Landgericht Leipzig

Zivilkammer

Aktenzeichen: **05 O 1196/24**

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

[redacted]

- Kläger -

Prozessbevollmächtigte:
BK Baumeister & Kollegen Verbraucherkanzlei, Viktoria-Luise-Platz 7, 10777 Berlin, Gz.: DTS-013318-24

gegen

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

- Beklagte -

Prozessbevollmächtigte:
[redacted]

wegen Feststellung, Auskunft und Unterlassung

hat die 5. Zivilkammer des Landgerichts Leipzig durch

Richter [redacted] als Einzelrichter

auf Grund der mündlichen Verhandlung vom 30.01.2026 am 12.03.2026

für Recht erkannt:

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks "Facebook" unter dem Benutzernamen „[redacted]" die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem 25.05.2018 nicht gestattet:

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

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

sowie folgende personenbezogene Daten der Klagepartei

b) auf Websites

-die URLs der Websites samt ihrer Unterseiten
-der Zeitpunkt des Besuchs
-der „Referrer" (die Website, über die der Benutzer zur aktuellen Website gekommen ist),
-die von der Klagepartei auf der Website angeklickten Buttons sowie

-weitere von der Meta „Events“ genannte Daten, die die Interaktionen der Klagepartei auf der jeweiligen Website dokumentieren

c) in mobilen Dritt-Apps

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

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

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

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

Wahl der Beklagten zu löschen.

5. Die Beklagte wird verurteilt, an die Klagepartei eine Entschädigung in Höhe von 5.000,- EUR nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 20.06.2024 zu zahlen.

6. Im Übrigen wird die Klage abgewiesen.

7. Die Kosten des Rechtsstreits trägt die Beklagte.

8. Das Urteil ist gegen Sicherheitsleistungen i.H.v. 22.000,- EUR vorläufig vollstreckbar.

Beschluss:

Der Streitwert wird auf 15.000,00 EUR festgesetzt.

Tatbestand

Die Klagepartei macht im Zusammenhang mit der Verwendung und Bereitstellung sog. „Meta Business Tools“ durch die Beklagte wegen behaupteter rechtswidriger Verarbeitung personenbezogener Daten Feststellungs-, Unterlassungs-, Löschungs- und Schadensersatzansprüche geltend.

Die Beklagte betreibt u.a. die sozialen Netzwerke Instagram und Facebook.

Die Klagepartei nutzt ausschließlich privat das Netzwerk Facebook unter dem Nutzernamen „[redacted]“ seit dem 27.06.2011.

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), 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. 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“. 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, 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 Pro-

dukte. …

b. Vorbehaltlich von Abschnitt 1.d teilen wir keine Business-Tool-Daten, die du uns bereitstellst, 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 Datenverarbeitungsbedingungen 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 … die Mittel und Zwecke festlegst, erkennen du und … 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 …, 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 … zusammen mit diesen Nutzungsbedingungen für Business-Tools. … bleibt für jegliche Verarbeitung dieser Daten nach deren Übermittlung an … ein unabhängiger Verantwortlicher gemäß Artikel 4 (7) DSGVO.

iii. Du bleibst bzw. … 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. 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 Da-

ten 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, die wiederum auf eine Datenschutzrichtlinie (aktualisierte Fassung vom 26.06.2024) und eine sog. Cookie-Richtlinie 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). 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. Offsite-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“

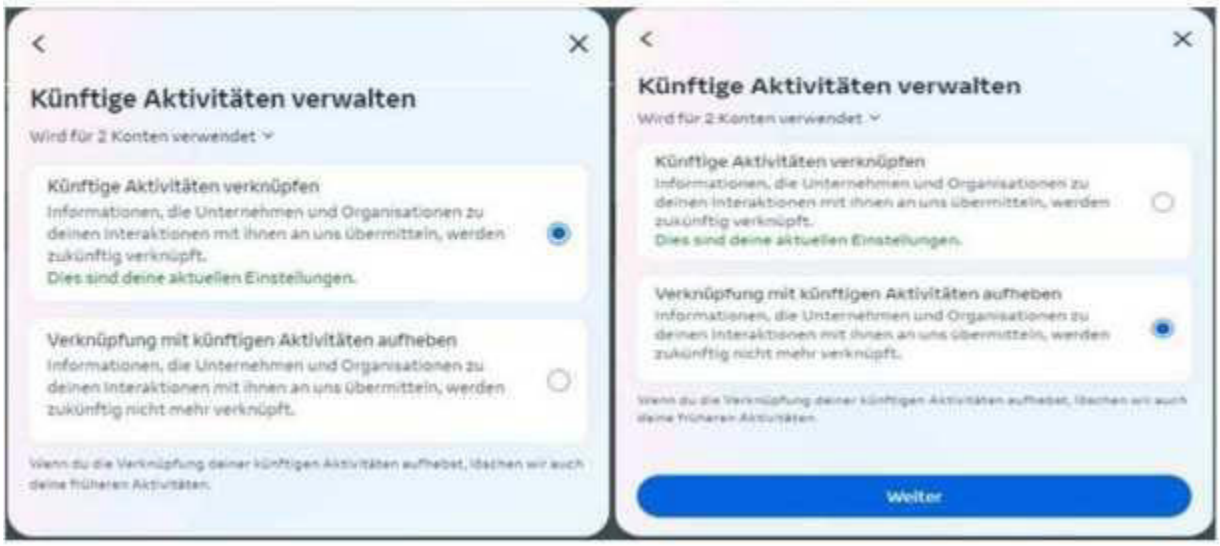
Nach Auswahl „Bestimmte Aktivitäten trennen“ erscheint die Mitteilung:

„…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 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, lösche 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.

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. 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 Server 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 zuletzt:

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks "Facebook" unter dem Benutzernamen [redacted] die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem 25.05.2018 nicht gestattet:

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

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

sowie folgende personenbezogene Daten der Klagepartei

b) auf Websites

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

c) in mobilen Dritt-Apps

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

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

3. Die Beklagte wird verurteilt, die über die aktuelle Speicherung hinausgehende Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO sämtlicher unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits von der Beklagten verarbeiteten personenbezogenen Daten bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzli-

chen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, bis zur Erfüllung des Löschungsanspruchs nach rechtskräftigem Abschluss des Verfahrens zu unterlassen, insbesondere diese nicht an Dritte zu übermitteln.

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

5. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 5.000,00 EUR beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 26.04.2024, zu zahlen.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte 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 Drittunternehmen getroffen, 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 übertra-

gen werden, bis eine Einwilligung eingeholt worden sei; hierüber habe die Beklagte auch informiert. 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.

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.

Entscheidungsgründe

Die zulässige Klage hat auch in der Sache überwiegend Erfolg.

I. Die Klage ist vollumfänglich zulässig.

1. Das Landgericht Leipzig ist in internationaler, sachlicher und örtlicher Hinsicht zuständig.

a) Die internationale Zuständigkeit der deutschen Gerichtsbarkeit ergibt sich aus Art. 79 Abs. 2 S. 2 (i.V.m. Art. 82 Abs. 6) DSGVO. Gem. Art. 79 Abs. 2 S. 1 DSGVO sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Daneben dürfte auch Art. 18 Abs. 1 EuGVVO die internationale Zuständigkeit begründen (so OLG Dresden, Urt. v. 10.12.2024, Az. 4 U 815/24, GRUR-RS 2024, 38639 Rn. 2).

aa) Das Gericht verweist zur Herleitung der Verantwortlichkeit der Beklagten i.S.d. DSGVO in unmittelbarem Bezug auf die Plattform umfassend auf die Ausführungen des LG Lübeck (Urt. v. 10.1.2025 – 15 O 269/23, GRUR-RS 2025, 81 Rn. 25): *„Die Beklagte ist Verantwortliche bzw. Auftragsverarbeitende im Sinne der DSGVO. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte hat vorliegend als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden, sodass sie insoweit als Verantwortliche im Sinne der DSGVO anzusehen ist (vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris; vgl. im Einzelnen auch unten); sie ist auch keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.“*

bb) Die Beklagte ist nach dem tatsächlichen Vortrag der Klägerseite ebenfalls Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die streitgegenständlichen Business Tools. Insoweit wird auf die zutreffenden Ausführungen des LG Stuttgart verwiesen (Urt. v. 24.10.2024, Az. 12 O 170/23, GRUR-RS 2024, 36702 Rn. 23): „*Die Beklagte trägt selbst vor, dass Drittunternehmen Business Tools der Beklagten auf ihrer Website oder in ihrer App integrieren und sich dazu entscheiden können, Kundendaten mit der Beklagten zu teilen, um bessere und interaktivere Inhalte und Werbeanzeigen zu erstellen und ein Publikum für Werbekampagnen aufzubauen. Es führt zu keinem anderen Ergebnis, dass die Drittunternehmen – auch – maßgebliche Pflichten gegenüber den Besuchern ihrer Website und/oder App haben und insofern die maßgeblich Verantwortlichen für die Installation und Nutzung der streitgegenständlichen Business Tools, die Offenlegung von Informationen gegenüber den Besuchern ihrer Website oder Apps in Bezug auf die Nutzung der Meta Business Tools und die Erhebung und Übermittlung der Daten die Beklagte durch Tools wie die streitgegenständlichen Business Tools sind. Hieraus ergeben sich allenfalls weitere datenschutzrechtliche Ansprüche der Nutzer der jeweiligen Seiten gegen die jeweiligen Betreiber. Maßgeblich ist jedoch, dass die erhobenen Daten letztlich nicht bei den Drittunternehmern zur dortigen Verarbeitung und Nutzung verbleiben, sondern vielmehr zweckgerichtet mit der Beklagten geteilt werden. Ob diese Daten dabei anonymisiert oder sonst verfremdet werden, kann dahinstehen. Im Ergebnis führt die Weitergabe zu einer Personalisierung des Nutzererlebnisses bei der Beklagten und damit zu einer erneuten Nutzung der Daten durch die Beklagte. Dieser Umstand ist der Beklagten auch bewusst, da sie ihre Nutzer um eine entsprechende Einwilligung bei der Einstellung „Informationen über Aktivitäten von Werbepartnern“ bittet und gegen Gebühr auch eine werbefreie Nutzung der Plattform Facebook als werbefreies Abonnement anbietet.“*

b) Die örtliche Zuständigkeit ergibt sich jedenfalls aus § 44 Abs. 1 S. 2 BDSG, da die Klagepartei ihren gewöhnlichen Aufenthaltsort an ihrem Wohnsitz in Grimma im Landgerichtsbezirk Leipzig hat.

2. Auf das streitgegenständliche Vertragsverhältnis ist nach Art. 3 Abs. 1, 6 Abs. 2 der VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO; ABl. 2008 L 177, 6) das von den Parteien gewählte deutsche Recht anzuwenden.

Die Anwendbarkeit der DSGVO ergibt sich in räumlicher Hinsicht aus Art. 3 Abs. 1 DSGVO und sachlich aus Art. 2 Abs. 1 DSGVO. Nach Art. 99 Abs. 2 DSGVO ist die Verordnung seit dem 25.05.2018 unmittelbar in den Mitgliedsstaaten anwendbar. Die streitgegenständliche Datenverarbeitung fand jedenfalls in der Zeit danach statt.

3. Soweit die Anträge aus der Klageschrift vom 06.05.2024 mit der Replik vom 26.03.2025 teilweise geändert wurden, ist dies zulässig.

a) Bei der Änderung der ursprünglichen Klageanträge unter Ziffern 1, 2 und 3 handelt es sich um einen Fall des § 264 Nr. 1 ZPO und damit nicht um eine echte Klageänderung. Eine darüberhinausgehende Klagerücknahme i.S.v. §§ 264 Nr. 2 und 269 Abs. 1 ZPO ist hierin nicht zu erkennen, da die Anträge lediglich präzisiert wurden und eine Veränderung des ursprünglichen Streitgegenstands nicht stattfand (vgl. die Ausführungen von Stein/Roth ZPO § 264 Rn. 6 unter dem Stichwort eines „*unzutreffend formulierten Klageantrags*“, siehe auch OLG Dresden, Urt. v. 1. 12. 2010, Az. 1 U 475/10, NJW-RR 2011, 924, 927).

b) Bei Antrag Ziffer 4 aus der Replik handelt es sich um einen Fall des § 264 Nr. 2 ZPO.

c) Das Fallenlassen der ursprünglichen hilfsweisen Stufenklage stellt hingegen eine Beschränkung des Streitgegenstands nach § 264 Nr. 2 ZPO dar. Da die Änderung der Klage bereits vor der mündlichen Verhandlung erfolgte, war eine Einwilligung der Beklagten nach § 269 Abs. 1 ZPO entbehrlich.

4. Der Antrag gerichtet auf die Feststellung, dass der Nutzungsvertrag der Parteien die Verarbeitung der aufgeführten Daten nicht gestattet, ist zulässig.

a) Voraussetzung für die Zulässigkeit der Feststellungsklage ist gem. § 256 Abs. 1 ZPO das Bestehen bzw. Nichtbestehen eines Rechtsverhältnisses sowie ein rechtliches Interesse an der alsbaldigen Feststellung dieses Verhältnisses.

aa) Ein Rechtsverhältnis ist eine aus dem vorgetragenen Sachverhalt abgeleitete rechtliche Beziehung von Personen untereinander, die ein subjektives Recht enthält oder aus der ein solches Recht entspringen kann. Nur das Rechtsverhältnis selbst kann Gegenstand der Feststellung sein, nicht Vorfragen oder einzelne Elemente, wohl aber einzelne Rechte, Pflichten oder Folgen eines Rechtsverhältnisses sowie Inhalt und Umfang einer Leistungspflicht (BGH, Urt. v. 22.1.2015, Az. VII ZR 353/12, NJW-RR 2015, 398 Rn. 17). Das Rechtsverhältnis muss hinreichend konkret bezeichnet sein, um eine eindeutige Individualisierung insbesondere in Bezug auf den Umfang der Rechtskraft herstellen zu können (BGH, Urt. v. 4. 10. 2000, Az. VIII ZR 289/99, NJW, 2001, 445). Eine Klage gerichtet auf die bloße Feststellung der Rechtswidrigkeit eines Verhaltens ist unzulässig (BGH, Urt. v. 20.4.2018, Az. V ZR 106/17, NJW 2018, 3441 Rn. 13).

Die aus dem in der Klage vorgetragenen Sachverhalt abgeleitet rechtliche Beziehung ist die Beziehung zwischen dem Kläger und der Beklagten, welche sich aus dem Nutzungsvertrag bei der Nutzung des Netzwerks der Beklagten ergibt. Insoweit erstreckt sich der Feststellungsantrag auf die Frage, ob es der Beklagten anhand der Ausgestaltung dieses Vertrags – in den AGB – gestattet ist, die im Antrag unter Ziff. 1 genannten personenbezogenen Daten zu verarbeiten.

In diesem Zusammenhang nicht erforderlich war es für den Kläger vorzutragen, welche Daten konkret gespeichert wurden. Es reichte aus, für die Datenkategorien Sammelbezeichnungen zu verwenden. Dies folgt daraus, dass eine nähere Bestimmung der einzelnen Datensätze

der Klägerseite aufgrund des fehlenden Vortrags der Beklagten im Rahmen ihrer sekundären Darlegungslast bis zuletzt nicht erfolgt ist. Da der Kläger selbst keinen Einblick in die von der Beklagten verarbeiteten Daten hat, muss es ihm zur Gewährung eines effektiven Rechtsschutzes prozessual gestattet sein, seinen Vortrag auf die ihm bekannten Umstände zu beschränken. Diesem Erfordernis wurde durch die Aufzählung der einzelnen Datenkategorien hinreichend Rechnung getragen.

Entgegen der Ansicht der Beklagten handelt es sich bei dem festzustellenden Rechtsverhältnis nicht um eine abstrakte Feststellung der Rechtswidrigkeit einer Handlung (so aber LG Stuttgart, Urt. v. 05.02.2025, Az. 27 O 190/23, GRUR-RS 2025, 920, Rn. 17). Der hier gestellte Antrag erschöpft sich nicht in der bloßen Feststellung der Rechtswidrigkeit der Datenerhebung, sondern geht darüber hinaus. Beantragt wird, festzustellen, dass der Nutzungsvertrag mit den AGB die Verarbeitung von bestimmten personenbezogenen Daten nicht gestattet. Hierdurch werden die konkreten Rechte und Pflichten des Nutzungsvertrags – insbesondere deren Grenzen nach der DSGVO – der gerichtlichen Überprüfung vorgelegt. Es soll die vertragliche Zulässigkeit des von der Beklagten praktizierten Verhaltens geklärt werden bzw. sollen die zulässigen Grenzen der Datenverarbeitung anhand des Nutzungsvertrags überprüft werden. Über die bloße Feststellung der Unwirksamkeit einer einzelnen AGB-Klausel hinaus soll als Negativtatsache gerichtlich geklärt werden, welche Rechte der Beklagten aus dem konkreten Nutzungsvertrag unter Berücksichtigung der weiteren Umstände, insbesondere des Fehlens einer Einwilligung, – ganz grundsätzlich – nicht erwachsen können. Auch der BGH geht in seiner Rechtsprechung davon aus, dass die Zulässigkeit eines Verhaltens anhand eines konkreten Vertrags der Überprüfung in Gestalt der Feststellungsklage zugänglich ist (BGH, Urt. v. 20. 2. 2008, Az. VIII ZR 139/07, NJW 2008, 1303, Rn. 9).

bb) „Ein rechtliches Interesse an der Feststellung des Rechtsverhältnisses ergibt sich, wenn dem Recht oder der Rechtsposition eine gegenwärtige Gefahr oder Unsicherheit droht und das angestrebte Urteil geeignet ist, diese Gefahr zu beseitigen“ (Thomas/Putzo/*Seiler*, § 256 ZPO, Rn. 13 m.w.N.). Eine Unsicherheit tatsächlicher Art besteht, wenn Streit zwischen den

Parteien darüber besteht, ob der Beklagte Rechten des Klägers zuwiderhandelt oder er sie ernsthaft bestreitet (BGH, Urt. v. 07.02.1986, Az. V ZR 201/84, NJW 1986, 2507). Das Feststellungsinteresse entfällt dann, sobald dem Kläger ein einfacherer Weg zur Verfügung steht, um sein Ziel zu erreichen. Es fehlt insbesondere dann, wenn der Kläger statt einer negativen Feststellungsklage eine positive Leistungsklage erheben kann (BGH, Urt. v. 13.12.1984, Az. I ZR 107/82, NJW 1986, 1815).

Der Kläger muss sich nicht auf eine Leistungsklage, gerichtet auf Unterlassung der Datenverarbeitung, verweisen lassen, da die Reichweite seines Rechtsschutzinteresses, welches er mit der Feststellungsklage geltend macht, über die Unterlassung der Datenverarbeitung allein hinausgeht (so auch LG Ellwangen (Jagst), Urt. v. 06.12.2024, Az. 2 O 222/24, amtlicher Ausdruck, mitgeteilt durch die Klägerseite; a.A. LG Lübeck, Urt. v. 10.01.2025, Az. 15 O 269/23, GRUR-RS 2025, 81, Rn. 33 ff. mit der Begründung, dass sich die Feststellungsklage in den parallel gestellten Leistungsanträgen, gerichtet auf Schadensersatz und Unterlassung, vollständig erschöpfe). Die Klärung der streitgegenständlichen Rechtsfrage ist auch für weitere Folgeansprüche von Bedeutung, denen durch den bloßen Unterlassungsantrag nicht hinreichend Rechnung getragen wird. Zudem wird mit der Feststellungsklage dem von der Rechtsprechung des BGH anerkannten Ziel der Prozessökonomie Rechnung getragen (vgl. BGH, Urt. v. 9.11.2022, Az. VIII ZR 272/20 NJW 2023, 1567 Rn. 30).

Es kann insoweit eine Parallele zur zulässigen Feststellung einer Schadensersatzpflicht „dem Grunde nach“ bei nicht abgeschlossenen Schadensentwicklungen gezogen werden. In diesen Fällen reicht bereits die entfernte Möglichkeit, dass weitere Folgeschäden aus demselben (abgeschlossenen) haftungsbegründenden Ereignis zu erwarten sind, aus, um ein Feststellungsinteresse zu begründen (BGH, Urt. v. 15.7. 1997, Az. VI ZR 184/96, NJW 1998, 160). Der Sachvortrag zur Wahrscheinlichkeit gehört dabei zur materiellen Klagebegründung (Thomas/Putzo/*Seiler*, § 256 ZPO, Rn. 14). Dies muss erst recht im hier vorliegenden Fall gelten, bei dem das haftungsbegründende Verhalten noch nicht abgeschlossen ist, sondern weiter fortdauert, indem die streitgegenständliche Datenverarbeitung weiter stattfindet. Kann in einem Schadensersatzprozess zulässigerweise die Feststellung begehrt werden, dass die

Beklagtenseite verpflichtet ist, sämtliche materiellen und immateriellen Schäden aus einem bestimmten (Unfall-)Ereignis auszugleichen, so ist die hier vorliegende Feststellungsklage das Pendant hierzu. Bei der Feststellung der Schadensersatzverpflichtung ist das haftungsbegründende Ereignis abgeschlossen und liegt vollständig in der Vergangenheit; anders im hier vorliegenden Fall: die Schadenszufügung hat noch kein Ende gefunden. Dem Kläger verbleibt in dieser Konstellation nur die Möglichkeit, feststellen zu lassen, dass der Nutzungsvertrag die Form der Datenerhebung, deren Zulässigkeit sich aber die Beklagte berühmt, nicht erlaubt ist.

Aus Sicht des Gerichts ist es im hiesigen Fall nach dem Sachvortrag der Klägerseite wahrscheinlich, dass dem Kläger weitere Ansprüche wegen der streitgegenständlichen Datenverarbeitung bereits jetzt zustehen oder zustehen werden. Da der Kläger gegenwärtig noch nicht alle bisherigen und künftigen Datenschutzverstöße und deren konkrete Handlungsformen benennen kann, wäre er bei der Ablehnung eines Feststellunginteresses gezwungen, für jeden weiteren klageweise geltend gemachten Anspruch, der seinen Ursprung in der hier streitgegenständlichen Datenverarbeitung hat, die Rechtswidrigkeit der Datenverarbeitung erneut darzulegen und ggfs. zu beweisen. Insofern wäre er einem erheblichen Prozessrisiko ausgesetzt. Es würde zudem eine Mehrbelastung der Gerichte bedeuten. Dies kann durch eine vorgreifliche Feststellungsklage – und allein durch diese – verhindert werden. Der Kläger befürchtet nach seinem Sachvortrag, dass die Beklagte die von ihr gesammelten Daten an Dritte weitergibt oder bereits weitergegeben hat und sie somit weitere potenziell rechtswidrige Handlungen verübt. Diese Befürchtungen hat die Beklagte nicht ausgeräumt. Insbesondere hat sie durch ihre fehlende prozessuale Erklärung zu den klägerischen Behauptungen zur Überzeugung des Gerichts zu erkennen gegeben, dass sie trotz prozessualer Wahrheitspflicht einen intransparenten Umgang mit Nutzerdaten auch gegenüber dem Gericht praktiziert. Schließlich ist es dem Kläger unbenommen, auch in Zukunft einen weiteren immateriellen Schaden, der aus der fortdauernden Rechtsverletzung resultiert, geltend zu machen. Der Unterlassungstitel bietet insoweit lediglich die Möglichkeit, als Grundlage zur Festsetzung von Ordnungsmitteln gem. § 890 ZPO herangezogen zu werden. Er ist jedoch gerade keine Grundlage für weitere Schadensersatzansprüche und damit nicht äquivalent.

Eine Entscheidung des Gerichts in Bezug auf den Feststellungsantrag ist geeignet, die Unsicherheit der Parteien zu beseitigen, indem sie klarstellen kann, ob die Verarbeitung der personenbezogenen Daten anhand des Nutzungsvertrags gestattet ist. Die Entscheidung bietet den Parteien eine „Richtschnur“ (Thomas/Putzo/*Seiler*, § 256 ZPO, Rn. 14) für ihr zukünftiges Verhalten.

Die Beklagte berühmt sich bis zuletzt auch prozessual mit der Aussage, die Datenverarbeitung, so wie sie im Antrag unter Ziff. 1 dargestellt wird, werde von ihr nicht vorgenommen, da der Kläger eine Einwilligung in die Datenverarbeitung nicht abgegeben habe. Darüber hinaus erklärt sie jedoch im Widerspruch zu der ersten Aussage, dass sie personenbezogene Daten, welche sie von Drittunternehmen über die Business Tools erhalten hat, zu anderen Zwecken rechtmäßig verarbeitet. Die Beklagte setzt demnach das von der Klägerseite zur rechtlichen Prüfung vorgelegte Verhalten bewusst oder unbewusst fort. Insofern bedarf es einer gerichtlichen Klärung.

Schließlich hat der Kläger auch ein alsbaldiges Feststellungsinteresse, da er die Nutzung seines Accounts auf dem Beklagtennetzwerk fortsetzen möchte. Eine sofortige Klärung der Nutzungsverhältnisse ist für die weitere Nutzung von Relevanz.

b) Der Feststellungsantrag ist hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO. Soweit die Beklagte meint, dass der Kläger konkret vortragen müsse, welche Websites und Apps Dritter die Business Tools nutzen, kann dies nicht überzeugen. Der Kläger hat mit der Anlage „Liste häufig besuchter Websites in Deutschland mit Meta Pixel“ hinreichend dargelegt, dass die Vielzahl der von einem nicht näher bestimmten Internetnutzer regelmäßig aufgerufenen Websites die Business Tools der Beklagten nutzt. Bei der Liste der Websites handelt es sich um einen Querschnitt von Websites, von denen ein Internetnutzer im Regelfall mindestens eine Seite pro Tag aufruft. Die Websites bilden sämtliche Kategorien der Internetnutzung ab (Nachrichten, Politik, Gesundheit, Sexualität, Religion, Finanzen usw.). Es kann nach allgemeiner Lebenserfahrung unterstellt werden, dass Internetnutzer Websites aus der dargelegten Liste aufrufen. Würde das Gericht im Rahmen der Darlegungslast dem Kläger

abverlangen, dass er jede von ihm besuchte Website der letzten Jahre im Sinne eines Browserverlaufs offenlegen müsste, würde der Sinn einer auf die Verletzung von Datenschutzvorschriften gestützten Klage ad absurdum geführt werden, da es gerade das klägerische Ziel ist, die Erhebung von personenbezogenen Daten durch die Beklagte zu verhindern, und damit auch Informationen über den eigenen Browserverlauf – soweit nur der Beklagten bekannt – vor anderen geheim zu halten.

Soweit die Beklagtenseite die Formulierung des ursprünglichen Antrags aus der Klageschrift „bei rechtskonformer Auslegung des Nutzungsvertrages der Partei zur Nutzung des Netzwerkes ‚Facebook‘“ als zu unbestimmt moniert hat, wurde der Antrag mit der Klageänderung aus der Replik vom 05.09.2024 entsprechend angepasst, sodass hierüber nicht mehr zu entscheiden war.

5. Auch die Unterlassungsanträge sind zulässig. Dem Kläger stehen keine einfacheren Mittel zur Verfügung, die streitgegenständliche Datenerhebung und weitere -verarbeitung zu verhindern. Soweit die Beklagte in ihren Einstellungen ermöglicht, dass eine Trennung der Schnittstelle zwischen den Business Tools und dem Nutzerkonto des Klägers möglich ist, beschränkt sich dies allein auf die Zwecke der Bereitstellung personalisierter Werbung. Stets beziehen sich die Ausführungen der Beklagten auf die "streitgegenständliche Datenverarbeitung", wobei sie diese abweichend von dem gerichtlich festgelegten Streitgegenstand der Datenverarbeitung durch die Business Tools im Allgemeinen nur auf die Datenverarbeitung zu Werbezwecken beschränkt. Die Beklagte spricht deshalb in diesem Zusammenhang von durch "Werbepartner[n] bereitgestellte Informationen". Darüber hinaus findet die Datenverarbeitung weiterhin dauerhaft unstreitig zu Integritäts- und Sicherheitszwecken statt. Zudem ist unstreitig, dass die Datenerhebung und -verarbeitung innerhalb der Business Tools und die Weiterleitung der Daten an die Beklagte in jedem Fall praktiziert wird. Da beide Unterlassungsanträge ein unterschiedliches Rechtsschutzziel verfolgen – einmal die Neuerfassung und -verarbeitung von Daten mittels der Business Tools und das andere Mal die über die aktuelle Speicherung hinausgehende Verarbeitung bereits erhobener Daten – besteht hinsichtlich beider Anträge ein gesondertes

Rechtsschutzinteresse.

6. Schließlich ist der Antrag auf Löschung der unter Ziffer 1 a) und auf Anonymisierung der unter Ziffern 1 b) und 1 c) genannten personenbezogenen Daten zulässig. Er ist insbesondere hinreichend bestimmt. Insoweit schließt sich das Gericht den überzeugenden Ausführungen des OLG Dresden an:

> *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 Fortsetzung 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.*

(OLG Dresden, Urt. v. 3.2.2026 – 4 U 292/25, BeckRS 2026, 1138 Rn. 72, beck-online).

II. Die Klage ist überwiegend begründet.

1. Der Feststellungsantrag hat in der Sache Erfolg.

Der Nutzungsvertrag zwischen den beiden Parteien gestattet die Verarbeitung der durch die Klägerseite aufgeführten personenbezogenen Daten seit dem 25.05.2018 nicht. Die dem Urteil zugrunde zulegenden Datenverarbeitungsvorgänge sind nicht von einer Einwilligung der Klägerseite abgedeckt. Die Beklagte kann sich insbesondere nicht auf eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO berufen, da der Kläger eine entsprechende Einwilligung in den Profileinstellungen seines Accounts nicht erteilt hat. Sonstige Rechtfertigungsgründe nach Art. 6 und 9 DSGVO hat die Beklagte nicht hinreichend vorgetragen.

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

Wie der EuGH im Urteil vom 04.07.2023 ausführt (Urt. v. 4.7.2023, Az. C-252/21, NJW 2023, 2997), ist für den Fall, dass keine Einwilligung i.S.v. Art. 6 Abs. 1 UnterAbs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a DSGVO vorliegt, zu prüfen, ob die Verarbeitung jedenfalls gem. Art. 6 Abs. 1 UnterAbs. 1 Buchst. b bis f DSGVO gerechtfertigt ist. Nach Art. 5 DSGVO trägt der Verantwortliche die Beweislast dafür, dass *„die Daten u. a. für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.“*

In seiner Entscheidung vom 4.7.2023 hat der EuGH (a.a.O. = NJW 2023, 2997) die Anforderungen an die Rechtfertigung einer Datenverarbeitung nach den o.g. Vorschriften präzisiert. Er führt wie folgt aus:

„4. Art. 6 I UAbs. 1 Buchst. b der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als im Sinne dieser Vorschrift für die Erfüllung eines Vertrags, dessen Vertragsparteien die betroffenen Personen sind, erforderlich angesehen werden kann, wenn diese Verarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte.

5. Art. 6 I UAbs. 1 Buchst. f der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich im Sinne dieser Vorschrift angesehen werden kann, wenn der fragliche Betreiber den Nutzern, bei denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses absolut notwendig ist und wenn sich aus einer Abwägung der einander gegenüberstehenden Interessen unter Würdigung aller relevanten Umstände ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten dieser Nutzer gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.

6. Art. 6 I UAbs. 1 Buchst. c der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nach dieser Vorschrift gerechtfertigt ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche gemäß einer Vorschrift des Unionsrechts oder des Rechts des betreffenden Mitgliedstaats unterliegt, tatsächlich erforderlich ist, diese Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel steht und diese Verarbeitung in den Grenzen des absolut Notwendigen erfolgt.

7. Art. 6 I UAbs. 1 Buchst. d und e der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, grundsätzlich – vorbehaltlich einer Überprüfung durch das vorlegende Gericht – nicht als im Sinne von Buchst. d erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, oder als im Sinne von Buchst. e für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, angesehen werden kann."

In der Entscheidung vom 04.07.2023, C-252/21, führt der EuGH zudem aus (EuGH, a.a.O., NJW 2023, 2997, Rn. 239 ff.):

„Desgleichen wird das vorlegende Gericht nach Maßgabe von Art. 6 Abs. 1 Un-

terabs. 1 Buchst. e DSGVO zu beurteilen haben, ob Meta Platforms Ireland mit einer Aufgabe betraut ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, etwa im Hinblick auf die Forschung zum Wohle der Gesellschaft oder die Förderung von Schutz, Integrität und Sicherheit, wobei es angesichts der Art und des im Wesentlichen wirtschaftlichen und kommerziellen Charakters der Tätigkeit dieses privaten Wirtschaftsteilnehmers allerdings wenig wahrscheinlich erscheint, dass ihm eine solche Aufgabe übertragen worden ist.

Außerdem wird das vorlegende Gericht gegebenenfalls zu prüfen haben, ob die von Meta Platforms Ireland vorgenommene Datenverarbeitung unter Berücksichtigung ihres Umfangs und ihrer erheblichen Auswirkungen auf die Nutzer des sozialen Netzwerks Facebook in den Grenzen des unbedingt Notwendigen erfolgt.“

In ihren Schriftsätzen beruft sich die Beklagte allein auf eine Datenverarbeitung zum Zwecke der Sicherheit und Integrität ihrer Systeme, d.h. auf Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO:

„Meta wird Informationen dieses Nutzers, die über Cookies und ähnliche Technologien erhobenen wurden, nur für begrenzte Zwecke, wie Sicherheits- und Integritätszwecke, nutzen. Zu diesen Sicherheits- und Integritätszwecken gehören der Schutz und die Schadensverhütung (z. B. die Sicherheit von Kindern und die Bekämpfung potenzieller krimineller Aktivitäten (einschließlich gefährlicher Organisationen) und von Hassrede) sowie die Bekämpfung bestimmter bekannter Sicherheitsbedrohungen, wie z. B. die Bedrohungen der Cybersicherheit (z. B. durch Hackerangriffe, Cyberspionage). Zur Veranschaulichung: Meta‘s Systeme können überprüfen, ob eine IP-Adresse, die in Daten enthalten ist, die durch die Meta Business Tools übermittelt wurden, deckungsgleich ist mit einer von relativ wenigen IP-Adressen, die mit in der Vergangenheit identifizierten Bedrohungen in Verbindung steht.“

Über diesen pauschalen Vortrag hinaus trägt die Beklagte nicht weiter substantiiert vor. Der übrige Vortrag reicht indes nicht aus, um den strengen Anforderungen des EuGHs zu Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gerecht zu werden. Die Beklagte erklärt nicht, wie perso-

nenbezogene Daten der Nutzer eingesetzt werden können, um den genannten Zwecken gerecht zu werden. Insofern wird bereits dem Erforderlichkeitskriterium des EuGHs nicht hinreichend Rechnung getragen. Zudem wird nicht klar, in welchem Umfang und auf welche Art und Weise personenbezogene Daten erhoben werden. Insofern kann das Gericht keine Überprüfung zur Angemessenheit der Datenverarbeitung vornehmen. Zu den sonstigen Rechtfertigungsgründen innerhalb von Art. 6 DSGVO wurde ebenfalls nicht hinreichend vorgetragen. Da es bereits an diesen Voraussetzungen fehlt, sind erst Recht die strengeren Anforderungen nach Art. 9 DSGVO nicht erfüllt. Im Übrigen verstößt das Vorgehen der Beklagten aus den gleichen Gründen gegen Art. 5 Abs. 2 DSGVO. Nach dem in dieser Vorschrift verankerten Grundsatz der Rechenschaftspflicht muss der Verantwortliche nachweisen können, das die personenbezogenen Daten unter Einhaltung der in Art. 5 Abs. 1 DSGVO genannten Grundsätze erhoben und verarbeitet werden (EuGH, Urt. v. 4.10.2024, Az. C-446/21, NJW 2025, 207 Rn. 55). In Artikel 5 Abs. 1 DSGVO ist unter anderem der Grundsatz der Datenminimierung (lit. c) verankert, der bestimmt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (EuGH, a.a.O, NJW 2023, 2997).

2. Der auf Unterlassung gerichtete Antrag ist begründet.

a) Die Klagepartei hat zwar keinen Unterlassungsanspruch aus Art. 17, 18 DSGVO i.V.m. Art. 79 DSGVO. Art. 17, 18 DSGVO gewähren betroffenen Personen unter bestimmten Voraussetzungen einen Anspruch auf Löschung sowie auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten. Dessen ungeachtet wurde aus der Verpflichtung zur Löschung von Daten zugleich implizit die Verpflichtung hergeleitet, diese Daten künftig nicht wieder zu speichern (LG Berlin II, Urt. v. 11.04.2025, Az. 58 O 72/24, S. 8, amtlicher Ausdruck; einen Unterlassungsanspruch aus Art. 17 DSGVO ebenfalls herleitend OLG Düsseldorf, Urt. v. 05.10.2023, 16 U 127/22, GRUR-RS 2023, 28156 und BeckOK DatenschutzR/Worms, 52. Ed. 1.11.2024, DS-GVO Art. 17 Rn. 77a). Allerdings gewähren sie nach der Rechtsprechung des EuGH (Urteil vom 4.9.2025 – C-655/23 (IP/Quirin Privatbank AG - anders als der Generalanwalt Campos Sánchez-Bordona in seinen Schlussanträgen) Betroffenen keinen Unterlassungsanspruch (NJW 2025, 3137, beck-online). Art. 79 DSGVO eröffne Betroffenen den Zugang zu gerichtlichen Rechtsbehelfen zur Durchsetzung ihrer Rechte aus der DSGVO, be-

gründe aber ihrem Wortlaut nach keinen eigenständigen Unterlassungsanspruch. Nach Ansicht des EuGH steht dieser einschränkenden Auslegung auch nicht das unionsrechtliche Effektivitätsgebot entgegen. Andrerseits werden Unterlassungsansprüche nach nationalem Recht auch nicht von der DSGVO verdrängt:

„Insoweit ist darauf hinzuweisen, dass die DS-GVO zwar eine grundsätzlich vollständige Harmonisierung der nationalen Rechtsvorschriften zum Schutz personenbezogener Daten sicherstellen soll, mehrere ihrer Bestimmungen den Mitgliedstaaten aber ausdrücklich die Möglichkeit eröffnen, zusätzliche – strengere oder einschränkende – nationale Vorschriften vorzusehen, die ihnen ein Ermessen hinsichtlich der Art und Weise der Durchführung dieser Bestimmungen lassen („Öffnungsklauseln“) (EuGH ECLI:EU:C:2024:846 Rn. 57 mwN = NJW 2025, 33 – Lindenapotheke). Zwar enthalten die Bestimmungen von Kap. VIII DS-GVO keine solche spezielle Öffnungsklausel, die es den Mitgliedstaaten ausdrücklich erlaubt, der betroffenen Person, die den Verantwortlichen von einem Verstoß gegen die materiellen Bestimmungen dieser Verordnung abhalten möchte, die Möglichkeit einzuräumen, einen Rechtsbehelf einzulegen, um gegenüber dem Verantwortlichen eine entsprechende Unterlassungsanordnung zu erwirken. Der Unionsgesetzgeber wollte jedoch keine umfassende Harmonisierung der bei einem Verstoß gegen die Bestimmungen dieser Verordnung zur Verfügung stehenden Rechtsbehelfe vornehmen und hat insbesondere eine solche Rechtsbehelfsmöglichkeit nicht ausgeschlossen (vgl. idS EuGH ECLI:EU:C:2024:846 Rn. 59 u. 60 = NJW 2025, 33 – Lindenapotheke). Diese Auslegung wird durch die mit der DS-GVO verfolgten Ziele bestätigt. Diese Verordnung zielt nämlich, wie aus ihrem zehnten Erwgr. hervorgeht, unter anderem darauf ab, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten. Außerdem heißt es im elften Erwgr. dieser Verordnung insbesondere, dass ein wirksamer
Schutz dieser Daten die Stärkung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen erfordert, die personenbezogene Daten verarbeiten und darüber entscheiden (vgl. idS EuGH ECLI:EU:C:2024:846 Rn. 61 = NJW 2025, 33 – Lindenapotheke). Die Möglichkeit für die betroffene Person, Klage gegen den Verantwortlichen auf künftige Unterlassung eines Verstoßes gegen die materiellen Bestimmungen der DS-GVO zu erheben, beeinträchtigt diese Ziele nicht, sondern kann vielmehr die praktische Wirksamkeit dieser Bestimmungen verstärken und damit das mit dieser Verordnung angestrebte hohe

Schutzniveau für die betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten verbessern. Somit stehen die Bestimmungen von Kap. VIII DS-GVO einer nationalen Regelung, die der betroffenen Person eine solche Möglichkeit eines präventiven Rechtsbehelfs einräumt, nicht entgegen (vgl. idS EuGH ECLI:EU:C:2024:846 Rn. 62 u. 73 = NJW 2025, 33 – Lindenapotheke).
Daraus folgt, dass die DS-GVO dem nicht entgegensteht, dass ein Rechtsbehelf zur Erwirkung einer Anordnung, mit der eine etwaige Begehung eines Verstoßes gegen die materiellen Bestimmungen dieser Verordnung – insbesondere durch eine potenzielle Wiederholung einer unrechtmäßigen Verarbeitung – verhindert werden kann, nach den Bestimmungen des Rechts eines Mitgliedstaats, die vor dem angerufenen nationalen Gericht anwendbar wären, zur Verfügung steht“ (NJW 2025, 3137 Rn 47-52, beck-online).

Insoweit lässt sich mangels Sperrwirkung der Unterlassungsanspruch auch auf nationales Recht, also auf § 823 i.V.m. § 1004 BGB stützen.

b) Materielle Voraussetzung des Anspruchs ist die konkrete Gefahr einer rechtswidrigen Verarbeitung personenbezogener Daten. Diese liegt hier vor.

aa) Die Beklagte ist Verantwortliche i.S.d. DSGVO (s.o.) und verarbeitet personenbezogene Daten i.S.v. Art. 4 Nr. 1 und 2 DSGVO in der folgenden Form:

Die Beklagte bietet die streitgegenständlichen Business Tools an, die Dritte auf ihren Apps oder Websites implementieren können. Werden die Business Tools der Beklagten aktiviert, werden personenbezogene Daten auf den Drittwebsites oder -apps erhoben und an die Server der Beklagten weitergeleitet. Entgegen der bisherigen Feststellungen des Gerichts werden die Business Tools nicht in jedem Fall automatisch beim Aufrufen der Website aktiviert. Hierbei handelt es sich nur dann um einen Automatismus, wenn der Dritte keine Einwilligungslogik in seiner Website oder App verwendet. Wird eine Einwilligungslogik verwendet, dann kann die Aktivierung der Business Tools an bestimmte Bedingungen geknüpft werden, etwa dass der jeweilige Nutzer über die Cookie-Consent-Box eine „Einwilligung“ zur Verwendung von (technisch) nicht notwendigen Cookies erteilt.

Es kann unterstellt werden, dass die Klägerpartei im Rahmen ihrer Internetnutzung mit den streitgegenständlichen Business Tools ausgestattete Websites aufgerufen hat, die entweder nicht über eine Einwilligungslogik verfügen und/oder sie Websites aufgerufen hat, bei denen sie auch nicht notwendigen Cookies/Tools zugestimmt hat. Grund hierfür ist, dass die Klagepartei zu keiner Zeit erkennen konnte, welche Websites oder Apps über eine Einwilligungslogik verfügen und welche nicht. Es ist keineswegs so, und das wurde auch nicht von der Beklagten behauptet, dass sämtliche die Conversions API oder sonstige Business Tools verwendenden Drittunternehmen/-apps den Nutzer darüber aufklären, dass überhaupt Business Tools dieser Art verwendet werden. Häufig wird – wenn überhaupt – lediglich über die Verwendung von Meta Pixel oder ähnlichen Cookies informiert, d.h. es erfolgt gerade keine Information über die Verwendung der Conversions API. Schließlich kann der Nutzer in vielen Fällen die Website überhaupt nicht aufrufen, wenn er nicht in die Verwendung von Cookies wie Meta Pixel „einwilligt“, wie das Beispiel der Website „www.spiegel.de“ zeigt. Nach alldem wäre es gerade die Aufgabe der Beklagten gewesen, darzulegen, dass keine Daten vom Kläger über die streitgegenständlichen Business Tools, insbesondere die Conversions API abgeflossen sind, denn sie hat bzw. muss den Überblick darüber haben, auf welchen Websites Daten des jeweiligen Nutzers erhoben und abgeflossen sind. Dafür kann auch folgende Hilfsüberlegung im Bereich der analogen Überwachung angestellt werden: Wird in einem von einer Person A gemieteten Raum eine versteckte Videokamera aufgestellt, die von einer Person B mit Einwilligung von A betrieben wird und nur einen Teil des Raums überwacht, kann sich die Person B im Verhältnis zu einer dritten Person C, die sich im Raum aufgehalten hat und die wissen möchte, was von ihr aufgezeichnet worden ist, nicht darauf berufen, dass C doch zunächst erstmal selbst darlegen und beweisen müsse, dass die Kamera eingeschaltet war und sie sich in dem Teil des Raums aufgehalten hat, sodass die Kamera ihr Verhalten aufzeichnen konnte. Auch in diesem Fall müsste man der Beklagten als Person B im Rahmen der sekundären Beweislast aufgeben, dass sie in den Aufnahmen schaut, ob diese die Person C als Klagepartei aufgezeichnet hat. Ausgehend von dieser Annahme können auch Datenerhebung und Datenabfluss an die Beklagte unterstellt werden. Soweit die Beklagte vorträgt, dass in einem Parallelverfahren vor dem LG Traunstein in der mündlichen Verhandlung durch das erkennende Gericht festgestellt

worden sei, dass die Tools Meta-Pixel der Beklagten beim Aufruf einer der streitgegenständlichen Websites überhaupt nicht aktiviert worden seien, handelt es sich um eine Aussage, die für den streitgegenständlichen Sachverhalt keine erhebliche Bedeutung hat. Das LG Traunstein untersuchte lediglich, ob Cookies (Meta Pixel) der Beklagten aktiviert waren, während es streitgegenständlich insbesondere um die Conversions API geht, die unstreitig für den Nutzer nicht sichtbar sind. Die fehlende Aktivierung der Meta Pixel schließt also gerade nicht aus, dass im Hintergrund die Conversions API aktiv waren.

Nach deren Erhebung verarbeitet die Beklagte die gewonnenen Daten. Das Gericht verweist insoweit auf die überzeugenden Ausführungen des OLG Dresden, die auch auf den hiesigen Fall übertragbar sind:

> *„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 Perso-*

nen 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 („Offsite 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 I./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 di-

rekte 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 Offsite Aktivitäten bzw. Third-Party Activity Data gewonnenen Datenpunkte und Informationen es zumindest nicht ausgeschlossen erscheint, dass einzelne Nutzer und/oder ihm zugeordnete Events identifizierbar bleiben. Welche Daten konkret aggregiert und von der Beklagten genutzt werden, sei es für eigene Zwecke, sei es, indem sie sie weiterleitet bzw. teilt, wird durch die Datenschutzbedingungen nur beispielhaft und damit unzureichend erläutert wie folgt:

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

Wie viele Personen mit den Inhalten, Produkten oder Diensten unserer Partner interagiert haben Allgemeine demografische Daten und Interessen der Personen, die mit ihnen interagiert haben Wie Personen die Produkte und Dienste unserer Partner nutzen, um sich mit Meta-Produkten zu verbinden, und ihre Verbin-

dungs- 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 deidentifiziert, 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. dehasht (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 Busi-*

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

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

(8) Ohne Erfolg beruft sich die Beklagte angesichts dessen darauf, sie habe „freiwillig“ Maßnahmen wie eine Kategorisierung der Datenquellen, eine automati-

sierte Filterung sowie erweiterte Datenbeschränkungen wie beispielsweise das „Core Setup“ 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.

(OLG Dresden, Urt. v. 3.2.2026 – 4 U 292/25, BeckRS 2026, 1138 Rn. 45-54, beck-online).

Soweit die Beklagte im Rahmen des Bestreitens einwendet, dass es sich teilweise um Daten handele, die nach der Eigenart des Internets stets erhoben und verarbeitet werden, kann dies nicht verfangen. Auch diese Daten fallen unter den Anwendungsbereich der DSGVO. Der Verordnungsgesetzgeber war sich dessen bewusst und stellte in Erwägungsgrund 30 fest, dass natürlichen Personen unter Umständen Online-Kennungen wie IP-Adressen, Cookie-Kennungen oder andere Identifikatoren zugeordnet werden können, die mit ihrem Gerät, Softwarean-

wendungen, Tools oder Protokollen zusammenhängen. Im Übrigen geht die Datenverarbeitung der Beklagten über diese technischen Standarddaten weit hinaus.

bb) Rechtfertigungsgründe für die streitgegenständliche Datenverarbeitung liegen nicht vor (s.o.).

c) Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr ist gegeben. Der bereits begangene und fortdauernde Verstoß der Beklagten begründet die tatsächliche Vermutung für seine Wiederholung (BGH, Urt. v. 17.07.2008, Az. I ZR 219/05, GRUR 2008, 996, Rn. 32).

d) Die Androhung des Ordnungsmittels beruht auf § 890 Abs. 2 ZPO. Der Rückgriff auf die nationale Vorschrift ist erforderlich, da die DSGVO mit der Sanktionsnorm in Art. 83 DSGVO keine äquivalente Regelung bereithält, die gleichermaßen geeignet ist, den Unterlassungstitel zur Gewährung effektiven Rechtsschutzes durchzusetzen (so auch LG Landau, Versäumnisurteil vom 26.02.2024, Az. 2 O 239/23, S. 13, amtlicher Ausdruck, mitgeteilt durch die Klägerseite).

3. Auch der weitere Unterlassungsantrag zu 3., der die Weitergabe von bereits erfassten und bei Meta bereits gespeicherten Daten an Dritte unterbinden will, ist begründet, da die Beklagte die unrechtmäßig erlangten Daten nicht ohne Einwilligung der Klagepartei an Dritte weitergeben darf.

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

a) Die in Antrag Ziffer 1. aufgeführten personenbezogenen Daten wurden durch die Beklagte durch die Verwendung der Business Tools unrechtmäßig verarbeitet (s.o.).

b) Soweit die Daten unter Antrag Ziff. 1 lit. b und c anstelle der Löschung die Anonymisierung

der Daten beantragt wird, sieht Art. 17 DSGVO ein solches Recht zwar nicht ausdrücklich vor. Es ist jedoch als „Minus“ von der Norm erfasst (OLG Dresden Endurteil v. 3.2.2026 – 4 U 292/25, BeckRS 2026, 1138 Rn. 75, beck-online).

c) Der klägerische Anspruch auf Löschung bzw. Anonymisierung ist des Weiteren nicht bereits durch die Zurverfügungstellung des Self-Service-Tools der Beklagten erfüllt. Zwar ist der Beklagten die Verwendung von automatisierten Verfahrensweisen zur Löschung bzw. Anonymisierung der Nutzerdaten grundsätzlich zuzubilligen (vgl. Paal/Pauly/*Paal*, 3. Aufl. 2021, DS-GVO Art. 17 Rn. 29), jedoch hat die Beklagte nicht hinreichend dazu vorgetragen, dass die von ihr zur Verfügung gestellten Tools eine vollständige Löschung sämtlicher Daten, insbesondere der unter Antrag Ziff. 1 genannten, ermöglichen. Insofern schließt sich die Kammer den Ausführungen des LG Stuttgart an, das ausführt: "*Der Kläger kann in seinen Datenschutzeinstellungen zwar die Löschung durch Auswahl der Optionen „Frühere Aktivitäten Löschen“ bzw. „Künftige Aktivitäten trennen“ vornehmen. Hierdurch werden die Off-Site-Daten jedoch lediglich vom Account des Klägers getrennt, nicht hingegen gelöscht*" (LG Stuttgart, Urt. v. 05.02.2025, Az. 27 O 190/23, GRUR-RS 2025, 920 Rn. 27). Nach dem Vortrag des Klägers, dem die Beklagte nicht hinreichend entgegengetreten ist, bedeutet die Trennung lediglich eine Pseudonymisierung der Daten, die letztlich umkehrbar ist (s. Art. 4 Nr. 5 DSGVO). Dies ist gerade nicht ausreichend.

d) Schließlich muss sich die Klagepartei nicht auf eine eigene Löschung des Nutzerprofils verweisen lassen. Die Beklagte nimmt im Bereich der Social-Media-Plattformen eine überragende marktübergreifende Stellung ein, welche bereits das Bundeskartellamt i.S.v. § 19a GWB festgestellt hat (BKartA, Beschl. v. 02.05.2022, Az. B6-27/21). Gerade für die Teilhabe am gesellschaftlichen Leben handelt es sich bei den Netzwerken der Beklagten mittlerweile um für den durchschnittlichen Bürger essenzielle Dienstleistungen (vgl. Erwägungsgründe Nr. 1, 3 zur VO 2022/2065), die faktisch nicht durch ein alternatives Netzwerk ersetzt werden können (zusammenfassend zu den Hintergründen siehe *Mohr*, EuZW 2019, 265 unter Bezugnahme auf die Facebook-Entscheidung des Bundeskartellamts vom 06.02.2019). Dem Nutzer ist es deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nut-

zung beendet. Vielmehr muss ihm die Möglichkeit eröffnet bleiben, die Netzwerke der Beklagte zu nutzen, ohne dass die streitgegenständliche Datenverarbeitung über die Business Tools stattfindet.

5. Die Klagepartei hat einen Anspruch auf Ersatz des immateriellen Schadens i.H.v. 5.000 EUR gem. Art. 82 DSGVO nebst Zinsen hieraus im tenorierten Umfang. Ob im Weiteren auch ein Anspruch gem. § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG besteht, kann dahinstehen, da dieser jedenfalls keinen höheren Schadensersatzanspruch begründet.

a) Der haftungsbegründende Tatbestand ist erfüllt. Auf der Seite der Beklagten liegt ein Verstoß gegen die Vorgabe der DSGVO vor (s.o.).

b) Die Klagepartei hat einen immateriellen Schaden erlitten. Ein Schaden i.S.d. Art. 82 DSGVO kann jede materielle oder immaterielle Einbuße sein. Der bloße Verstoß gegen die DSGVO reicht zwar selbst noch nicht für die Begründung eines Schadensersatzanspruchs aus (EuGH, Urt. v. 04.05.2023, Az. C-300/21, GRUR-RS 2023, 8972 Ls. 1), es gibt jedoch umgekehrt auch keine Erheblichkeitsschwelle, deren Überschreitung es festzustellen gilt (siehe nur EuGH, a.a.O., GRUR-RS 2023, 8972). Als Schäden sind insbesondere in der Rspr. bereits anerkannt der Verlust von Kontrolle über personenbezogene Daten oder die Befürchtung der missbräuchlichen Verwendung der eigenen Daten (BGH, Urt. v. 18.11.2024, Az. VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 30 u.a. mit Verweis auf den EuGH). Steht der Kontrollverlust fest, bedarf es darüber hinaus erst einmal nicht der Darlegung besonderer Ängste oder Befürchtungen der betroffenen Person, da diese Umstände lediglich zur Feststellung einer weiteren Schadensvertiefung herangezogen werden können (BGH, a.a.O., GRUR-RS 2024, 31967 Rn. 31).

Nach dem der Klage zugrundeliegenden Tatbestand wurde *„[Das] nahezu gesamte Online-Verhalten des Klägers dokumentiert und in Persönlichkeitsprofilen ausgewertet. Damit ist auch der unantastbare Kernbereich der privaten Lebensgestaltung des Klägers tangiert. Gerade auch dieses sogenannte Profiling stellt einen sehr intensiven Eingriff dar. Nach Erwägungsgrund 60, 63 der DSGVO ist die betroffene Person insbesondere*

darauf hinzuweisen, dass Profiling stattfindet und welche Folgen das hat. Nach Erwägungsgrund 75 stellt insbesondere die Verarbeitung persönlicher Daten zum Zwecke der Erstellung persönlicher Profile ein besonderes Risiko für einen Schaden dar. Dieser führt aus: Die Risiken für die Rechte und Freiheiten natürlicher Personen - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Oberzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhangende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“ (LG Ellwangen (Jagst), a.a.O., S. 42 f.). Hierin liegen in jedem Fall ein erheblicher Kontrollverlust sowie das Risiko einer weiteren missbräuchlichen Verwendung der Daten. Da die Verarbeitung personenbezogener Daten im hiesigen Fall besonders umfangreich ist – sie betrifft potenziell unbegrenzte Datenmengen und hat nahezu die vollständige Überwachung des Online-Verhaltens

des Nutzers zur Folge – ist es nach der Feststellung des EuGHs bereits abstrakt möglich, dass beim Nutzer das Gefühl einer kontinuierlichen Überwachung verursacht wird (EuGH, a.a.O., GRUR 2023, 1131, Rn. 118).

c) Der Schaden ist kausal auf das Verhalten der Beklagten zurückzuführen, da diese den Kontrollverlust insbesondere durch den Einsatz der Business Tools verursacht hat.

d) Art und Umfang des Schadensersatzanspruchs richten sich nach den nationalen Vorschriften in §§ 249 ff. und § 287 BGB i.V.m. den europarechtlichen Vorgaben des haftungsbegründenden Tatbestands in Art. 82 DSGVO.

aa) Nach der Rspr. des EuGHs ermöglicht die DSGVO ausschließlich einen Schadensersatz zum Zwecke des Ausgleichs, nicht auch zur Genugtuung. Die Vorschrift verlangt nicht, dass der Grad der Schwere und die Vorsatzform des Verantwortlichen bei der Schadensbemessung berücksichtigt werden. Im Gegenzug gibt der EuGH den nationalen Gerichten jedoch vor, dass die Höhe des geschuldeten immateriellen Schadensersatzes „seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung“ (zum Ganzen EuGH, Urt. v. 20.06.2024, Az. C-182/22, C-189/22, NJW 2024, 2599). Im Einzelnen:

(1) Der EuGH stellt klar, dass die Art. 83 und 84 DSGVO, welche im Wesentlichen Strafzwecke erfüllen, nicht im Rahmen von Art. 82 DSGVO herangezogen werden dürfen, da die Vorschrift auf den Ausgleich für erlittene Einbußen abzielt (EuGH, a.a.O., NJW 2024, 2599 Rn. 22). Abschreckungs- und Strafzwecke sind der Vorschrift damit nicht zugänglich, sodass ein sog. Strafschadensersatz ausscheidet.

(2) In Ermangelung eigener europäischer Regelungen zur Bestimmung der Höhe des Anspruchs nach Art. 82 DSGVO haben die nationalen Gerichte nach der Rspr. des EuGHs die bestehenden nationalen Vorschriften im Lichte der Äquivalenz und Effektivität des Unionsrechts anzuwenden (EuGH, a.a.O., NJW 2024, 2599 Rn. 27).

(3) Soweit es der EuGH ausschließt, dass im Rahmen der Ausgleichsfunktion des Schadensersatzanspruchs i.S.v. Art. 82 DSGVO ein möglicher Vorsatz des Verantwortlichen oder der Grad der Schwere des Verstoßes berücksichtigt wird, gibt er jedoch auch zu erkennen, dass der Schadensersatz der Höhe nach den konkret erlittenen Schaden vollständig ausgleichen muss (EuGH, a.a.O., NJW 2024, 2599 Rn. 29).

(4) Mit Blick auf den Vergleich physischer, materieller und immaterieller Schäden rekurriert der EuGH auf den 146. Erwägungsgrund der DSGVO und weist insoweit darauf hin, dass *„[d]er Begriff des Schadens … im Lichte der Rechtsprechung des EuGH weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht“*, und dass *„[d]ie betroffenen Personen … einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten [sollten]“* (EuGH, a.a.O., NJW 2024, 2599 Rn. 36). Weiterhin führt er aus, dass durch die nationalen Vorschriften zur Umsetzung des immateriellen Schadensersatzanspruchs die Ausübung der durch das Unionsrecht verliehenen Rechte, insbesondere der DSGVO, nicht unmöglich gemacht oder übermäßig erschwert werden darf (EuGH, a.a.O., NJW 2024, 2599 Rn. 34.)
Hiermit bringt der EuGH zum Ausdruck, dass an der deutschen Rechtsprechung, die bislang immateriellen Schadensersatz bei Persönlichkeitsrechtsverletzungen grundsätzlich nur höchst ausnahmsweise und insgesamt lediglich in geringem Umfang zugesprochen hat, bei der Anwendung der DSGVO nicht festgehalten werden darf (so auch Kühling/Buchner/*Bergt*, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18a; Ehmann/Selmayr/*Nemitz*, 3. Aufl. 2024, DS-GVO Art. 82 Rn. 38). Daraus folgt nicht zuletzt, dass trotz der Beschränkung auf den bloßen Ausgleich der erlittenen Nachteile, die Höhe des Schmerzensgeldes über die in der nationalen Rechtsprechungspraxis etablierten Beträge aus Schmerzensgeldtabellen o.ä. hinausgehen kann (so auch Kühling/Buchner/*Bergt*, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18d m.w.N.). Ein „Sich-Einfügen“ in die bisherige nationale Rechtsprechungspraxis stünde geradezu im Widerspruch zur europarechtsautonomen Auslegung des Schadensersatzanspruchs gem. Art. 82 DSGVO. Soweit andere Gerichte teilweise auf nationale Schadensersatzansprüche wie § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG zurückgreifen, um die erweiterten Schutzkatego-

rien dieser Ansprüche einbeziehen zu können (Genugtuung und Prävention) – letztlich um die vermeintlichen Restriktionen des EuGHs mithilfe dieser Ansprüche dogmatisch zu umgehen – ist dieses Vorgehen ob der oben genannte Gründe redundant.

(5) Der EuGH betont bei alldem, dass der Schadensersatzanspruch nach Art. 82 DSGVO neben den Sanktionen des Art. 83 DSGVO ebenfalls geeignet sein muss, die Einhaltung der Vorschriften der DSGVO sicherzustellen (EuGH, a.a.O., NJW 2024, 1561 Rn. 62).

bb) Die Höhe des Schadensersatzanspruchs ist nach der nationalen Vorschrift des § 287 ZPO zu schätzen. Nach § 287 Abs. 1 S. 1 ZPO entscheidet das Gericht nach Würdigung aller Umstände nach freier Überzeugung. Hierbei handelt es sich um das Einfallstor für die o.g. europarechtlichen Vorgaben. Nach § 287 Abs. 1 S. 2 ZPO steht es schließlich im Ermessen des Gerichts, ob es im Rahmen der Schadensbemessung eine Beweisaufnahme durchführt.

(1) Anknüpfungspunkte für die Bemessung eines immateriellen Schadensersatzanspruchs muss hier vordergründig der auf der Klägerseite eingetretene Verlust der Daten sein. Dieser ist hinsichtlich des unterschiedlichen grundrechtlich garantierten Schutzniveaus der betroffenen Daten zu differenzieren. Dies gilt insbesondere, wenn besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO betroffen sind (OLG Dresden, Urt. v. 10.12.2024, Az. 4 U 808/24, ZD 2025, 221 Rn. 20).
Zudem sind vor allem der Umfang der gesammelten Daten und die Dauer des Verstoßes zw. der Verletzungshandlung zu berücksichtigen. Hierbei handelt es sich um Kategorien zur Feststellung der Schadenstiefe bzw. -intensität, die nicht gleichzusetzen sind mit dem Grad der Schwere des Verstoßes, den der EuGH für nicht berücksichtigungsfähig erklärt (EuGH, a.a.O., NJW 2024, 2599 Rn. 26). Darüber hinaus kann die Möglichkeit des Betroffenen an der Wiedererlangung seiner Daten bzw. der Kontrolle über diese eine Rolle spielen (OLG Dresden, a.a.O., ZD 2025, 221, Rn. 20).
Weiterhin hat das Gericht bei der Schadensschätzung für den Wert der personenbezogenen Daten einen entsprechenden Anknüpfungspunkt festgelegt. Hierfür hat es auf den Wert personenbezogener Daten für die Beklagte – soweit dieser geschätzt werden konnte – abgestellt,

zudem auf den allgemeinen Wert personenbezogener Daten auf dem hierfür relevanten legalen oder auch illegalen Markt. Die Berücksichtigung des Wertes der Daten für den Verletzer wird jedenfalls im Bereich der kommerziellen Nutzung auch in der Literatur gefordert (Simitis/Hornung/Spiecker *gen. Döhmann*, Datenschutzrecht, DS-GVO Art. 82 Rn. 31, m.w.N.).

(2) Für das Ausmaß und den Umfang der betroffenen Daten wird auf die Ausführungen weiter oben verwiesen, auch für die Grundrechtssensibilität der betroffenen Daten. Hinzutritt, dass es aufgrund des bis zum Schluss der mündlichen Verhandlung bestehenden Schweigens der Beklagten zur streitgegenständlichen Datenverarbeitung aussichtlos erscheint, dass die Klagepartei konkrete Kenntnis davon erhält, ob sie die Kontrolle der Daten durch Löschung o.ä. wiedererlangen könnte. Zudem ist über die Geständnisfiktion hinaus rein tatsächlich nicht feststellbar, ob und in welchem Umfang die Daten bereits an Dritte weitergegeben wurden und eine Datensicherung auch aus diesem Grund ausgeschlossen ist.
Erschwerend kommt hinzu, dass sogar wenn in Bezug auf die Erhebung und Verarbeitung von Daten zu Zwecken personalisierter Werbung die von der Beklagten vorgesehene Einwilligung abgegeben worden wäre, diese unwirksam gewesen wäre (s.o.).
Für den Wert der Daten für die Beklagte hat das Gericht auf die Feststellungen des BKartA (Beschl. v. 02.05.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) zurückgegriffen. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der Werbeeinnahmen einen Anteil i.H.v. 97 % ausmachte (BKartA a.a.O., Rn. 7). Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O., Rn. 53). Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon über-

zeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studien (siehe nur die Studie "Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?", Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz; Infografik "Preis, den Erwachsene in den USA für personenbezogene Daten aufrufen würden (in US-Dollar)", Statista mit Quelldaten von Morning Consult aus dem Jahr 2019, abgerufen unter https://cdn.statcdn.com/Infographic/images/normal/18449.jpeg).
Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d.h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. Kühling/Buchner/*Bergt*, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18b, beck-online).

(3) Obwohl der BGH in seiner Rspr. (BGH, a.a.O., GRUR-RS 2024, 31967 Rn. 31) ausführt, dass die entwickelten besonderen Befürchtungen und Ängste der betroffenen Person als Grundlage für das Gericht dienen, wie groß der eingetretene Schaden ist, bedurfte es im hiesigen Fall keiner Anhörung, da sich die Klagepartei jedenfalls auf die sich aus der o.g. Reichweite des Schadens ergebende Mindestbeeinträchtigung für den Durchschnittsbetroffenen i.S.d. DSGVO im konkreten Fall berufen kann. Mit dem EuGH (zuletzt Urt. v. 04.10.2024, a.a.O., NJW 2025, 207 Rn. 62) hat die potenziell unbegrenzte Datenverarbeitung der Beklagten zur Folge, dass bei den Betroffenen ein Gefühl der kontinuierlichen Überwachung des Privatlebens eintreten kann. Ausgehend von einem Durchschnittsbetroffenen i.S.d. DSGVO, der sich den o.g. Verletzungshandlungen ausgesetzt sieht, ist es dem Gericht möglich, den hieraus erwachsenden Grad der individuellen Betroffenheit zu schätzen.

(a) Nach der Rechtsprechung des BGH ist es dem Tatgericht nach der nationalen Norm des § 286 ZPO grundsätzlich erlaubt, "allein aufgrund des Vortrags der Parteien und ohne Beweiserhebung festzustellen, was für wahr und was für nicht wahr zu erachten ist" (BGH, Beschl. v. 27.09.2017, Az. XII ZR 48/17, NJW-RR 2018, 249). Obwohl diese Rechtsprechung konkret auf die Überzeugungsbildung des Tatgerichts anhand einer informatorischen Anhörung abzielt, ist sie darüber hinaus auch so zu verstehen, dass das Gericht frei darin ist, seine Überzeugung nach § 286 ZPO jenseits der Strengbeweismittel zu bilden. Dies gilt insbesondere im Falle der Schadensschätzung nach § 287 ZPO, bei der die Freiheit der richterlichen Überzeugungsbildung zusätzlich geweitet ist. Insofern war es dem Gericht freigestellt, auf eine informatorische Anhörung – so wie sie die meisten anderen Gerichte bislang vorgenommen haben – zu verzichten. Bei einer Anhörung wäre nach Überzeugung des Gerichts gerade kein weiterer Erkenntnisgewinn zu erwarten gewesen, der über die Mitteilung des im Allgemeinen eher diffusen Gefühls des Datenverlusts und der Verunsicherung hinausgeht. Grund hierfür ist, dass es gerade das Problem der klägerischen Partei und auch des Gerichts ist, festzustellen, was konkret die Beklagte mit den Daten vorhat bzw. was sie bereits jetzt unternimmt. Da dies bis zuletzt nicht bekannt wird, können sich sich Erwartungen oder Befürchtungen nicht auf ein bestimmtes Verhalten konkretisieren. Dies kann und darf der betroffenen Person nicht zum Nachteil gereichen.

(b) Wie der EuGH in seiner Rechtsprechung jenseits des Datenschutzrechts, bspw. im Markenrecht, betont, ist auch unionsrechtlich für eine Dienstleistung, die sich an ein allgemeines Publikum richtet, Prüfungsmaßstab für die Gerichte ein normal informierter, angemessen aufmerksamer und verständiger Durchschnittsverbraucher (siehe nur EuGH, Urt. v. 29. 04. 2004, Az. C-456/01 P und C-457/01 P, GRUR Int 2004, 631, Rn. 35; Urt. v. 08.10.2020, Az. C-456/19, GRUR 2020, 1195, Rn. 32). Diese Grundsätze lassen sich auch auf den hiesigen Fall übertragen, da die Dienstleistungen bzw. das Produkt der Beklagten dem allgemeinen Verkehr gegenüber eröffnet sind. Damit lässt sich neben der spezifischen Betroffenheit einer einzelnen Person auch die des Durchschnittsbetroffenen i.S.d. DSGVO feststellen. Soweit – wie im vorliegenden Fall – die vorgetragene spezifische Betroffenheit nicht über das Maß der

allgemeinen Betroffenheit hinausgeht und sich damit keine Schadensvertiefung aus dem klägerischen Vortrag ableiten lässt, kann sich das Gericht allein auf die allgemeine Beeinträchtigung des Durchschnittsbetroffenen i.S.d. DSGVO beziehen.
Das Gericht konnte daher ohne auf das jeweilige subjektive Empfinden eines konkreten Klägers abstellen zu müssen, eine durchschnittliche, aufgeklärte und verständige betroffene Person zu Grunde legen, und deren Betroffenheit als Maßstab für einen Mindestschaden zu nehmen.

(4) Die Mindestbeeinträchtigung ist ohne das Hinzutreten weiterer Umstände bereits besonders schwerwiegend und hebt sich maßgeblich von den sog. Scraping-Fällen ab, in denen ein Mindestschaden i.H.v. 100 EUR für den bloßen Kotrollverlust für angemessen erachtet wird (siehe nur OLG Dresden, a.a.O., ZD 2025, 221 Rn. 20 m.w.N.). Anders als in den Scraping-Fällen ist die Quantität und Qualität der streitgegenständlichen Daten um ein Vielfaches größer, sodass der Mindestschaden weitaus höher einzustufen ist. Die Datenverarbeitung durch die Beklagte stellt nach der Rspr. des EuGHs per se einen schweren Eingriff in die durch Art. 7 und 8 GrCh gewährleisteten Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten dar (EuGH, a.a.O., NJW 2025, 207 Rn. 63), der nicht gerechtfertigt ist.
Die Verletzung dieser Grundrechte wird auch durch den Durchschnittsbetroffenen i.S.d. DSGVO als erhebliche Beeinträchtigung im o.g. Sinne wahrgenommen. Der aufgeklärte und verständige Durchschnittsbetroffenen i.S.d. DSGVO wird sich der Bedeutung und Tragweite der über ihn gesammelten Daten bewusst, denn er kennt die Relevanz von personenbezogenen Daten innerhalb einer digitalisierten Gesellschaft und Wirtschaft (s.o. zur Wahrnehmung der Gesellschaft hinsichtlich der Werthaltigkeit von Daten). Der Kontrollverlust über nahezu sämtliche Daten seiner Online-Nutzungsaktivitäten bedeutet für ihn eine dauerhafte und nicht ohne Weiteres zu beseitigende negative Beeinflussung, die sich nach außen hin in unterschiedlichen Sorgen und Ängsten manifestiert. In jedem Falle setzt sich der Nutzer gezwungener Maßen mit dem Verlust der personenbezogenen Daten auseinander und wird hierdurch in Bezug auf sein weiteres Verhalten bei der Nutzung des Internets dauerhaft beeinflusst.

Das Gericht erachtet anhand der obigen Ausführungen in der Gesamtschau im Wege der Schadensschätzung nach § 287 ZPO einen Betrag i.H.v. 5.000 EUR für einen angemessenen Schadensersatz. Im Rahmen der nach § 287 ZPO vorzunehmenden Schadensschätzung sind auch bei Art. 82 DSGVO allgemein die Art, Schwere, Dauer des Verstoßes, Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, frühere einschlägige Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten in die Erwägung mit einzubeziehen (OLG Dresden, Urteil vom 30.11.2021 – 4 U 1158/21, ZD 2022, 159, beck-online). Zu berücksichtigen sind aber auch der Wert der Daten und ihre wirtschaftliche Verwertbarkeit.

Ist unter den Parteien streitig, ob ein Schaden entstanden sei und wie hoch sich der Schaden oder ein zu ersetzendes Interesse belaufe, so entscheidet hierüber gem. § 287 Abs. 1 Satz 1 ZPO das Gericht unter Würdigung aller Umstände nach freier Überzeugung. Aus der Rechtsprechung des EuGH ergeben sich dem BGH zufolge jedoch Vorgaben sowohl in Bezug auf die Untergrenze als auch auf die Obergrenze des nach Art. 82 I DSGVO zu gewährenden Schadensersatzes, die das Schätzungsermessen des Tatgerichts nach § 287 ZPO rechtlich begrenzen (Stögmüller, Immaterieller Schadensersatz bei Datenschutzverstoß, Überblick und Analyse der aktuellen Rechtsprechung zu Art. 82 I DS-GVO, RDi 2025, 200 Rn. 32, beck-online). Auch Erfahrungswerte wie z.B. Schmerzensgeldtabellen können einfließen. Allerdings hat sich zu Art. 82 DSGVO noch keine verlässliche Entschädigungstabelle gebildet. Entschädigungsbeträge fallen für vergleichbare Sachverhalte demnach überraschend unterschiedlich aus. So hat beispielsweise das OLG Dresden bei einer Persönlichkeitsrechtsverletzung durch die Datenerhebung von Vorstrafen des Betroffenen, die lediglich ausnahmsweise und nur unter den Voraussetzungen des Art. 10 DS-GVO zulässig ist, einen Schadensersatz i.H.v. 5.000 EUR zugesprochen (Urteil vom 30.11.2021 – 4 U 1158/21, ZD 2022, 159), obwohl es sich lediglich um einen einmaligen Verstoß handelte, sich aber u.a. auch darauf gestützt, dass nach Erwägungsgrund Nr. 146 DS-GVO der Begriff des Schadens im Lichte der Rspr. des EuGH weit und auf eine Art und Weise ausgelegt werden soll, „die den Zielen dieser Verordnung in vollem Umfang entspricht“ und nach dem Effektivitätsprinzip (effet utile) auch eine abschreckende Sanktion nicht ausgeschlossen sein soll.

Auch vorliegend bei der Bemessung der Schadenshöhe wegen des Einsatzes von Business

Tools für die Betroffenen weist die Ausübung des tatrichterlichen Ermessens nach § 287 ZPO ein weites Spektrum auf. Soweit ein Schaden bejaht wird, sprechen die Landgerichte einen Schadensersatz von 1500 EUR (etwa LG Aachen Urt. v. 21.11.2024 – 12 0 470/23, GRUR-RS 2024, 50751, beck-online; Landgericht Münster, Urteil. v. 12.03.202512 - O 53/24; LG München I Urt. v. 11.11.2024 - 6 0 14304/23) über 2.000 EUR (Landgericht Berlin II Urteil. v. 04.04.2025 - 39 O 56/24, 39 O 67/24, 39 O 57/24, 39 O 97/24, 39 O 218/24, 39 O 184/24) über 2.500 EUR (LG Karlsruhe Urt. v.14.04.2025 - 6 O 72/24) über 3.000 EUR (Landgericht Hamburg Urteil. v. 17.04.2025 - 325 O 261/23) über 5.000 EUR (LG Leipzig Endurteil v. 15.8.2025 – 5 O 1939/24, GRUR-RS 2025, 21426, beck-online; LG Leipzig, Urteil vom 4.7.2025 – 05 O 2351/23, ZD 2025, 580, beck-online; LG Augsburg, Urteil. v. 28.03.2025 -082 0 262/24) bis zu 10.000 EUR (LG Mainz Urt. v. 27.6.2025 – 3 O 29/24, GRUR-RS 2025, 16871, beck-online; LG Ellwangen, Urteil. v. 06.12.2024 – 2 O 222/24) zu. Auch die Oberlandesgerichte, die sich mit diesen Fällen befasst haben, legen in Ausübung ihres Ermessens unterschiedliche Schadensbeträge fest, so von 750 EUR (OLG München Urt. v. 18.12.2025 – 14 U 1068/25) über 1.200 EUR (OLG Naumburg Urteil. v. 06.02.2026 - 9 U 124/24) über 1.250 EUR (OLG Naumburg Urteil. v. 06.02.2026 - 9 U 44/24) bis zu 1.500 EUR (OLG Dresden, Endurteil vom 03.02.2026 – 4 U 292/25).

Aus den vorgenannten, oben im Einzelnen erläuterten Gründen bleibt das Gericht dabei, in Ausübung tatrichterlichen Ermessens einen Schadensersatz in Höhe von 5.000 EUR für angemessen zu halten, da u.a. nach dem als zugestanden anzusehenden klägerischen Vortrag dessen gesamtes im digitalen Bereich stattfindendes Privatleben dauerhaft und nicht nur auf einzelne Aspekte begrenzt aufgezeichnet wurde und immer noch wird. Seit dem Inkrafttreten der DSGVO handelt es sich bei dem als zugestanden anzusehenden Vorgehen der Beklagten um einen solch weitgehenden Verstoß, der den Rahmen der bisher bekannten Fälle bei weitem überschreitet, sodass ein solcher Mindestbetrag ohne Darlegung einer besonderen individuellen Betroffenheit als Schadensausgleich anzusetzen ist.

Das Gericht erachtet anhand der obigen Ausführungen in der Gesamtschau im Wege der Schadensschätzung nach § 287 ZPO einen Betrag i.H.v. 5.000 EUR für einen angemessenen Schadensersatz. Im Rahmen der nach § 287 ZPO vorzunehmenden Schadensschätzung sind auch bei Art. 82 DSGVO allgemein die Art, Schwere, Dauer des Verstoßes, Grad des

Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, frühere einschlägige Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten in die Erwägung mit einzubeziehen (OLG Dresden, Urt. v.- 30.11.2021 – 4 U 1158/21, ZD 2022, 159, beck-online). Zu berücksichtigen sind aber auch der Wert der Daten und ihre wirtschaftliche Verwertbarkeit.

Ist unter den Parteien streitig, ob ein Schaden entstanden sei und wie hoch sich der Schaden oder ein zu ersetzendes Interesse belaufe, so entscheidet hierüber gem. § 287 Abs. 1 Satz 1 ZPO das Gericht unter Würdigung aller Umstände nach freier Überzeugung. Aus der Rechtsprechung des EuGH ergeben sich dem BGH zufolge jedoch Vorgaben sowohl in Bezug auf die Untergrenze als auch auf die Obergrenze des nach Art. 82 I DSGVO zu gewährenden Schadensersatzes, die das Schätzungsermessen des Tatgerichts nach § 287 ZPO rechtlich begrenzen (Stögmüller, Immaterieller Schadensersatz bei Datenschutzverstoß, Überblick und Analyse der aktuellen Rechtsprechung zu Art. 82 I DS-GVO, RDi 2025, 200 Rn. 32, beck-online). Auch Erfahrungswerte wie z.B. Schmerzensgeldtabellen können einfließen. Allerdings hat sich zu Art. 82 DSGVO noch keine verlässliche Entschädigungstabelle gebildet. Entschädigungsbeträge fallen für vergleichbare Sachverhalte demnach überraschend unterschiedlich aus. So hat beispielsweise das OLG Dresden bei einer Persönlichkeitsrechtsverletzung durch die Datenerhebung von Vorstrafen des Betroffenen, die lediglich ausnahmsweise und nur unter den Voraussetzungen des Art. 10 DS-GVO zulässig ist, einen Schadensersatz i.H.v. 5.000 EUR zugesprochen (Urteil vom 30.11.2021 – 4 U 1158/21, ZD 2022, 159), obwohl es sich lediglich um einen einmaligen Verstoß handelte, sich aber u.a. auch darauf gestützt, dass nach Erwägungsgrund Nr. 146 DS-GVO der Begriff des Schadens im Lichte der Rspr. des EuGH weit und auf eine Art und Weise ausgelegt werden soll, „die den Zielen dieser Verordnung in vollem Umfang entspricht“ und nach dem Effektivitätsprinzip (effet utile) auch eine abschreckende Sanktion nicht ausgeschlossen sein soll.

Auch vorliegend bei der Bemessung der Schadenshöhe wegen des Einsatzes von Business Tools für die Betroffenen weist die Ausübung des tatrichterlichen Ermessens nach § 287 ZPO ein weites Spektrum auf. Soweit ein Schaden bejaht wird, sprechen die Landgerichte einen Schadensersatz von 1500 EUR (etwa LG Aachen Urt. v. 21.11.2024 – 12 0 470/23, GRUR-RS 2024, 50751, beck-online; Landgericht Münster, Urteil. v. 12.03.202512 - O 53/24; LG München

I Urt. v. 11.11.2024 - 6 0 14304/23) über 2.000 EUR (Landgericht Berlin II Urteil. v. 04.04.2025 - 39 O 56/24, 39 O 67/24, 39 O 57/24, 39 O 97/24, 39 O 218/24, 39 O 184/24) über 2.500 EUR (LG Karlsruhe Urt. v.14.04.2025 - 6 O 72/24) über 3.000 EUR (Landgericht Hamburg Urteil. v. 17.04.2025 - 325 O 261/23) über 5.000 EUR (LG Leipzig Endurteil v. 15.8.2025 – 5 O 1939/24, GRUR-RS 2025, 21426, beck-online; LG Leipzig, Urteil vom 4.7.2025 – 05 O 2351/23, ZD 2025, 580, beck-online; LG Augsburg, Urteil. v. 28.03.2025 -082 0 262/24) bis zu 10.000 EUR (LG Mainz Urt. v. 27.6.2025 – 3 O 29/24, GRUR-RS 2025, 16871, beck-online; LG Ellwangen, Urteil. v. 06.12.2024 – 2 O 222/24) zu. Auch die Oberlandesgerichte, die sich mit diesen Fällen befasst haben, legen in Ausübung ihres Ermessens unterschiedliche Schadensbeträge fest, so von 750 EUR (OLG München Urt. v. 18.12.2025 – 14 U 1068/25) über 1.200 EUR (OLG Naumburg Urteil. v. 06.02.2026 - 9 U 124/24) über 1.250 EUR (OLG Naumburg Urteil. v. 06.02.2026 - 9 U 44/24) bis zu 1.500 EUR (OLG Dresden, Endurteil vom 03.02.2026 – 4 U 292/25).

Aus den vorgenannten, oben im Einzelnen erläuterten Gründen bleibt das Gericht dabei, in Ausübung tatrichterlichen Ermessens einen Schadensersatz in Höhe von 5.000 EUR für angemessen zu halten, da u.a. nach dem als zugestanden anzusehenden klägerischen Vortrag dessen gesamtes im digitalen Bereich stattfindendes Privatleben dauerhaft und nicht nur auf einzelne Aspekte begrenzt aufgezeichnet wurde und immer noch wird. Seit dem Inkrafttreten der DSGVO handelt es sich bei dem als zugestanden anzusehenden Vorgehen der Beklagten um einen solch weitgehenden Verstoß, der den Rahmen der bisher bekannten Fälle bei weitem überschreitet, sodass ein solcher Mindestbetrag ohne Darlegung einer besonderen individuellen Betroffenheit als Schadensausgleich anzusetzen ist.

Das Gericht ist sich bei dieser Entscheidung der Tatsache bewusst, dass das Zusprechen eines Betrags i.H.v. 5.000 EUR ohne das Erfordernis der spezifischen Darlegung einer über das gerichtlich festgestellte Maß der Mindestbeeinträchtigung hinausgehenden Intensität praktisch bedeutet, dass eine Vielzahl von Nutzern der Beklagten ohne größeren Aufwand Klage erheben kann. Dem stehen jedoch keine durchgreifenden Bedenken gegenüber, denn diese Form der privaten Rechtsdurchsetzung ist nach dem Willen des europäischen Gesetzgebers und der Rechtsprechung des EuGHs nach den obigen Ausführungen gerade bezweckt und dient

in Form des sog. Private Enforcement dazu, die Einhaltung der Vorschriften der DSGVO und damit deren Effektivität zu gewährleisten. Die Tendenz des europäischen Gesetzgebers zur Ermöglichung eines Private Enforcement ist dabei in jüngerer Zeit nicht zu verkennen, bspw. im Rahmen des Digital Markets Act (Kersting/Meyer-Lindemann/Podszun/*Dietrich/Jung*, 5. Aufl. 2025, DMA Art. 20-Art. 27 Rn. 54 m.w.N.). Art. 82 DSGVO ist i.d.S. „nur“ eine weitere Facette der Entwicklung hin zu mehr Private Enforcement (so auch Paal/Kritzer, NJW 2022, 2433 Rn. 2). Insoweit ist es gerade kein Grund, der gegen die Zusprechung eines erheblichen Schadensersatzanspruchs spricht, dass nahezu jeder Nutzer der Beklagten gleichermaßen betroffen ist (so aber LG Stuttgart, a.a.O., Rn. 66). Ebenso muss sich der Kläger auch nicht darauf verweisen lassen, dass die Sanktionierung der „Geschäftspraktiken“ der Beklagten nicht Aufgabe zivilrechtlicher Ansprüche sei, sondern es hierfür das öffentliche Recht i.S.e. Public Enforcement gebe (so aber LG Lübeck, a.a.O., Rn. 90).

Nicht anspruchsmindernd i.S.e. widersprüchlichen Verhaltens wirkt sich aus, wenn ein Nutzer die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Aufgrund der überragenden marktübergreifenden Stellung der Beklagten auf Social-Media-Plattformen (s.o.) ist es dem Nutzer, auch wenn er Kenntnis von den Datenschutzverletzungen der Beklagten erlangt nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass ein Nutzer ihre Netzwerke DSGVO-konform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage wird zum Ausdruck gebracht, dass Datenschutzverstöße der Beklagten nicht gleichgültig hingenommen werden, sondern eine DSGVO-konforme Nutzung durchgesetzt werden soll.

Demnach scheidet auch ein Mitverschulden des Geschädigten i.S.v. § 254 BGB aus, wobei für den Schadensersatzanspruch nach Art. 82 DSGVO umstritten ist, ob lediglich unter den Voraussetzungen von Art. 82 Abs. 3 DSGVO ein Ausschluss der Haftung i.S.e. Alles-oder-Nichts-Regelung in Betracht kommt (siehe Kühling/Buchner/*Bergt* DS-GVO Art. 82 Rn. 59 m.w.N. auch der Gegenansicht).

e) Der Kläger hat des Weiteren einen Anspruch auf Verzugszinsen aus der Schadensersatzforderung ab Rechtshängigkeit gem. §§ 286 Abs. 1, 291 Abs. 1 BGB.

6. Der Kläger kann von der Beklagten keine Freistellung seiner vorgerichtlichen Rechtsanwaltskosten verlangen.

Die Beklagte hat bestritten, ein außergerichtliches Aufforderungsschreiben, wie es sich in Anlage K3 findet, erhalten zu haben. Voraussetzung für das Entstehen eines Freistellungsanspruchs ist, dass ein Gebührenanspruch des Prozessbevollmächtigten des Klägers gegen diesen besteht, deren Entstehung wiederum ein außergerichtliches Tätigwerden gegenüber der Beklagten voraussetzt. Hierfür ist der Kläger darlegungs- und beweisbelastet. Auf den spätestens mit der Duplik erhobenen Einwand, keine außergerichtliche Aufforderung erhalten, sondern von dieser erst mit der Klageschrift Kenntnis erlangt zu haben, ist der Kläger inhaltlich nicht weiter eingegangen.

lll. Die Kostenentscheidung beruht auf § 92 Abs. 2 Nr. 1 ZPO. Der Kläger unterliegt lediglich mit den eingeklagten außergerichtlichen Kosten. Dieser Betrag ist jedenfalls als Unterliegen mit weniger als zehn Prozent anzusetzen (vgl. OLG Köln, Urt. v. 2.9.2022, Az. 20 U 266/21 NJOZ 2022, 1325 Rn. 56). Nichts anderes ergibt sich aus der Regelung in § 45 Abs. 1 S. 2 GKG hinsichtlich der vor der Entscheidung des Gerichts zurückgenommenen Hilfsansprüche.

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus § 709 S. 1 ZPO.

lV. Der Streitwert wird nach §§ 63 Abs. 2, 39 Abs. 1, 40, 43 Abs. 1, 48 Abs. 2 Satz 1, 48 Abs. 1 S. 1 GKG i.V.m. §§ 3 ff. ZPO auf insgesamt 15.000 EUR festgesetzt und setzt sich wie folgt zusammen:

- Feststellung: 5.000 EUR
- Beide Anträge auf Unterlassung zusammen: 4.500 EUR
- Antrag auf Löschung und Anonymisierung: 500 EUR
- Entschädigung: 5.000 EUR

Der Antrag auf Zahlung außergerichtlicher Kosten war im Rahmen der Streitwertfestsetzung nicht zu berücksichtigen, da dieser den Gebührenstreitwert gem. § 43 Abs. 1 GKG (auch über § 48 Abs. 1 S. 1 GKG i.V.m. § 4 Abs. 1 S. 1 ZPO) nicht beeinflusst. Die zwischenzeitlich fallengelassenen Hilfsanträge sind gemäß § 45 Abs. 1 S. 2 GKG ebenfalls nicht zu berücksichtigen.

Rechtsbehelfsbelehrung:

Gegen die Festsetzung des Streitwertes findet die **Beschwerde** statt, wenn der Wert des Beschwerdegegenstands 300 EUR übersteigt oder wenn die Beschwerde in dieser Entscheidung zugelassen wurde.

Die Beschwerde ist nur zulässig, wenn sie innerhalb einer Frist von **sechs Monaten**, nachdem die Entscheidung in der Hauptsache Rechtskraft erlangt oder das Verfahren sich anderweitig erledigt hat eingelegt wird.

Ist der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt worden, kann sie noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden.

Die Beschwerde ist bei dem

Landgericht Leipzig
Harkortstraße 9
04107 Leipzig

einzulegen.

Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle eingelegt. Die Beschwerde kann auch zur Niederschrift der Geschäftsstelle eines anderen Amtsgerichts erklärt werden; die Frist ist jedoch nur gewahrt, wenn die Niederschrift rechtzeitig bei dem oben genannten Gericht eingeht.

Die Beschwerde kann auch als elektronisches Dokument eingereicht werden. Das elektronische Dokument muss für die Bearbeitung durch das Gericht gemäß §§ 2 und 5 der Elektronischer-Rechtsverkehr-Verordnung (ERVV) geeignet sein.
Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht. Rechtsbehelfe, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument einzureichen. Das elektronische Dokument muss

1. mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein und gemäß § 4 ERVV übermittelt werden, wobei mehrere elektronische Dokumente nicht mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden dürfen, oder
2. von der verantwortenden Person signiert und auf einem der sicheren Übermittlungswege, die in § 130a Abs. 4 der Zivilprozessordnung abschließend aufgeführt sind, eingereicht werden.

Informationen hierzu können über das Internetportal https://justiz.de/laender-bund-europa/elektronische_kommunikation/index.php aufgerufen werden.

[redacted]
Richter