriften der DSGVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. nur EuGH, Urt. v. 04.10.2024 - C-200/23, DB 2024, 2952 Rn. 140; BGH Urt. v. 18.11.2024 - VI ZR 10/24, BGHZ 242, 180 Rn. 21). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft grundsätzlich die Person, die auf der Grundlage von Art. 82 Ziff. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH a.a.O Rn. 141, BGH, a.a.O m.w.N). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruches nach Art. 82 Ziff. 1 DSGVO ein Verschulden des Verantwortlichen. Art. 82 DSGVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DSGVO dem Verantwortlichen (vgl. EuGH, Urt. v. 11.04.2024 - C-741/21, NJW 2024, 1561 Rn. 44 ff. BGH, a.a.O m.w.N). Der europäische Gerichtshof stützt sich auf den 146. Erwägungsgrund, der auf „Schäden“ abstellt, „die einer Person aufgrund einer Verarbeitung entstehen“. Zwar muss der Schaden nicht eine gewisse Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urt. v. 04.05.2023 - C - 300/21, 49, 50 - juris). Allerdings muss der Schaden tatsächlich und sicher entstanden sein (vgl. EuGH, Urt. v. 04.04.2017 - C - 337/15, Rn 91 - juris; vgl. Senat, Urt. v. 10.12.2024 - 4 U 732/24, Rn 17 - juris).

Im Anschluss an die mittlerweile gefestigte Rechtsprechung des Bundesgerichtshofes (Urt. v. 18.11.2024 - VI ZR 10/24 - juris) und des EuGH (Urt. v. 04.09.2025 (C-655/23; Rn 60 - juris) kann bereits ein Kontrollverlust über personenbezogene Daten als Schaden angesehen werden, sofern die betroffene Person nachweist, dass sie tatsächlich einen solchen Schaden - so geringfügig er auch sein mag - erlitten hat, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (vgl EuGH, Urt. v. 04.09.2025 - C-655, Rn 60 - juris). Der Bundesgerichtshof hat hierzu in seinem Urteil vom 18.11.2024 (VI ZR 10/24 - juris) u.a. folgendes ausgeführt:

"Ist dieser Nachweis erbracht, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern."

Die Beklagte verarbeitet die personenbezogenen Daten der Klagepartei ohne Rechtfertigungsgrund gemäß Art. 6 Ziff. 1 DSGVO. Insoweit wird auf die Ausführungen unter 2.) Bezug genommen.

Es ist zudem ein Kontrollverlust eingetreten, denn die Klagepartei hat keine Kenntnis darüber, auf welchen der von ihr besuchten Webseiten die von der Beklagten entwickelten Business-Tools eingesetzt werden, welche Daten dort über sie erhoben sowie an die Beklagte weitergeleitet und in welchem Ausmaß diese Daten bei der Beklagten gespeichert, aggregiert und genutzt werden. Wie bereits ausgeführt, ist die Datenverarbeitung durch die Beklagte besonders umfassend, da sie potenziell unbegrenzte Daten über die Online-Aktivitäten der Nutzer betrifft und das Gefühl auslösen kann, dass das Privatleben der Nutzer kontinuierlich überwacht wird (vgl. EuGH, Urt. v. 04.10.2024 - C-446/21 -, Rn 62, - juris). Dieses Gefühl des ständigen Überwachtwerdens ist eine nachteilige Folge, die über einen "bloßen" Kontrollverlust und die hiermit verbundenen Unannehmlichkeiten hinausgeht und daher einen immateriellen Schaden begründet (vgl. Meyer MMR 2025, 173 (177) m.w.N.). Dies gilt umso mehr, als nach dem hier zugrunde zu legenden Vorbringen anzunehmen ist, dass auch bei verweigerter Einwilligung eines Nutzers über Business-Tools erlangte Daten zu einem Profiling im Sinne des Art. 22 DSGVO verwendet werden. Nach der Rechtsprechung des EuGH (Urt. v. 04.10.2024 – C-446/21 (Schrems) – juris, dort Rn 63) stellt das Erstellen detaillierter Profile der Nutzer in Verbindung mit der zeitlich unbegrenzten Weiterverarbeitung einen schweren Eingriff in die Grundrechte der betroffenen Nutzer, insbesondere auf Achtung ihres Privatlebens und den Schutz personenbezogener Daten dar (EuGH aaO. Rn 63). Dies gilt nach Auffassung des Senats auch in den Fällen – wie hier –, in denen nicht nachgewiesen ist, dass die über Busi-

ness-Tools erlangten Daten für Zwecke der personalisierten Werbung verwendet werden. Dass vorliegend überdies nicht ausgeschlossen werden kann, dass durch die Business-Tools auch BKD im Sinne von Art. 9 Abs. 1 DSGVO von der streitgegenständlichen Datenverarbeitung betroffen sind, verstärkt diesen Eindruck und kann dazu führen, dass Nutzer davon absehen, Webseiten etwa zu Gesundheitsthemen oder zum Sexualleben zu besuchen. Anders als in den sog. Scraping-Fällen werden vorliegend zwar die über die Business-Tools erlangten Daten nicht im Internet veröffentlicht, sondern lediglich bei der Beklagten verknüpft und gespeichert. Im Unterschied zu den Scraping-Sachverhalten, bei denen es im Wesentlichen um die Verknüpfung von Telefonnummer und/oder E-Mail-Anschrift mit einem Facebook-Nutzerkonto geht, erfasst die Verarbeitung von Daten aus den Business-Tools aber eine unabsehbare Vielzahl personenbezogener Daten, darunter je nach Einzelfall auch Gesundheitsdaten oder Daten zur sexuellen Orientierung. Des Weiteren ist die nicht bestehende Möglichkeit der Klagepartei, durch eigenes Handeln die Kontrolle über diese Daten zurückzuerlangen zu berücksichtigen (zu diesen Kriterien vgl. Senat, Urt. v. 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688 Rn. 20, beck-online). Insofern kann vorliegend nicht außer Betracht bleiben, dass weder durch die Änderung der Datenschutzeinstellungen noch durch die Löschung des Kontos eine vollumfängliche Löschung der bei der Beklagten gespeicherten Daten möglich wäre. Der Senat geht nach alledem davon aus, dass bereits dieser abstrakt bestehende Kontrollverlust in Verbindung mit dem nachvollziehbar hieraus abgeleiteten Unsicherheitsgefühl für einen immateriellen Schaden ausreicht, ohne dass die Klagepartei diesen noch weiter individualisieren müsste. Die sehr umfassende Verarbeitung von personenbezogenen Daten durch die Beklagte sowie das allgemeine Gefühl der Beobachtung im privaten Umfeld sind ohne weiteres geeignet, bei jedem davon betroffenen Nutzer negative Gefühle in Form von Sorge und Ärger auszulösen, weshalb diese Empfindungen bei der Bemessung des immateriellen Schadens berücksichtigt werden können, ohne dass es auf weiteren Vortrag ankommt, welche Daten genau erhoben worden sind (so wohl auch Ehmann/Selmayr/Nemitz, 3. Aufl., DS-GVO Art. 82 Rn. 17; Kühling/Buchner/Bergt, 4. Aufl., DS-GVO Art. 82 Rn. 18c). Das unbestimmte Gefühl einer Überwachung ihres Verhaltens nicht nur im Internet liegt nachvollziehbar darin begründet, dass die Klägerseite nicht weiß und auch nicht wissen kann, welche und wie viele Daten die Beklagte aus ihrer Privat- und Intimsphäre über sie gesammelt hat und auch nicht weiß und wissen kann, was die Beklagte mit diesen Daten macht (so auch LG Leipzig, Urt. v. 04.07.2025 - 5 O 2351/23 -, Rn. 72 ff., Juris). Der Senat hält für diesen sich bereits aus abstrakten Überlegungen ergebenden und jeden einzelnen Nutzer betreffenden Schaden einen immateriellen Schadensersatz in Höhe von 1.500 € für ausreichend und angemessen. Bei dieser Bemessung geht der Senat davon aus, dass die Klagepartei einen einheitlichen Anspruch

auf immateriellen Schadensersatz aus Art. 82 Ziff. 1 DSGVO geltend macht, der sich auf eine Vielzahl einzelner, nicht konkretisierter Datenschutzverstöße der Beklagten stützt, aber in einem einheitlichen Geschehen (dem fortlaufenden Einsatz der Business-Tools) wurzelt. Auf den von der Beklagten erhobenen Verjährungseinwand kam es hierfür nicht an, weil sie eine Kenntnis der Klagepartei vor Klageerhebung weder behauptet noch unter Beweis gestellt hat.

Eine höhere immaterielle Entschädigung hätte die auf den Einzelfall bezogene Darlegung der Klagepartei erfordert, infolge der streitgegenständlichen Datenverarbeitung eine psychische Beeinträchtigung erlitten zu haben. Unabhängig vom Nachweis eines Kontrollverlusts reicht für einen Anspruch auf einen immateriellen Schadensersatz nämlich auch die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, um einen Schadensersatzanspruch zu begründen (vgl. EuGH, Urt. v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 67 – MediaMarktSaturn; vom 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 85 – Natsionalna agentsia za prihodite). Die Befürchtung samt ihren negativen Folgen muss dabei ordnungsgemäß nachgewiesen sein (vgl. EuGH, Urt. v. 20.07.2024 – C-590/22, DB 2024,1676 Rn. 36 – PS GbR; vom 14.12.2023 – C-340/21, NJW 2024, 1091 Rn. 75-86 – Natsionalna agentsia za prihodite). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (vgl. EuGH, Urt. v. 20.06.2024 – C-590/22, DB 2024, 1676 Rn. 35 – PS GbR; v. 25.01.2024 – C-687/21, CR 2024, 160 Rn. 68 – MediaMarkt-Saturn). Sind derartige psychische Beeinträchtigungen infolge einer Anhörung des Betroffenen nachgewiesen, ist der Entschädigungsbetrag in einer Höhe festzusetzen, die über dem im Falle eines bloßen Kontrollverlustes zuzusprechenden Betrag liegt (BGH, Urt. v. 18.11.2024 – Rn VIII 2 c) cc)). Zu einer solchen emotionalen Betroffenheit hat die Klagepartei jedoch keinerlei individualisierbare Anhaltspunkte vorgetragen; der Vortrag ihrer Prozessbevollmächtigten ist vielmehr identisch mit demjenigen in zahlreichen Parallelverfahren. Ihre Anhörung nach § 141 ZPO hält der Senat bei dieser Sachlage nicht für geboten.

6.

Der Klagepartei steht kein Anspruch auf Erstattung von außergerichtlichen Anwaltskosten zu, §§ 280, 286 BGB, denn es ist nicht ersichtlich, dass diese Kosten erforderlich waren. Bei der Beurteilung der Frage, ob und in welchem Umfang der dem Geschädigten zustehende Schadensersatzanspruch gemäß § 249 Abs. 1 BGB auch die Erstattung von Rechtsanwaltskosten umfasst, ist zwischen dem Innenverhältnis des Geschädigten zu dem für ihn tätigen Rechtsanwalt und dem Außenverhältnis des Geschädigten zum Schädiger zu unterscheiden (BGH,

Beschl. v. 23.06.2022 - VII ZR 394/21 - juris). Voraussetzung für einen Erstattungsanspruch ist grundsätzlich, dass der Geschädigte im Innenverhältnis zur Zahlung der in Rechnung gestellten Kosten verpflichtet ist und die konkrete anwaltliche Tätigkeit im Außenverhältnis aus der maßgeblichen Sicht des Geschädigten mit Rücksicht auf seine spezielle Situation zur Wahrnehmung seiner Rechte erforderlich und zweckmäßig war (BGH, Beschl. v. 23.06.2022, a.a.O.).

Ob eine vorprozessuale anwaltliche Zahlungsaufforderung im Innenverhältnis des Mandanten zum Rechtsanwalt eine Geschäftsgebühr nach Nr. 2300 VV RVG auslöst oder als der Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 Satz 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 VV RVG abgegolten ist, bestimmt sich nach Art und Umfang des im Einzelfall erteilten Mandats. Erteilt der Mandant den unbedingten Auftrag, im gerichtlichen Verfahren tätig zu werden (vgl. Vorbemerkung 3 Abs. 1 Satz 1 VV RVG), lösen bereits Vorbereitungshandlungen die Gebühren für das gerichtliche Verfahren aus, und zwar auch dann, wenn der Anwalt zunächst nur außergerichtlich tätig wird. Für das Entstehen der Geschäftsgebühr nach Nr. 2300 VV RVG ist dann kein Raum mehr (BGH, Beschl. v. 23.06.2022, a.a.O.). Anders liegt es, wenn sich der Auftrag auf die außergerichtliche Tätigkeit des Anwalts beschränkt oder der Prozessauftrag jedenfalls unter der aufschiebenden Bedingung erteilt wird, dass zunächst vorzunehmende außergerichtliche Einigungsversuche erfolglos bleiben. Ein lediglich (aufschiebend) bedingt für den Fall des Scheiterns des vorgerichtlichen Mandats erteilter Prozessauftrag steht der Gebühr aus Nr. 2300 VV RVG nicht entgegen (BGH, Beschl. v. 23.06.2022,a.a.O.).

Die Beauftragung eines Rechtsanwalts zur außergerichtlichen Vertretung im Sinne der Nr. 2300 VV RVG soll schnelle und einverständliche Regelungen ohne Einschaltung der Gerichte ermöglichen. Sie ist zweckmäßig und regelmäßig erforderlich, wenn der Versuch einer - vom Gesetzgeber gewünschten - außergerichtlichen Streiterledigung nicht von vornherein ausscheidet, wie etwa im Falle einer ernsthaften und endgültigen Erfüllungsverweigerung. Ist der Schädiger bekanntermaßen zahlungsunwillig und erscheint der Versuch einer außergerichtlichen Forderungsdurchsetzung auch nicht aus sonstigen Gründen erfolgversprechend, sind die dadurch verursachten Kosten nicht zweckmäßig (vgl. BGH, a.a.O.).

Vorliegend ist schon nicht dargelegt, dass die Klagepartei ihren Anwälten einen auf eine außergerichtliche Tätigkeit beschränkten Auftrag oder einen aufschiebend bedingten Prozessauftrag erteilt hätte. Unabhängig davon war die außergerichtliche Tätigkeit nicht zweckmäßig, weil mit einer auch nur teilweisen Erfüllung der Forderungen vernünftiger Weise nicht gerech-

net werden konnte. Der Klagepartei und ihren Prozessbevollmächtigten musste bei Begründung des Mandatsverhältnisses klar sein, dass die Beklagte vorgerichtlich nicht auf die Forderungen eingehen würde. Wie schon in den Masseverfahren bei den Scraping Fällen hat sich die Beklagte weder vorgerichtlich noch nach Klageerhebung auf Verhandlungen eingelassen. Bei vernünftiger Betrachtung der Sachlage war nicht zu erwarten, dass die Beklagte sich bei dem zu erwartenden Masseverfahren zu den Business-Tools mit mehreren Tausend Klageparteien und zahlreichen Anträgen, die letztendlich ihr Geschäftsmodell in Frage stellen, auf die Forderungen einlassen würde.

Unabhängig davon enthält das vorprozessuale Aufforderungsschreiben der Anwälte der Klagepartei - bis auf die Zahlungsforderung - keine verzugsbegründenden Mahnung. Vielmehr wird die Beklagte darin letztendlich aufgefordert, sich in Zukunft an die Regelungen der DSGVO zu halten. So wird sie z.B. aufgefordert, die Daten zu löschen, sobald sie dazu aufgefordert wird und anzuerkennen, dass sie auf Anfrage der Klagepartei Auskunft erteilen wird sowie eine Verarbeitung ohne wirksame Einwilligung zu unterlassen hat. Lediglich die Aufforderung, an die Klagepartei ein Schmerzensgeld von 5.000 EUR zu zahlen, enthält eine Aufforderung zur Leistung.

7.

Der Anspruch auf Zinsen seit Rechtshängigkeit ergibt sich aus §§ 291, 288 BGB.

III.

1.

Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 10, 713 ZPO.

Die Revision ist nicht zuzulassen. Der Senat verkennt dabei nicht, dass die hier streitgegenständliche Sachverhaltskonstellation in der erstinstanzlichen Rechtsprechung sehr unterschiedlich beurteilt wird. Eine grundsätzliche Bedeutung der Rechtssache im Sinne des § 543 Abs. 2 Nr. 1 ZPO folgt hieraus indes nicht. Dies würde voraussetzen, dass eine klärungsbedürftige Rechtsfrage im Streit steht, die der BGH noch nicht entschieden hat und die in der obergerichtlichen Rechtsprechung unterschiedlich beurteilt wird oder in der Literatur in gewissem Umfang umstritten ist (Zöller-Feskorn, ZPO, 36. Aufl. § 543 Rn 13 m.w.N.). Allein der Umstand, dass zu einer Sachverhaltskonstellation zahlreiche Parallelverfahren anhängig sind und ein Interesse an einer gleichlautenden Entscheidung besteht, reicht insofern nicht aus. Vorlie-

gend besteht eine solche unterschiedliche Beurteilung in der obergerichtlichen Rechtsprechung aber nicht, das Urteil des OLG München vom 18.11.2025 (14 U 1068/25 e n.v.) wirft keine klärungsbedürftigen Rechtsfragen auf und gelangt ebenfalls zu einer Verurteilung der Beklagten wegen eines Verstoßes gegen den Grundsatz der Datenminimierung. Zwar hat das OLG München dort einen gleichlautenden Feststellungsantrag für zulässig gehalten und ist lediglich zu einer immateriellen Entschädigung in Höhe von 750,- € gelangt, ohne dabei allerdings einen abstrakten Rechtssatz aufzustellen, der von der Rechtsprechung des Senats im vorliegenden Fall abweicht. Die hier zugrunde liegenden Rechtsfragen, insbesondere die Frage, ob sich die Beklagte für die einwilligungslose Verarbeitung von Daten aus den Business-Tools auf Art. 6 lit f) DSGV berufen kann und unter welchen Voraussetzungen ein Kontrollverlust einen immateriellen Schaden im Sinne des Art. 82 DSGVO begründet, sind durch die Rechtsprechung des EuGH geklärt. Eine abweichende obergerichtliche oder höchstrichterliche Rechtsprechung, die weitere Rechtsfragen aufwirft, was im Rahmen von § 543 Abs. 2 Nr. 2 ZPO die Zulassung der Revision erfordern würde, gibt es – bislang - nicht. Die vorliegende Fallgestaltung wirft nach Auffassung des Senats vielmehr vorwiegend die tatsächliche Frage auf, welche Daten die Beklagte in der hier streitgegenständlichen Konstellation in welchem Ausmaß verarbeitet und welche Anforderungen an den hierfür zugrunde zulegenden Vortrag und an die Beweislast zu stellen sind.

2.

Die Streitwertfestsetzung beruht auf § 3 ZPO. Der Feststellungsantrag war mit 1.000 EUR zu bemessen. Für den Unterlassungsantrag war ein Streitwert von 2.000 EUR festzusetzen. Der Verpflichtungsantrag und die Anträge auf Löschung und Anonymisierung waren mit jeweils 500 EUR zu bewerten. Der Schadenersatzantrag bemisst sich nach dem Zahlbetrag.