I-9 U 8/25
7 O 160/23
Landgericht Krefeld

Oberlandesgericht Düsseldorf

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

des Herrn [redacted]

Klägers und Berufungsklägers,

Prozessbevollmächtigte: BK Verbraucherkanzlei Rechtsanwaltsgesellschaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin,

gegen

die **Meta Platforms Ireland Ltd.**, Merrion Road, Dublin 4, D04 X2K5, Irland, vertreten durch die Geschäftsführer David Harris, Majella Goss, Yvonne Cunnane und Anne O'Leary, jeweils ebenda,

Beklagte und Berufungsbeklagte,

Prozessbevollmächtigte: [redacted]

hat der 9. Zivilsenat des Oberlandesgerichts Düsseldorf auf die mündliche Verhandlung vom 09.02.2026 durch den Vorsitzenden Richter am Oberlandesgericht [redacted] den Richter am Oberlandesgericht [redacted] und die Richterin am Oberlandesgericht [redacted]

für Recht erkannt:

Auf die Berufung des Klägers wird das am 06.11.2024 verkündete Urteil der 7. Zivilkammer des Landgerichts Krefeld, Az. 7 O 188/23, unter Zurückweisung des Rechtsmittels im Übrigen teilweise abgeändert und insgesamt wie folgt neu gefasst:

1. Die Beklagte wird verurteilt, an den Kläger 750,00 Euro nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 27.10.2023 zu zahlen.

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

   a) auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten des Klägers, ob direkt oder in gehashter Form übertragen, d.h. E-Mail, Telefonnummer, Vorname, Nachname, Geburtsdatum, Geschlecht, Ort, 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 des Klägers

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

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

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft 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 gemäß Ziffer 2. zu verarbeiten.

4. Die Beklagte wird verpflichtet, sämtliche unter Ziffer 2 aufgeführten, seit dem 25.05.2018 bereits verarbeiteten personenbezogenen Daten ab sofort unverändert am gespeicherten Ort zu belassen, d. h. insbesondere diese erst zu löschen, wenn der Kläger sie hierzu auffordert, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden und nicht an Dritte weiterzugeben.

5. Die Beklagte wird verpflichtet, sämtliche unter Ziffer 2 a. aufgeführten, seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten des Klägers auf seine Aufforderung hin, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, vollständig zu löschen und dem Kläger die Löschung zu bestätigen sowie sämtliche gemäß Ziffer 2 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise zu löschen.

6. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten in Höhe von 367,23 Euro freizustellen.

7. Im Übrigen wird die Klage abgewiesen.

Von den Kosten des Rechtsstreits beider Instanzen haben der Kläger 59 % und die Beklagte 41 % zu tragen.

Das Urteil ist vorläufig vollstreckbar, hinsichtlich der Verurteilungen zu 3., 4. und 5. jedoch nur gegen Sicherheitsleistung in Höhe von 1.800,00 Euro. Die Beklagte darf die Vollstreckung des Klägers in der Hauptsache im Übrigen und wegen der Kosten

durch Sicherheitsleistung in Höhe von 3.000,00 Euro abwenden, wenn nicht der Kläger zuvor Sicherheit in gleicher Höhe leistet. Der Kläger darf die Vollstreckung der Beklagten wegen der Kosten durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die Beklagte zuvor Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.

Die Revision wird zugelassen.

Gründe:

I.

Die Parteien streiten um Feststellungs-, Unterlassungs-, Löschungs-, Anonymisierungs- und Schadenersatzansprüche wegen behaupteter bzw. angenommener Datenschutzverstöße der Beklagten im Zusammenhang mit der Verwendung sogenannter „Business-Tools".

Der Kläger ist Nutzer des sozialen Netzwerks Instagram. Er registrierte sich am 23.12.2017 unter dem Benutzernamen [redacted] auf dieser Plattform und nutzt sie seither kostenfrei ausschließlich zu privaten Zwecken. Daneben ist er auch in dem sozialen Netzwerk Facebook registriert. Betreiberin dieser sozialen Netzwerke ist die Beklagte. Das Geschäftsmodell der Beklagten besteht unter anderem darin, Unternehmen gegen Entgelt die Möglichkeit einzuräumen, den kostenfreien Nutzern der Plattform Werbeanzeigen zu präsentieren, die sich grundsätzlich an dem jeweiligen Nutzerverhalten sowie den hieraus abgeleiteten Interessen der Nutzer ausrichten. Daneben bietet die Beklagte ein kostenpflichtiges Abonnement an, das es erlaubt, die Plattform komplett werbefrei zu nutzen. Ein solches Abonnement hat der Kläger nicht abgeschlossen.

Für werbende Drittunternehmen stellt die Beklagte verschiedene von ihr entwickelte so genannte „Business-Tools" zur Verfügung. Hierzu zählen insbesondere Softwareprodukte wie „Meta-Pixel", die „Conversions API", „App-Events über Facebook-SDK",

„Offline-Conversions“ und die „App Events API“. Diese Anwendungen können Websitebetreiber und Werbetreibende in ihre Websites und Apps einbinden, um die Reichweite und Effizienz ihrer Werbemaßnahmen zu steigern.

Voraussetzung für die Nutzung der „Business-Tools“ ist die Zustimmung der Drittunternehmen zu den von der Beklagten vorgegebenen "Nutzungsbedingungen für Meta-Business-Tools". Dort heißt es in Ziffer 3 („Besondere Bestimmungen für die Nutzung bestimmter Business-Tools“) auszugsweise:

> "c. Du sicherst zu und gewährleistest, dass du einen stabilen und hinreichend auffälligen Hinweis für Nutzer bezüglich dem Erfassen, Teilen sowie der Verwendung der Business-Tool-Daten bereitgestellt hast, der mindestens folgende Angaben enthalten muss:
>
> i. Für Websites: Einen eindeutigen und auffälligen Hinweis auf jeder Seite der Website, auf der unsere Pixel genutzt werden. Ein solcher Hinweis hat auf eine klare Erläuterung zu verlinken, die besagt, (a) dass Dritte, einschließlich Meta, möglicherweise Cookies, Web Beacons und sonstige Speichertechnologien nutzen, um Informationen von deinen Websites und anderen Stellen im Internet zu erfassen oder zu erhalten, und diese Informationen dann für die Bereitstellung von Messlösungen, das Anzeigen-Targeting und die Auslieferung von Anzeigen verwenden, (b) wie Nutzer sich für ein Opt-out bezüglich der Erfassung und Verwendung von Informationen für das Anzeigen-Targeting entscheiden können und (c) wo Nutzer auf einen Mechanismus zugreifen können, um eine solche Auswahl zu treffen (z. B. durch Bereitstellung von Links zu http://www.aboutads.info/choices und http://www.youronlinechoices.eu/).
>
> ii. Für Apps: Einen eindeutigen und auffälligen Link, der in deinen App-Einstellungen oder in jeder Datenrichtlinie und aus jedem Store bzw. von jeder Website aus, in der/dem deine App vertrieben wird, leicht zugänglich ist. Dieser Link muss auf eine klare Erläuterung verlinken, die besagt, (a) dass Dritte, einschließlich Meta, möglicherweise Informationen von deiner App und anderen Apps erfassen bzw. erhalten und diese Informationen dann für die Bereitstellung von Messlösungen und das Anzeigen-Targeting und die Auslieferung von Anzeigen verwenden, und (b) wie und wo Nutzer sich für ein Opt-out bezüglich der Erfassung und Verwendung von Informationen für das Anzeigen-Targeting entscheiden können.
>
> d. In Rechtsordnungen, in denen für das Speichern von Cookies oder sonstigen Informationen auf dem Gerät eines Endnutzers und das Zugreifen auf diese eine informierte Einwilligung erforderlich ist (wie u. a. in der Europäischen Union), musst du in nachprüfbarer Weise sicherstellen, dass ein Endnutzer alle erforderlichen Einwilligungen erteilt, bevor du Meta-Business-Tools nutzt, um Meta das Speichern von Cookies oder sonstigen Informationen auf dem Gerät des Endnutzers und den Zugriff auf diese zu ermöglichen. (Vorschläge zur Implementierung von Einwilligungsmechanismen findest du in unserer Ressource zur Cookie-Einwilligung.)"

Wegen des weiteren Inhalts der Nutzungsbedingungen wird auf Anlage B5 Bezug genommen. Daneben vereinbart die Beklagte mit Drittunternehmen, die die "Meta Business Tools" in ihre Systeme implementieren, die von ihr als "Vertragszusatz" bezeichneten Datenverarbeitungsbedingungen mit dem aus Anlage B9 ersichtlichen Inhalt. Ob eine Einwilligung zur Datenübermittlung im Einzelfall erteilt worden ist, überprüft die Beklagte nicht.

Besuchen Nutzer eine mit Business-Tools ausgestattete Webseite oder verwenden sie eine entsprechende App, erheben die Tools automatisch Informationen über das Gerät der Nutzer (unter anderem Geräte- und Browsermerkmale, IP-Adressen, Standortdaten und Cookie-Informationen) und weitere personenbezogene Informationen. Dazu gehören zum einen Kontaktinformationen, wie Name, E-Mail-Adresse und Telefonnummer, mit denen Einzelpersonen identifiziert werden können, und zum anderen so genannte „Event-Daten", also Informationen über Handlungen, die Nutzer auf Websites, in Apps oder Shops durchführen, wie Besuche, Installationen und Käufe.

Die „Meta Business Tools" werden im Hintergrund der jeweiligen Drittwebseiten oder Apps ausgeführt, ohne dass dies für die Nutzer unmittelbar erkennbar ist. Dies gilt auch dann, wenn der betroffene Nutzer nicht in dem sozialen Netzwerk der Beklagten angemeldet ist. Sie übertragen Daten teils auch unabhängig von browserbasierten Technologien – wie dem Einsatz von Cookies – unmittelbar vom Server des Drittanbieters an die Systeme der Beklagten. Eine solche Datenübertragung kann daher durch den Einsatz cookieblockierender Maßnahmen, insbesondere die Nutzung des „Inkognito-Modus", von „Ad-Blockern" oder eines Virtual Private Network (VPN) nicht vollständig verhindert werden. Die Beklagte empfiehlt Drittunternehmen ausdrücklich, die Tools „Meta-Pixel" und „Conversions API" in Kombination zu verwenden, um die von ihr so genannte „Customer Journey vollständig erfassen" zu können (zum Ganzen: „Meta-Playbook", Anlage K10, dort Seite 4 f.).

Im Rahmen ihrer Registrierung bei dem von der Beklagten betriebenen sozialen Netzwerk stimmen die Nutzer den Nutzungsbedingungen der Beklagten (Anlage B2) zu. Diese verweisen ihrerseits auf die Datenschutzrichtlinie (Anlage B10), die wiederum die Cookie-Richtlinie der Beklagten in Bezug nimmt.

In der Datenschutzrichtlinie führt die Beklagte aus, wie die von den Nutzern bereitgestellten Informationen und Geräteinformationen sowie sämtliche über die „Business-

Tools“ übermittelten Informationen von Drittanbietern erfasst und zusammengeführt werden. Darüber hinaus übermitteln Partnerunternehmen demnach Informationen wie E-Mail-Adressen, Cookies und Geräte-IDs zu Werbezwecken an die Beklagte, und zwar unabhängig davon, ob die betroffene Person bei den Produkten der Beklagten angemeldet ist oder über ein entsprechendes Nutzerkonto verfügt. Zudem leiten die Partnerunternehmen Kommunikationsdaten an die Beklagte weiter. Ferner wird in der Datenschutzrichtlinie ausgeführt, dass Partnerunternehmen zur Übermittlung der Informationen insbesondere „Business-Tools“, Integrationen sowie Technologien des „Meta Audience Network“ einsetzen. Verwendet würden die Informationen zur Bereitstellung, Personalisierung und Verbesserung der Produkte der Beklagten, um Schutz, Sicherheit und Integrität zu fördern, zur Bereitstellung von „Messungs- und Analysediensten“ sowie „Unternehmens-Services“, für Forschung und Innovation für soziale Zwecke. Die Verarbeitung der Informationen für die in der Datenschutzrichtlinie beschriebenen Zwecke stütze sich auf verschiedene Rechtsgrundlagen. Unabhängig von einer Einwilligung des Nutzers diene sie der Erfüllung des Vertrages (insbesondere der Bereitstellung der vereinbarten Dienste), den berechtigten Interessen der Beklagten (insbesondere der Bereitstellung eines innovativen, personalisierten, sicheren und profitablen Dienstes), anderen wesentlichen Interessen (wie dem Schutz von Leib und Leben), der Erfüllung rechtlicher Verpflichtungen und öffentlichen Interessen.

Die Plattform bietet den Nutzern, die sie wie der Kläger kostenfrei nutzen, die Möglichkeit, optionale „Meta-Cookies auf anderen Apps und Websites“ zu aktivieren sowie festzulegen, ob Informationen von Werbepartnern für „personalisierte Werbung“ oder lediglich für „weniger personalisierte Werbung“ verwendet werden sollen. Diese Einstellungsmöglichkeiten haben jedoch auf die Erhebung der von Drittanbietern generierten Daten oder deren Übermittlung an die Beklagte keinen Einfluss. Sie betreffen ausschließlich die Verarbeitung der bereits empfangenen Daten durch die Beklagte selbst. Die Beklagte gleicht die ihr übermittelten Daten mit den vorhandenen Nutzerinformationen ab und ordnet sie dem jeweiligen Nutzerprofil konkret zu, um sodann über die weitere Verwendung dieser Daten zu entscheiden.

Hat der Nutzer die Verwendung von „Meta-Cookies auf anderen Apps und Websites“ nicht ausdrücklich zugelassen, verwendet die Beklagte die über Cookies und ähnliche Technologien auf anderen Apps und Websites erhobenen Daten nach eigenen Angaben nur zu so genannten „Sicherheits- und Integritätszwecken“. Hierunter sollen die Identifizierung von Akteuren, deren Verhalten gegen die Meta-Richtlinien

verstoßen könnte, die Fehlerbehebung und Betriebsprotokollierung sowie die Erkennung auffälliger Verhaltensmuster, Geräte- und Netzwerkaktivitäten fallen. Für diese Datenverarbeitung bestehen nach den Angaben der Beklagten keine festen Speicherfristen. Die Löschung der Daten macht die Beklagte davon abhängig, ob sie eine weitere Datenverarbeitung und -speicherung zum Zwecke weiterer Untersuchungen für erforderlich hält.

Hat sich ein Nutzer dazu entschieden, „weniger personalisierte" Werbung zu erhalten, beschränkt die Beklagte den Umfang der Daten, den sie zur Ausrichtung von Werbeanzeigen auf den Nutzer verwendet.

Will ein zunächst mit der Übersendung personalisierter Werbung einverstandener Nutzer die Verknüpfung künftiger Aktivitäten mit seinem Konto aufheben und frühere Aktivitäten löschen (Anlage B7, S. 44 ff.), werden zwar binnen 24 Stunden künftige Verknüpfungen zwischen seinem Konto und seinen Aktivitäten ausgeschaltet und der vorherige Verlauf des Nutzers gelöscht; die Beklagte erhält aber nach eigenen Angaben (Anlage B7, S. 56) weiterhin Informationen zu seinen Aktivitäten, die für Messungen sowie zur Verbesserung der Werbesysteme verwendet werden.

Dazu, ob sich der Kläger mit der Übersendung personalisierter Werbung einverstanden erklärt hat, haben die Parteien unterschiedlich und teils widersprüchlich vorgetragen.

Die Business-Tools werden auf zahlreichen reichweitenstarken Webseiten und Apps in und außerhalb Deutschlands eingesetzt, darunter auf Nachrichtenseiten großer überregionaler Tageszeitungen und Wochenmagazine, Seiten großer Reiseportale, Seiten und Apps mit Angeboten medizinischer Hilfe durch Ärzte, Apotheken und Gesundheitsportale, auf Datingseiten und Erotikportalen sowie auf Internetseiten zu besonders sensiblen Inhalten wie Krebserkrankungen, Kinderwunschbehandlungen, Alkoholabhängigkeit und Sterbehilfe. Allein die Software „Meta-Pixel" findet auf 30% bis 40% aller größeren Webseiten weltweit Anwendung.

Mit anwaltlichem Schreiben vom 28.09.2023 (Anlage K3) ließ der Kläger die Beklagte unter Fristsetzung auf den 19.10.2023 erfolglos auffordern, die Unzulässigkeit der Verarbeitung ihrer personenbezogenen Daten anzuerkennen und sich zu verpflichten, die erhobenen Daten bis zu einer Aufforderung unverändert aufzubewahren und je nach

Aufforderung zu löschen oder zu anonymisieren. Daneben machte er Schadensersatz-, Auskunfts- und Unterlassungsansprüche geltend.

Das Landgericht hat den Kläger persönlich angehört. Mit am 06.11.2024 verkündetem Urteil hat es die Klage abgewiesen. Gegen dieses Urteil, auf das wegen des weiteren Sach- und Streitstands und der erstinstanzlich gestellten Anträge Bezug genommen wird, wendet sich die Berufung des Klägers, mit der er sein erstinstanzliches Klagebegehren weiterverfolgt.

Er beantragt nunmehr,

das Urteil des Landgerichts Krefeld vom 06.11.2024 abzuändern und wie folgt neu zu fassen:

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

   a) auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der Klagepartei, ob direkt oder in gehashter Form übertragen, d.h. E-Mail der Klagepartei, Telefonnummer der Klagepartei, Vorname der Klagepartei, Nachname der Klagepartei, Geburtsdatum der Klagepartei, Geschlecht der Klagepartei, Ort der Klagepartei, Externe IDs anderer Werbetreibender (von der Meta Ltd. "external_ID" genannt), IP-Adresse des Clients, User-Agent des Clients (d.h. gesammelte Browserinformationen), interne Klick-ID der Meta Ltd., interne Browser-ID der Meta Ltd., Abonnement-ID, Lead-ID, anon_id

   sowie folgende personenbezogene Daten der Klagepartei

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

c) in mobilen Dritt-Apps der Name der App sowie der Zeitpunkt des Besuchs, die in der App angeklickten Buttons sowie die von der Meta „Events“ genannte Daten, die die Interaktionen des Klägers 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 gemäß des Antrags zu 1. zu verarbeiten.

3. Die Beklagte wird verpflichtet, sämtliche unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 26.02.2019 bereits verarbeiteten personenbezogenen Daten ab sofort unverändert am gespeicherten Ort zu belassen, d. h. insbesondere diese erst zu löschen, wenn die Klagepartei sie hierzu auffordert, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden, und nicht an Dritte weiterzugeben.

4. Die Beklagte wird verpflichtet, sämtliche gemäß dem Antrag zu 1 a. seit dem 26.02.2019 bereits gespeicherten personenbezogenen Daten der Klagepartei auf ihre Aufforderung hin, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, vollständig zu löschen und der Klagepartei die Löschung zu bestätigen sowie sämtliche gemäß dem Antrag zu 1 b. sowie c. seit dem 26.02.2019 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise zu löschen.

5. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 27.10.2023, zu zahlen.

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

Die Beklagte beantragt,

die Berufung zurückzuweisen.

Sie verteidigt das erstinstanzliche Urteil als zutreffend.

II.

Die zulässige Berufung ist in dem aus dem Tenor ersichtlichen Umfang auch in der Sache begründet.

1.
Die Klage ist zulässig.

a)
Die internationale Zuständigkeit der deutschen Gerichte, die auch in der Berufungsinstanz von Amts wegen zu prüfen ist, folgt aus Art. 82 Abs. 6, Art. 79 Abs. 2 Satz 2 DSGVO und aus Art. 17 Abs. 1 lit. c), 18 Abs. 2, 2. Alt. Brüssel Ia-VO. Der Kläger hat seinen Aufenthaltsort und Wohnsitz in Deutschland und ist Verbraucher.

b)
Entgegen der Auffassung der Beklagten ist der mit dem Klageantrag zu 1. verfolgte Feststellungsantrag zulässig (wie hier OLG München, Urt. v. 18.12.2025 – 14 U 1068/25e, juris-Rn. 237 ff.; a. A. OLG Dresden, Urt. v. 03.02.2026 – 4 U 292/25, juris-Rn. 136 ff.). Die Zulässigkeit folgt aus § 256 Abs. 2 ZPO.

Der Antrag ist auf die Feststellung eines Rechtsverhältnisses im Sinne des § 256 ZPO gerichtet. Ein Rechtsverhältnis ist die aus einem vorgetragenen Sachverhalt abgeleitete rechtliche Beziehung einer Person zu einer anderen Person oder zu einer Sache (BGH, Urt. v. 02.09.2021 – VII ZR 124/20, juris-Rn. 25; Urt. v. 09.05.2019 – VII ZR 154/18, juris-Rn. 26; Greger in: Zöller, ZPO, 36. Aufl. 2025, § 256 Rn. 4,

jeweils m. w. N.). Gegenstand einer Feststellungsklage können auch einzelne aus einem umfassenderen Rechtsverhältnis resultierende Rechte und Pflichten sowie Inhalt und Umfang einer Leistungspflicht sein (BGH, Urt. v. 19.11.2014 – VIII ZR 79/14, juris-Rn. 24).

Der Kläger begehrt die Feststellung, dass der zwischen den Parteien bestehende Nutzungsvertrag der Beklagten nicht gestattet, bestimmte personenbezogene Daten von Dritt-Webseiten und Dritt-Apps zu verarbeiten. Damit stellt er den Umfang der sich aus dem Vertragsverhältnis ergebenden Rechte der Beklagten zur gerichtlichen Klärung. Dies betrifft ein konkretes gegenwärtiges Rechtsverhältnis, weil sich der Kläger erkennbar gegen die Verarbeitung sämtlicher Daten wendet, die bei Nutzung von Dritt-Webseiten und Dritt-Apps anfallen, auf denen die von der Beklagten eingesetzten Business-Tools aktiv sind. Eine weitergehende Spezifizierung kann von ihm nicht verlangt werden. Die Beklagte allein verfügt über die vollständige Kenntnis darüber, auf welchen Seiten und Anwendungen ihre Tools eingebunden sind. Würde man vom Kläger eine abschließende Auflistung verlangen, überspannte dies die Darlegungslast.

Es kann dahinstehen, ob dem Kläger mit Blick auf die von ihm zusätzlich erhobenen Ansprüche auf Unterlassung und Schadensersatz ein eigenständiges Feststellungsinteresse im Sinne von § 256 Abs. 1 ZPO zusteht. Denn die Klage erfüllt zumindest die Voraussetzungen einer Zwischenfeststellungsklage gemäß § 256 Abs. 2 ZPO. In diesem Fall tritt die Vorgreiflichkeit der begehrten Feststellung an die Stelle des sonst erforderlichen besonderen Feststellungsinteresses (BGH, Urt. v. 23.04.2013 – II ZR 74/12, juris-Rn. 29).

Die begehrte Feststellung ist für die zugleich erhobenen Leistungsanträge – insbesondere auf Unterlassung und Schadensersatz – vorgreiflich. Ob der zwischen den Parteien bestehende Nutzungsvertrag die streitgegenständliche Datenverarbeitung gestattet, bildet eine zentrale Vorfrage für deren Begründetheit. Die Feststellung erschöpft sich auch nicht in ihrer Bedeutung als bloße Vorfrage. Erforderlich ist eine über den gegenwärtigen Streitgegenstand hinausgehende rechtliche Relevanz; hierfür genügt die Möglichkeit, dass aus dem streitigen Rechtsverhältnis weitere Ansprüche entstehen können (BGH, Urt. v. 23.04.2012 – II ZR 75/10, juris-Rn. 41 m. w. N.). Diese Möglichkeit besteht hier. Es lässt sich nämlich nicht ausschließen, dass personenbezogene Daten des Klägers, die von Drittanbietern stammen und Gegenstand der be-

gehrten Feststellung sind, künftig unbefugt Dritten zugänglich werden und hieraus weitere Ansprüche resultieren (vgl. auch OLG München, Urt. v. 18.12.2025 – 14 U 881/25e, juris-Rn. 109).

c)
Auch gegen die Zulässigkeit der Unterlassungsanträge bestehen keine Bedenken. Die Anträge sind insbesondere hinreichend bestimmt (wie hier OLG München, Urt. v. 18.12.2025 – 14 U 1068/25e, juris-Rdn. 237 ff; OLG Dresden, Urt. v. 03.02.2026 – 4 U 292/25, juris-Rdn. 139 ff.).

aa)
Nach § 253 Abs. 2 Nr. 2 ZPO muss ein Verbotsantrag den Streitgegenstand so genau bezeichnen, dass Gegenstand und Umfang der gerichtlichen Entscheidungsbefugnis (§ 308 Abs. 1 ZPO) erkennbar abgegrenzt sind, der Beklagte sich sachgerecht verteidigen kann und die Entscheidung darüber, was dem Beklagten verboten ist, nicht erst dem Vollstreckungsgericht überlassen bleibt (BGH, Urt. v. 30.04.2025 – I ZR 196/13, juris-Rn. 10). Diesen Anforderungen genügen die Anträge. Der Kläger hat die Daten, deren Verarbeitung die Beklagte unterlassen soll, konkret bezeichnet (E-Mail-Adresse, Telefonnummer sowie weitere im Antrag aufgeführte personenbezogene Daten).

bb)
Es begegnet auch keinen Bedenken, dass der Kläger die „Verarbeitung" im Sinne des Art. 4 Nr. 2 DSGVO insgesamt untersagt wissen will, ohne einzelne Verarbeitungshandlungen gesondert aufzuführen. Da der Kläger die Vorgänge, die bei den Drittunternehmen und der Beklagten im Einzelnen stattfinden, nicht aus eigener Kenntnis beschreiben kann, muss es ihm möglich sein, sich auf den im Gesetz verwendeten Oberbegriff zu beziehen. Welche konkreten Unterlassungs- oder Handlungspflichten sich hieraus ergeben, kann die Beklagte unter Heranziehung der Entscheidungsgründe unschwer bestimmen (vgl. BGH, Urt. v. 15.08.2013 – I ZR 80/12, juris-Rn. 21 m. w. N.).

cc)
Auch der Umstand, dass die Beklagte zur Erfüllung des Unterlassungsgebots gegebenenfalls organisatorische oder technische Maßnahmen ergreifen und etwa ihre Business-Tools entsprechend anpassen muss, steht der Zulässigkeit des Antrags nicht entge-

gen. Ein Unterlassungsanspruch kann den Schuldner zu aktivem Tun verpflichten, sofern nur so der Störungszustand beendet wird. Hierzu kann auch die Einwirkung auf Dritte zählen (zum Ganzen BGH, Urt. v. 14.03.2017 – VI ZR 721/15, juris-Rn. 35).

dd)
Schließlich entfällt das Rechtsschutzbedürfnis nicht deshalb, weil der Kläger über die Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien" selbst Einfluss auf die weitere Behandlung seiner Daten nehmen könnte. Nach dem eigenen Vortrag der Beklagten erfolgt eine Datenverarbeitung unabhängig von der jeweiligen Auswahl des Nutzers. Die Einwilligung betrifft lediglich die weitere Verarbeitung bereits erhobener Daten zum Zweck personalisierter Werbung im Netzwerk der Beklagten.

d)
Der Antrag, die Daten am gespeicherten Ort zu belassen, d. h. insbesondere diese erst zu löschen, wenn die Klagepartei sie hierzu auffordert, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden, und nicht an Dritte weiterzugeben (hier Antrag zu 3.), ist zulässig: Die grundsätzliche Möglichkeit eines entsprechenden Anspruchs ergibt sich aus Art. 18 DSGVO. Es handelt sich auch nicht um einen im Verfahren der einstweiligen Verfügung geltend gemachten Eilantrag. Die Durchsetzung des Anspruchs im Zeitraum bis zur Rechtskraft des Urteils (im Falle einer stattgebenden Entscheidung) richtet sich vielmehr nach den Vorschriften über die vorläufige Vollstreckbarkeit (§§ 708 ff. ZPO, vgl. OLG München, Urt. v. 18.12.2025 – 14 U 1314/25e, juris-Rn. 343). Die Löschung der Daten wird nach Aufforderung der Klagepartei, im Übrigen sechs Monate nach rechtskräftigem Verfahrensabschluss verlangt. Beides stellt einen im Vollstreckungsverfahren zweifelsfrei feststellbaren und damit hinreichend bestimmten Zeitpunkt dar (vgl. OLG Thüringen, Urt. v. 02.03.2026 – 3 U 31/25, juris- Rn. 134).

e)
Auch der auf die Löschung oder Anonymisierung von Daten gerichtete Antrag zu 4. ist zulässig. Anhaltspunkte dafür, dass der Kläger entgegen § 260 ZPO („dieselbe Prozessart") eine einstweilige Regelung dahingehend anstrebt, es der Beklagten zu untersagen, den bestehenden Löschungsanspruch zu erfüllen, bestehen angesichts der Formulierung des Antrages nicht.

Soweit der Kläger von der Beklagten verlangt, bestimmte Daten „vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen", ist der Antrag zu 4. hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 a. E. ZPO. Die Einräumung eines Wahlrechts führt nicht zu einer von außen in den Prozess hineingetragenen Unsicherheit; die Beklagte wird durch das ihr eingeräumte Wahlrecht nicht beschwert (vgl. OLG Düsseldorf, Urt. v. 21.09.2023 – VI-5 U 4/22 (Kart), juris-Rn. 68; ebenso Roth in: Stein, ZPO, 24. Aufl. 2024, § 260 Rn. 10). Dass es prozessual zulässig ist, der Beklagten ein Wahlrecht einzuräumen, zeigt § 264 Abs. 1 BGB, der den – hier nicht einschlägigen – Fall der Wahlschuld betrifft. Es handelt sich auch nicht um einen unzulässigen, weil zu unbestimmten alternativen Klageantrag. Denn die Entscheidung, ob die Daten gelöscht oder stattdessen anonymisiert werden, ist nicht dem Gericht, sondern der Beklagten überlassen. Eine für die Beklagte unzumutbare Unbestimmtheit ergibt sich daher nicht (zur Abgrenzung vgl. Becker-Eberhard in: MüKo-ZPO, 7. Aufl. 2025, § 260 Rn. 23).

2.
Der Kläger hat einen Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO in Höhe von 750,00 Euro.

Der Kläger macht mit seinem mit dem Antrag zu 5. verfolgten Schadensersatzanspruch einen einheitlichen Anspruch auf Ersatz eines immateriellen Schadens geltend, der sich zwar aus einer Vielzahlt einzelner Datenschutzverstöße der Beklagten ergeben soll, aber in einem einheitlichen Geschehen – nämlich dem fortlaufenden Einsatz der „Business-Tools" – wurzelt. Die Beklagte hat gegen die Datenschutzgrundverordnung im Sinne des Art. 82 Abs. 1 DSGVO verstoßen, indem sie personenbezogene Daten des Klägers ohne die nach Art. 6 Abs. 1 DSGVO erforderliche Rechtsgrundlage verarbeitet hat.

a)
An der Eröffnung des sachlichen und räumlichen Anwendungsbereichs nach Art. 2 Abs. 1, Art. 3 Abs. 1 DSGVO bestehen keine Zweifel, da der Sachverhalt die automatisierte Verarbeitung personenbezogener Daten des Klägers durch die Beklagte als in der Europäischen Union, konkret in Irland, niedergelassene Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO betrifft. Weiterhin ist die Datenschutzgrundverordnung gemäß Art. 99 Abs. 2 DSGVO auch in zeitlicher Hinsicht anwendbar. Der Kläger beschränkt sich ausdrücklich auf Ansprüche in Verbindung mit Datenverarbeitungsvorgängen, die

bei der Beklagten nach dem 25.05.2018 und damit nach dem Inkrafttreten der DSGVO an diesem Tag vorgenommen worden sind.

b)
Mit den streitgegenständlichen Business Tools hat die Beklagte eine unbegrenzte Menge an Daten des Klägers im Sinne des Art. 4 Nr. 1 DSGVO verarbeitet, indem sie sich personenbezogene Informationen hat übermitteln lassen und so die Aktivitäten des Klägers auf Dritt-Webseiten und -Apps verfolgt hat.

Neben den von der Beklagten in ihrer Duplik vom 03.09.2024 (dort Rn. 23 ff.) genannten, bei einem Aufruf einer Webseite oder App im Rahmen einer HTTP-Anfrage notwendigerweise übermittelten Standarddatenpunkten (HTTP-Daten, die automatisch für die Internetfunktionalität übertragen werden), teilen Drittunternehmen, die die streitgegenständlichen Business Tools in ihre Webseiten oder Apps integrieren, Nutzerdaten mit der Beklagten. Erst nach der Erhebung und Übermittlung von persönlichen Daten eines Nutzers auf der Seite eines Drittunternehmens entscheidet die Beklagte über die weitere Verwendung dieser Daten in Abhängigkeit von den von dem Nutzer auf der Plattform vorgenommenen Einstellungen. Selbst wenn sich ein Nutzer dazu entschieden hat, optionale „Meta-Cookies auf anderen Apps und Webseiten" nicht zu erlauben, nutzt die Beklagte die über Cookies und ähnliche Technologien erhoben Daten zumindest für Sicherheits- und Integritätszwecke. Unabhängig von der vorgenommenen Einstellung werden die in anderen Apps und auf anderen Websites erhobenen Daten also an die Beklagte übermittelt, mit dem Kundenkonto des Benutzers verknüpft und nach Angaben der Beklagten – wenn auch zu eingeschränkten Zwecken – verarbeitet.

c)
Der Kläger ist von diesen Datenerhebungen betroffen.

(1)
Der Kläger besucht im Internet regelmäßig Webseiten, in die die „Meta-Business-Tools" integriert sind. Er hat unwidersprochen vorgetragen, dass „auf zahlreichen reichweitenstarken Webseiten und Apps in Deutschland (...) der "Meta Pixel" oder das "App Events über Facebook-SDK" der Meta Ltd. im Hintergrund läuft" (S. 9 der Klageschrift)", und eine Auflistung großer Webseiten vorgelegt, die den Meta Pixel derzeit nutzen (Anlage K2 zur Klageschrift).

In seiner persönlichen Anhörung vor dem Landgericht hat der Kläger zudem angegeben, dass er das Internet beruflich und privat für insgesamt etwa zwei bis vier Stunden am Tag nutze. Neben der Inanspruchnahme von Online-Dienstleistungen wie Shopping oder Zahlungsdiensten (u. a. PayPal) nutze er das Internet auch zur Recherche persönlicher Inhalte, wie Gesundheits- und Finanzangelegenheiten. Hier komme es auch zu Abschlüssen über check 24de. Etwa eine halbe bis eine Stunde recherchiere er zum aktuellen Weltgeschehen, insbesondere zum politischen Geschehen in Deutschland. Ihm sei aufgefallen, dass ihm personalisierte Werbung zu Themen angezeigt werde, zu denen er recherchiert habe.

Weitergehender Vortrag war von dem Kläger – anders als von der Beklagten vertreten – nicht zu verlangen. Vor dem Hintergrund der unstreitigen Verbreitung der „Meta-Business-Tools" spricht bereits die allgemeine Lebenserfahrung dafür, dass der Kläger Im Rahmen seiner regelmäßigen Internetnutzung auch Seiten besucht, auf denen solche Technologien eingesetzt werden.

Es kann deshalb dahinstehen, in welchem Umfang ein durchschnittlicher Internet-Nutzer seine Internetaktivitäten (ggfls. unter Rückgriff auf Browserverläufe verschiedener Endgeräte) über längere Zeiträume tatsächlich nachvollziehen und dokumentieren kann (zweifelnd etwa OLG Thüringen, Urt. v. 02.03.2026 – 3 U 31/25, juris-Rn. 173). Der Vortrag des Klägers gilt bereits deshalb gemäß § 138 Abs. 3 ZPO als zugestanden, weil das pauschale Bestreiten der Beklagten unbeachtlich ist.

Im Grundsatz hängt die Substantiierungslast des Bestreitenden davon ab, wie eingehend die darlegungspflichtige Gegenpartei vorgetragen hat (st. Rspr.; vgl. z. B. BGH, Urt. v. 15.06.2000 – I ZR 55/98, juris-Rn. 43; Urt. v. 03.02.1999 –VIII ZR 14/98, juris-Rn. 19 und Urt. v. 12.10.1989 – IX ZR 184/88, juris-Rn. 15). In der Regel genügt aber gegenüber einer Tatsachenbehauptung der darlegungspflichtigen Partei ein einfaches Bestreiten des Gegners (BGH, Urt. v. 15.06.2000 und 03.02.1999 jeweils a. a. O.; Urt. v. 11.07.1995 – X ZR 42/93, juris-Rn. 9; Urt. v. 23.03.1993 – VI ZR 176/92, juris-Rn. 14). Eine weitergehende Substantiierungslast trifft die nicht darlegungsbelastete Partei im Regelfall nur dann, wenn der darlegungspflichtige Gegner außerhalb des von ihm darzulegenden Geschehensablaufs steht und die maßgeblichen Tatsachen nicht kennt, während sie der anderen Partei bekannt und ihr ergänzende Angaben zuzumuten sind (vgl. nur BGH, Urt. v. 15.06.2000, a. a. O.; Urt. v. 19.04.1999 – II ZR 331/97, juris-Rn. 7; Urt. v. 03.02.1999, a. a. O.; Urt. v. 07.12.1998 – II ZR 266/97, juris-Rn. 11;

Urt. v. 17.10.1996 – IX ZR 293/95, juris-Rn. 17 und v. 11.06.1990 – II ZR 159/89, juris-Rn. 10). Diese Voraussetzungen liegen hier vor.

Hinsichtlich der konkreten technischen Abläufe– insbesondere der Frage, auf welchen Drittwebseiten und in welchen Apps Meta-Business-Tools eingesetzt werden und welche Daten hierbei an die Beklagte übermittelt werden – befindet sich der Kläger außerhalb des maßgeblichen Geschehensablaufs. Er kann und muss nicht wissen, auf welchen (Dritt-) Webseiten und Apps die Business-Tools der Beklagten Verwendung finden, er ist insoweit auf Vermutungen angewiesen (vgl. dazu auch BGH, Beschl. v. 20.05.2015 – IV ZR 127/14, juris-Rn. 15). Demgegenüber verfügt die Beklagte, die die entsprechenden Systeme betreibt, über sämtliche relevanten Informationen und ist in der Lage, anhand ihrer internen Datenverarbeitung sowie der Nutzerkonten die Herkunft und den Umfang der Datenübermittlungen nachzuvollziehen.

(2)
Es steht auch fest, dass der Beklagten ungeachtet der technischen Möglichkeit, die Zustimmung zur Verwendung nicht notwendiger Cookies auf den Drittwebseiten zu verweigern mithilfe der dort installierten „Business-Tools“ regelmäßig personenbezogene Daten des Klägers übermittelt worden sind.

In diesem Zusammenhang kann offenbleiben, ob sich die Übermittlung von Daten durch die Verweigerung der Zustimmung auf den Drittwebseiten tatsächlich vollständig unterbinden lässt oder ob zumindest cookie-unabhängige Datenübertragungen durch einzelne (“resiliente”) Business-Tool-Anwendungen unberührt bleiben, wie es die Hinweise im „Meta-Playbook“ nahelegen. Es ist nämlich davon auszugehen, dass der Kläger im Rahmen der üblichen Internetnutzung regelmäßig Cookie-Einwilligungen erteilt hat, ohne sich zuvor eingehend mit Inhalt, Reichweite und Folgen der jeweiligen Erklärung auseinanderzusetzen, und dass er hierdurch die technische Übermittlung von Daten an die Beklagte ermöglicht hat. Es ist allgemein bekannt, dass Einwilligungen angesichts der alltäglichen und massenhaften Konfrontation mit Cookie-Hinweisen vielfach routinemäßig und mit dem Ziel erteilt werden, einen schnellen Zugang zu den gewünschten Inhalten oder Funktionen der Webseite zu erhalten, nicht jedoch aufgrund bewusster Prüfung und vertiefter Auseinandersetzung mit den datenschutzrechtlichen Konsequenzen der Erklärung. Die Zustimmung zu Cookie-Bannern erfolgt typischerweise unter Bedingungen eingeschränkter Aufmerksamkeit bei gleichzeitig erheblicher Informationskomplexität. Zudem sind die Einwilligungsoberflächen häufig

„nutzerlenkend“ so gestaltet, dass sie das „Akzeptieren“ der Voreinstellungen nahelegen.

Dass der Kläger aufgrund fehlender Transparenz in die Verwendung von Cookies zumindest teilweise eingewilligt hat, liegt auch deshalb nahe, weil ein durchschnittlicher Nutzer der einzelnen Drittwebseiten regelmäßig weder erwartet noch erkennt, in welchem Umfang die dort erhobenen Daten bei der Beklagten zusammengeführt und mit seinem Nutzerprofil verknüpft werden. Auch der Umstand, dass die Beklagte selbst in ihren Einstellungen die Möglichkeit bietet, „Meta-Cookies auf Drittwebseiten“ abzuwählen, legt aus Sicht eines durchschnittlichen Nutzers nahe, dass hierdurch die Erhebung und Übermittlung von Daten beim Besuch von Drittwebseiten bereits umfassend unterbunden werden kann, ohne dass den Cookie-Einstellungen auf der Drittwebseite noch besondere Bedeutung zukommt; der Benutzer wird durch diese Einstellung also regelrecht zu der irrtümlichen Annahme verleitet, an anderer Stelle und insbesondere auch auf den Drittwebseiten oder den entsprechenden Apps nichts weiter tun zu müssen.

d)
Die an die Beklagte übermittelten Daten stellen auch personenbezogene Daten im Sinne des Art. 4 Nr. DSGVO dar, denn die Beklagte ist in der Lage, diese Daten (z.B. über die verwendete IP-Adresse oder individuelle Geräteinformationen) dem Benutzerkonto des Klägers zuzuordnen.

e)
Die Beklagte ist auch für die Erhebung, Übermittlung, Speicherung und Verwendung dieser Daten verantwortlich i.S.v. Art. 4 Nr. 7 DSGVO. Soweit sie die Daten bei sich speichert und verwendet, ist diese Verantwortlichkeit offensichtlich. Anders als von ihr angenommen ist die Beklagte – gemeinsam mit dem jeweiligen Drittanbieter – auch in Bezug auf die Erhebung und Übermittlung als verantwortlich anzusehen (EuGH, Urt. v. 29.07.2019 – C-40/17, juris-Rn. 79, 96).

Nach Einbettung der Business-Tools in eine Webseite oder App übernehmen diese fortlaufend automatisch die jeweils aktuelle Version des Tools. Die Kontrolle über die Programmierung und in der Folge über die Funktionalität des Tools verbleibt damit bei der Beklagten. Diese übt damit Einfluss darauf aus, welche Daten erhoben und über-

mittelt werden. Auch die Beklagte selbst geht von einer mit den Drittunternehmen gemeinsamen Verantwortlichkeit für die Erhebung und Übermittlung zusätzlicher Daten über die „Meta-Business-Tools“ aus (vgl. die Nutzungsbedingungen für Meta-Business-Tools in Anlage B5, dort S. 5 unter 5. a. ii.).

f)
Mit ihren Datenerhebungen verstößt die Beklagte gegen den Grundsatz der Datenminimierung, der in Art. 5 Abs. 1 lit. b), lit. c), Art. 25 Abs. 2 S. 1, 3 DSGVO verankert ist. Der Grundsatz der Datenminimierung sichert die Verhältnismäßigkeit der Datenverarbeitung und besagt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (EuGH, Urt. vom 04.10.2024 – C-446/21, Rn. 49 f. und vom 04.07.2023 – C-252/21, juris-Rn. 109). Der Verantwortliche darf die Daten nicht allgemein und unterschiedslos erheben, sondern muss von der Erhebung solcher Daten absehen, die für die Zwecke der Verarbeitung nicht unbedingt notwendig sind (EuGH, Urt. v. 04.10.2024 – C-446/21, Rn. 59). In zeitlicher Hinsicht ist der Zeitraum der Datenerhebung als solcher und der Zeitraum, in dem die Möglichkeit besteht, den Betroffenen zu identifizieren, auf das im Hinblick auf den Zweck der beabsichtigten Verarbeitung absolut Notwendige zu beschränken (EuGH a.a.O., Rn. 52 f.).

Demgegenüber verarbeitet die Beklagte die von den (Dritt-)Webseiten und Apps stammenden „Kontaktinformationen“ und/oder „Event-Daten“ ihrer Nutzer schon nach ihrem allgemeinen Vortrag allgemein und unterschiedslos, indem sie sämtliche über die „Meta-Business Tools“ übermittelten personenbezogenen Daten ohne Differenzierung nach dem Einzelfall empfängt, zumindest vorübergehend speichert und weiterverarbeitet. Weil ein vorheriger Abgleich mit den Nutzereinstellungen auf der Plattform der Beklagten oder auf den jeweiligen Drittseiten nicht stattfindet, ist für diese Datenverarbeitung unmaßgeblich, ob Nutzer in ihren Einstellungen die Funktion „Meta-Cookies auf anderen Apps und Websites“ deaktiviert und ihr Einverständnis zur Erhebung von Informationen über ihre außerhalb der Plattformen der Beklagten stattfindende Internetnutzung damit verweigert haben. Soweit die Beklagte vorträgt, die von Drittanbietern übermittelten Businesstool-Daten zunächst mit einem Nutzerkonto zu verknüpfen und erst auf dieser Grundlage anhand der jeweiligen Einstellungen über eine etwaige weitere Verarbeitung zu entscheiden, steht dies der Annahme einer zunächst unterschiedslosen Datenerfassung nicht entgegen. Zwar ist nach dem Vortrag der Beklag-

ten davon auszugehen, dass Nutzer, die entsprechende Cookies ablehnen, keine personalisierte Werbung erhalten und die Daten teilweise lediglich zu Sicherheits- und Integritätszwecken verwendet werden. Gleichwohl verfügt die Beklagte bereits im Zeitpunkt der Übermittlung über denselben Umfang an personenbezogenen Daten, die unabhängig von einer Zweckdifferenzierung erhoben und zentral verarbeitet werden. Diese anlasslose und unterschiedslose Erhebung oder sogar Bevorratung von Daten ohne vorherige Zweckbegrenzung ist mit dem Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 lit. b) DSGVO nicht zu vereinbaren (zum Ganzen auch OLG Thüringen, Urt. v. 02.03.2026 – 3 U 31/25, juris-Rn. 204 ff.).

g)
Die Datenverarbeitung seitens der Beklagten ist nicht nach Art. 6 Abs. 1 DSGVO gerechtfertigt.

Die Darlegungs- und Beweislast dafür, dass die Daten unter anderem 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, trägt nach Art. 5 DSGVO der Verantwortliche. Außerdem obliegt es ihm nach Art. 13 Abs. 1 lit. c) dieser Verordnung, wenn personenbezogene Daten bei der betroffenen Person erhoben werden, diese Person über die Zwecke, für die diese Daten verarbeitet werden sollen, sowie über die Rechtsgrundlage für die Verarbeitung zu informieren (EuGH, Urt. v. 04.07.2023 – C-252/21, juris-Rn. 95). Anders als die Beklagte meint, muss folglich nicht der Kläger bestimmte Verarbeitungszwecke in Frage stellen, sondern hat die Beklagte zu erklären, zu welchem Zweck sie welche Daten erhoben hat und weshalb die Verarbeitung der Daten rechtmäßig sein soll. Dem ist die Beklagte nicht hinreichend nachgekommen.

Eine Rechtfertigung der Datenverarbeitung nach Art. 6 Abs. 1 DSGVO bzw. nach Art. 9 Abs. 2 DSGVO scheitert schon daran, dass die Beklagte nicht hinreichend genau bezeichnet, welche Daten sie zu welchem Zweck erhebt. Sollte ihr dies angesichts der Menge der betroffenen Daten womöglich nicht oder nur mit unverhältnismäßigem Aufwand möglich sein, würde dies das erhebliche Ausmaß ihres Verstoßes gegen den Grundsatz der Datenminimierung verdeutlichen. In ihrer Datenschutzrichtlinie (Anlage B10) stützt sich die Beklagte für die von ihr genannten unterschiedlichen Verarbeitungszwecke auf vielfältige, dort genannte Rechtfertigungsgründe im Sinne des Art. 6

Abs. 1 DSGVO. Eine hinreichende Rechtfertigung lässt sich weder dort, noch in dem weiteren Vorbringen der Beklagten erkennen.

Im Einzelnen:

(1)
Die streitgegenständliche Datenverarbeitung ist nicht durch eine Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO gerechtfertigt. Eine etwaige Einwilligung des Klägers konnte in der erforderlichen Weise allenfalls auf den Websites der Beklagten selbst erfolgen und erfüllt aus den oben schon zu Ziffer 2 c) (2) dargelegten Gründen nicht den Anforderungen an eine informierte Einwilligung im Sinne des Art. 7 DSGVO. Auf die von der Beklagten widersprüchlich behandelte Frage, ob der Kläger vorliegend in die Bereitstellung personalisierter Werbung eingewilligt hat, kommt es daher im Ergebnis nicht an.
Selbst wenn man nämlich zugunsten der Beklagten eine Einwilligung des Klägers in die Bereitstellung personalisierter Werbung unterstellt, rechtfertigt dies die konkrete Datenverarbeitung nicht im Sinne des Art. 6 Abs. 1 lit. a) DSGVO. Nach den Schilderungen der Datenerhebungs- und Übermittlungsvorgänge von den Drittunternehmen an die Beklagte ergibt sich nämlich, dass die Beklagte zunächst eine Vielzahl von Daten von den Drittunternehmen erhält und speichert, ohne sie sämtlich zu benötigen, um – der Einwilligung entsprechend – personalisierte Werbung anzuzeigen. Auch insoweit trägt die Beklagte selbst nicht vor, welche Daten genau sie denn von der Einwilligung zur Bereitstellung personalisierter Werbung als erfasst ansieht. Dies zeigt sich bereits in dem von der Beklagten selbst verwendeten Katalog zu Rechtsgrundlagen und Verarbeitungszwecken in ihrer Datenschutzrichtlinie. Daraus ergibt sich nämlich, dass zahlreiche von den Drittunternehmen erhobene und an die Beklagte übermittelte Daten jedenfalls auch der Verfolgung weiterer Zwecke dienen. Die hierfür herangezogenen Rechtfertigungsgründe tragen die jeweilige Datenverarbeitung jedoch nicht, wie die nachfolgenden Ausführungen zu Art. 6 Abs. 1 lit. b) bis f) DSGVO zeigen werden.

(2)
Die Verarbeitung ist nicht sämtlich im Sinne des Art. 6 Abs. 1 lit. b) für die Erfüllung des Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen. Damit eine Verarbeitung personenbezo-

gener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte. Der etwaige Umstand, dass eine solche Verarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist, ist insoweit für sich genommen unerheblich.

Entscheidend für die Anwendung des in Art. 6 Abs. 1 lit. b) DSGVO genannten Rechtfertigungsgrundes ist nämlich, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen (EuGH, Urt. v. 04.07.2023 – C-252/21, juris-Rn. 98 f.). Der Zweck der von der Beklagten betriebenen Social-Media-Plattform besteht darin, mit anderen Nutzern in Kontakt treten zu können. Dieser Zweck kann jedoch – wie auch der Umstand zeigt, dass die Plattform (wenn auch kostenpflichtig) ohne den Empfang personalisierter Werbung genutzt werden kann – auch durch die Verwendung reiner Onsite-Daten erreicht werden. Selbst, wenn der Nutzer sich für personalisierte Werbung entschieden hätte, würde sich dieses Ziel auch durch die Erhebung der Daten zum Verhalten des Nutzers in Bezug auf die von der Beklagten selbst angezeigte Werbung erreichen lassen.

(3)
Eine Rechtfertigung nach Art. 6 Abs. 1 lit. c) DSGVO scheidet von vornherein aus, weil sich die Beklagte nicht darauf beruft, aufgrund gesetzlicher Vorgaben verpflichtet zu sein, personenbezogene Daten präventiv zu erheben und auf Vorrat zu speichern, um etwaige Auskunftsverlangen nationaler Behörden erfüllen zu können. Eine solche Verpflichtung ist auch sonst nicht ersichtlich.

(4)
Eine Rechtfertigung nach Art. 6 Abs. 1 lit. d) DSGVO kommt bei der gebotenen engen Auslegung des Art. 6 Abs. 1 DSGVO (EuGH, Urt. v. 04.07.2023 – C-252/21, juris-Rn. 93) nur in Betracht, wenn die Verarbeitung dem Schutz lebenswichtiger Interessen dient. Der Normgeber hatte dabei insbesondere humanitäre Zwecke im Blick, etwa die

Überwachung von Epidemien und deren Ausbreitung sowie Maßnahmen in humanitären Notfällen, namentlich bei Naturkatastrophen oder vom Menschen verursachten Katastrophen (46. ErwG). Anhaltspunkte, die eine Einordnung der streitgegenständlichen Datenverarbeitung in diesen Schutzbereich tragen könnten, sind weder vorgetragen noch sonst ersichtlich. Angesichts der von der Beklagten angebotenen Dienste wirtschaftlicher und kommerzieller Art scheidet eine Rechtfertigung nach Art. 6 Abs. 1 lit. d) DSGVO aus (EuGH, Urt. v. 04.07.2023 – C-252/21, juris-Rn. 137).

(5)
Eine Rechtfertigung nach Art. 6 Abs. 1 lit. e) DSGVO kommt ebenfalls nicht in Betracht, weil die Voraussetzungen nicht vorliegen. Die Beklagte hat weder dargelegt, dass ihr Aufgaben im öffentlichen Interesse übertragen wurden, noch dass sie öffentliche Gewalt ausübt.

(6)
Nach Art. 6 Abs. 1 lit. f) DSGVO ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn der Verantwortliche oder ein Dritter ein berechtigtes Interesse verfolgen, die Verarbeitung zur Wahrnehmung dieses Interesses erforderlich ist und die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person gegenüber dem berechtigten Interesse nicht überwiegen (EuGH, Urt. v. 04.07.2023 – C-252/21 juris-Rn. 106). Diese Voraussetzungen legt die Beklagte nicht schlüssig dar, weil sie weder hinreichend konkret bezeichnet, welche personenbezogenen Daten sie zu welchen Zwecken erhebt und verarbeitet, noch begründet, warum die Daten dazu erforderlich sein sollen. Angesichts von Art und Umfang der verarbeiteten Daten erscheint auch zweifelhaft, dass die von der Beklagten lediglich in allgemeiner Form dargestellten Verarbeitungszwecke gegenüber den Interessen und Grundrechten der Nutzer aus Art. 7 und 8 GRCharta überwiegen könnten (vgl. EuGH, Urt. v. 04.07.2023 – C-252/21 juris-Rn. 123 zum Zweck der Produktverbesserung).

(7)
Eine Rechtfertigung der Datenverarbeitung scheidet ebenfalls aus, soweit sich die Beklagte nunmehr darauf beruft, dass die übermittelten und gespeicherten personenbezogenen Daten für Zwecke der Sicherheit und Integrität ihrer Plattformen gebraucht würden, woraus sich eine Rechtfertigung nach Art. 6 Abs. 1 lit. b) und f) DSGVO, d.h. aus Gründen der Vertragserfüllung und wegen Bestehens eines überwiegenden Interesses ergeben soll.

Eine Rechtfertigung nach Art. 6 Abs. 1 lit. b) DSGVO setzt voraus, dass die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union ist der Begriff der Erforderlichkeit eng auszulegen. Die Verarbeitung muss objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der gegenüber der betroffenen Person geschuldeten Vertragsleistung ist.

Diesen Anforderungen genügt der Vortrag der Beklagten auch im Hinblick auf die angeführten Sicherheits- und Integritätszwecke nicht. Zwar macht sie geltend, die Verarbeitung der erhobenen Daten diene dazu, atypische Verhaltensmuster zu erkennen, die missbräuchliche Erstellung von Konten zu verhindern und sicherheitsrelevante Angriffe abzuwehren. Weshalb die in Rede stehende Verarbeitung personenbezogener Daten hierfür jedoch objektiv erforderlich sein soll, legt sie nicht dar. Insbesondere fehlt es an nachvollziehbarem Vortrag dazu, weshalb die beschriebenen Sicherheitszwecke ohne Erhebung und Speicherung der Daten über das Verhalten der Nutzer auf Drittseiten nicht erreicht werden kann oder weniger eingriffsintensive Maßnahmen hierzu nicht ausreichen, dies zumal auch vor dem Hintergrund, dass sich die nach dem Vortrag der Beklagten zu bekämpfenden Sicherheitsprobleme im Zweifel auch erst als Folge aus dem durch die Verwendung der Business-Tools eröffneten Datenverkehr überhaupt ergeben.

Aus denselben Gründen scheidet auch eine Rechtfertigung nach Art. 6 Abs. 1 lit. f) DSGVO aus. Zwar kann die Gewährleistung der Sicherheit und Integrität digitaler Dienste grundsätzlich ein berechtigtes Interesse des Verantwortlichen begründen. Die Verarbeitung personenbezogener Daten ist jedoch auch dann nur zulässig, wenn sie zur Wahrung dieses Interesses erforderlich ist. Auch insoweit fehlt es an einer substantiierten Darlegung, dass sich die Verarbeitung der betreffenden Daten innerhalb dieser Grenzen hält. Die allgemein gehaltenen Hinweise der Beklagten darauf, dass missbräuchliche Akteure ihre Vorgehensweisen fortlaufend anpassen, Sicherheitsmaßnahmen zu umgehen versuchen und sich Bedrohungslagen fortwährend verändern, genügen hierfür nicht.

Darüber hinaus fehlt es an hinreichendem Vortrag zu den Speicherfristen der verarbeiteten Daten. Die Beklagte legt weder im Einzelnen dar, wie lange die erhobenen Daten gespeichert werden, noch aus welchen Gründen die jeweilige Speicherdauer

für die geltend gemachten Sicherheitszwecke erforderlich sein soll. Die Beklagte betont zwar, dass sie personenbezogene Daten auch zu Sicherheits- und Integritätszwecken nicht auf unbestimmte Zeit nur für den Fall speichere, dass eine Untersuchung künftig erforderlich werden könnte. Grundsätzlich würden Daten zu den genannten Zwecken nicht länger als drei Stunden in den Systemen gespeichert, sobald sie mit einem Konto verknüpft worden seien, das „Meta-Cookies auf anderen Apps und Websites" ablehne. Weil sich der Umfang einer Bedrohung teils jedoch erst im Laufe einer Untersuchung herausstelle, könne ebenso gut die Aufbewahrung dieser Daten erforderlich sein. Selbst wenn man der Beklagten das zuletzt beanspruchte weite Ermessen bei der Frage zubilligte, was zu Sicherheits- und Integritätszwecken als geboten anzusehen ist, lässt sich anhand ihres Vorbringens nicht feststellen, dass die Datenverarbeitung gerechtfertigt wäre. Anhand ihrer Angaben kann nicht überprüft werden, ob sie ihr Ermessen unter Beachtung der Nutzerinteressen fehlerfrei ausgeübt hat.

h)

Das nach Art. 82 Abs. 3 DSGVO vermutete Verschulden hat die Beklagten nicht ausgeräumt. Sie beruft sich darauf, rechtmäßig gehandelt zu haben. Dass sie für die anspruchsbegründenden Umstände nicht verantwortlich sei, macht sie demgegenüber nicht geltend. Soweit sie sich auf eine Verantwortung der Drittunternehmen beruft, wird auf die Ausführungen oben Bezug genommen. Im Übrigen ist dieses Vorbringen schon nicht geeignet, ihre eigene Verantwortung für die von ihr vorgenommene Verarbeitung der ihr von dort übermittelten Daten auszuräumen.

i)

Dem Kläger ist infolge des Datenschutzverstoßes der Beklagten auch ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO entstanden, der in einem Verlust der Kontrolle über seine personenbezogenen, von der Beklagten verarbeiteten Daten – darunter besonders sensibler Daten – besteht. Darüberhinausgehende Schäden ergeben sich nicht, so dass ein immaterieller Schadenersatz in Höhe von 750,00 Euro zur vollständigen und wirksamen Schadensausgleichung genügt.

(1)

Der Begriff des immateriellen Schadens ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (BGH, Urt. v. 18.11.2024 – VI ZR

10/24, Rn. 28). Maßgeblich ist danach das sich aus der Rechtsprechung des Gerichtshofs der Europäischen Union ergebende Begriffsverständnis. Ein haftungsbegründender immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO kann nach der Rechtsprechung des Gerichtshofs schon in dem – selbst kurzzeitigen – Verlust der Kontrolle über personenbezogene Daten liegen, ohne dass der Begriff des „immateriellen Schadens" den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (vgl. BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 30). Unter einem Verlust der Kontrolle ist dabei eine Situation zu verstehen, in der der Betroffene seine personenbezogenen Daten nicht mehr beherrschen kann, weil sie etwa an ihm unbekannte Dritte gelangt oder ohne nennenswerte Eingrenzung preisgegeben sind.

Für den Kläger stellt die Tatsache, dass sich eine erhebliche Menge personenbezogener Daten, die seinem Benutzerkonto zugeordnet sind oder die ihm – z.B. mittels eines Abgleiches von IP-Adressen – zugeordnet werden können, auf Servern der Beklagten in der ganzen Welt (vgl. Datenschutzrichtlinie, Anlage B10, S. 72 f.) und bei bestimmten Dritten befinden, einen Kontrollverlust dar. Als Dritte, mit denen Informationen geteilt werden, bezeichnet die Datenschutzrichtlinie der Beklagten (dort S. 48 f.) Werbetreibende, Unternehmen, die Produkte für die Beklagten vermarkten oder die mit Kundenservice oder Umfragen beauftragt werden und Forscher.

(2)
Die Datenschutz-Grundverordnung enthält keine Bestimmung über die Bemessung des aus Art. 82 Abs. 1 DSGVO geschuldeten Schadensersatzes. Insbesondere können aufgrund des unterschiedlichen Zwecks der Vorschriften nicht die in Art. 83 DSGVO genannten Kriterien herangezogen werden (vgl. EuGH, Urt. v. 04.09.2025 – C-655/23, juris-Rn. 70). In Deutschland ist somit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden (BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 93). Jedoch unterliegt die innerstaatliche Verfahrensautonomie bei der Ermittlung des nach Art. 82 DSGVO zu ersetzenden Schadens mehreren aus dem Unionsrecht folgenden Einschränkungen (BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 94).

In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld als „vollständig und wirksam" anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO

dagegen nicht erfüllen. Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen und ob er vorsätzlich oder fahrlässig gehandelt hat (BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 96; EuGH, Urt. v. 04.09.2025 – C-655/23, juris-Rn. 71, 73).

Ist allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten gegeben, ist bei der Schätzung des Schadens insbesondere die Sensibilität der konkret betroffenen personenbezogenen Daten (vgl. Art. 9 Abs. 1 DSGVO) und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Weiter ist die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle in den Blick zu nehmen (BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 99).

Der Kläger hat in seiner persönlichen Anhörung vor dem Landgericht am 05.09.2024 angegeben, dass er das Gefühl habe, sich in einer Blase zu bewegen, in der ihm nur bestimmte Informationen angezeigt würden. Sein Gefühl hinsichtlich der in Rede stehenden Datenerhebung gab er als „spooky" an, räumte aber auch ein, dass ihn diese Datenerhebung nicht völlig überrascht habe, sondern ihm schon bewusst gewesen sei, dass Hintergrundalgorithmen liefen. Die Tiefe und der Umfang der Datenerhebung habe ihn aber schon überrascht. Hinsichtlich seines Surfverhaltens hat er angegeben, unter anderem zu den Themen Gesundheit und Finanzen regelmäßig zu recherchieren. Dabei suche er zum Thema Gesundheit situativ, wenn er eine Diagnose erhalte. Beim Thema Finanzen recherchiere er sehr zielgerichtet, da er gelernter Bankkaufmann sei. Hier komme es auch zu Abschlüssen über check 24.de. Schließlich recherchiere er auch zum aktuellen politischen Geschehen, das ihn als Gewerkschaftssekretär sehr interessiere.

(3)
In Gesamtwürdigung aller maßgeblichen Umstände erscheint der in dem Kontrollverlust liegende Schaden des Klägers mit einem Betrag von 750.00 Euro wirksam ausgeglichen. Bei dieser Schadensschätzung ist berücksichtigt, dass der Kläger von der Erkenntnis seines Datenverlustes zwar nur durchschnittlich emotional betroffen ist, in seinem Fall aber auch sensible Daten in der Form von Gesundheitsdaten erhoben worden sind. Berücksichtigt ist weiter, dass der Empfängerkreis der Daten vorliegend begrenzt

ist und die Beklagte und solche Dritte, mit denen sie bestimmte Informationen teilt, umfasst, die Daten aber nicht im Internet frei verfügbar sind. Weiter war einzubeziehen, dass die Beklagte ausweislich der Datenschutzrichtlinie (Anlage B10, dort S. 67 ff.) die Daten nur so lange speichert, wie sie benötigt werden, um die Produkte der Beklagten bereitzustellen, rechtliche Verpflichtungen zu erfüllen oder bestimmte Interessen zu schützen. Auf der anderen Seite fällt der potentiell unbegrenzte Umfang der Datenerhebung ins Gewicht, aufgrund dessen sich ein dichtes Verhaltens- und Persönlichkeitsmodell des Klägers erstellen ließe.

j)
Ein darüberhinausgehender Zahlungsanspruch des Klägers wegen einer Verletzung des allgemeinen Persönlichkeitsrechts nach § 823 Abs. 1 BGB in Verbindung mit Art. 1 Abs. 1, Art. 2 Abs. 1 GG besteht nicht. Die Anwendbarkeit deutschen Rechts auch über die DSGVO hinaus folgt aus der Rechtswahl der Parteien in der Zustimmung zu den Nutzungsbedingungen der Beklagten (Anlage B2, dort Ziffer 4.4.) in Verbindung mit Art. 3 Abs. 1, 6 Abs. 2 Rom I-VO, weil der Kläger Verbraucher ist und seinen gewöhnlichen Aufenthalt in Deutschland hat.

Eine schuldhafte Verletzung des allgemeinen Persönlichkeitsrechts (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) kann einen Anspruch auf Geldentschädigung begründen, wenn der Eingriff schwerwiegend ist und sich die Beeinträchtigung nicht auf andere Weise angemessen kompensieren lässt (ständige Rechtsprechung des Bundesgerichtshofs; vgl. etwa BGH, Urt. v. 12.03.2024 – VI ZR 1370/20, juris-Rn. 70). Dies soll verhindern, dass schwerwiegende Beeinträchtigungen der Menschenwürde und der persönlichen Ehre – insbesondere durch Presseveröffentlichungen – sanktionslos bleiben und der Persönlichkeitsschutz leerliefe (BGH, Urt. v. 17.12.2013 – VI ZR 211/12, juris-Rn. 40 m. w. N.). Bei der Bemessung der Höhe der Entschädigung sollen die „Bedeutung und Tragweite des Eingriffs, also das Ausmaß der Verbreitung der Veröffentlichung, die Nachhaltigkeit und Fortdauer der Interessen- oder Rufschädigung des Verletzten, ferner Anlass und Beweggrund des Handelnden sowie der Grad seines Verschuldens“ berücksichtigt werden (BGH, Urt. v. 17.12.2013 – VI ZR 211/12, juris-Rn. 38).

Ein derart schwerwiegender Eingriff ist hier jedoch nicht feststellbar. Die personenbezogenen Daten des Klägers sind nicht an die allgemeine Öffentlichkeit gelangt. Der erhebliche Umfang der Datenverarbeitung, die Art der verarbeiteten Daten sowie der

Umstand, dass von einem vorsätzlichen Verhalten auszugehen ist, begründen die notwendige besondere Schwere des Eingriffs nicht. Hinzu tritt, dass Art. 82 DSGVO für Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung einen eigenständigen Schadensersatzanspruch vorsieht. Durch die zugesprochene Entschädigung für den erlittenen Kontrollverlust wird die Beeinträchtigung des Klägers insgesamt angemessen und ausreichend kompensiert; eines ergänzenden Rückgriffs auf das deutsche Recht der unerlaubten Handlung bedarf es daneben nicht.

k)
Der Zinsanspruch folgt aus §§ 286 Abs. 1, 288 Abs. 1 Satz 2 BGB. Mit Ablauf der im Schreiben vom 28.09.2023 auf den 19.10.2023 gesetzten Zahlungsfrist ist die Beklagte in Verzug geraten. Ab dem Folgetag schuldet sie Verzugszinsen in gesetzlicher Höhe, so dass ihr – ihrem Antrag entsprechend allerdings erst auf dieses Datum bezogen – Zinsen in dieser Höhe seit dem 27.10.2023 zuzuerkennen sind.

3.
Die festgestellte Rechtswidrigkeit der Datenverarbeitung hat zur Folge, dass auch die mit dem Antrag zu 1. begehrte Feststellung zu treffen war.

4.
Der Kläger kann aufgrund der Rechtswidrigkeit der von der Beklagten praktizierten Datenverarbeitung auch deren Unterlassung im tenorierten Umfang verlangen.

Ein solcher Anspruch folgt zwar nicht unmittelbar aus der DSGVO (EuGH, Urt. v. 04.09.2025 – C-655/23, juris-Rn. 43), jedoch hindert dies die Mitgliedsstaaten nicht daran, präventiven Rechtsschutz mit dem Ziel vorzusehen, dem Verantwortlichen aufzuerlegen, jede weitere Verletzung dieser Rechte zu unterlassen (EuGH, Urt. v. 04.09.2025 – C-655/23, juris-Rn. 47 ff.). Im deutschen Recht ergibt sich ein solcher Anspruch wegen der Verletzung der aus dem Nutzungsvertrag folgenden Rücksichtnahmepflicht aus §§ 280 Abs. 1, 241 Abs. 2 BGB sowie aus einer entsprechenden Anwendung der §§ 1004 Abs. 1 S. 2, 823 Abs. 1 BGB.

a)
Aus der Verletzung von Vertragspflichten nach § 280 Abs. 1 BGB kann sich ein vorbeugender Unterlassungsanspruch ergeben, wenn eine Erstbegehungs- bzw. Wiederholungsgefahr besteht (vgl. BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 83; Urt. v.

02.05.2024 – I ZR 12/23, juris-Rn. 14 f.). Hier liegt die Pflichtverletzung der Beklagten in der Verarbeitung der auf den Drittseiten erhobenen Daten, die sie ohne wirksame Einwilligung des Klägers bzw. über dessen Einwilligung hinausgehend vorgenommen hat.

Die Verschuldensvermutung des § 280 Abs. 1 Satz 2 BGB hat die Beklagte nicht widerlegt.

Für die für den Unterlassungsanspruch notwendige Wiederholungsgefahr spricht nach der von der Beklagten begangenen Pflichtverletzung eine tatsächliche Vermutung (vgl. BGH, Urt. v. 29.07.2021 – III ZR 179/20, juris-Rn. 103 m. w. N.). Dabei kann die Verletzung einer Vertragspflicht die Vermutung der Wiederholungsgefahr nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen begründen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urt. v. 29.07.2021 – III ZR 192/20, juris-Rn. 116 m. w. N.). Einen für die Entkräftung dieser Vermutung hinreichenden Vortrag, an den strenge Anforderungen zu stellen sind (vgl. BGH, Urt. v. 27.04.2021 – VI ZR 166/19, juris-Rn. 23), hat die Beklagte nicht gehalten.

b)
Ein Unterlassungsanspruch folgt auch aus einer entsprechenden Anwendung der §§ 1004 Abs. 1 S. 2, 823 Abs. 1 BGB. Die in ihrem Ausmaß nicht erforderliche und auch nicht durch eine Einwilligung oder einen anderen Rechtsfertigungsgrund im Sinne des Art. 6 Abs. 1 DSGVO gedeckte Datenverarbeitung verletzt den Kläger in seinem allgemeinen Persönlichkeitsrecht (Recht auf informationelle Selbstbestimmung, vgl. hierzu Art. 7, 8 GRCh; Art. 8 EMRK; EuGH, Urt. v. 12.1.1969 – C-29/69, st. Rspr.; BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, Volkszählung, st. Rspr.).

Das rechtswidrige Verhalten dauert auch an, so dass eine Wiederholungsgefahr indiziert ist. Die Beklagte hat nichts zur Widerlegung der Vermutung vorgetragen.

c)
Der Kläger kann nach beiden Anspruchsgrundlagen nicht beanspruchen, der Beklagten jegliche Verarbeitung der streitgegenständlichen Daten zu untersagen. Sein Unterlassungsanspruch erfasst vielmehr nur solche Verarbeitungen, die nicht gerechtfertigt sind.

Dass die Beklagte im vorliegenden Verfahren die beanstandeten Datenverarbeitungsvorgänge nicht zu rechtfertigen vermag, lässt nicht den Schluss zu, ihr werde eine Rechtfertigung auch künftig stets misslingen. Vielmehr ist nicht auszuschließen, dass bestimmte Datenverarbeitungsvorgänge nach den Regelungen der DSGVO gerechtfertigt sein könnten, wenn der Kläger eine Einwilligung zur Verarbeitung bestimmter personenbezogener Daten für einen oder mehrere bestimmte Zwecke freiwillig, in informierter Weise und unmissverständlich i. S. v. Art. 4 Nr. 11 DSGVO erteilt (vgl. EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 91 f.). Ebenso kann die Beklagte die Verarbeitung bestimmter Daten gegebenenfalls auf einen oder mehrere der weiteren – grundsätzlich abschließenden – Rechtfertigungsgründe des Art. 6 Abs. 1 DSGVO stützen, soweit dies nicht pauschal in abstrakter und präventiver Weise, sondern bezogen auf spezifische Verarbeitungsvorgänge erfolgt (vgl. dazu auch OLG München, Urt. v. 18.12.2025, 14 U 1314/25e, juris-Rn. 423 m. w. N.). Ebenso ist nicht auszuschließen, dass die Verarbeitung besonders sensibler Daten in bestimmten Fällen unter den Voraussetzungen des Art. 9 Abs. 2 DSGVO erlaubt ist.

Eine Einschränkung der Unterlassungsverpflichtung mit Blick auf eine mögliche spätere erteilte Einwilligung oder einen erst künftig entstehenden Rechtfertigungsgrund ist gleichwohl nicht veranlasst. Sollte der Kläger zu einem späteren Zeitpunkt wirksam in die zu beanstande Datenverarbeitung einwilligen oder sich nachträglich ein Rechtfertigungsgrund für die Verarbeitung ergeben, kann die Beklagte dies im Wege der Vollstreckungsabwehrklage nach § 767 ZPO geltend machen. Dies gilt auch für titulierte Unterlassungsansprüche (OLG Köln, Urt. v. 26.06.2019 – I-15 U 91/19, juris-Rn. 57).

4.
Der Kläger hat nach Art. 18 Abs. 1 DSGVO einen Anspruch darauf, die bereits verarbeiteten personenbezogenen Daten ab sofort unverändert am bisherigen Speicherort zu belassen und sie erst auf Aufforderung oder spätestens sechs Monate nach rechtskräftigem Abschluss des Verfahrens zu löschen.

Nach Art. 18 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt sowie stattdessen die Einschränkung ihrer Nutzung verlangt.

Der Antrag des Klägers ist dahin auszulegen, dass er eine solche Einschränkung der Datenverarbeitung begehrt. Er verlangt, dass die bei der Beklagten noch vorhandenen personenbezogenen Daten bis zum Abschluss des Verfahrens gespeichert bleiben, jedoch keiner weiteren Verarbeitung unterliegen. Der Antrag erfasst dabei nur solche Daten, die von der Beklagten noch vorgehalten werden und nicht bereits etwa aufgrund interner Löschfristen entfernt worden sind.

Das Recht auf Einschränkung der Verarbeitung kann von der betroffenen Person im Fall einer rechtswidrigen Verarbeitung personenbezogener Daten, wie er hier vorliegt, auch im Zusammenhang mit einem Löschungsverlangen geltend gemacht werden. Art. 18 Abs. 1 lit. b) DSGVO räumt der betroffenen Person insoweit ein Wahlrecht ein. Damit wird ihrem berechtigten Interesse Rechnung getragen, die Daten als Beweismittel oder zur Durchsetzung eigener Rechte zu erhalten, zugleich aber ihre weitere Nutzung zu verhindern (vgl. Dix in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, Art. 18 DSGVO Rn. 3, 6). Die Einschränkung der Verarbeitung bedeutet, dass die personenbezogenen Daten am Speicherort verbleiben, jedoch keiner weiteren Nutzung zugeführt werden dürfen.

5.
Der Kläger kann aus Art. 17 Abs. 1 lit. d) DSGVO die Löschung der personenbezogenen Daten verlangen, die er durch Bezugnahme auf den Feststellungsantrag hinreichend bestimmt bezeichnet hat und deren Verarbeitung durch die Beklagte unrechtmäßig war. Aus Art. 12 Abs. 3 DSGVO folgt sein Anspruch, über die durchgeführte Löschung der Daten Mitteilung zu erhalten.

Ihm steht ferner – nach Wahl der Beklagten – ein Anspruch auf Anonymisierung der unter Ziffer 1 b) und c) seines Antrages bezeichneten Daten zu. Rechtsgrundlage hierfür ist Art. 17 DSGVO. Zwar sieht die Datenschutz-Grundverordnung kein ausdrückliches Recht auf Anonymisierung vor. Die Anonymisierung stellt jedoch ein Minus gegenüber der vollständigen Löschung dar (vgl. Roßnagel in Simitis/Hornung/Spieker gen. Döhmann, Art. 4 Nr. 2 DSGVO Rn 32) und wird deshalb vom Löschungsanspruch erfasst. Der Verantwortliche kann seiner Pflicht aus Art. 17 DSGVO deshalb auch dadurch nachkommen, dass personenbezogene Daten in einer Weise anonymisiert werden, die einen Personenbezug dauerhaft und irreversibel beseitigt, sofern die betroffene Person ihr Verlangen auf die bloße Anonymisierung anstelle der vollständigen Löschung beschränkt (ebenso OLG Dresden, Urt. v. 03.02.206 – 4 U 292/25, juris-Rn.

191; a. A. OLG München, Urt. v. 18.12.2025 – 14 U 881/25, juris-Rn. 201 ff.; OLG Stuttgart, Urt. v. 29.04.2026 – 4 U 372/24, juris-Rn. 220 ff.).

Das Löschungsrecht dient dem Schutz des informationellen Selbstbestimmungsrechts der betroffenen Person. Sie kann daher grundsätzlich selbst bestimmen, in welchem Umfang sie ihr Recht geltend macht. Insbesondere ist sie nicht darauf beschränkt, die vollständige Löschung sämtlicher Daten zu verlangen, sondern kann ihr Begehren auf bestimmte Datenkategorien, Verarbeitungsformen oder Verarbeitungszwecke beschränken (vgl. BGH, Beschl. v. 04.06.2024 – II ZB 10/23, juris-Rn. 19) und/oder dem Verantwortlichen – wie hier – ein entsprechendes Wahlrecht zubilligen.

6.
Der Anspruch auf Freistellung von außergerichtlichen Rechtsanwaltskosten ist nur in Höhe von 367,23 Euro begründet.

a)
Aus Art. 82 Abs. 1 DSGVO ergibt sich ein materiell-rechtlicher Kostenerstattungsanspruch für die anwaltliche Tätigkeit, wenn und soweit die Rechtsverfolgungskosten zur Wahrnehmung der Rechte erforderlich und zweckmäßig waren (vgl. BGH, Urt. v. 18.11.2024 – VI ZR 10/24, Rn. 78 ff.). Danach sind dem Kläger die Rechtsanwaltskosten zu ersetzen, die durch die außergerichtliche Geltendmachung seiner begründeten Ansprüche entstanden sind. Ein Fall, in dem die Haftung von vornherein nach Grund und Höhe derart klar ist, dass aus der Sicht des Geschädigten kein vernünftiger Zweifel daran bestehen kann, dass der Schädiger ohne weiteres seiner Ersatzpflicht nachkommen werde (vgl. dazu BGH, a.a.O., Rn. 79), ist nicht gegeben, weil die betroffenen Rechtsfragen höchstgerichtlich noch ungeklärt sind (vgl. dazu BGH, a.a.O., Rn. 80).

b)
Zugrunde zu legen ist ein Gegenstandswert in Höhe von 3.000,00 Euro (begründeter Schadensersatzbetrag in Höhe von 750,00 Euro, Unterlassen 750,00 Euro, Feststellung 500,00 Euro, Belassen und Löschen der Daten je 500,00 Euro). Der Freistellungsanspruch berechnet sich demnach als 1,3 Geschäftsgebühr nach Nr. 2300 VV RVG aus diesem Gegenstandswert zuzüglich Post- und Telekommunikationspauschale in Höhe von 20,00 Euro und Mehrwertsteuer. Hieraus ergibt sich ein Betrag in Höhe von 367,23 Euro.

III.

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 10, 709 Satz 1 und 2, 711 ZPO.

Die Revision ist zuzulassen, weil die Rechtssache angesichts der Vielzahl geführter Verfahren grundsätzliche Bedeutung hat und die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Revisionsgerichts erfordert.

Der **Streitwert** beläuft sich für beide Instanzen auf **7.250,00 Euro** (Schadensersatz 5.000,00 Euro, Feststellung 500,00 Euro, Unterlassung: 750,00 Euro, Vorhalten und Löschen der Daten: jeweils 500,00 Euro).

[redacted] [redacted] [redacted]