Landgericht Frankfurt am Main

2-31 O 39/24

Im Namen des Volkes

Urteil

In dem Rechtsstreit

[redacted]

- Klägerin -

Prozessbevollmächtigte:
Rechtsanwälte und Rechtsanwältinnen BK Automotive
Rechtsanwaltsgesellschaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin
Geschäftszeichen: DTS-009610-24

gegen

Meta Platforms Ireland Ltd. v.d.d. GF Yvonne Cunnane, Anne O`Leary, Genevieve Hughes, Majella Mungovan u. David Harris, Merrion Road, Dublin 4, D04 X2K5, IRLAND

- Beklagte -

Prozessbevollmächtigte:
[redacted]

hat das Landgericht Frankfurt am Main – 31. Zivilkammer – durch den Richter am Landgericht [redacted] als Einzelrichter auf die mündliche Verhandlung vom 27.03.2026 für Recht erkannt:

1. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps

außerhalb der Netzwerke der Beklagten die folgenden genannten personenbezogenen Daten der Klägerin

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**
- **die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid" genannt)**

sowie folgende personenbezogene Daten der Klagepartei

b) auf Webseiten

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

c) in mobilen Dritt-Apps

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

mit Hilfe einer Software Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden, sofern die Beklagte die Verarbeitung der personenbezogenen Daten nicht auf eine informierte Einwilligung i. S. d. Art. 6 I 1 lit. a) DSGVO oder einen Rechtfertigungsgrund nach Art. 6 I 1 lit. b) bis f) oder Art. 9 II DSGVO stützen kann.

2. Die Beklagte wird verurteilt, die über die aktuelle Speicherung hinausgehende weitere Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO sämtlicher unter dem Tenor zu 1) 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 weiterzugeben.

3. Die Beklagte wird verpflichtet, sämtliche gemäß Tenor zu 1) 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 gemäß dem Tenor zu 1) seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.

4. Die Beklagte wird verurteilt, an die Klägerin immateriellen Schadensersatz in Höhe von 2.000,00 EUR nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 03.04.2024 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits hat die Klägerin zu 40% und hat die Beklagte zu 60% zu tragen.

7. Das Urteil ist für die Klägerin hinsichtlich des Tenors zu 1. und 2. sowie 3. gegen Sicherheitsleistung in Höhe von 6.000,00 € (Tenor zu 1: 3.500 €, Tenor zu 2: 1.250 €, Tenor zu 3: 1.250 €), bezüglich des Tenors zu 4 sowie bezüglich der Kosten gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar; das Urteil ist für die Beklagte vorläufig vollstreckbar, die Klägerin kann die Zwangsvollstreckung durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Zwangsvollstreckung Sicherheit in Höhe von 110% des zu vollstreckenden Betrags leistet.

8. Der Streitwert wird für den Rechtsstreit auf 12.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten über Feststellungs-, Löschungs-, Unterlassungs- und Schadensersatzansprüche im Zusammenhang mit der Verarbeitung personenbezogener Daten der Klagepartei durch sog. Business Tools der Beklagten. Die Klägerin macht Ansprüche aus der behaupteten Praxis der Beklagten geltend, diese missachte das europäische Datenschutzrecht, indem sie die Nutzer überwache, deren persönliche und höchstpersönliche Daten rechtswidrig erhebe, in unsichere Drittstaaten übertrage, dort unbefristet speichere, diese in unbekannten Maße auswerte und an Dritte weitergebe, ohne den betroffenen Nutzer hiervon zu informieren.

Die Klägerin nutzt als Privatperson seit dem 01.01.2017 zu privaten Zwecken das soziale Netzwerk „Instagram“ unter dem Benutzernamen [redacted] Betreiberin des Netzwerks, somit Vertragspartnerin der Klagepartei und Verantwortliche i.S.d. Art. 4 DSGVO, ist die Beklagte, die bis zum 27.10.2021 als “Facebook Ireland Ltd.” (nunmehr „Meta“, wobei unverändert „Instagram“ betrieben wird) firmierte. Die Beklagte ist in Irland, Europa, geschäftsansässig.

Die Klägerin besuchte nach dem Beginn der Nutzung des sozialen Netzwerks „Instagram“ unter anderem Internetseiten wie „paypal.com“, „booking.com“ und „idealo.de“, wobei auch Nutzungen im kontextualen Zusammenhang mit dem Nutzen von „Instagram“ erfolgte. Die Beklagte betreibt auch das soziale Netzwerk „Facebook“. Als Gegenleistung für die Nutzung des Netzwerks fordert die Beklagte kein Geld. Der Klagepartei wird bei Nutzung des Netzwerks Werbung angezeigt, die auf ihren Interessen basiert, welche die Algorithmen der „Meta Ltd.“ aus den Tätigkeiten der Klagepartei in Instagram sowie den sozialen Kontakten, die sie in Instagram pflegt, extrahieren können. Wahlweise können die Nutzer seit November 2023 ein Abo-Modell wählen, bei dem sie gegen Zahlung einer monatlichen Gebühr die Anzeige von Werbung abschalten können. Dafür nutzt und verarbeitet die Beklagte verschiedene Daten, die sie in ihrer Datenschutzrichtlinie (Anlage K 1, S. 5 ff.) aufführt und auf die sie bei der Registrierung ebenso hinweist wie auf die Cookie-Richtlinie. Zu diesen Daten gehören neben den persönlichen Informationen, die der Nutzer bei der Registrierung angibt, wie Name, E-Mail-Adresse und Telefonnummer (vgl. Nutzungsbedingungen S. 1, Anlage B 1), das Nutzungsverhalten des jeweiligen Nutzers in Produkten der Beklagten (= sog. On-Site-Daten), Informationen über Freunde und Follower des Nutzers und deren Nutzungsverhalten in Produkten der Beklagten sowie Informationen über die technischen Geräte, mit deren Hilfe der Nutzer die Produkte der Beklagten nutzt. Zudem sammelt die Beklagte sog. Eventdaten, die sie bezeichnet als „Informationen von Partnern über Handlungen, die du sowohl innerhalb als auch außerhalb unserer Produkte durchführst. Dazu können z. B. andere von dir besuchte Websites, von dir verwendete Apps oder von dir gespielte Online-Spiele gehören.“ Weiter heißt es: „Partner teilen auch Informationen wie deine E-Mail-Adresse, Cookies und deine Geräte-ID für Werbezwecke mit uns. … Wir erhalten diese Informationen unabhängig davon, ob du bei unseren Produkten angemeldet bist bzw. ein Konto auf ihnen hast oder nicht. Partner geben außerdem ihre Kommunikation mit dir an uns weiter, wenn sie uns anweisen, Dienstleistungen für ihr Unternehmen zu erbringen, wie Unterstützung bei der Verwaltung ihrer Kommunikation […] … Partner nutzen unsere Tools, Integrationen und … Audience Network-Technologien, um Informationen mit uns zu teilen. Diese Partner erheben deine Informationen, wenn du ihre Website oder App besuchst oder ihre Dienste nutzt…“. (vgl. im Einzelnen auch S. 9 der Anlage K 1). Bei Letzteren handelt es sich um sog. Off-Site-Daten. Die Daten werden „gehasht“ (verschlüsselt) übersandt, wobei die gleichen Daten über den gleichen Schlüssel zur gleichen Verschlüsselung führen, so dass jeweils gleichartige „Hashs“ zusammengeführt und sodann dem Nutzer zugeordnet werden können (vgl. S. 9, 10, Anlage K 1 – Datenschutzrichtlinie und S. 2 Anlage K 4 – Parameter für Kund*inneninformation). Die Klägerin hat sich nicht für das Abo-Modell mit einer Bezahlung entschieden; ein solches Modell existiert auch für Instagram. Das Geschäftsmodell des sozialen Online-Netzwerks Instagram beruht, neben der Variante mit der Bezahlung im Abo-Modell, auf der Finanzierung durch Onlinewerbung, die sich gezielt an den individuellen Nutzer des sozialen Netzwerks insbesondere nach Maßgabe seines Konsumverhaltens, seiner Interessen und seiner Lebenssituation richtet. Diese Art der Werbung wird technisch ermöglicht, indem automatisiert detaillierte Profile der Nutzer erstellt werden.

Die Beklagte unterhält unter dem Begriff “M Business Tools“ zusammengefasste Software-Produkte wie insbesondere „M Pixel“, „App Events über F SDK“ (bzw. „F SDK“), „Conversions API“ und „App Events API“. Diese stellt sie Webseiten- und App-Betreibern (nachfolgend: Dritte) zur Verfügung. Dritte können die “M Business Tools“ in ihre eigenen Webseiten- und App-Angebote technisch einbinden, um durch Erfassung des Nutzerverhaltens ihrer Besucher u.a. spezifisch auf den einzelnen Nutzer zugeschnittene Werbung auf den sozialen Netzwerken der Beklagten, darunter dem vom Kläger genutzten „I“, zu schalten. Auch können Dritte anhand der „M Business Tools“ die Effektivität ihrer Werbemaßnahmen messen. Dritte, die die “M Business Tools“ entweder einzeln oder in Kombination nutzen, übermitteln zu den genannten Zwecken Daten über die Kundenaktivität auf ihrer Webseite bzw. in ihrer App an die Beklagte. Dabei erfolgt – je nach genutztem „Tool“ auf unterschiedlichem technischen Weg – eine individuelle Zuordnung der erfassten Kundenaktivität zum Nutzerprofil auf der jeweiligen Plattform der Beklagten, hier also zum Profil der Klägerin bei Instagram. Das Geschäftsmodell des sozialen Netzwerks „Instagram“ beruht auf der Finanzierung durch Onlinewerbung, die sich gezielt an den individuellen Nutzer des sozialen Netzwerks insbesondere nach Maßgabe seines

Konsumverhaltens, seiner Interessen und seiner Lebenssituation richtet. Diese Art der Werbung wird technisch ermöglicht, indem automatisiert detaillierte Profile der Nutzer erstellt werden. Die Individualisierung bezüglich einer einzelnen Person gelingt, indem zahlreiche Daten wie etwa die IP-Adresse, das Betriebssystem, die Sprache, die Zeitzone, die Bildschirm-Auflösung, das Tastaturlayout und unterstützte Audioformate erfasst werden, die zwar jeweils für sich keine Aussagekraft haben, in der Zusammenschau indes eine individuelle Zuordnung mit Wahrscheinlichkeiten von über 99% ermöglichen. Vorstehende Informationen fallen dabei als sog. HTTP-Standarddaten gleichsam automatisch an, wenn ein Nutzer durch eine entsprechende Eingabe einer Webseitenadresse im Browser die Webseite eines Dritten ansteuert. Denn sie werden nach dem maßgeblichen HTTP-Protokoll dem Webserver des Dritten zwingend mitgeteilt, damit dieser die Webseite in funktionsfähiger Weise auf dem jeweils genutzten Endgerät bereitstellen kann. Die Erfassung von Nutzerdaten durch die „M Business Tools" und Übermittlung an die Beklagte erfolgt unabhängig davon, ob der Nutzer zum jeweiligen Zeitpunkt mit dem betreffenden Endgerät auf einer Plattform der Beklagten angemeldet ist oder nicht. Neben den die individuelle Zuordnung ermöglichenden HTTP-Standarddaten ermöglichen die „M Business Tools" auch die Erfassung weiterer Informationen, sog. Kunden- bzw. Aktivitätsdaten. Diese betreffen das spezifische Nutzungsverhalten auf einer Webseite oder in einer App, darunter auch Eingaben in Formularfelder, in Suchmasken oder das Betrachten einzelner Videos. Die Business-Tools dienen dazu, personenbezogene Daten zu sammeln, die diese Unternehmen aus online und offline erfolgten Kunden-Interaktionen gewinnen; hierzu gehören sog. „Kontaktinformationen" und sog. „Event-Daten" (vgl. Anlage B 5). 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 Datenschutzrichtlinien der Beklagten (Anlage K 1), die auf die Nutzung des Meta-Business-Tools durch Dritte hinweisen,

Arten von Partnern

Partner

Unsere Partner[3] nutzen unsere Produkte, u. a. unsere Business-Tools und andere Technologien, mit denen Unternehmen ihre Produkte bewerben oder unterstützen können. Außerdem können unsere Partner mithilfe der Business-Tools feststellen und messen, wie ihre Produkte und Dienstleistungen genutzt werden und wie gut ihre Werbeanzeigen funktionieren. Beispielsweise können sie eines unserer Business-Tools, das Meta-Pixel, auf ihrer Website platzieren. Oder sie verwenden die Meta Audience Network-Tools, um mit ihren Apps Geld

Informationen, die wir erheben und erhalten, wenn du unsere Produkte nutzt oder mit ihnen interagierst, abei kein Konto hast

Auch wenn du kein Konto hast, kannst du Meta-Produkte[4] nutzen oder mit ih· nen interagieren. Dann erheben wir u. a. Folgendes:

- Browser- und App-Protokolle über deine Besuche von öffentlichen Inhalten, wie Facebook-Seiten, Videos und Räumen
- Allgemeine Informationen über Geräte[12], die unsere Apps heruntergelader haben, darunter Gerätemodell und Betriebssystem

Wir erhalten außerdem Informationen mithilfe von Cookies und ähnlichen Tecl nologien wie dem Meta-Pixel oder sozialen Plugins, wenn du andere Websites und Apps besuchst, die unsere Business-Tools oder andere Meta-Produkte

:book.com/privacy/policy/printable/

Meta-Datenschutzrichtlinie – So erfasst und verwendet Meta Nutzerdaten

nutzen. In dieser Richtlinie und in unserer Cookies-Richtlinie erfährst du mehr

sowie Hinweise der Beklagten (Anlage B 3), in der auf die Meta-Business-Tools als Produkt ausdrücklich hingewiesen wird,

Unsere Produkte

Zu den Meta-Produkten zählen folgende:

- Facebook (einschließlich der mobilen Facebook-App und dem mobilen app-internen Browser)
- Messenger
- Instagram (einschließlich Apps wie Threads und Boomerang)
- Portal-Gerate von Meta
- Meta Platforms Technologies-Produkte wie etwa Meta Horizon Worlds oder Meta Quest (sofern ein Facebook- oder Meta-Konto verwendet wird)
- Shops
- Meta Spark
- Meta Audience Network
- NPE Team-Apps
- Meta-Business-Tools
- Alle weiteren Features, Apps, Technologien, Softwares, Produkte oder Dienstleistungen, die von Meta Platforms, Inc. oder Meta Platforms Ireland Limited angeboten werden und unserer Datenschutzrichtlinie unterliegen.

Die Meta-Business-Tools

Link kopieren

Die Meta-Business-Tools sind Technologien, die von Meta Platforms, Inc. und Meta Ireland Limited angeboten werden. Sie unterstutzen Websitebetreiber*innen, Publisher*innen, App-Entwickler*innen und Business-Partner, darunter auch Werbetreibende, bei der Integration ihrer Apps und Websites mit Meta. Damit können sie die Leistung ihrer Produkte und Dienstleistungen besser verstehen und messen. Gleichzeitig können sie Personen, die diese nutzen oder daran Interesse haben, besser erreichen und ihnen einen besseren Service bieten. Zu diesen Business-Tools gehoren beispielsweise das Meta-Pixel, die Conversions API, App-Events uber Facebook-SDK, Offline-Conversions und die App Events API. Wir empfangen außerdem Daten der Business-Tools als Impressionen und Klickdaten (z. B. „Gefällt mir"-Angaben oder die Anzahl der Klicks auf den „Teilen"-Button), die durch soziale Plugins von Facebook und Facebook Login ubermittelt werden. Daruber hinaus empfangen wir Daten von bestimmten APIs, beispielsweise den Messenger-Kund*innenabgleich von der Send API oder aus bestimmten Pilot-, Test-, Alpha- oder Beta-Programmen, die wir von Zeit zu Zeit anbieten. Weitere Informationen findest du in den Nutzungsbedingungen fur Meta-Business-Tools.

und Nutzungsbedingungen für Meta-Business-Tools (Anlage B 5) ist auszugsweise hinterlegt:

In der Anlage B 5

1. Teilen von Business-Tool-Daten mit Meta
   a. Du kannst die Meta-Business-Tools nutzen, um uns eine oder beide der folgenden Arten von personenbezogenen Informationen („**Business-Tool-Daten**") für die in Abschnitt 2 beschriebenen Zwecke zu senden:
      i. „**Kontaktinformationen**" sind Informationen, mit denen Einzelpersonen identifiziert werden können, wie Namen, E-Mail-Adressen und Telefonnummern. Diese verwenden wir nur für Abgleichzwecke. Wir hashen vor der Übermittlung die Kontaktinformationen, die du uns über ein Meta-JavaScript-Pixel für Abgleichzwecke sendest. Wenn du oder dein Dienstanbieter ein Meta-Image-Pixel oder andere Meta-Business-Tools nutzt, musst du bzw. muss dein Dienstanbieter vor der Übermittlung die Kontaktinformationen auf eine von uns vorgegebene Art und Weise hashen.
      ii. „**Event-Daten**" sind sonstige Informationen, die du über Personen und ihre Handlungen teilst, die sie auf deinen Websites und in deinen Apps oder Shops vornehmen, wie z. B. Besuche auf deinen Websites, Installationen deiner Apps und Käufe deiner Produkte. Event-Daten umfassen zwar Informationen, die erfasst und übermittelt werden, wenn Personen mit Facebook Login oder sozialen Plugins (z. B. dem „Gefällt mir"-Button) auf eine Website oder App zugreifen, jedoch keine Informationen, die erstellt werden, wenn ein Nutzer über Facebook Login, soziale Plugins oder auf sonstige Weise mit unserer Plattform interagiert (beispielsweise indem er sich einloggt oder einen Artikel oder ein Lied mit „Gefällt mir" markiert oder teilt). Für Informationen, die erstellt werden, wenn eine Person über Facebook Login, soziale Plugins oder auf sonstige Weise mit unserer Plattform interagiert, gelten die Plattform-Nutzungsbedingungen.
      iii. Hinweis: Im Sinne dieser Nutzungsbedingungen für Business-Tools bezeichnen Bezugnahmen in bestehenden Nutzungsbedingungen oder Vereinbarungen auf „Kundendaten" jetzt die „Business-Tool-Daten".
   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 Busi 389
Tool-Daten gegen den zufälligen oder unberechtigten Zugriff bzw. gegen die versehentlic
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. (Sie werden von Zeit zu Zeit aktualisiert, um beispielsweise technologischen Entwicklungen Rechnung zu tragen.)

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).
f. Du informierst uns unverzüglich schriftlich über jegliche tatsächliche oder drohende Beschwerde oder Anfechtung im Zusammenhang mit der Verwendung irgendwelcher Business-Tool-Daten gemäß diesen Nutzungsbedingungen für Business-Tools. Außerdem arbeitest du mit uns zusammen bei der Reaktion auf eine derartige Beschwerde oder Anfechtung.
g. Wenn du die Business-Tool-Daten im Auftrag eines Dritten oder zusammen mit diesem verwendest oder teilst, versicherst und gewährleistest du zudem, dass du als dessen Vertreter berechtigt bist, diese Daten in seinem Auftrag zu verwenden, zu teilen und zu verarbeiten und einen solchen Dritten an diese Nutzungsbedingungen für Business-Tools zu binden. Du verwendest oder teilst die Business-Tool-Daten bzw. jegliche durch die Verwendung der Business-Tool-Daten erzeugten Zielgruppen oder Berichte nur zusammen mit einem solchen Dritten bzw. in seinem Auftrag.
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).

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, einschließlich (a) um in deinem Auftrag Berichte über die Wirkung deiner Werbekampagnen und sonstigen Online-Inhalte anzufertigen, z. B. um deine Conversions zu den über unsere Plattform verzeichneten Impressionen zuzuordnen („**Kampagnenberichte**"), und (b) um Analysen und Einblicke über Nutzer und ihre Nutzung deiner Apps, Websites, Produkte und Dienstleistungen zu erstellen („**Analysen**").
2. Wir gewähren dir eine nicht-exklusive und nicht übertragbare Lizenz, die Kampagnenberichte und Analysen ausschließlich für deine internen Geschäftszwecke bzw. ausschließlich in aggregierter und anonymisierter Form für Messungen zu verwenden. Du darfst ohne unsere schriftliche Zustimmung die Kampagnenberichte oder Analysen bzw. irgendeinen Teil dieser nicht gegenüber irgendeinem Dritten offenlegen. Wir legen ohne deine Erlaubnis die Kampagnenberichte oder Analys[illegible] irgendeinen Teil dieser nicht gegenüber irgendeinem Dritten offen, es sei denn, (i) sie sind mit Kampagnenberichten und Analysen von zahlreichen anderen Dritten kombiniert worden und (ii) deine identifizierenden Informationen werden aus den kombinierten Kampagnenberichten und Analysen entfernt.

390

iii. **Event-Daten für das Targeting deiner Werbeanzeigen**

1. Du stellst möglicherweise Event-Daten bereit, um deine Werbekampagnen auf Personen auszurichten, die mit deinem Unternehmen interagieren. Du kannst uns anweisen, Custom Audiences, also auf Event-Daten basierende Gruppen von Nutzern von **Meta-Produkten**, zu erstellen, um Werbekampagnen auszurichten (einschließlich Custom Audiences über Websites, Custom Audiences über mobile Apps und Offline-Custom Audiences). Meta verarbeitet Event-Daten, um solche Zielgruppen für dich zu erstellen. Du darfst diese Zielgruppen nicht verkaufen oder übertragen und auch nicht irgendeinen Dritten autorisieren, diese Zielgruppen zu verkaufen bzw. zu übertragen. Meta stellt solche Zielgruppen nicht anderen Werbekunden bereit, es sei denn, du oder deine Dienstanbieter teilen über Tools, die wir zu diesem Zweck zur Verfügung stellen, Zielgruppen mit anderen Werbetreibenden. Dies unterliegt dann den Einschränkungen und Anforderungen dieser Tools sowie unseren Nutzungsbedingungen.
2. Diese Nutzungsbedingungen für Business-Tools gelten für die Nutzung von Custom Audiences über Websites, Custom Audiences über mobile Apps und Offline-Custom Audiences, die mithilfe der Meta-Business-Tools erstellt wurden. Auf Kundenlisten beruhende Custom Audiences, die über unser separates Custom Audience-Feature bereitgestellt werden, unterliegen den **Nutzungsbedingungen für Kundenlisten-Custom Audiences**

Audiences

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; außerdem (ii) gestatten wir anderen Werbekunden oder Dritten nicht, Werbung ausschließlich auf der Grundlage deiner Event-Daten auszurichten.
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. Diese Nutzungsbedingungen für Business-Tools ersetzen keine Nutzungsbedingungen, die für deinen Kauf von Werbeinventar von uns gelten (wie u. a. die **Nutzungsbedingungen für Self-Serve**

392

Ads und die **Meta-Werbestandards**). Solche Nutzungsbedingungen gelten auch weiterhin für deine Werbekampagnen. Die **Meta-Nutzungsbedingungen für Kundenlisten-Custom Audiences** gelten nicht für Zielgruppen, die gemäß diesen Nutzungsbedingungen für Business-Tools durch Verarbeitung von Business-Tool-Daten erstellt wurden.

c. Wir behalten uns das Recht vor, deine Einhaltung dieser Nutzungsbedingungen für Business-Tools zu überwachen bzw. zu überprüfen.

d. Diese Nutzungsbedingungen für Business-Tools ergänzen und ändern die **Bedingungen für die gewerbliche Nutzung**. Meta kann diese Nutzungsbedingungen für Business-Tools von Zeit zu Zeit aktualisieren. Durch deine weitere Nutzung der bzw. den Zugriff auf die Business-Tools nach jeglicher Aktualisierung, stimmst du zu, an die aktualisierten Nutzungsbedingungen gebunden zu sein.

e. Kein Teil in diesen Nutzungsbedingungen für Business-Tools hindert uns daran, Offenlegungen im Zusammenhang mit Meta-Business-Tools gegenüber unseren Nutzern vorzunehmen, zu denen wir angewiesen werden können oder die wir möglicherweise für angemessen oder gemäß geltendem Recht für erforderlich erachten.

f. Falls sich irgendein ausdrücklicher Widerspruch zwischen diesen Nutzungsbedingungen für Business-Tools und den Bedingungen für die gewerbliche Nutzung ergibt, so gelten diese Nutzungsbedingungen für Business-Tools lediglich hinsichtlich deiner Nutzung der Meta-Business-Tools und auch nur im Umfang des Widerspruchs.

5. Zusätzliche Bedingungen für die Verarbeitung personenbezogener Informationen

a. **DSGVO**. Sofern die Business-Tool-Daten personenbezogene Informationen enthalten, die du gemäß der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) (die „DSGVO") 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 Limited, Block J, Serpentine Avenue, Dublin 4, Ireland („Meta 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 Meta Ireland die Mittel und Zwecke festlegst, erkennen du und Meta Ireland an und stimmen zu, gemeinsam Verantwortliche gemäß Artikel 26 DSGVO zu sein. Die gemeinsame Verantwortlichkeit umfasst die Erhebung solcher personenbezogenen Informationen über die Meta-Business-Tools und ihre anschließende Übermittlung an Meta Ireland, um sie für die oben in den Abschnitten 2.a.iii bis 2.a.v.1 („Gemeinsame Verarbeitung") dargelegten Zwecke zu verwenden. Klicke **hier**, um weitere Informationen zu erhalten. Die gemeinsame Verarbeitung unterliegt dem **Zusatz für Verantwortliche**, der durch Bezugnahme ausdrücklich Bestandteil dieser Nutzungsbedingungen wird, und gilt zwischen dir und Meta Ireland zusammen mit diesen Nutzungsbedingungen für Business-Tools. Meta Ireland bleibt für jegliche Verarbeitung dieser Daten nach deren Übermittlung an Meta Ireland ein unabhängiger Verantwortlicher gemäß Artikel 4(7) DSGVO.

https://www.facebook.com/legal/businesstech?paipv=0&eav=AfbXinCq68_P0zIHbFNCOkf33MX7jX8cOaRNRyvolo56uDX4lVlQ3d3ZlGWlpeZg9z… 5/7

1/12/24, 4:16 PM (12) Facebook

iii. Du bleibst bzw. Meta Ireland bleibt für jegliche Verarbeitung von in Business-Tool-Da enthaltenen personenbezogenen Informationen gemäß DSGVO, die nicht den Absch 5.a.i und 5.a.ii unterliegt, unabhängiger Verantwortlicher gemäß Artikel 4(7) DSGVO.

393

In einem weiteren Informationsblatt (Anlage B 6) ist bezüglich des Business-Tools hinterlegt:

„Identifizieren von potenziell unzulässigen Informationen und entsprechende Benachrichtigungen. Du wirst z. B. möglicherweise per E-Mail, im Meta Events Manager oder im Meta-Werbeanzeigenmanager benachrichtigt, wenn Metas System in den von dir geteilten Daten potenziell unzulässige Informationen entdeckt und daraus entfernt. … Metas Systeme sind zwar darauf ausgelegt, potenziell unzulässige Informationen herauszufiltern, die sie erkennen können, aber letztendlich bist du für die Daten verantwortlich, die du mit Meta teilst. Du kannst am besten gewährleisten, dass deine Integration keine vertraulichen oder unzulässigen Informationen an Meta sendet. Metas Systeme sollen deine eigenen Mechanismen zur Einhaltung dieser Regeln lediglich ergänzen. …

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

Ausnahme bestimmter Daten, die für begrenzte Zwecke wie Sicherheit und Integrität verwendet werden können.

Mit der Registrierung bei einem von der Beklagten betriebenen sozialen Netzwerk (wie „Instagram“) stimmen Nutzer – so auch die Klägerin – diesbezüglichen Nutzungsbedingungen zu (Anlage B2, Fassung vom 15.01.2024), die wiederum auf eine Datenschutzrichtlinie (Anlage B10, aktualisierte Fassung vom 07.03.2024) 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 sinngemäß mit:

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

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

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:

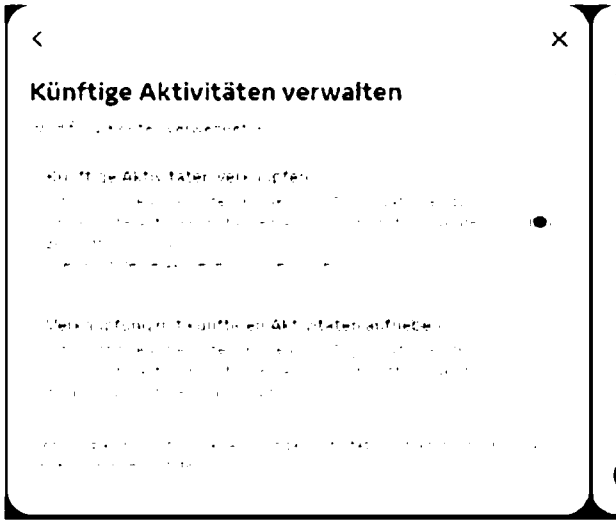

Abbildung 30



Abbildung 31

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

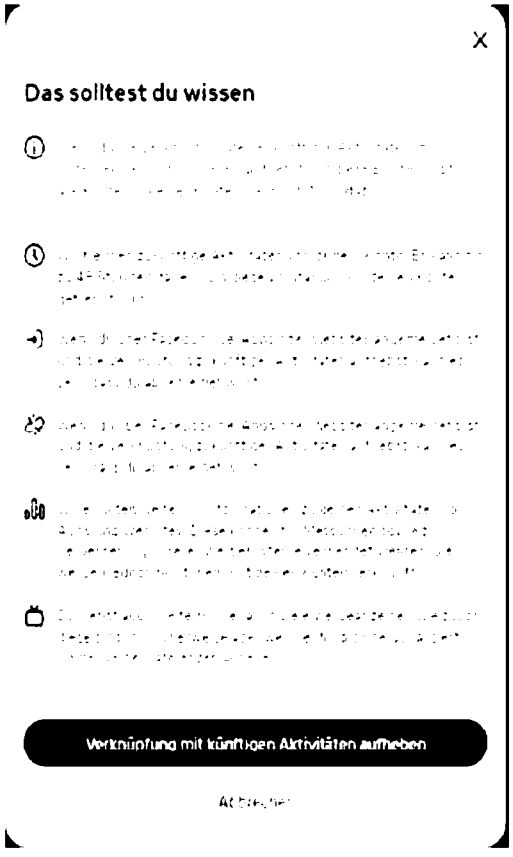

Abbildung 32

Ferner bietet die Beklagte den Nutzern ihrer sozialen Netzwerke „Kontoverlauf“- und „Deine Informationen herunterladen“-Tools an, welche es ihnen ermöglichen sollen, ihre I.-Profilinformationen anzusehen und von ihnen eine Kopie herunterzuladen, einschließlich Informationen zu den Aktivitäten, die Meta von Drittunternehmen auf den sozialen Netzwerken erhält (vgl. zu den Einzelheiten Anlage B 7).

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. Die Klageschrift wurde am 02.04.2024 zugestellt (Schreiben vom 12.02.2024, dortige Seite 3).

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-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.

Die Klägerin beantragte zunächst wörtlich,

> 1. Es wird festgestellt, dass bei rechtskonformer Auslegung des Nutzungsvertrages der Parteien zur Nutzung des Netzwerks "Instagram" unter dem Benutzernamen [redacted] abweichend von den Regelungen des Nutzungsvertrags die Verarbeitung von folgenden personenbezogenen Daten, die die Beklagte auf Drittwebseiten und –Apps außerhalb der Netzwerke der Beklagten verarbeitet und im Zuge dessen mit dem obigen Nutzeraccount der Klagepartei verknüpft hat, in folgendem Umfang seit dem 25.05.2018 nicht zulässig war:
>
> a) auf besuchten Dritt-Webseiten und -Apps die personenbezogenen Daten, die der Identifizierung der Klagepartei dienen, 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 die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid“ genannt)

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

> b) auf Dritt-Webseiten
>
> die URLs der Webseiten samt ihrer Unterseiten der Zeitpunkt des Besuchs der Referrer (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist), die von der Klagepartei auf der Webseite angeklickten Buttons sowie weitere von der

Meta „Events“ genannte Daten, die die Interaktionen der Klagepartei auf der jeweiligen Webseite dokumentieren

c) in mobilen Dritt-Apps

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

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihre 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, ohne wirksame Einwilligung der Klagepartei auf Drittseiten – und Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten gem. des Antrags zu 1. zu verarbeiten, solange im Einzelfall kein Rechtfertigungsgrund gem. Art. 6 Abs 1 b – e DSGVO vorliegt.

3. Die Beklagte wird verurteilt, die weitere 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, zu unterlassen, insbesondere diese nicht an Dritte weiterzugeben.

4. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, der aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 06.02.2024, zu zahlen.

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

sowie hilfsweise im Wege der Stufenklage die Anträge zu 6., 7. und 8., falls der Antrag zu 1. dem Grunde nach zugesprochen, dem Antrag zu 4. jedoch nicht vollständig stattgegeben wird:

6. Die Beklagte wird verurteilt, Auskunft nach Art. 15 I lit. a), c), g) und h) darüber zu erteilen, welche personenbezogenen Daten gem. des Antrags zu 1. a.-c. die Beklagte seit dem 25.05.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Instagram“ unter dem Benutzernamen [redacted] der Klagepartei verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business Tools“,

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 25.05.2018 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat, unter Benennung dieser Dritten,

ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte seit dem 25.05.2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

inwieweit die Daten der Klagepartei für eine automatisierte Entscheidungsfindung einschließlich Profiling verwendet wurden und werden. Die Beklagte hat hierfür aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für die betroffene Person zu erteilen.

7. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 6. sämtliche gem. des Antrags zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu löschen und der Klagepartei die Löschung zu bestätigen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren

sowie auf zweiter Stufe (Stufenklage):

8. Die Beklagte wird verurteilt, an die Klagepartei materiellen und immateriellen Schadensersatz aufgrund der Verarbeitung der gem. des Antrags zu 6. beauskunfteten Daten, dessen Höhe in das Ermessen des Gerichts gestellt wird, und dessen Mindestsumme nach erfolgter Auskunftserteilung konkretisiert wird, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 06.02.2024, zu zahlen

sowie hilfsweise der Antrag zu 9., falls der Antrag zu 1. dem Grunde nach zugesprochen und dem Antrag zu 4. vollständig stattgegeben wird:

9. Die Beklagte wird verpflichtet, sämtliche gem. des Antrags zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten der Klagepartei hin vollständig zu löschen und der Klagepartei die Löschung zu bestätigen, sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren.

Mit Schreiben vom 08.01.2025 hat die Klägerin die Anträge umgestellt (Bl. 816 ff. d. A.).

Die Klägerin beantragt zuletzt wörtlich,

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

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

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

- Lead-ID
- anon_id
- die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid" genannt)

sowie folgende personenbezogene Daten der Klagepartei

b) auf Webseiten

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

c) in mobilen Dritt-Apps

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

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

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

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

5. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber

mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 06.02.2024, zu zahlen.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Sie ist der Auffassung, streitgegenständlich sei allein die Datenverarbeitung zur Bereitstellung personalisierter Werbung gemäß Art. 6 I 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. . 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 (wie etwa 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. Die Beklagte bestreite mit Nichtwissen, dass die Klägerin diese Webseiten besucht hätte; auch habe nicht dargetan werden können, ob hier eine konkrete Verletzung der Klägerin überhaupt vorgelegen habe.

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 Klage ist, soweit nicht Gegenteiliges dargetan wird, überwiegend zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet.

A.

Die internationale Zuständigkeit deutscher Gerichte ist gemäß Art. 18 I EuGVVO sowie gemäß Art. 79 II 2 DSGVO gegeben, denn die Klägerin hat ihren gewöhnlichen Aufenthalt in Deutschland, Frankfurt am Main; die Beklagte ist in Irland (Mitgliedsstaat der Europäischen Union) ansässig. Der sachliche, räumliche und zeitliche Anwendungsbereich der am 25.05.2018 in Kraft getretenen Datenschutzgrundverordnung (DSGVO) ist eröffnet. Der sachliche Anwendungsbereich folgt aus Art. 2 I DSGVO, der für die automatisierte Verarbeitung personenbezogener Daten gilt. Dass die Beklagte personenbezogene Daten der Klagepartei verarbeitet hat, ist zwischen den Parteien unstreitig. Die Eröffnung des räumlichen Anwendungsbereichs der DSGVO beruht auf ihrem Art. 3 I der auf die Verarbeitung personenbezogener Daten Anwendung findet, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen in der Europäischen Union erfolgt. Bei der Beklagten handelt es sich um ein Unternehmen nach dem Recht der Irischen Republik mit Sitz in Irland. Ebenso ergibt sich die internationale Zuständigkeit aus Art. 17 I lit. c), 18 I Brüssel Ia-VO, da die Klägerin ersichtlich und unbestritten als Verbraucherin gehandelt hat – gegenteilige Anhaltspunkte sind nicht gegeben und trägt die Beklagte auch nicht konkret vor. Da die Beklagte das soziale Netzwerk „Instagram“ für Nutzer in der Europäischen Union betreibt, ist sie auch Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO, und zwar auch und entgegen ihrer Ansicht, soweit über die streitgegenständlichen Business Tools die Daten auch durch die Drittanbieter verarbeitet werden. Der Begriff „Verantwortlicher“ wird in Art. 4 Nr. 7 DSGVO weit definiert als die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, die Daten für sich verarbeitet oder für sich durch andere Personen oder Stellen verarbeiten lässt (EuGH, Urteil vom 2. Dezember 2025, C-492/23, Rn. 56; zuvor bereits Urteil vom 29. Juli 2019, Fashion ID, C-40/17, Rn. 74) – dazu sodann unter B. ausführlich. Gegen die Zuständigkeit des Landgerichts Frankfurt am Main hat sich die Beklagte zuletzt auch nicht mehr negativ eingelassen.

Auf den vorliegenden Fall ist nach Art. 6 I lit. b) Rom I-VO wegen des Vorliegens eines Verbrauchervertrages deutsches Recht anzuwenden.

Der Antrag zu 1. (Feststellung) ist bereits unzulässig. Der auf die Feststellung gerichtete Antrag, dass das zwischen den Parteien bestehende Nutzungsverhältnis die Speicherung und Verwendung von über Business Tools erhobenen personenbezogenen Daten nicht gestatte, ist unzulässig. Er beinhaltet kein feststellungsfähiges Rechtsverhältnis im Sinne des § 256 ZPO. Zudem liegt das für den Antrag erforderliche Feststellungsinteresse nicht vor. Nach ständiger Rechtsprechung können bloße Elemente oder Vorfragen eines Rechtsverhältnisses, reine Tatsachen oder etwa die Wirksamkeit von Willenserklärungen oder die Rechtswidrigkeit eines Verhaltens nicht Gegenstand einer Feststellungsklage sein (vgl. BGH, Versäumnisurteil vom 27.03.2015 – V ZR 296/13 – NJW-RR 2015, 915, Tz 7 –; vgl. Urt. v. 20.04.2018 – V ZR 106/17 – NJW 2018, 3441, Tz 13; vgl. LG Stuttgart, Urt. v. 05.02.2025 – 27 O 190/23 –; vgl. LG Braunschweig, Urt. v. 04.06.2025 – 9 O 2615/23 –). Für die Zwischenfeststellungsklage gemäß § 256 II ZPO gilt nichts anderes. Auch sie kann nicht auf die Feststellung der Rechtswidrigkeit bzw. Unzulässigkeit eines Verhaltens gerichtet werden (vgl. BGH, Urt. v. 20.04.2018 – V ZR 106/17 – a.a.O.). Entgegen der Auffassung der Klagepartei richtet sich der Feststellungsantrag vorliegend indes gerade nicht auf die Feststellung des Bestehens oder Nichtbestehens des

zugrundeliegenden Vertrags über die Nutzung des sozialen Netzwerks der Beklagten, sondern beschränkt sich auf die Feststellung der Rechtswidrigkeit („… nicht gestattet“) eines Verhaltens der Beklagten, nämlich der im Einzelnen aufgeführten Datenverarbeitungsvorgänge (a.A. allerdings ohne nähere Begründung OLG München GRUR-RS 2025, 36455). Der Feststellungsantrag ist überdies auch nicht hinreichend bestimmt, weil in das Feststellungsbegehren eine Vielzahl weiterer Rechtsverhältnisse zwischen der Beklagten und Dritten einbezogen werden, da als Anknüpfungspunkt die „Erhebung mit Hilfe der Meta Business-Tools“ und „Weitergabe an die Server der Beklagten“ dienen soll. Die Erhebung und Weitergabe erfolgt aber nach dem unstreitigen Parteivortrag allein bei Drittunternehmen, die Business-Tools einsetzen. Eine generelle Feststellung der Rechtswidrigkeit all dieser jeweiligen Datenerhebungen und -weitergaben ist schon wegen der letztlich unbekannten Anzahl dieser Dritten und wegen der Möglichkeit von jeweils abweichenden Cookie- und Einwilligungsvereinbarungen, auch in Bezug auf die Klagepartei, unmöglich. Unabhängig hiervon liegt für den Antrag auch kein Feststellungsinteresse i.S.v. § 256 I ZPO vor. Voraussetzung hierfür ist, dass dem subjektiven Recht der Klägerseite eine gegenwärtige Gefahr der Unsicherheit dadurch droht, dass die Beklagtenseite es ernstlich bestreitet oder sie sich eines Rechts gegen die Klägerseite berühmt, und dass das erstrebte Urteil infolge seiner Rechtskraft geeignet ist, diese Gefahr zu beseitigen. Ist der Klägerseite eine Klage auf Leistung möglich und zumutbar und erschöpft sie das Rechtsschutzziel, fehlt grundsätzlich das Feststellungsinteresse, weil die Klägerseite im Sinne einer besseren Rechtsschutzmöglichkeit den Streitstoff in einem Prozess klären kann (vgl. Greger in: Zöller, Zivilprozessordnung, 36. Auflage 2026, § 256, Rn 14 ZPO). Dies ist hier der Fall. Soweit es der Klagepartei darum geht, für künftige Ansprüche Klarheit über die Pflichtverletzungen der Beklagten zu schaffen, erschöpft sich ihr Rechtsschutzziel in dem ebenfalls gestellten Antrag auf Unterlassung der Verarbeitung. Auf eine noch nicht abgeschlossene Schadensentwicklung, mit der sie ihr Interesse an der Feststellung begründen will, kann sich die Klagepartei schon deswegen nicht berufen, weil ihr Antrag nicht auf die Feststellung einer Schadensersatzpflicht der Beklagten zielt, sondern auf die Vorfrage, ob deren Geschäftsverhalten rechtswidrig ist

Der Unterlassungsantrag (Antrag zu 2) ist ausreichend bestimmt nach § 253 II Nr. 2 ZPO. Vorliegend bestehen keine Bedenken für eine fehlende „Abgrenzbarkeit“ bezüglich des Gegenstandes und Umfangs, weil die Klägerin in ihren Anträgen die Daten, von deren Verarbeitung die Beklagte absehen soll, exakt bezeichnet (E-Mail der Klagepartei; Telefonnummer der Klagepartei; […]) und auch die beanstandeten Verarbeitungsformen präzise benennt. Dass sich die Klägerin dabei an den – durch Rechtsprechung und Literatur deutlich konturierten – Begriffen des Art. 4 Nr. 2 DSGVO orientiert, sorgt für mehr und nicht für weniger Klarheit. Die Klägerin begehrt nach alledem gerade kein Verbot im Umfang des Gesetzeswortlauts, sondern orientiert sich mit ihrem Unterlassungsbegehren an der konkreten Verletzungshandlung (vgl. hierzu BGH NJW 2020, 3386 Rn. 39.). Dass die Beklagte – z.B. durch eine entsprechende Gestaltung der … – Tools – (aktiv) handeln muss, um den Unterlassungsanspruch erfüllen zu können, hindert die Unterlassungsanordnung nicht (st. Rspr., z.B. BGH GRUR 2013, 1030 Rn. 21; BGH GRUR 2018, 1044 Rn. 57). Unter die von der Beklagten vorzunehmenden Handlungen kann auch die Einwirkung auf Dritte fallen (vgl. BGH NJW 2017, 2119 Rn. 35). An dem erforderlichen Rechtsschutzinteresse fehlt es nicht deshalb, weil der Klagepartei die Möglichkeit zusteht, die Löschung durch Auswahl in den Datenschutzeinstellungen bei den Optionen „Frühere Aktivitäten Löschen“ bzw. „Künftige Aktivitäten trennen“ selbst durchzuführen. Denn es ist nicht ersichtlich, dass die Klagepartei hierdurch die Off-Site-Daten nicht lediglich von ihrem Account trennen, sondern die von der Beklagten gespeicherten Daten insgesamt löschen kann. Unter Löschung ist die endgültige Unbrauchbarmachung der Daten zu verstehen. Es muss irreversibel sichergestellt sein, dass die entsprechenden personenbezogenen Daten nicht mehr Gegenstand der (produktiven) Datenverarbeitung sein können (vgl. Plath/Kamlah, Kommentar zur DSGVO, 4. Aufl 2023, Art. 17 DSGVO, Rn 2).

Betreffend den Antrag zu 3. ist zu beachten, dass eine Löschung sechs Monate nach rechtskräftigem Verfahrensabschluss begehrt wird, was einen im Vollstreckungsverfahren zweifelsfrei feststellbaren und damit hinreichend bestimmbaren Zeitpunkt darstellt. Es handelt

sich um eine nach § 264 Nr. 2 ZPO privilegierte und damit ohne Zustimmung des Gegners oder Sachdienlichkeit nach § 263 ZPO zulässige Antragsänderung. Denn der Streitgegenstand bleibt gleich, während lediglich das diesem zugeordnete klägerische Begehren qualitativ modifiziert wird.

Soweit die Klägerin von der Beklagten verlangt, bestimmte Daten „vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen", erweist sich der Antrag zu 4. als hinreichend bestimmt i.S.v. § 253 II Nr. 2 a.E. ZPO. Durch die Einräumung einer Wahlmöglichkeit wird keine Unsicherheit von außen in den Prozess hineingetragen, die Beklagte wird durch das ihr eingeräumte Wahlrecht nicht beschwert (vgl. OLG Düsseldorf, Urteil vom 21. September 2023 – VI-5 U 4/22 (Kart). Dass es prozessual möglich sein muss, der Beklagten ein Wahlrecht einzuräumen, beweist § 264 I BGB, der unmittelbar den – hier nicht einschlägigen – Fall der Wahlschuld betrifft. Es handelt sich prozessual dabei auch nicht um einen grundsätzlich unzulässigen, weil zu unbestimmten alternativen Klageantrag. Denn es soll anders als bei einem alternativen Klageantrag nicht dem Gericht, sondern der Beklagten überlassen bleiben, ob sie löscht oder stattdessen anonymisiert, sodass sich für die Beklagte keine unzumutbare Unbestimmtheit ergäbe (wie hier: OLG München GRUR-RS 2025, 36455).

Anhaltspunkte dafür, dass die Voraussetzungen von § 260 ZPO nicht gegeben sind, sind nicht ersichtlich. Die objektive Klagehäufung ist zulässig.

Soweit die Klägerin zunächst noch andere Anträge angekündigt hatte (hilfsweise Stufenklage für die angekündigten Hilfsanträge 6, 7, 8 und 9), diese vor einer Verhandlung zurückgenommen, § 269 I ZPO. Auf eine Zustimmung der Beklagten kam es daher nicht mehr an nach § 269 I ZPO. Soweit die Klägerin teilweise die angekündigten Anträge geändert hat, war eine solche Klageänderung unter Beachtung von § 263 ZPO zumindest sachdienlich. Die Beklagte hat auch ohne weitere Rüge zu den geänderten Anträgen verhandelt. Die Sachdienlichkeit ist gegeben, weil es prozessökonomisch ist, die geänderten Anträge zuzulassen, da sich insoweit ein weiterer Rechtsstreit erspart wird und für die Beklagte sich keine prozessualen Nachteile ergeben.

B.

Der Klägerin stehen die geltend gemachten Ansprüche überwiegend zu.

I.

Der Klageantrag zu 2) ist begründet.

Die Klägerin kann verlangen, dass die Beklagte es unterlässt, ihre personenbezogenen Daten anlässlich eines Besuchs auf Drittwebseiten und -Apps zu verheben. Allerdings ergibt sich ein Unterlassungsanspruch nicht aus der DSGVO (EuGH, Urteil vom 4. September 2025, C-65/23, Rn. 43). Er ergibt sich wegen der Verletzung von Vertragspflichten gemäß § 280 I, § 241 II BGB aus dem mit der Beklagten geschlossenen Nutzungsvertrag selbst und zum anderen aus §§ 1004 I 2 analog, 823 I BGB, wenn, ebenso wie bei einem gesetzlichen Unterlassungsanspruch nach § 823 I BGB i.V.m. § 1004 I 2 BGB analog, eine Erstbegehungsbeziehungsweise Wiederholungsgefahr besteht (vgl. BGH, Urteil vom 18. November 2024, VI ZR 10/24, Rn. 83, mit Verweis auf BGH, Urteile vom 2. Mai 2024, I ZR 12/23, Rn. 14; vom 29. Juli 2021, III ZR 179/20, Rn. 102 f. und vom 8. November 2022, II ZR 91/21, Rn. 64). Dabei begründet ein einmal erfolgter Vertragsverstoß die tatsächliche Vermutung für seine Wiederholung, nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urteil vom 29. Juli 2021, III ZR 192/20, Rn. 115 – 116; Urteil vom 20. Juni 2013, I ZR 55/12, Rn. 18; Beschluss vom 3. April 2014, I ZB 42/11, Rn. 12).

Da es sich bei diesen Verarbeitungsvorgängen um interne Abläufe in den Systemen der Beklagten handelt, trifft sie dabei eine sekundäre Darlegungslast zu den Datenverarbeitungsvorgängen bei der Erhebung und Verarbeitung personenbezogener Daten mittels Business-Tools. Die Klagepartei hat demgegenüber nicht darzulegen, welche konkreten Webseiten sie aufgesucht hat und auf welchen dieser Webseiten Business-Tools zum Einsatz kommen. Schon aus diesem Grund kann von ihr – anders als die Beklagte meint – auch nicht verlangt werden, darzulegen und zu beweisen, dass sie auf diesen Webseiten die Einwilligung in die Datenerhebung über Business-Tools verweigert hat. Zwingende Voraussetzung für eine Datenübermittlung an die Beklagte ist die Cookie-Einwilligung des Nutzers auf Drittwebseiten ohnehin nicht, weil unstreitig die Implementierung der Business-Tools auf zahlreichen Drittwebseiten fehlerhaft ist, so dass dort Daten auch dann an die Beklagte weitergeleitet werden, wenn der Nutzer eine solche Einwilligung nicht erteilt hat. Nachdem unstreitig ist, dass die Klagepartei bei der Beklagten als Nutzer registriert ist und dass auf einer erheblichen Anzahl namhafter und reichweitenstarker Webseiten in Deutschland die Business-Tools der Beklagten in ihren verschiedenen Ausprägungen zum Einsatz kommen, ist vielmehr davon auszugehen, dass auch von der Klagepartei Business-Tool-Daten erhoben werden. Soweit sich die Beklagte darauf beruft, dass dies ausnahmsweise nicht der Fall ist, trägt sie auch hierfür die Darlegungslast (vgl. OLG Dresden ZD 2026, 106 und mit überzeugender Begründung: LG Lübeck, Urt. v. 27.11.2025 – 15 O 15/24 –, Rn. 88 ff.).

Bei Anwendung dieser Maßstäbe hat die Beklagte die Behauptung, die ihr seitens ihrer Geschäftspartner über Business-Tools übermittelten personenbezogenen Daten der Klagepartei verarbeite sie auch bei fehlender Einwilligung des Nutzers, nicht substantiiert bestritten. Hierfür ist nicht entscheidend, ob sie die von Drittunternehmern übermittelten Daten verarbeitet, um der Klagepartei personalisierte Werbung zu zeigen. Entscheidend ist vielmehr, dass sie diese Daten auf ihrer Plattform jedenfalls vorübergehend speichert und mit den sog. onsite-Daten der Klagepartei zusammenführt, bevor diese in einem weiteren Schritt durch Zuweisung von Ad-IDs, Hash-Werten und Cookie-IDs pseudonymisiert werden. Diese Zusammenfassung in für die Beklagte auswertbaren individuellen Nutzerprofilen stellt ein Verknüpfen i.S.d.Art. 4 Nr. 2 DSGVO dar, weil hiermit eine inhaltliche Umgestaltung erfolgt und die verknüpften Daten einen neuen Aussagewert erhalten (vgl. hierzu Schaffland/Wiltfang/ Schaffland/Holthaus, DS-GVO/BDSG, April 2026, Art. 4 EUV 2016/679, Rn. 116). Die hiermit einhergehende Bildung individueller Nutzerprofile stellt zugleich ein Profiling der Nutzer im Sinne von Art. 4 Nr. 4 DSGVO dar, weil die mit der o.a Verknüpfung verbundene Erstellung eines Profils einer Person durch Auswertung von Daten und Bewertungen aufgrund von Algorithmen zur Erstellung eines Persönlichkeits-, Verhaltens- oder Bewegungsprofils durch Sammlung von Daten, unter anderem durch (im Internet) hinterlassene (Cookies), getätigte und veröffentlichte Informationen z. B. zu sozialen Kontakten, politischer Einstellung, persönlichem Weltbild, persönlichen Vorlieben, finanziellen Verhältnissen, gesundheitlicher Situation und weiteren Angaben ein modellhaftes, auf Algorithmen beruhendes Gesamtbild der individuellen Persönlichkeit ergeben (vgl. auch insoweit Schaffland/Wiltfang, aaO, Art. 4 EUV 2016/679, Rn. 125). Dies steht zur Auffassung des Gerichts aufgrund des Sachvortrags der Parteien und in Würdigung der vorgelegten NB-MBT sowie der Nutzungsbedingungen für Plattform-Nutzer (im Folgenden NB-PN) fest.

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

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

datenschutzkonform konfiguriert haben, und der Nutzer diese abgelehnt hat. Ob alle diese Voraussetzungen zutreffen, überprüft die Beklagte freilich nicht.

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

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 direkte Identifizierung ermöglichen.

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 Verbindungs- und Netzwerkleistung Werbetreibende erhalten auch andere Informationen. …"

ass 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, bezieht sie sich ausschließlich auf (eigene) Werbe- und nicht auf andere, in ihren Nutzungsbedingungen genannten Zwecke, die hierüber hinausgehen.

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.

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.

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 seitens der Beklagten konkret nicht weiter aufgeklärt. Sie verweist lediglich darauf, sie müsse zumindest eine „gewisse" Verarbeitung von Business-Tools Daten vornehmen, um festzustellen, ob sie diese einem bestimmten Nutzerkonto zuordnen könne und um die Einstellungen des Nutzers zu erkennen und anzuwenden. Es erschließt sich bereits nicht, aus welchem Grund die Beklagte nicht nur übermittelte Kontaktinformationen für den Abgleich mit Nutzerkonten ("abgeglichene Nutzer-ID") nutzt, sondern darüber hinaus auch eine weitere Verarbeitung der Event-Daten in Form einer Kombination beider vornimmt, so jedenfalls nach den NB-MBT und den Parametern für Kund*innen-Informationen. 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 nicht konkret darlegen, ob und ggfls. wie lange die Daten, die von Drittunternehmen übermittelt werden und die sich auf konkrete Nutzer beziehen, bei ihr zunächst zwischengespeichert werden, bevor sie darüber entscheidet, ob sie diese bei Vorliegen der entsprechenden Einwilligungserklärungen für personenbezogene Werbung verwendet oder nicht.

Dies gilt auch hinsichtlich der besonderen Kategorien personenbezogener Daten (im folgenden BKD) i.S.d. Art. 9 I 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). 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.

Ohne Erfolg beruft sich die Beklagte angesichts dessen darauf, sie habe „freiwillig“ Maßnahmen wie eine Kategorisierung der Datenquellen, eine automatisierte Filterung sowie erweiterte Datenbeschränkungen wie beispielsweise das „Core 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 I DSGVO auch in Widerspruch zu den tatbestandlichen Feststellungen in den „Schrems-Verfahren“ (vgl. OGH aaO.; EuGH aaO.).

Die Beklagte verarbeitet personenbezogene Daten der Klagepartei. Bei den im Klageantrag zu 1. genannten Daten handelt es sich um personenbezogene Daten. Gemäß Art. 4 Nr. 1 DSGVO bezeichnet der Ausdruck „personenbezogene Daten“ im Sinne der DSGVO. Hierunter sind nach der Begriffsbestimmung dieser Vorschrift alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wobei klargestellt wird, dass „als identifizierbar eine natürliche Person angesehen wird, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen,

die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (vgl. EuGH, Urteil vom 2. Dezember 2025, C-492/23, Rn. 48). Er umfasst auch alle Informationen, die erst aus einer Verarbeitung zuvor vorhandener personenbezogener Daten resultieren (EuGH, Urteil vom 4. Mai 2023, C 487/21, Rn. 26). Insoweit sind als personenbezogene Daten zu qualifizieren die E-Mail, die Telefonnummer, der Zu- und Nachname, das Geburtsdatum, das Geschlecht und der Ort, an dem sich die Klägerin befindet, da die Daten eine Zuordnung zur Identifizierung der natürlichen Person, der Klägerin, genutzt werden können. (OLG Naumburg BeckRS 2026, 4548 Rn. 105). Dies gilt auch für die IP-Adresse des jeweiligen Clients, um sich in das Internet einzuwählen, da hiermit nachvollzogen werden kann, mittelbar, von welchem Standort aus man sich „in das Internet einwählt". Weiter sind auch die Lead-ID, die Abonnement-ID sowie die externe ID besuchter Webseiten (external ID) personenbezogene Daten. Die „ID's" sind Identitätsdokumente bzw. Kennungen der Klagepartei bezüglich ihrer Aktionen/Kontakte im Internet als potenzieller Kunde („Lead"), als Abonnent sowie die Kennung der Klagepartei bei anderen Werbetreibenden. Die Daten zum User-Agent des Clients, welche ausweislich des klägerischen Vortrags, welchem die Beklagte nicht entgegengetreten ist, die für das Digital Fingerprinting nutzbaren Daten darstellen, stellen somit ebenfalls personenbezogene Daten dar. Auch die URLs der besuchten Webseiten samt ihrer Unterseiten, der Zeitpunkt des Besuchs, der „Referrer" (d. h. die Webseite, über die der Nutzer zur aktuellen Webseite gekommen ist), die von der Klagepartei angeklickten Buttons sowie die weiteren, von der Beklagten „Events" genannten Daten, die die Interaktion der Klagepartei auf der jeweiligen Webseite dokumentieren sind personenbezogene Daten, da sie jeweils in Verbindung mit weiteren Informationen der Klagepartei zugeordnet werden können und dadurch Informationen über diese beinhalten. So kann dadurch ermittelt werden, welche Webseiten die Klagepartei besuchte, wann dies geschah, von welcher Webseite sie dort hingelangte, sowie welche Aktionen sie dort durchgeführt hat, beispielsweise, ob sie bestimmte Artikel gekauft hat. Aus den gleichen Gründen handelt es sich schließlich bei dem Namen der App, sowie dem Zeitpunkt des Besuchs, den von der Klagepartei in der App angeklickten Buttons, sowie den von der Beklagten „Events" genannten Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren, um personenbezogene Daten.

Ohne Erfolg beruft sich die Beklagte angesichts dessen darauf, sie habe „freiwillig" Maßnahmen wie eine Kategorisierung der Datenquellen, eine automatisierte Filterung sowie erweiterte Datenbeschränkungen wie beispielsweise das „Core 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 I DSGVO auch in Widerspruch zu den tatbestandlichen Feststellungen in den „Schrems-Verfahren" (vgl. OGH aaO.; EuGH aaO.). Diese Verantwortlichkeit kann sie weder durch vertragliche Vereinbarungen mit den Drittanbietern auf diese abwälzen, noch kann sie sich durch etwaige Belehrungen der Drittanbieter im Hinblick auf deren datenschutzrechtlichen Pflichten von der eigenen Verantwortlichkeit freizeichnen, schon weil sie selbst gegenüber ihren Business-tools-Kunden die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO feststellt ("…-Tools Nutzungsbedingungen, Anlage B 5 Seite 5 unter 5 a. ii.). Aus denselben Gründen kann sich die Beklagte daher auch nicht darauf berufen, entsprechend ihren NB-MBT unter Ziff. 5. hinsichtlich bestimmter Verarbeitungszwecke (Abgleich-, Messung- und Analysedienste)

lediglich als Auftragsverarbeiter i.S.d. Art. 4 Nr. 9 DSGVO der Drittunternehmer tätig zu werden. Nimmt eine Stelle – wie hier die Beklagte – aus Eigeninteresse auf die Verarbeitung Einfluss und wirkt auf diese Weise neben einem anderen Beteiligten an der Entscheidung über Zweck und Mittel der Verarbeitung mit, führt dies regelmäßig zu einer (gemeinsamen) Verantwortlichkeit (EuGH, Urt. v. 29.7.2019, a.a.O.; Simitis/Hornung/Spiecker gen. Döhmann/ Petri/Stief, Datenschutzrecht, 2. Aufl. 2025, DSGVO, Art. 26 Rn. 25, Art. 4 Nr. 7, Rn. 24; BeckOK-Datenschutzrecht/Spoerr, 54. 02.2026, DS-GVO Art. 26 Rn. 18 ff.).

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

Damit der Rechtfertigungsgrund einer Einwilligung der Klagepartei als betroffene Person greift, muss die Beklagte nachweisen, dass die Weitergabe von Daten der Klagepartei an sie von einer auf konkrete Zwecke bezogenen freiwilligen Einwilligung gedeckt ist, vgl. Art. 6, Art. 7 Ziff. 2 und 4 DSGVO. Dieser Nachweis ist ihr nicht gelungen. Dies betrifft die im Unterlassungsantrag genannten Verarbeitungsvorgänge der Datenerhebung mittels Business-Tools bei den Drittunternehmen, der Weitergabe an die Server der Beklagten, die Speicherung und die anschließende Verwendung. Unstreitig hat die Klagepartei der Beklagten weder über die „Meta-Cookies in anderen Apps und auf anderen Webseiten“ noch über die Schaltfläche „Informationen über deine Aktivitäten“ eine Einwilligung zur Nutzung von Business-Tool-Daten erteilt. Eine solche Einwilligung nimmt die Beklagte auch nicht für sich in Anspruch, sie beruft sich auch nicht auf eine vor dem 25.05.2018 erklärte Einwilligung, die ohnehin unter der Geltung der DSGVO keine rechtfertigende Wirkung mehr entfalten könnte (vgl. OLG Hamm, Urt. v. 15.08.2023 – 7 U 19/23, Rn 114). Die Beklagte kann sich auch nicht auf eine etwaig erteilte Einwilligung der Klagepartei auf Drittwebseiten und -Apps berufen, da sich diese nur auf Datenverarbeitungszwecke des Webseiten- bzw. App-Betreibers als Business-Tools Verwender, aber nicht auf diejenigen des Anbieters dieser Technologien bezieht (vgl. EuGH, Urt. v. 29.7.2019 – C-40/17 (Fashion ID) a.a.O., Rn. 97). Es obliegt somit nicht den Drittunternehmen, eine Einwilligung des Nutzers für eine Verarbeitung von Daten für Zwecke der Beklagten einzuholen. Ob die Klagepartei die (Nicht-)Erteilung einer Einwilligung hierin auf Drittseiten substantiiert dargelegt hat, ist daher nicht entscheidend.

Die Beklagte kann sich auch nicht mit Erfolg darauf berufen, sie verarbeite Business-Tools Daten als für die Erfüllung der Verträge mit geschäftsfähigen Nutzern erforderlich gemäß Art. 6 Ziff. 1 lit. b) DSGVO. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH, Urt. v. 04.07.2023, C-252/21, Rn. 98). Entscheidend ist dabei, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen. Zudem ist bei einem Vertrag, der mehrere Dienstleistungen oder mehrere eigenständige Elemente einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit des Rechtfertigungstatbestandes für jede dieser Dienstleistungen gesondert zu beurteilen (vgl. EuGH, a.a.O., Rn. 100). Dass die Verwendung der Business-Tools und die Verarbeitung der durch sie gewonnenen personenbezogenen Daten zur Nutzung der sozialen Plattform unerlässlich wäre, lässt sich nicht feststellen. Der Betrieb und die Nutzung der streitgegenständlichen Plattform sind vielmehr ohne Einbindung der Business-Tools möglich,

was nicht zuletzt die Einführung des Bezahlmodells seit dem 03.11.2023 verdeutlicht. Für fernliegend ist für das Gericht die Annahme, die Verarbeitung von Business-Tools-Daten sei aus Sicherheits- und Integritätszwecke geboten. Insoweit fehlt es aber schon an nachvollziehbaren, hinreichend konkreten Sachvortrag, dass der Hauptgegenstand des Vertrags, der hier in der Nutzung der Social-media-Plattform der Beklagten liegt, ohne die zusätzliche und außerhalb des eigentlichen Vertragszwecks liegende, umfassende Verarbeitung von Offsite Daten ihrer Geschäftspartner nicht erfüllt werden könnte, diese also objektiv unerlässlich für den mit der Klagepartei bestehenden Nutzungsvertrag sind.

Die nach Art. 6 Ziff. 1 lit. f) DSGVO vorzunehmende Interessenabwägung ergibt gleichfalls kein zugunsten der Beklagten überwiegendes Interesse an der Verarbeitung von Business-Tool-Daten (vgl. zu den Voraussetzungen EuGH, Urt. v. 04.07.2023, C-252/21, a.a.O., Rn. 114). Dem berechtigten Interesse der Beklagten an einem „profitablen Dienst" kommt kein höheres Gewicht zu, als dem Recht der Nutzer auf Datensicherheit und -minimierung sowie informationelle Selbstbestimmung. Der EuGH (a.a.O.) hat insoweit bereits entschieden, dass auch wenn die Dienste eines sozialen Online-Netzwerks unentgeltlich sind, der Nutzer dieses Netzwerks vernünftigerweise nicht damit rechnen müsse, dass dessen Betreiber seine personenbezogenen Daten ohne seine Einwilligung zum Zweck der Personalisierung der Werbung verarbeitet oder sogar noch umfänglicher nutzt. Daher sei davon auszugehen, dass die Interessen und Grundrechte eines solchen Nutzers bereits gegenüber dem Interesse dieses Betreibers an einer solchen Personalisierung der Werbung, mit der er seine Tätigkeit finanziert, überwiegen, so dass die von ihm zu solchen Zwecken vorgenommene Verarbeitung nicht unter Art. 6 Ziff. 1 lit. f) DSGVO fallen könne (vgl. EuGH, Urt. v. 4.07.2023, a.a.O., Rn. 117). Davon ausgehend kann erst recht die der Nutzung der Plattform der Beklagten vorgelagerte oder gar unabhängig von einer Plattformnutzung erfolgte Verarbeitung von personenbezogenen Daten nicht gemäß Art. 6 Ziff.1 lit. f) DSGVO gerechtfertigt sein.

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

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

Bei der gebotenen Gesamtabwägung nach Art. 6 I lit f) DSGVO ist zudem zu berücksichtigten, dass die von der Beklagten angegebene Speicherpraxis mit wesentlichen Grundgedanken der DSGVO nicht im Einklang steht. Die auch nach Vortrag der Beklagten bestehende längerfristige Speicherung von abgeglichenen Daten, also Nutzer-IDs und Event-Daten, begründet sie mit Sicherheits- und Integritätsprozessen, für die sie nach ihrem Sachvortrag „aufgrund deren

Komplexität und Feinheiten“ keinen „konkreten Zeitrahmen“ angeben könne, da sie sicherstellen müsse, dass „schwerwiegende oder böswillige Aktivitäten keine negativen Auswirkungen auf die Nutzer, Produkte oder Systeme von Meta haben“. Die „maximalen Aufbewahrungsfristen“ lege sie im Rahmen eines umfassenden, funktionsübergreifenden Überprüfungsprozesses fest, Daten werden „in der Regel bis zu 90 Tage aufbewahrt“, u.U. auch länger. Eine solche Speicherpraxis verstößt gegen Art. 5 Ziff. 1 lit. e) DSGVO. In EG 39 S. 8 wird gefordert, „dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt“. Dass die Speicherung sämtlicher zunächst zu Zwecken wie Verbesserung des Erlebnisses für Nutzer von Meta-Produkten, Förderung von Schutz und die Sicherheit auf und außerhalb von Meta-Produkten, für Forschungs- und Entwicklungszwecke, Erhalt der Integrität der Meta-Produkte, für deren Bereitstellung und Verbesserung übermittelter personenbezogener Daten für einen unbestimmten Zeitraum nunmehr mit Sicherheits- und Integritätsprozessen und -interessen begründet wird, ist nicht nachvollziehbar und insoweit unbeachtlich.

Schließlich verstößt die streitgegenständliche Datenverarbeitung auch gegen den Grundsatz der Datenminimierung, Art. 5 Ziff 1 lit. c) DSGVO, der verlangt, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt ist („limited to what is necessary“). Aus diesem Grundsatz folgt, dass der Verantwortliche nicht allgemein und unterschiedslos personenbezogene Daten erheben darf und er von der Erhebung von Daten absehen muss, die für die Zwecke der Verarbeitung nicht unbedingt notwendig sind (EuGH, Urt. v. 04.10.2024 – C-446/21, a.a.O.). Die Beklagte erhält über ihre Business-Tools – wie bereits ausgeführt – umfassende Offsite Daten ihrer Nutzer über deren Tätigkeiten und verfolgt allgemein auch das Navigationsverhalten der Nutzer (vgl. EuGH a.a.O.; Bundeskartellamt, NZKart 2024, 651 [655]; vgl. Hense, K& R 2023, 556-562 m.w.N.). Eine solche Verarbeitung ist besonders umfassend, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Onlineaktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von der Beklagten aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird (EuGH a.a.O., und MMR 2023, 669 [678, Rn. 118] – M. Plat – forms/Sosna, GSZ 2024, 53 [57]). Es steht dem Grundsatz der Datenminimierung entgegen, wenn -wie hier – sämtliche personenbezogenen Daten, die ein Verantwortlicher wie der Betreiber einer Onlineplattform für ein soziales Netzwerk von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für Zwecke der zielgerichteten Werbung aggregiert, analysiert und verarbeitet werden.

II.

Der Klägerin steht gegen die Beklagten ein Anspruch aus Art. 18 Ziff. 1 lit. b) DSGVO dahingehend zu, dass die Beklagte ihre personenbezogenen Daten ab sofort unverändert am gespeicherten Ort belässt, sie nur mit ihrer Einwilligung weiterverarbeitet und erst nach Abschluss des Verfahrens auf ihre Aufforderung hin löscht. Der Antrag ist aufgrund des erkennbaren Rechtsschutzziels, die Verarbeitung der gespeicherten Daten bis zum Abschluss des Verfahrens zu unterbinden, dahingehend auszulegen, dass damit eine Einschränkung der Verarbeitung i.S.d. Art. 18 Ziff. 1 lit. b) DSGVO statt der sofortigen Löschung verlangt werden soll und dass sich der Antrag nur auf Daten bezieht, die derzeit bei der Beklagten noch vorhanden sind und die sie nicht bereits z.B. aufgrund Ablaufs interner Speicherfristen gelöscht hat.

Das Recht auf Einschränkung der Verarbeitung kann von der betroffenen Person im Fall einer rechtswidrigen Verarbeitung personenbezogener Daten (lit. b) auch im Zusammenhang mit einem Löschungsverlangen geltend gemacht werden. Die Vorschrift räumt der betroffenen Person ein echtes Wahlrecht ein, denn diese kann in Fällen der rechtswidrigen Verarbeitung statt der Löschung die Einschränkung der Verarbeitung verlangen, denn die betroffene Person hat ein schützenswertes Interesse daran, dass der Verantwortliche die fraglichen Daten nicht unbeschränkt weiterverarbeitet, während er prüft, ob ein Anspruch auf Löschung tatsächlich besteht. Es kann auch auf eine längerfristige oder dauerhafte Einschränkung gerichtet sein, von

der vorliegend angesichts der absehbar längeren Verfahrensdauer auszugehen ist (Simitis/Hornung/Spiecker gen. Döhmann/Dix, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 18 Rn. 3, 6). Ausdrücklich heißt es in Erwägungsgrund 67, dass in automatisierten Dateisystemen die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen soll. Sichergestellt werden soll hierdurch, dass die personenbezogenen Daten „in keiner Weise weiter verarbeitet und nicht verändert werden können". Hierbei soll auf die Beschränkung in dem System unmissverständlich hingewiesen werden (BeckOK Datenschutzrecht/Worms, 11.2024, DS-GVO Art. 18, Rn. 15).

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

III.

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

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

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

IV.

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

Nach ständiger Rechtsprechung des EuGH erfordert ein Schadensersatzanspruch im Sinne des Art. 82 I DSGVO einen Verstoß gegen Vorschriften der DSGVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (vgl. nur EuGH, Urt. v. 04.10.2024 – C-200/23, DB 2024, 2952 Rn. 140; BGH Urt. v. 18.11.2024 – VI ZR 10/24, BGHZ 242, 180 Rn. 21). Die Darlegungs- und Beweislast für diese Voraussetzungen trifft grundsätzlich die Person, die auf der Grundlage von Art. 82 Ziff. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH a.a.O Rn. 141, BGH, a.a.O m.w.N). Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruches nach Art. 82 Ziff. 1 DSGVO ein Verschulden des Verantwortlichen. Art. 82 DSGVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 III DSGVO dem Verantwortlichen (vgl. EuGH, Urt. v. 11.04.2024 – C-741/21, NJW 2024, 1561 Rn. 44 ff.

BGH, a.a.O m.w.N). Der europäische Gerichtshof stützt sich auf den 146. Erwägungsgrund, der auf „Schäden" abstellt, „die einer Person aufgrund einer Verarbeitung entstehen". Zwar muss der Schaden nicht eine gewisse Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urt. v. 04.05.2023 – C – 300/21, 49, 50). Allerdings muss der Schaden tatsächlich und sicher entstanden sein (vgl. EuGH, Urt. v. 04.04.2017 – C – 337/15, Rn 91; vgl. OLG Dresden GRUR-RS 2024, 38616).

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

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

Die Beklagte hat – wie dargetan – ohne Rechtfertigungsgrund personenbezogene Daten der Klägerin verarbeitet.

Es ist zudem ein Kontrollverlust eingetreten, denn die Klagepartei hat keine Kenntnis darüber, auf welchen der von ihr besuchten Webseiten die von der Beklagten entwickelten Business-Tools eingesetzt werden, welche Daten dort über sie erhoben sowie an die Beklagte weitergeleitet und in welchem Ausmaß diese Daten bei der Beklagten gespeichert, aggregiert und genutzt werden. Wie bereits ausgeführt, ist die Datenverarbeitung durch die Beklagte besonders umfassend, da sie potenziell unbegrenzte Daten über die Online-Aktivitäten der Nutzer betrifft und das Gefühl auslösen kann, dass das Privatleben der Nutzer kontinuierlich überwacht wird (vgl. EuGH, Urt. v. 04.10.2024 – C-446/21 –, Rn 62). Dieses Gefühl des ständigen Überwachtwerdens ist eine nachteilige Folge, die über einen „bloßen" Kontrollverlust und die hiermit verbundenen Unannehmlichkeiten hinausgeht und daher einen immateriellen Schaden begründet (vgl. Meyer MMR 2025, 173, 177, m.w.N.). Dies gilt umso mehr, als nach dem hier zugrunde zu legenden Vorbringen anzunehmen ist, dass auch bei verweigerter Einwilligung eines Nutzers über Business-Tools erlangte Daten zu einem Profiling im Sinne des Art. 22 DSGVO verwendet werden. Nach der Rechtsprechung des EuGH (Urt. v. 04.10.2024 – C-446/21 (Schrems), dort Rn 63) stellt das Erstellen detaillierter Profile der Nutzer in Verbindung mit der zeitlich unbegrenzten Weiterverarbeitung einen schweren Eingriff in die Grundrechte der betroffenen Nutzer, insbesondere auf Achtung ihres Privatlebens und den Schutz personenbezogener Daten dar (EuGH aaO. Rn 63). Dies gilt nach Auffassung des Gerichts auch in den Fällen – wie hier –, in denen nicht nachgewiesen ist, dass die über Business-Tools erlangten Daten für Zwecke der personalisierten Werbung verwendet werden. Dass vorliegend überdies nicht ausgeschlossen werden kann, dass durch die Business-Tools auch BKD im Sinne von Art. 9 I DSGVO von der streitgegenständlichen Datenverarbeitung betroffen sind, verstärkt diesen Eindruck und kann dazu führen, dass Nutzer davon absehen, Webseiten etwa zu Gesundheitsthemen oder zum Sexualleben zu besuchen. Anders als in den sog. Scraping-Fällen werden vorliegend zwar die über die Business-Tools erlangten Daten nicht im Internet veröffentlicht, sondern lediglich bei der Beklagten verknüpft und gespeichert. Im Unterschied zu den Scraping-Sachverhalten, bei denen es im Wesentlichen um die Verknüpfung von Telefonnummer und/oder E-Mail-Anschrift mit einem Facebook-Nutzerkonto geht, erfasst die Verarbeitung von Daten aus den Business-Tools aber eine unabsehbare Vielzahl personenbezogener Daten, darunter je nach Einzelfall auch Gesundheitsdaten oder Daten zur sexuellen Orientierung. Des Weiteren ist die nicht bestehende Möglichkeit der Klagepartei, durch eigenes Handeln die Kontrolle über diese Daten zurückzuerlangen zu berücksichtigen

(zu diesen Kriterien vgl. OLG Dresden GRUR-RS 2024, 35688 Rn. 20). Insofern kann vorliegend nicht außer Betracht bleiben, dass weder durch die Änderung der Datenschutzeinstellungen noch durch die Löschung des Kontos eine vollumfängliche Löschung der bei der Beklagten gespeicherten Daten möglich wäre. Das Gericht geht nach alledem davon aus, dass bereits dieser abstrakt bestehende Kontrollverlust in Verbindung mit dem nachvollziehbar hieraus abgeleiteten Unsicherheitsgefühl für einen immateriellen Schaden ausreicht, ohne dass die Klagepartei diesen noch weiter individualisieren müsste. Die sehr umfassende Verarbeitung von personenbezogenen Daten durch die Beklagte sowie das allgemeine Gefühl der Beobachtung im privaten Umfeld sind ohne weiteres geeignet, bei jedem davon betroffenen Nutzer negative Gefühle in Form von Sorge und Ärger auszulösen, weshalb diese Empfindungen bei der Bemessung des immateriellen Schadens berücksichtigt werden können, ohne dass es auf weiteren Vortrag ankommt, welche Daten genau erhoben worden sind (so wohl auch Ehmann/Selmayr/Nemitz, DSGVO, 3. Aufl. 2024, DSGVO Art. 82, Rn. 17). Das unbestimmte Gefühl einer Überwachung ihres Verhaltens nicht nur im Internet liegt nachvollziehbar darin begründet, dass die Klägerseite nicht weiß und auch nicht wissen kann, welche und wie viele Daten die Beklagte aus ihrer Privat- und Intimsphäre über sie gesammelt hat und auch nicht weiß und wissen kann, was die Beklagte mit diesen Daten macht (so auch LG Leipzig, Urt. v. 04.07.2025 – 5 O 2351/23 –, Rn. 72 ff.). Das Gericht hält für diesen sich bereits aus abstrakten Überlegungen ergebenden und jeden einzelnen Nutzer betreffenden Schaden einen immateriellen Schadensersatz in Höhe von 2.000 € für ausreichend und angemessen. Bei dieser Bemessung geht das Gericht davon aus, dass die Klagepartei einen einheitlichen Anspruch auf immateriellen Schadensersatz aus Art. 82 Ziff. 1 DSGVO geltend macht, der sich auf eine Vielzahl einzelner, nicht konkretisierter Datenschutzverstöße der Beklagten stützt, aber in einem einheitlichen Geschehen (dem fortlaufenden Einsatz der Business-Tools) wurzelt. Auf den von der Beklagten erhobenen Verjährungseinwand kam es hierfür nicht an, weil sie eine Kenntnis der Klagepartei vor Klageerhebung weder behauptet noch unter Beweis gestellt hat.

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

IV.

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

Rechtsanwalt und dem Außenverhältnis des Geschädigten zum Schädiger zu unterscheiden (BGH, Beschluss vom 23.06.2022 – VII ZR 394/21). Voraussetzung für einen Erstattungsanspruch ist grundsätzlich, dass der Geschädigte im Innenverhältnis zur Zahlung der in Rechnung gestellten Kosten verpflichtet ist und die konkrete anwaltliche Tätigkeit im Außenverhältnis aus der maßgeblichen Sicht des Geschädigten mit Rücksicht auf seine spezielle Situation zur Wahrnehmung seiner Rechte erforderlich und zweckmäßig war. Ob eine vorprozessuale anwaltliche Zahlungsaufforderung im Innenverhältnis des Mandanten zum Rechtsanwalt eine Geschäftsgebühr nach Nr. 2300 VV RVG auslöst oder als der Vorbereitung der Klage dienende Tätigkeit nach § 19 I 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 VV RVG abgegolten ist, bestimmt sich nach Art und Umfang des im Einzelfall erteilten Mandats. Erteilt der Mandant den unbedingten Auftrag, im gerichtlichen Verfahren tätig zu werden (vgl. Vorbemerkung 3 I 1 VV RVG), lösen bereits Vorbereitungshandlungen die Gebühren für das gerichtliche Verfahren aus, und zwar auch dann, wenn der Anwalt zunächst nur außergerichtlich tätig wird. Für das Entstehen der Geschäftsgebühr nach Nr. 2300 VV RVG ist dann kein Raum mehr (BGH, Beschluss vom 23.06.2022, a.a.O.). Anders liegt es, wenn sich der Auftrag auf die außergerichtliche Tätigkeit des Anwalts beschränkt oder der Prozessauftrag jedenfalls unter der aufschiebenden Bedingung erteilt wird, dass zunächst vorzunehmende außergerichtliche Einigungsversuche erfolglos bleiben. Ein lediglich (aufschiebend) bedingt für den Fall des Scheiterns des vorgerichtlichen Mandats erteilter Prozessauftrag steht der Gebühr aus Nr. 2300 VV RVG nicht entgegen (BGH, Beschluss vom 23.06.2022, a.a.O.). Die Beauftragung eines Rechtsanwalts zur außergerichtlichen Vertretung im Sinne der Nr. 2300 VV RVG soll schnelle und einverständliche Regelungen ohne Einschaltung der Gerichte ermöglichen. Sie ist zweckmäßig und regelmäßig erforderlich, wenn der Versuch einer – vom Gesetzgeber gewünschten – außergerichtlichen Streiterledigung nicht von vornherein ausscheidet, wie etwa im Falle einer ernsthaften und endgültigen Erfüllungsverweigerung. Ist der Schädiger bekanntermaßen zahlungsunwillig und erscheint der Versuch einer außergerichtlichen Forderungsdurchsetzung auch nicht aus sonstigen Gründen erfolgversprechend, sind die dadurch verursachten Kosten nicht zweckmäßig (vgl. BGH, a.a.O.). Vorliegend ist schon nicht dargelegt, dass die Klagepartei ihren Anwälten einen auf eine außergerichtliche Tätigkeit beschränkten Auftrag oder einen aufschiebend bedingten Prozessauftrag erteilt hätte. Unabhängig davon war die außergerichtliche Tätigkeit nicht zweckmäßig, weil mit einer auch nur teilweisen Erfüllung der Forderungen vernünftiger Weise nicht gerechnet werden konnte. Der Klagepartei und ihren Prozessbevollmächtigten musste bei Begründung des Mandatsverhältnisses klar sein, dass die Beklagte vorgerichtlich nicht auf die Forderungen eingehen würde. Wie schon in den Masseverfahren bei den „Scraping Fällen“ hat sich die Beklagte weder vorgerichtlich noch nach Klageerhebung auf Verhandlungen eingelassen. Bei vernünftiger Betrachtung der Sachlage war nicht zu erwarten, dass die Beklagte sich bei dem zu erwartenden Masseverfahren zu den Business-Tools mit mehreren Tausend Klageparteien und zahlreichen Anträgen, die letztendlich ihr Geschäftsmodell in Frage stellen, auf die Forderungen einlassen würde. Unabhängig davon enthält das vorprozessuale Aufforderungsschreiben der Anwälte der Klagepartei – bis auf die Zahlungsforderung – keine verzugsbegründenden Mahnung. Vielmehr wird die Beklagte darin letztendlich aufgefordert, sich in Zukunft an die Regelungen der DSGVO zu halten. So wird sie z.B. aufgefordert, die Daten zu löschen, sobald sie dazu aufgefordert wird und anzuerkennen, dass sie auf Anfrage der Klagepartei Auskunft erteilen wird sowie eine Verarbeitung ohne wirksame Einwilligung zu unterlassen hat. Lediglich die Aufforderung, an die Klagepartei ein Schmerzensgeld von 5.000 € zu zahlen, enthält eine Aufforderung zur Leistung. Im Übrigen hätte der Prozessbevollmächtigte die Klägerin vorab auch darüber informieren müssen, dass eine vorgerichtliche Geltendmachung in Ansehung der unzählig vielen vergleichbaren Fällen ersichtlich ohne Erfolg bleiben wird – auch das ist nicht erfolgt.

Da es sich hierbei um eine Nebenforderung handelt, war ein prozessualer Hinweis nicht nötig, § 139 I 1 ZPO.

Der Anspruch auf Zinsen seit Rechtshängigkeit ergibt sich aus §§ 291, 288 BGB. Soweit die Klägerin bereits zu einem früheren Zeitpunkt Verzugszinsen ausgeurteilt wissen wollte (06.02.2024), ist nicht ersichtlich, woher sich der Verzugsbeginn ergeben haben soll. Hierauf

musste das Gericht als Nebenforderung auch nicht hinweisen. Dazu hat die Klägerin auch keinen konkreten Sachvortrag geleistet; abzustellen war daher auf die Zustellung der Klageschrift, die am 02.04.2024 erfolgte, sodass ab dem Folgetag, 03.04.2024, Verzugszinsen als Prozesszinsen zu zahlen sind, § 187 I BGB analog.

C.

Die Kostenentscheidung folgt aus § 92 I ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 709 S. 1, 2, 711 ZPO.

D.

Der Streitwert des Rechtsstreits wird auf 12.000,00 € festgesetzt und folgt bezüglich dem Leistungsbegehren dem Interesse der Klägerin nach § 48 I 1 GKG in Verbindung mit §§ 3, 4 I Hs. 2 ZPO – 5.000,00 € (Antrag zu 5). Den Feststellungsantrag hat das Gericht mit 2.000,00 € bewertet, § 3 ZPO (Antrag zu 1). Für den Unterlassungsantrag (Antrag zu 2) war ein Streitwert von 3.000 € festzusetzen. Der Verpflichtungsantrag und die Anträge auf Löschung und Anonymisierung waren mit jeweils 1.000 € zu bewerten (Anträge zu 3 und 4) – mithin 2.000 €. Die einzelnen Werte waren nach § 5 ZPO zu addieren und ergeben insgesamt 12.000,00 €.

Rechtsbehelfsbelehrung

Diese Entscheidung kann hinsichtlich der Wertfestsetzung mit der Beschwerde angefochten werden. Sie ist nur zulässig, wenn sie innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache rechtskräftig geworden ist oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Frankfurt am Main, Gerichtsstraße 2, 60313 Frankfurt am Main, eingeht. Wird der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung der Festsetzung bei dem Gericht eingelegt werden.
Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 300,00 € übersteigt oder das Gericht die Beschwerde in diesem Beschluss zugelassen hat. Beschwerdeberechtigt ist, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist.
Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle des genannten Gerichts eingelegt. Sie kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichts erklärt werden, wobei es für die Einhaltung der Frist auf den Eingang bei dem genannten Gericht ankommt. Sie ist zu unterzeichnen. Die Einlegung kann auch mittels elektronischen Dokuments erfolgen. Informationen zu den weiteren Voraussetzungen zur Signatur und Übermittlung sind auf dem Justizportal des Bundes und der Länder (www.justiz.de) im Themenbereich zur elektronischen Kommunikation zu finden. Eine Einlegung per einfacher E-Mail ist unzulässig. Rechtsanwältinnen, Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts einschließlich der zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse sind zur Einlegung mittels elektronischen Dokuments verpflichtet.
Die Beschwerde muss die Bezeichnung des angefochtenen Beschlusses sowie die Erklärung enthalten, dass Beschwerde gegen diesen Beschluss eingelegt wird. Soll die Entscheidung nur zum Teil angefochten werden, so ist der Umfang der Anfechtung zu bezeichnen.

Diese Entscheidung kann mit der Berufung angefochten werden. Sie ist innerhalb einer Notfrist von einem Monat bei dem Oberlandesgericht Frankfurt am Main, Zeil 42, 60313 Frankfurt am Main einzulegen. Die Frist beginnt mit der Zustellung der in vollständiger Form abgefassten Entscheidung.
Die Berufung ist nur zulässig, wenn der Beschwerdegegenstand 1.000,00 € übersteigt oder das Gericht die Berufung in diesem Urteil zugelassen hat. Zur Einlegung der Berufung ist berechtigt, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist.
Die Berufung ist mittels elektronischen Dokuments einzulegen. Die Berufung kann nur durch eine Rechtsanwältin oder einen Rechtsanwalt eingelegt werden.

[redacted]
Richter am Landgericht