



Landgericht Leipzig

Zivilkammer

Aktenzeichen: 05 O 1939/24

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

[REDACTED]

- Kläger -

Prozessbevollmächtigte:

BK Baumeister & Kollegen Verbraucherkanzlei, Viktoria-Luise-Platz 7, 10777 Berlin,
Gz.: DTS-013317-24

gegen

Meta Platforms Ireland Limited, Merrion Road, D04 X2K5 Dublin 4, Irland
vertreten durch die Geschäftsführer Yvonne Cunnane, David Harris, Genevieve Hughes, Marjella Mungovan und Anne O'Leary

- Beklagte -

Prozessbevollmächtigte:

[REDACTED]

wegen Auskunft und Schadensersatz

hat die 5. Zivilkammer des Landgerichts Leipzig durch

[REDACTED]

Richterin am Landgericht [REDACTED]

Richter [REDACTED]

auf Grund der mündlichen Verhandlung vom 20.05.2025 am 15.08.2025

für Recht erkannt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche der folgenden personenbezogenen Daten der Klagepartei seit dem 25.05.2018 mit Hilfe der „Meta Business Tools“ erfasst, an die Server der Beklagten weitergeleitet, dort gespeichert und anschließend verwendet wurden und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Instagram" unter dem Benutzernamen [REDACTED] der Klagepartei verknüpft wurden,

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

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

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

- die URLs der Websites samt ihrer Unterseiten
- der Zeitpunkt des Besuchs
- der „Referrer“ (die Website, über die der Benutzer zur aktuellen Website ge-

kommen ist),

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

c. in mobilen Dritt-Apps

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

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.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags 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.

3. Die Beklagte wird verurteilt, an die Klagepartei eine Entschädigung in Höhe von 5.000,00 EUR nebst Zinsen hieraus i. H. v. fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 26.04.2024 zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 Euro freizustellen.

5. Die Kosten des Rechtsstreits trägt die Beklagte.

6. Das Urteil ist gegen Sicherheitsleistungen i.H.v. 12.000 EUR vorläufig vollstreckbar.

Beschluss:

Der Streitwert wird auf 8.000,00 EUR festgesetzt.

Tatbestand

Der Kläger begehrt im Zusammenhang mit der Verwendung von sog. Business Tools neben der Erteilung von Auskunft über die Verarbeitung seiner personenbezogenen Daten die Löschung oder wahlweise Anonymisierung der bereits gespeicherten Daten nach erfolgter Auskunftserteilung sowie Geldentschädigung aufgrund behaupteter rechtswidriger Verarbeitung personenbezogener Daten.

Die Beklagte betreibt u.a. die sozialen Netzwerke „instagram“ und „facebook“. Die Beklagte entwickelte verschiedene Business Tools, die Websitesbetreibern und App-Entwicklern Werbeeinnahmen verschaffen können und aus diesem Grund von diesen auf ihren Websites und in ihren Apps eingebunden werden.

Die Klagepartei nutzt ausschließlich privat das Netzwerk "Instagram" unter der E-Mail-Adresse [REDACTED] seit dem 03.08.2012. Der Kläger willigte nicht über die Einstellung "Informationen von Werbepartnern über deine Aktivitäten" zur Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung ein.

Als Gegenleistung für die Nutzung des Netzwerks fordert die Beklagte kein Geld. Das soziale

Netzwerk wird maßgeblich durch Online-Werbung finanziert. Dem Kläger wird bei Nutzung des Netzwerks Werbung angezeigt, die auf seinen Interessen basiert, welche die Algorithmen der Beklagten ausgewertet haben. Wahlweise können die Nutzer seit November 2023 ein Abonnement-Modell wählen, bei dem sie gegen Zahlung einer monatlichen Gebühr die Anzeige von Werbung abschalten können.

Die Einrichtung eines Kontos im Netzwerk der Beklagten setzt voraus, dass der Nutzer den Nutzungsbedingungen (Fassung vom 07.09.2023, Anlage K 1) zustimmt. Diese sehen unter anderem vor, dass der Kläger die von der Beklagten erhobenen Daten, einschließlich solcher, die sich aus der Nutzung anderer konzerneigener Dienste sowie aus sonstigen Internetaktivitäten des Nutzers außerhalb der Netzwerke der Beklagten ergeben, der Beklagten zur Darbietung "personalisierter Erlebnisse" sowie zu "anderen Zwecken" zur Verfügung stellt. Als andere Zwecke werden in den Nutzungsbedingungen aufgeführt (Anlage K1, S. 81 ff.): "Als Reaktion auf eine rechtliche Anfrage", "Um geltende Gesetze einzuhalten", "Zu Zwecken von Schutz, Sicherheit und Integrität", "Für Rechtsstreitigkeit". Die Nutzungsbedingungen verweisen auf die Datenrichtlinie der Beklagten, in der unter anderem erläutert wird, dass die vom Nutzer bereitgestellten Informationen und Geräte für alle benutzten Produkte der Beklagten, einschließlich der über die Business Tools übersandten Informationen der Partner der Beklagten, erfasst und miteinander verbunden werden. Eine Cookie-Richtlinie, auf die wiederum die Datenrichtlinie verweist, enthält die Mitteilung, dass die Beklagte seitenbezogene Textinformationen (Cookies) auf dem Nutzergerät platziert und so Informationen erhalten kann, die dort gespeichert werden, wenn der Nutzer Anwendungen der Beklagten oder Internetseiten von anderen Unternehmen, die Business Tools der Beklagten nutzen, aufruft, und zwar ohne dass eine weitere Handlung des Nutzers erforderlich wäre. Die Beklagte teilt die „Informationen“ der Klagepartei mit Partnern, die die „Analysedienste“ der Beklagten nutzen, „integrierten“ Partnern, Anbietern für Messlösungen, Anbietern für Marketinglösungen, verschiedensten „Dienstleistern“ und „externen Forschern“.

Die Integration der streitgegenständlichen Business Tools Apps und Websites von Drittunternehmen geschieht durch Einfügen eines einfachen Skripts im Code der Websites und Apps ("Meta Pixel" für Websites und "App Events über Facebook-SDK" für Apps), das vom technisch durchschnittlich versierten Nutzer nicht bemerkt wird, und seit 2021 wahlweise durch Einbindung eines Skripts auf den Servern der Website- und App-Betreiber ("Conversions API" und "App Events API"), wodurch die Erfassung der Daten nicht mehr auf dem Rechner des Nutzers durchgeführt wird. Auch dies wird vom technisch versierten Nutzer nicht bemerkt und kann auch nicht mehr verhindert werden.

Auf zahlreichen reichweitenstarken Websites und Apps in Deutschland laufen "Meta Pixel" oder "App Events über Facebook-SDK" im Hintergrund, unter anderem bei zahlreichen großen Nachrichtenseiten und -Apps (z.B. spiegel.de, bild.de, welt.de, fAz.net, stern.de), großen Reise- und -Apps (z.B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de, momondo.de), Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, aerzte.de, helios-gesundheit.de, jameda.de), Dating- und Erotikseiten (parship.de, amorelie.de, orion.de, lovescout24.de), sowie Seiten mit Inhalten aus der innersten Intimsphäre (krebshilfe.de, tfp-fertility.com (Samenbank), nie-wieder-alkohol.de, nvve.nl (Sterbehilfe; siehe hierzu Auflistung der Recherche der Klägervertreter im Anlagenkonvolut "Liste_Meta_Pixel_auf_sensiblen_Websites" und Anlage "Liste_meistbesuchte_Websites_Meta_Pixel"). Die Business Tools verarbeiten dort persönliche und höchstpersönliche Daten zur Gesundheit, zur politischen Einstellung, zur Weltanschauung, zu Finanzen sowie zur Sexualität.

Jeder Nutzer ist zu jeder Zeit individuell erkennbar, sobald er sich im Internet bewegt oder eine App benutzt, auch wenn er nicht bei den Netzwerken der Beklagten eingeloggt ist oder deren Apps installiert hat. Diese Erkennung erfolgt durch sogenanntes "Digital Fingerprinting", durch welches ein Nutzer dauerhaft online zurückverfolgbar ist. Zum anderen ist jeder einzelne Klick und jede Texteingabe auf solchen Dritt-Websites und -Apps durch die Beklagte nachverfolgbar. Diese weiß, welche Seiten- und Unterseiten wann besucht wurden, was dort angeklickt, gesucht oder gekauft wurde (vgl. Beispiele der Seiten niewiederalkohol.de, shop-apotheke.com, medikamente-per-klick.de, jameda.de, amorelie.de, Klageschrift S. 9-11, Bl. 9-11 d. Akte). Die angefallenen Daten sendet die Beklagte weltweit in Drittstaaten, insbesondere die USA, und gibt sie bei Bedarf an Dritte sowie an Behörden weiter.

Das "Digital Fingerprinting" führt die Beklage anhand der im Antrag zu 1 aufgeführten personenbezogenen Daten des Nutzers durch. All diese Daten werden im Rahmen des "Advanced Matching" der individuellen Meta-ID zugewiesen und zusammen mit den Standortdaten des Mobilgeräts verknüpft, verwendet und so vollständig individualisiert. Aufgrund des Fingerprintings funktioniert die Zuordnung eines technischen Geräts zum Nutzer mit einer Genauigkeit von über 99 % auch dann, wenn der Nutzer seinen Account bei der Beklagten nicht nutzt bzw. nicht eingeloggt ist und ihre Cookies nicht zulässt. Entsprechend werden sämtliche Daten auch gesammelt, wenn Nutzer nicht bei ihren Netzwerken eingeloggt sind. Da die Anbieter der wichtigsten Browser (Apple Safari, Mozilla Firefox, Google Chrome) seit 2019 die Cookie-Setzung von Drittanbietern stückweise unterbinden und auch die Ausführung von Skriptanwendungen zumindest im Inkognito-Modus schwieriger gemacht wird, führte die Beklagte 2021 die

"Conversions API" und die "App Events API" ein. Deren einziger Zweck besteht nach dem unbestrittenen Klagevortrag darin, unter Mitwirkung der Websitesbetreiber und App-Anbieter alle Schutzversuche der Nutzer und der Browserhersteller zu umgehen und die – in diesem Fall auch für den technisch versierten Nutzer nicht bemerkbare – Datenerhebung weiterhin zu ermöglichen; dies auch, wenn der Nutzer den Inkognito-Modus benutzt und Cookies von Drittseiten nicht zulässt und sogar dann, wenn er ein VPN (virtuelles privates Netzwerk) nutzt. Nutzer, die sich im Laufe ihres Lebens einmal auf den Netzwerken der Beklagten eingeloggt haben, kann sie zuordnen und verknüpft die Nutzer mit sämtlichen anderen aggregierten Daten. Dies wird möglich, indem sich die Conversions API serverseitig an den Server des Websitesbetreibers anbinden lässt und von dort die für Fingerprinting notwendigen Daten sowie "analoge" persönliche Daten wie den Namen oder die Anschrift des Nutzers in gehashter Form geben lässt, ohne dass der Nutzer dies nachvollziehen oder gar verhindern kann. Bildlich gesprochen sind Hashwerte die "Fingerabdrücke von Dateien". Die Business Tools der Beklagten zeichnen dabei unterschiedslos die Daten aller Nutzer auf, weil in den Business Tools keine Entscheidungsmöglichkeit eingebaut ist, welche Daten verarbeitet werden und welche nicht. Sodann werden sämtliche Daten an die Server der Beklagten geschickt. Erst dort wertet die Beklagte aus, ob sie die rechtliche Befugnis hat, die – bereits verarbeiteten – Daten weiter zu verarbeiten. Als "Digitalen Fingerabdruck" bezeichnet man eine Verknüpfung einer solchen Menge an im Browser (sog. "Browser-Fingerprint") oder vom Nutzergerät (sog. "Device-Fingerprint") abrufbaren Daten, die es ermöglichen, den jeweiligen Nutzer allein anhand dieser zu identifizieren. Eine solche Zuordnung ist nach den Feststellungen des Bundeskartellamts in über 99,24 % aller Fälle möglich (vgl. BKartA, Beschluss v. 06.02.2019, Az. B6-22/16, Rn. 580, BeckRS 2019, 4895; Liste der Identifizierungsparameter bei Meta Pixel, Anlage "Parameter_Kundeninfo"). Über diese persönlichen Daten kann die Beklagte dann den bereits als einzigartig identifizierten Browser mit absoluter Sicherheit mit dem tatsächlichen Menschen vor dem Rechner verbinden (advanced matching). Selbst wenn keinerlei Cookies gesetzt sind, übertragen die Business Tools alle in Antrag zu 1 genannten personenbezogenen Daten, die erhoben werden konnten, an die Beklagte. Die Beklagte kann alle Techniken – d. h. Third Party Cookies, First Party Cookies zum Aggregieren von Daten über einen langen Zeitraum ohne sofortige Zuordnung zum Nutzer, aber zum von diesem verwendeten Browser, First Party Cookies im Zusammenspiel mit der Klick-ID zur Zuordnung der aggregierten Daten zum Nutzer, Digital Fingerprinting zum Aggregieren von Daten über einen langen Zeitraum ohne sofortige Zuordnung zum Nutzer über Daten aus dem "HTTP-Header" und IP-Adresse sowie Digital Fingerprinting bei Vorliegen von Nutzerdaten – zur Zuordnung der aggregierten Daten zum Nutzer miteinander kombinieren und somit beispielsweise die über den First Party Cookie über einen langen Zeitraum aggregierten Daten über Aktivitäten auf Drittseiten durch

die einmalige Identifikation durch Digital Fingerprinting einem eindeutigen Nutzer zuordnen. Als "Events" bezeichnet die Beklagte Nutzeraktionen, die sie aufzeichnen kann. Dies kann zum Beispiel das Aufrufen einer Seite ("PageView"), das Absenden eines Suchbefehls ("Search"), das Ausfüllen eines Formulars ("Lead"), das Legen eines Artikels in den Warenkorb ("AddToCart") oder der Kauf eines Artikels ("Purchase") sein. Die Business Tools der Beklagten durchsuchen die Websites und Apps, auf denen sie aktiviert sind, selbstständig nach entsprechenden Events und ändern deren Code so um, dass die Nutzung der entsprechenden Schaltflächen oder die Tastatureingaben bei jeder Nutzung an die Beklagte gesendet werden.

Die Beklagte bewirbt ihr Geschäftsmodell gegenüber Dritten (Anlage "Parameter_Kundeninfo"). Die Conversions API erfüllt die gleiche Funktion wie Meta Pixel und stellt nach Auffassung des Klägers die Reaktion der Beklagten auf die DSGVO und die zunehmende Sensibilität der Nutzer dar. Die Beklagte bewirbt die Conversions API aktiv damit, dass sie von Websitesbetreibern eingesetzt werden soll, um Daten von denjenigen Nutzern zu erheben und an die Beklagte zu senden, welche einer Nutzung ihrer Daten nicht zustimmen (Anlage Meta_Playbook, insb. S. 23). Da sie nicht in den Browser des Nutzers geladen werden muss, kann der Nutzer sie nicht abschalten. Weder ein "Inkognito-Modus" noch eine AntiSpy-Software oder ein VPN helfen hier weiter (Anlage "Anlagenkonvolut_Conversions_API"). Die entsprechenden Systeme nutzt die Beklagte auch bei Nutzern, die die Schaltflächen "Optionale Cookies erlauben" und "Informationen über Aktivitäten von Werbepartnern" nicht aktiviert haben (vgl. Beispiel einer Nutzung von spiegel.de, Replik S. 25 bis 33).

Die verarbeiteten Informationen werden von den Business Tools ab dem Zeitpunkt ihrer Installation durch den jeweiligen Websitesbetreiber unmittelbar an die Server der Beklagten weitergeleitet. Es folgen serverseitig weitere Verarbeitungsvorgänge, wie die Speicherung, der Abgleich mit den bei der Beklagten hinterlegten Datensätzen zur eindeutigen Zuordnung, ggf. eine Veränderung durch Pseudonymisierung und die weitere Verwendung. Ob die erfassten und weitergeleiteten Informationen nun im Rahmen eines Abgleichs einem Nutzer zugeordnet werden können, der mit dieser Art der Verarbeitung einverstanden war, stellt die Beklagte erst jetzt fest und entscheidet sich sodann ggf. für eine Pseudonymisierung der Daten und eine weitere Verwendung für "eingeschränkte Zwecke". Aus den AGB der Beklagten ergibt sich, dass die Beklagte das hierfür erstellte Persönlichkeitsprofil auch zu nicht werberelevanten Zwecken nutzt. Hinsichtlich der weiteren technischen Einzelheiten der Datensammlung und -verarbeitung der Beklagten, zum Beispiel "Third Party Cookies", insbesondere den "User Login Cookie" der Beklagten, "First Party Cookies", insbesondere "_fbp" und "_fbc" der Beklagten, die durch die Business Tools generierte interne Browser-IDs und interne Klick-IDs beinhalten,

"Klick-ID" sowie den digitalen Fingerabdruck über "automatisiertes Advanced Matching" und "manuelles Advanced Matching", wird auf die Ausführungen in der Replik vom 26.03.2025 Bezug genommen.

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

Die irische Datenschutzbehörde DPC verhängte im Mai 2023 ein Bußgeld i.H.v. 1,2 Milliarden EUR wegen der unerlaubten Übermittlung von Daten der europäischen Nutzer der Beklagten in die USA.

Mit dem als Anlage K 3 vorgelegten anwaltlichen Schreiben vom 28.03.2024 forderte die Klagepartei die Beklagte auf, anzuerkennen, dass der Nutzungsvertrag bzgl. der Nutzung des Netzwerks "Instagram" eine Datenverarbeitung personenbezogener Daten des Klägers, die dessen Aktivitäten außerhalb des Netzwerks "Instagram" oder weiterer Produkte der Beklagten betreffen, und die über den Aufruf dritter Websites und Apps entstehen, ohne wirksame Einwilligung des Klägers grundsätzlich nicht zulasse. Weiterhin wurde die Beklagte zur Abgabe einer strafbewährten Verpflichtungserklärung aufgefordert. Darin sollte sich die Beklagte verpflichten, die personenbezogenen Daten des Klägers nur noch auf ausdrückliche Weisung des Klägers zu verarbeiten. Weiterhin sollte sich die Beklagte verpflichten, die personenbezogenen Daten zu löschen, sobald der Kläger sie hierzu auffordere. Darüber hinaus sollte die Beklagte anerkennen, dass sie auf Anfrage des Klägers Auskunft über die o.g. erhobenen per-

sonenbezogenen Daten erteile. Die Beklagte sollte ferner eine strafbewährte Unterlassungserklärung abgeben, wonach sie es zu unterlassen habe, personenbezogene Daten des Klägers, die deren Aktivitäten außerhalb des sozialen Netzwerks über den Aufruf dritter Websites und Apps betreffen, ohne nachweisbare wirksame Einwilligung des Klägers zu verarbeiten, solange im Einzelfall kein Rechtfertigungsgrund nach Art. 6 DSGVO vorliege. Schließlich sollte sich die Beklagte zur Zahlung eines Schmerzensgeldes i.H.v. 5.000 EUR verpflichten. In dem außergerichtlichen Schreiben wurde der Beklagten Frist bis zum 18.04.2024 gesetzt. Wegen des weiteren Inhalts wird auf die Anlage K3 verwiesen. Eine Zahlung durch die Beklagte erfolgte nicht.

Der Kläger behauptet, er habe Internetseiten besucht, auf denen die streitgegenständlichen Business Tools installiert seien. Durch die damit einhergehende Verarbeitung seiner personenbezogenen Daten habe er einen Kontrollverlust in Bezug auf diese Daten erlitten. Er fühle sich unwohl, überwacht und eingeschränkt. Er sei sich über das komplette Ausmaß der Spionage der Beklagten nicht bewusst gewesen und habe die Befürchtung, dass die Daten missbräuchlich verwendet werden. Er fühle sich – insbesondere, weil er keine Einwilligung diesbezüglich erteilt habe – in seiner Privatsphäre verletzt.

Der Kläger meint, er könne gegenüber der Beklagte umfassend Auskunft über die von ihr mittels der Business Tools erlangten personenbezogenen Daten verlangen. Nach erfolgter Auskunftserteilung habe er das Recht, die Löschung bzw. wahlweise Anonymisierung der Daten zu verlangen. Die Verarbeitung der über die Business Tools erlangten personenbezogenen Daten durch die Beklagte sei von Anfang an rechtswidrig und insbesondere nicht von einer Einwilligung gedeckt. Durch die Einbindung der Business Tools auf Websites Dritter werde die Beklagte nach der Rechtsprechung des EuGHs "Verantwortlicher" i.S.d. DSGVO für sämtliche Websites und Apps, auf denen ihr Code laufe. Der Kläger ist der Ansicht, der ihm zustehende Schadensersatzanspruch sei auf mindestens 1.500 EUR zu beziffern.

Der Kläger hat mit Schriftsatz vom 26.03.2025 die ursprünglichen Anträge aus der Klageschrift unter Ziff. 1 und 2 abgeändert. Innerhalb dieses Schriftsatzes hat der Kläger neben den prozessual gestellten Anträgen auf Auskunftserteilung ein außergerichtliches Auskunftsverlangen geltend gemacht (Schriftsatz vom 26.03.2025, S. 43 ff., Bl. 176 ff. d. Akte).

Der Kläger beantragt zuletzt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche der folgenden personenbezogenen Daten der Klagepartei

seit dem 25.05.2018 mit Hilfe der „Meta Business Tools“ erfasst, an die Server der Beklagten weitergeleitet, dort gespeichert und anschließend verwendet wurden und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Instagram“ unter dem Benutzernamen [REDACTED] der Klagepartei verknüpft wurden,

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

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

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

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

c. in mobilen Dritt-Apps

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

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.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags 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.

3. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 1.500,00 Euro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszins-

satz seit dem 26.04.2024, zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 Euro freizustellen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte meint, die Datenerhebung auf Drittwebsites- und Apps sei rechtmäßig. Sie erfolge gemäß der in der Datenschutzrichtlinie dargelegten und einschlägigen Rechtsgrundlagen. Im Gegensatz zu den Ausführungen des Klägers sei der Betreiber der Drittwebsite bzw. der App-Anbieter dafür verantwortlich, eine entsprechende Einwilligung beim Nutzer einzuholen. Die Drittunternehmen seien Hauptverantwortliche für die Installation und Nutzung der Business Tools, für die Bereitstellung von Informationen zur Nutzung der Business Tools für die Besucher der jeweiligen Website oder App, schließlich obliege ihnen die Verantwortung zur Schaffung einer rechtlichen Grundlage für die Sammlung und Übermittlung von Daten an die Beklagte mittels der streitgegenständlichen Business Tools. Gemäß Abs. 3d der Business Tool Geschäftsbedingungen seien Drittunternehmen dafür verantwortlich, die nach der ePrivacy-Richtlinie erforderliche Zustimmung für die Speicherung und den Zugriff auf Cookies oder andere Informationen auf dem Gerät eines Endbenutzers einzuholen.

Die Beklagte ist der Ansicht, mit dem außergerichtlichen Schreiben aus Anl. B8 habe sie das Auskunftsverlangen des Klägers bereits hinreichend beantwortet. Dem Kläger stünden zudem mehrere Tools zur Verfügung, mittels derer die angefragten Auskünfte jederzeit abgerufen werden könnten. Die übrigen angefragten Informationen seien in der beklagteigenen Datenschutzrichtlinie enthalten. Der Anspruch auf Anonymisierung der Nutzerdaten finde keine Grundlage in der DSGVO. Schließlich habe der Kläger stets die Möglichkeit, über die bereitgestellten Nutzertools die von Drittunternehmen geteilten Informationen über Aktivitäten von seinem Instagram-Konto zu trennen, auch könne er jederzeit seinen Account im Netzwerk der Beklagten vollständig löschen.

Auch sonst sei die Datenverarbeitung mittels der Business Tools rechtmäßig und im Einklang mit der DSGVO. Nach der Auffassung der Beklagten wende sich die Klägerseite in der Hauptsache lediglich gegen die Datenverarbeitung zu Zwecken der Bereitstellung von personalisierter Werbung. Insoweit setze die Beklagte stets auf eine wirksame Einwilligung gem. Art. 6 Abs 1 lit. a DSGVO. Eine Datenverarbeitung zu Werbezwecken finde hier jedoch nicht statt, da der Kläger eine entsprechende Einwilligung gerade nicht erteilt habe. Auch habe der Kläger keine

Einwilligung in die Verwendung von Meta-Cookies auf anderen Websites und Apps erteilt. Der Kläger habe die Möglichkeit, sich dafür zu entscheiden, das werbefreie Abonnement abzuschließen. Dann bekomme er überhaupt keine Werbung mehr angezeigt.

Die im Übrigen vorgenommene Datenverarbeitung sei insbesondere aus Sicherheits- und Integritätszwecken gerechtfertigt. Dies erkläre auch die Datenschutzrichtlinie der Beklagten. Des Weiteren werde innerhalb der Klage nicht hinreichend konkretisiert, welche spezifischen Verarbeitungszwecke der Kläger angreifen wolle. Eine Darlegung der konkret besuchten und mit einem Business Tool ausgestatteten Websites und Apps fehle, sodass die Beklagte ihr prozessuales Verhalten hierauf nicht einstellen könne. Tools wie die streitgegenständlichen Business Tools seien natürlicher und allgegenwärtiger Bestandteil des Internets.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze und die zu den Akten gereichten Unterlagen Bezug genommen.

Entscheidungsgründe

Die zulässige Klage hat auch in der Sache Erfolg.

I. Die Klage ist vollumfänglich zulässig.

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

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

aa) Die Kammer verweist zur Herleitung der Verantwortlichkeit der Beklagten i.S.d. DSGVO in unmittelbarem Bezug auf die Plattform umfassend auf die Ausführungen des LG Lüneburg (Urt.

v. 10.01.2025, Az. 15 O 269/23, GRUR-RS 2025, 81 Rn. 25): „Die Beklagte ist Verantwortliche bzw. Auftragsverarbeitende im Sinne der DSGVO. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte hat vorliegend als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden, sodass sie insoweit als Verantwortliche im Sinne der DSGVO anzusehen ist (vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris; vgl. im Einzelnen auch unten); sie ist auch keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.“

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

Gebühr auch eine werbefreie Nutzung der Plattform Facebook als werbefreies Abonnement anbietet.“

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

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

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

3. Soweit die Anträge aus der Klageschrift mit Schriftsatz vom 26.03.2025 teilweise geändert wurden, ist dies zulässig. Bei der Änderung der ursprünglichen Klageanträge unter Ziffern 1 und 2 handelt es sich um einen Fall des § 264 Nr. 1 ZPO und damit nicht um eine echte Klageänderung. Eine darüberhinausgehende Klagerücknahme i.S.v. §§ 264 Nr. 2 und 269 Abs. 1 ZPO ist hierin nicht zu erkennen, da die Anträge lediglich präzisiert wurden und eine Veränderung des ursprünglichen Streitgegenstands nicht stattfand (vgl. die Ausführungen von Stein/Roth, § 264 ZPO, Rn. 6 unter dem Stichwort eines „*unzutreffend formulierten Klageantrags*“, siehe auch OLG Dresden, Urt. v. 1. 12. 2010, Az. 1 U 475/10, NJW-RR 2011, 924, 927).

II. Die Klage ist begründet.

1. Dem Kläger stehen Auskunftsansprüche gegen die Beklagte gem. Art. 15 Abs. 1 lit. a, c, g und h DSGVO im tenorierten Umfang zu.

a) Bei sämtlichen Datums-Angaben, die vom Klageantrag unter Ziff. 1 umfasst sind, handelt es sich um vom sachlichen Anwendungsbereich der Vorschrift erfasste personenbezogene Daten. Insoweit wird auf die überzeugende Begründung des LG Münster (Urt. v. 20.11.2024, Az.: 04 O 241/23, amtlicher Ausdruck, mitgeteilt durch den Kläger) Bezug genommen:

"Bei den im Klageantrag zu 1) genannten Daten handelt es sich um personenbezogene Daten der Klägerin. Hierunter fallen nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, 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.

Unzweifelhaft sind danach die E-Mail der Klägerin, deren Telefonnummer, ihr Vor- und Nachname, ihr Geburtsdatum, ihr Geschlecht und der Ort, an dem sie sich befindet, personenbezogene Daten. Ebenso handelt es sich bei der IP-Adresse des genutzten Clients um ein personenbezogenes Datum.

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

Auch die URLs der 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 Klägerin angeklickten Buttons sowie die weiteren, von der Beklagten „Events“ genannten Daten, die die Interaktion der Klägerin auf der jeweiligen Webseite dokumentieren sind personenbezogene Daten, da sie jeweils in Verbindung mit weiteren Informationen der Klägerin zugeordnet werden können und dadurch Informationen über diese beinhalten. So kann dadurch ermittelt werden, welche Webseiten die Klägerin 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 Klägerin in der App angeklickten Buttons, sowie den von der Beklagten „Events“ genannten Daten, die

die Interaktionen der Klägerin in der jeweiligen App dokumentieren um personenbezogene Daten.

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

Schließlich sind auch die Lead-ID, die Abonnement-ID, die anon_id sowie die externe ID anderer Werbetreibender personenbezogene Daten. Denn als „ID“ stellen sie Identitätsdokumente bzw. Kennungen der Klägerin dar bezüglich ihrer Aktionen/Kontakte im Internet als potenzieller Kunde („Lead“), als Abonnent und hinsichtlich Installationen [...] sowie die Kennung der Klägerin bei anderen Werbetreibenden.“

Soweit nach Ansicht einzelner Gerichte ein spezifisches Interesse des Klägers am Erhalt dieser Daten fehle (so LG Aachen, Urt. v. 19.09.2024, Az.: 12 O 470/23, amtlicher Ausdruck, mitgeteilt durch den Kläger) kann die Kammer eine solche Argumentation nicht teilen. Gerade erst aufgrund des Zusammenspiels der einzelnen technischen Daten ergibt sich der Vorwurf des Klägers, wonach sämtliche Nutzeraktivitäten i.S.e. Digital Fingerprintings zusammengeführt wurden. Soweit für den Kläger einzelne Daten aufgrund deren Abstraktheit wertlos sein mögen, eröffnet die Addition aller erhobenen Daten die Möglichkeit, das Ausmaß des Digital Fingerprintings zu überprüfen. Aus diesem Grund darf es dem Kläger nicht verwehrt sein, Auskunft über die erhobenen Einzeldaten zu beanspruchen.

b) Die Beklagte ist Verantwortliche i.S.d. DSGVO (s.o.) und verarbeitet personenbezogene Daten i.S.v. Art. 4 Nr. 1 und 2 DSGVO in der im Tatbestand genannten Form: Die Beklagte erhebt personenbezogene Daten der Nutzer, sobald diese Websites oder Apps mit den Business Tools aufrufen bzw. wenn sie auf diese Websites Interaktionen durchführen. Sodann verknüpft die Beklagte die gewonnenen Daten mit dem Nutzerkonto der Klägerseite. Schließlich werden die Daten für die o.g. Zwecke verwendet (EuGH, Urt. v. 04.07.2023, Az. C-252/21, GRUR 2023, 1131, Rn. 71).

Gem. § 138 Abs. 3 und 4 ZPO ist der vollständige klägerische Vortrag zum Vorgehen der Beklagten in Bezug auf die Datenerhebung- und Verarbeitung – insbesondere zur Funktionsweise der Business Tools, der Übertragung der personenbezogenen Daten und der Erstellung von Nutzerprofilen – dem Urteil als unstreitig zugrunde zu legen. Die Beklagte ist dem klägeri-

schen Vortrag in nicht erheblicher Weise entgegengetreten. Der Vortrag der Beklagtenseite erschöpft sich im Wesentlichen darin, dass sie mangels Einwilligung des Klägers keine Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung vornehme. Darüber hinaus gesteht die Beklagte zu, dass sie die Daten, welche ihr über die Business Tools übermittelt werden, für andere Zwecke wie beispielsweise "Integrität und Sicherheit" nutzt (siehe u.a. Duplik vom 26.11.2024, Rn. 81, Bl. 522 d. Akte).

Entgegen der Meinung der Beklagten hat die Klägerseite ausreichend dargelegt, dass die Beklagte ihre Daten in den streitgegenständlichen Business Tools verarbeitet. Die Klagepartei muss im Rahmen der Festlegung des streitgegenständlichen Sachverhalts nicht den konkreten Zweck der Datenverarbeitung, die sie angreifen will, benennen. Die DSGVO nimmt lediglich auf der Seite der Rechtfertigung, insbesondere in Art. 6 und 9 DSGVO, eine Differenzierung nach dem Zweck der Datenverarbeitung vor. Demnach ist es allein die Aufgabe der Beklagten, im Rahmen der Darlegung eines Rechtfertigungsgrunds den von ihr verfolgten Zweck näher zu spezifizieren.

Die Beklagte, die über die Daten der Klägerin verfügt, kann sich überdies nicht auf ein Bestreiten mit Nichtwissen zurückziehen.

Soweit die Beklagte im Rahmen des Bestreitens einwendet, dass es sich teilweise um Daten handle, die nach der Eigenart des Internets stets erhoben und verarbeitet werden, kann dies nicht verfangen. Auch diese Daten fallen unter den Anwendungsbereich der DSGVO. Der Verordnungsgesetzgeber war sich dessen bewusst und stellte in Erwägungsgrund 30 fest, dass natürlichen Personen unter Umständen Online-Kennungen wie IP-Adressen, Cookie-Kennungen oder andere Identifikatoren zugeordnet werden können, die mit ihrem Gerät, Softwareanwendungen, Tools oder Protokollen zusammenhängen. Im Übrigen geht die Datenverarbeitung der Beklagten über diese technischen Standarddaten weit hinaus.

c) Der Auskunftsanspruch wurde bislang weder außergerichtlich noch gerichtlich durch die Beklagte i.S.v. § 362 Abs. 1 BGB erfüllt.

aa) Die Erfüllung des Auskunftsanspruchs nach Art. 15 DSGVO i.V.m. § 362 Abs. 1 BGB hat nach der Rspr. des BGH die folgenden Voraussetzungen:

"Erfüllt iSd § 362 I BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen

Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH NJW 2021, 765 = GRUR 2021, 110 Rn. 43 mwN).

Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (vgl. BGH Urt. v. 6.3.1952 – IV ZR 45/50 und IV ZR 16/51, BeckRS 1952, 103508 Rn. 28 f.; Staudinger/Bittner/Kolbe, BGB, Neubearb. 2019, § 260 Rn. 36 und § 259 Rn. 32)."

(BGH, Urt. v. 15.06.2021, Az. VI ZR 576/19, NJW 2021, 2726 Rn. 19, 20)

Die Kammer musste sich demgemäß die Frage stellen, ob die Beklagte nach Auslegung ihres Erklärungswillens anhand objektiver Kriterien (vgl. §§ 133, 157 BGB) eine Erfüllung sämtlicher Auskunftsverlangen des Klägers bezweckte oder ob die tatsächlich erteilte Auskunft erkennbar bestimmte Auskunftsfragen aussparte. Entscheidungsrelevanter Zeitpunkt ist insoweit der letzte Zeitpunkt der mündlichen Verhandlung. Eine Verurteilung der Beklagten kam demgemäß auch im Falle einer nur teilweisen Erfüllung in Betracht (siehe hierzu OLG Köln, Urt. v. 10.8.2023, Az. 15 U 184/22, NZA-RR 2023, 515 Rn. 17, beck-online).

bb) Im hier zu entscheidenden Fall argumentiert die Beklagte, sie habe dem Auskunftsverlangen des Klägers aus der Klageschrift bereits mit dem Schriftsatz in Anlage B8 ausreichend geantwortet. Soweit sich der Kläger in seinen prozessualen Schriftsätzen auf eine außergerichtliche Geltendmachung des Auskunftsverlangens vor Einreichung der Klageschrift bezieht, kann das Gericht eine solche Geltendmachung in der vorgelegten Anlage K3 zwar nicht erkennen – da dort allein die Anerkennung einer Auskunftspflicht geltend gemacht wurde –, dies kann jedoch dahinstehen, da es für die prozessuale Geltendmachung des Auskunftsanspruchs nicht auf eine außergerichtliche Geltendmachung ankommt. Obwohl der prozessuale Auskunftsantrag und das Antwortschreiben in Anl. B8 aus diesem Grund nicht vollständig inhaltlich korrespondieren, enthalten beide Schriftsätze inhaltlich dennoch die gleichen Aus-

kunftsfragen und Antworten, sodass sich die folgenden Ausführungen am Aufbau des außergerichtlichen Antwortschreibens der Beklagten in Anlage B8 orientieren.

(1) In dem Schreiben in Anl. B8 (S. 2, Bl. 129 Anlagenheft Beklagte) legt die Beklagte das Auskunftsverlangen des Klägers vorangestellt eigenständig aus, bevor sie auf die ihrer Ansicht nach begehrte Auskunft inhaltlich antwortet. Sie führt wie folgt aus:

"Meta versteht das Auskunftsverlangen Ihrer Mandantschaft wie folgt:

- *Begehren 1: Welche personenbezogenen Daten hat Meta seit dem 25. Mai 2018 über die streitgegenständlichen Business Tools im Rahmen der Datenverarbeitung zur Bereitstellung personalisierter Werbung verarbeitet. Insbesondere, ob dies die unter dem Auskunftsverlangen Unterabschnitt 1 a2, 1 b3 und 1 c4 aufgeführten Datenpunkte umfasst.*

Im Hinblick auf die obig genannten Daten:

- *Begehren 2: „[O]b, und wenn ja welche konkreten personenbezogenen Daten [Ihrer Mandantschaft] [Meta] 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“;*
- *Begehren 3: „[O]b, und wenn ja welche konkreten Daten [Ihrer Mandantschaft] [Meta] seit dem 25.05.2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat“;*
- *Begehren 4: „[I]nwieweit die Daten [Ihrer Mandantschaft] für eine automatisierten Entscheidungsfindung einschließlich Profiling verwendet wurden und werden. [Einschließlich] Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für [Ihre Mandantschaft].““*

Hierbei interpretiert die Beklagte das Auskunftsverlangen im Allgemeinen und spezifisch unter Begehren Ziff. 1 – wie später auch prozessual – dergestalt, als dass es dem Kläger allein um die Beantwortung der Frage ginge, welche personenbezogenen Daten die Beklagte über die streitgegenständlichen Business Tools im Rahmen der Datenverarbeitung zur Bereitstellung von personalisierter Werbung verarbeite. Eine Beschränkung auf die Bereitstellung zu Werbe-

zwecken hat der Kläger in seinem Auskunftsverlangen jedoch zu keiner Zeit vorgenommen. Auf diese "Fehlinterpretation" der streitgegenständlichen Vorwürfe ist die Beklagte im hiesigen und in auch in vielen anderen Verfahren hingewiesen worden. Insofern war es sowohl für die Beklagte selbst als auch für einen objektiven Dritten erkennbar, dass sich ihr Erklärungswille bei der Beantwortung der Auskunftsfrage auf eine vollkommen andere Fragestellung bezog. Die abweichende Auslegung der Fragestellung ist dabei nicht unwesentlich, denn sie führt gerade dazu, dass die Beklagte das streitgegenständliche Verhalten bei der Beantwortung des Auskunftersuchens vollständig ausspart.

Darüber hinaus stellt die Antwort der Beklagten unter Begehren Ziffer 1 auch im Übrigen keine geeignete Auskunft dar. Der Verweis der Beklagte auf die Service-Tools unter der Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien“ ist bereits grundsätzlich nicht geeignet, die Auskunftsfragen des Klägers zu beantworten, da auch diese Auskünfte allein nach dem Verständnis der Beklagten in Bezug auf die Verwendung personenbezogener Daten zu Werbezwecken erfolgen. Im Übrigen tritt die Beklagte der aus diesem Grund gem. § 138 Abs. 3 ZPO als zugestanden anzusehenden Behauptung des Klägers nicht entgegen, wonach über dieses Tool nur solche Drittwebsites angezeigt werden, die besucht wurden, währenddessen man auf dem gleichen Gerät im Netzwerk der Beklagten eingeloggt war. Dies gilt auch für Behauptung, die innerhalb des Tools zu findenden Informationen teilen nicht mit, an welche Dritte sie weitergegeben wurde. Zudem seien die Informationen auf einen Zeitraum von wenigen Monaten begrenzt.

Des Weiteren wird auf der von der Beklagten auf S. 3 ihres außergerichtlichen Schreibens angegebenen Hilfeseite "<https://www.facebook.com/help/2207256696182627/>" wortwörtlich ausgeführt: *„Wir erhalten mehr Einzelheiten und Aktivitäten, als du unter „Aktivitäten außerhalb von Meta-Technologien“ siehst.“* Hierdurch erklärt die Beklagte selbst, dass es noch weitere Daten gibt, die nicht von ihren Tools beauskunftet werden. Ihre Begründung hierzu *"Aus technischen Gründen und aus Gründen der Zuverlässigkeit zeigen wir nicht alle Aktivitäten, über die wir informiert wurden. Das betrifft unter anderem Informationen, die wir erhalten haben, während du nicht bei Facebook angemeldet warst, oder Situationen, in denen wir nicht überprüfen können, ob du auf einem bestimmten Gerät zuvor Facebook verwendet hast. Ebenso wenig zeigen wir Einzelheiten an, wie etwa den Artikel, den du zu deinem Einkaufswagen hinzugefügt hast."* ist ungeeignet, den Anspruch auszuschließen. Selbst wenn man eine Ausnahme von der Pflicht zur Auskunftserteilung wegen Unverhältnismäßigkeit anerkennen wollte, müsste die Beklagte zu den Ausschlussgründen gezielt vortragen. Dies hat sie jedoch in Kenntnis dieses Umstands aus weiteren Verfahren (siehe nur LG Münster, a.a.O.) nicht getan. Ebenso für eine Unmöglichkeit der Beauskunftung wurde nicht hinreichend vorgetragen.

Soweit die Beklagte ferner auf das Tool "Deine Informationen herunterladen" verweist, ist hierbei nicht dargelegt worden, ob diese Informationen überhaupt auf die Auskunftsfraße eingehen. In den Ausführungen der Beklagten ist lediglich die Rede von "*Wenn du eine Kopie von allem möchtest, was du auf Instagram geteilt hast, [...]*". Was hierunter konkret zu verstehen ist, wird jedoch nicht klar.

(2) Unter dem Punkt Begehren Ziff. 2 verkürzt die Beklagte zunächst das Auskunftsbegehren erneut auf die Datenverarbeitung ausschließlich zu Werbezwecken, geht anschließend jedoch auch darauf ein, dass der Kläger i. A. Auskunft über die Verarbeitung personenbezogener Daten im Zusammenhang mit seinem Konto verlangt. Hierauf führt die Beklagte zunächst aus, wie die Daten anhand der Datenschutzrichtlinie der Beklagte verarbeitet werden können. Es folgt eine Wiedergabe der Datenschutzrichtlinie. Im Anhang des Antwortschreibens findet sich zudem eine Anlage 1, die mit "*Identität der individuellen Empfänger*" bezeichnet ist. Die Tabelle besteht aus vier Spalten, die mit "Datum", "(Genutzte) Applikation", "Provider" und "Drittpartei" bezeichnet sind. Lediglich die ersten beiden Spalten, d.h. "Datum" und "(Genutzte) Applikation" sind ausgefüllt worden. Es findet sich jedoch nirgends eine Erklärung dazu, wie diese Angaben zu verstehen sind. Auch hierauf wurde die Beklagte bereits hinreichend durch die Klägerseite und andere Gerichte hingewiesen. Es wird zudem in der Tabelle weder dargestellt, welche konkreten personenbezogenen Daten verarbeitet wurden, wer der konkrete Empfänger dieser Daten war, noch zu welchen Zwecken dies erfolgte. Das Auskunftsrecht in Art. 15 Abs.1 DSGVO erfasst jedoch gerade das Recht auf Beantwortung dieser Fragen. Nach der Rspr. des EuGHs (Urt. v. 12.01.2023, Az. C-154/21, EuZW 2023, 226) muss die Identität des konkreten Empfängers mitgeteilt werden. Nach zutreffender Ansicht muss hierbei auch die ladungsfähige Anschrift angegeben werden (BeckOK DatenschutzR/*Schmidt-Wudy*, 52. Ed. 01.05.2025, DSGVO Art. 15 Rn. 58; Anmerkung *Aqilah Sandhu* zu EuGH, Urt. v. 12.01.2023, Az. C-154/21 in EuZW 2023, 226), um eine eindeutige Identifikation zur Geltendmachung weiterer Rechte der betroffenen Person zu ermöglichen.

Das Zitieren der Datenschutzrichtlinie der Beklagten ersetzt dabei nicht die Erteilung einer individuellen Auskunft. Die Richtlinie geht an keiner Stelle auf die konkret gestellten Auskunftsfragen ein. Dies gilt insbesondere in Bezug auf die Beauskunftung der Frage, inwieweit die Beklagte durch ihre Business Tools auf Drittwebsites- und -apps personenbezogene Daten des Klägers erhebt. Die zitierte Richtlinie beschränkt sich im Wesentlichen darauf, verallgemeinert zu erklären, welche Daten bei der unmittelbaren Nutzung der Beklagtennetzwerke verarbeitet werden können. Soweit dort ausgeführt wird, dass Nutzerdaten an externe Forscher oder sonstige Dritte weitergegeben werden, um "Forschung durchzuführen" oder "als Reaktion auf rechtliche Anfragen, um geltendes Recht einzuhalten oder um Schäden zu verhindern", ist

diese Auskunft vollkommen abstrakt und generell.

(3) Gleiches gilt für die Beauskunftung des Begehrens unter Ziff. 3. Dort erläutert die Beklagte anhand ihrer Datenschutzrichtlinie allgemein, anhand welcher Parameter sie die Speicherdauer für die erhobenen personenbezogenen Daten festlegt. Auf die konkrete Frage "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 [?]" wird hierbei nicht eingegangen. Die Beklagte beruft sich des Weiteren darauf, dass Art. 15 Abs. 1 DSGVO keinen Anspruch begründe, zu erfahren, welche Daten in welchem Drittstaat gespeichert wurden. Im Übrigen sei dies bereits mit der Datenschutzrichtlinie hinreichend geklärt.

Zutreffend ist, dass im Falle der Übermittlung personenbezogener Daten an ein Drittland nach Art. 15 Abs. 2 DSGVO ein Recht des Betroffenen besteht, über geeignete Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden. Dies schließt nach dem eindeutigen Wortlaut in Art. 15 Abs. 1 lit. c DSGVO das Recht des Betroffenen nicht aus, Auskunft über die Empfänger in Drittländern zu beanspruchen (a.A. LG Kiel, Az. 6 O 274/23, amtlicher Ausdruck, mitgeteilt durch die Beklagte).

(4) In Bezug auf die Auslegung des Begehrens unter Ziff. 4, d.h. für die Frage, ob eine Verarbeitung der personenbezogenen Daten stattfindet, die unter den Anwendungsbereich des Art. 22 Abs. 1 DSGVO fällt, antwortet die Beklagte, dass eine solche Verarbeitung nicht festgestellt werden konnte. Da auch diese Auskunft unter der grundlegend unzutreffenden Annahme getätigt wurde, dass sich das Auskunftsbegehren des Klägers allein auf die Verarbeitung der personenbezogenen Daten zu Werbezwecken beschränke, konnte auch an dieser Stelle durch die Kammer nicht auf einen Erklärungswillen in Bezug auf die konkrete Frage des Auskunftsersuchens erkannt werden.

cc) Auf die weitere Frage, ob die Beklagte über Art. 15 DSGVO oder ggfs. § 241 Abs. 2 BGB verpflichtet ist, Auskunft darüber zu erteilen, auf welchen Websites und Apps die Business Tools derzeit aktiviert sind, musste in der hiesigen Entscheidung nicht eingegangen werden, da eine solche Auskunft prozessual nicht geltend gemacht wurde.

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

a) Die in Antrag Ziff. 1 aufgeführten personenbezogenen Daten des Klägers wurden durch die Beklagte durch die Verwendung der Business Tools unrechtmäßig verarbeitet. Dies geschah ohne Einwilligung oder sonstige Rechtfertigung.

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

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

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

In seiner Entscheidung vom 04.07.2023 hat der EuGH die Anforderungen an die Rechtfertigung einer Datenverarbeitung nach den o.g. Vorschriften präzisiert. Er führt wie folgt aus:

„4. Art. 6 I UAbs. 1 Buchst. b der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen

Netzwerks verknüpft und verwendet werden, nur dann als im Sinne dieser Vorschrift für die Erfüllung eines Vertrags, dessen Vertragsparteien die betroffenen Personen sind, erforderlich angesehen werden kann, wenn diese Verarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte.

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

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

ein im öffentlichen Interesse liegendes Ziel verfolgt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel steht und diese Verarbeitung in den Grenzen des absolut Notwendigen erfolgt.

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

In derselben Entscheidung führt der EuGH zudem aus (EuGH, a.a.O., GRUR 2023, 1131, Rn. 133 ff.):

„Desgleichen wird das vorlegende Gericht nach Maßgabe von Art. 6 Abs. 1 Unterabs. 1 Buchst. e DSGVO zu beurteilen haben, ob Meta Platforms Ireland mit einer Aufgabe betraut ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, etwa im Hinblick auf die Forschung zum Wohle der Gesellschaft oder die Förderung von Schutz, Integrität und Sicherheit, wobei es angesichts der Art und des im Wesentlichen wirtschaftlichen und kommerziellen Charakters der Tätigkeit dieses privaten Wirtschaftsteilnehmers allerdings wenig wahrscheinlich erscheint, dass ihm eine solche Aufgabe übertragen worden ist.

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

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

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

(Duplik vom 15.04.2025, S. 47, Bl. 300 d. Akte)

Über diesen pauschalen Vortrag hinaus trägt die Beklagte nicht weiter substantiiert vor. Der übrige Vortrag reicht indes nicht aus, um den strengen Anforderungen des EuGHs zu Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gerecht zu werden. Die Beklagte erklärt nicht, wie personenbezogene Daten der Nutzer eingesetzt werden können, um den genannten Zwecken gerecht zu werden. Insofern wird bereits dem Erforderlichkeitskriterium des EuGHs nicht hinreichend Rechnung getragen. Zudem wird nicht klar, in welchem Umfang und auf welche Art und Weise personenbezogene Daten erhoben werden. Insofern kann das Gericht keine Überprüfung zur Angemessenheit der Datenverarbeitung vornehmen. Zu den sonstigen Rechtfertigungsgründen innerhalb von Art. 6 DSGVO wurde ebenfalls nicht hinreichend vorgetragen. Da es bereits an diesen Voraussetzungen fehlt, sind erst Recht die strengeren Anforderungen nach Art. 9 DSGVO nicht erfüllt. Im Übrigen verstößt das Vorgehen der Beklagten aus den gleichen Gründen gegen Art. 5 Abs. 2 DSGVO. Nach dem in dieser Vorschrift verankerten Grundsatz der Rechenschaftspflicht muss der Verantwortliche nachweisen können, dass die personenbezogenen Daten unter Einhaltung der in Art. 5 Abs. 1 DSGVO genannten Grundsätze erhoben und verarbeitet werden (EuGH, Urt. v. 04.10.2024, Az. C-446/21, NJW 2025, 207 Rn. 55). In Artikel 5 Abs. 1 DSGVO ist unter anderem der Grundsatz der Datenminimierung (lit. c) verankert, der bestimmt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“

müssen (EuGH, a.a.O, NJW 2023, 2997).

Eines Hinweises nach § 139 ZPO an die Beklagte bedurfte es nicht, da es der Beklagten hinreichend aus anderen Gerichtsverfahren bekannt war, dass ihr Vortrag zur Rechtfertigung nach den Vorschriften der DSGVO nicht ausreichend ist (siehe nur LG Ellwangen (Jagst), a.a.O., S. 30).

b) Soweit es der Kläger für die Daten unter Antrag Ziff. 1 lit. b und c der Beklagten freistellt, ob diese eine Löschung oder Anonymisierung der Daten vornimmt, kann dahinstehen, ob sich dogmatisch ein selbstständiger Anspruch auf Anonymisierung von Daten überhaupt aus der DSGVO herleiten lässt (dafür Kühling/Buchner/Herbst, 4. Aufl. 2024, DS-GVO Art. 17 Rn. 39a m.w.N.). Der von Art. 17 DSGVO verwendete Begriff der Löschung ist rechtlicher Art und legt selbst nicht fest, auf welche Art und Weise die Löschung vollzogen wird. Löschung meint im technischen Kontext *"die Unbrauchbarmachung der personenbezogenen Daten oder – wohl der Regelfall – die technische Löschung von elektronischen Daten. Eine Löschung im technischen Sinn – da auch Datenträger höchstens nur überschrieben werden können – meint einen Vorgang, nach dessen Ende auf die Daten bzw. deren Inhalt nicht mehr mit den üblichen Verfahren zugegriffen werden kann [...] Entscheidend ist, dass die Daten nicht mehr verarbeitet und zu diesem Zweck auch nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können [...] Die theoretische Möglichkeit einer Wiederherstellung mit Spezialprogrammen hat hierbei keinen Einfluss auf die Löschung iSd Norm "* (Paal/Pauly/Paal, 3. Aufl. 2021, DS-GVO Art. 17 Rn. 30 m.w.N.). Die Kammer versteht den Antrag des Klägers ausgehend hiervon demgemäß, dass die Unbrauchbarmachung der personenbezogenen Daten verlangt wird. Dies soll durch Löschung im Sinne des allgemeinen Sprachgebrauchs, d.h. durch Überschreibung des vollständigen Datensatzes erfolgen oder durch Anonymisierung, d.h. durch Überschreiben lediglich desjenigen Anteils des Datensatzes, der eine Personalisierung der abstrakten Daten ermöglicht. In diesem Sinne vertritt auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) die Ansicht, dass die Anonymisierung von Daten mit deren Löschung gleichgesetzt werden kann, da sowohl bei einer Löschung als auch bei einer Anonymisierung keine Daten mehr vorliegen, die in den Anwendungsbereich der relevanten DSGVO-Vorschriften fallen. Entscheidend für die Gleichsetzung ist, dass der Personenbezug wirksam beseitigt wird (BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 29.06.2020, S. 8, abgerufen unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=4, zuletzt abgerufen am

13.08.2025). Soweit der BfDI dabei in seinem Positionspapier (a.a.O., S. 9) eine Anwendung der Anonymisierung lediglich auf solche Daten beschränken will, die zunächst rechtmäßig erhoben wurden, greift dies nach der Auffassung der Kammer jedoch zu kurz. Auch im Falle der nicht rechtmäßigen Datenverarbeitung ist die Anonymisierung gleichermaßen zielführend. Das Risiko für den Betroffenen, dass die Anonymisierung tatsächlich erfolgreich war, besteht in eben jenem Maße auch bei der Löschung. Beide Vorgänge finden außerhalb des Zugriffsbereichs des Betroffenen statt. Absolute Gewissheit wird ggfs. nur gerichtlich zu erzielen sein.

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

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

stattfindet.

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

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

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

Nach dem der Klage zugrundeliegenden Tatbestand wurde *„[Das] nahezu gesamte Online-Verhalten des Klägers dokumentiert und in Persönlichkeitsprofilen ausgewertet. Damit ist auch der unantastbare Kernbereich der privaten Lebensgestaltung des Klägers tangiert. Gerade auch dieses sogenannte Profiling stellt einen sehr intensiven Eingriff dar. Nach Erwägungsgrund 60, 63 der DSGVO ist die betroffene Person insbesondere darauf hinzuweisen, dass Profiling stattfindet und welche Folgen das hat. Nach Erwägungsgrund 75 stellt insbesondere die Verarbeitung persönlicher Daten zum Zwecke der Erstellung persönlicher Profile ein besonderes Risiko für einen Schaden dar. Dieser führt aus: Die Risiken für die Rechte und Freiheiten natürlicher Personen - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Dis-*

kriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“ (LG Ellwangen (Jagst), a.a.O., S. 42 f.). Hierin liegen in jedem Fall ein erheblicher Kontrollverlust sowie das Risiko einer weiteren missbräuchlichen Verwendung der Daten. Da die Verarbeitung personenbezogener Daten im hiesigen Fall besonders umfangreich ist – sie betrifft potenziell unbegrenzte Datenmengen und hat nahezu die vollständige Überwachung des Online-Verhaltens des Nutzers zur Folge – ist es nach der Feststellung des EuGHs bereits abstrakt möglich, dass beim Nutzer das Gefühl einer kontinuierlichen Überwachung verursacht wird (EuGH, a.a.O., GRUR 2023, 1131, Rn. 118).

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

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

aa) Nach der Rspr. des EuGHs ermöglicht die DSGVO ausschließlich einen Schadensersatz zum Zwecke des Ausgleichs, nicht auch zur Genugtuung. Die Vorschrift verlangt nicht, dass der Grad der Schwere und die Vorsatzform des Verantwortlichen bei der Schadensbemes-

sung berücksichtigt werden. Im Gegenzug gibt der EuGH den nationalen Gerichten jedoch vor, dass die Höhe des geschuldeten immateriellen Schadensersatzes „seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung“ (zum Ganzen EuGH, Urte. v. 20.06.2024, Az. C-182/22, C-189/22, NJW 2024, 2599). Im Einzelnen:

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

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

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

(4) Mit Blick auf den Vergleich physischer, materieller und immaterieller Schäden rekurriert der EuGH auf den 146. Erwägungsgrund der DSGVO und weist insoweit darauf hin, dass „[d]er Begriff des Schadens ... im Lichte der Rechtsprechung des EuGH weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht“, und dass „[d]ie betroffenen Personen ... einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten [sollten]“ (EuGH, a.a.O., NJW 2024, 2599 Rn. 36). Weiterhin führt er aus, dass durch die nationalen Vorschriften zur Umsetzung des immateriellen Schadensersatzanspruchs die Ausübung der durch das Unionsrecht verliehenen Rechte, insbesondere der DSGVO, nicht unmöglich gemacht oder übermäßig erschwert werden darf (EuGH, a.a.O., NJW 2024, 2599 Rn. 34.)

Hiermit bringt der EuGH zum Ausdruck, dass an der deutschen Rechtsprechung, die bislang immateriellen Schadensersatz bei Persönlichkeitsrechtsverletzungen grundsätzlich nur höchst ausnahmsweise und insgesamt lediglich in geringem Umfang zugesprochen hat, bei der Anwendung der DSGVO nicht festgehalten werden darf (so auch Kühling/Buchner/Bergt,

4. Aufl. 2024, DS-GVO Art. 82 Rn. 18a; Ehmann/Selmayr/Nemitz, 3. Aufl. 2024, DS-GVO Art. 82 Rn. 38). Daraus folgt nicht zuletzt, dass trotz der Beschränkung auf den bloßen Ausgleich der erlittenen Nachteile, die Höhe des Schmerzensgeldes über die in der nationalen Rechtsprechungspraxis etablierten Beträge aus Schmerzensgeldtabellen o.ä. hinausgehen kann (so auch Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18d m.w.N.). Ein „Sich-Einfügen“ in die bisherige nationale Rechtsprechungspraxis stünde geradezu im Widerspruch zur europarechtsautonomen Auslegung des Schadensersatzanspruchs gem. Art. 82 DSGVO. Soweit andere Gerichte teilweise auf nationale Schadensersatzansprüche wie § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG zurückgreifen, um die erweiterten Schutzkategorien dieser Ansprüche einbeziehen zu können (Genugtuung und Prävention) – letztlich um die vermeintlichen Restriktionen des EuGHs mithilfe dieser Ansprüche dogmatisch zu umgehen – ist dieses Vorgehen ob der oben genannte Gründe redundant.

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

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

(1) Anknüpfungspunkte für die Bemessung eines immateriellen Schadensersatzanspruchs muss hier vordergründig der auf der Klägerseite eingetretene Verlust der Daten sein. Dieser ist hinsichtlich des unterschiedlichen grundrechtlich garantierten Schutzniveaus der betroffenen Daten zu differenzieren. Dies gilt insbesondere, wenn besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO betroffen sind (OLG Dresden, Urt. v. 10.12.2024, Az. 4 U 808/24, ZD 2025, 221 Rn. 20).

Zudem sind vor allem der Umfang der gesammelten Daten und die Dauer des Verstoßes zw. der Verletzungshandlung zu berücksichtigen. Hierbei handelt es sich um Kategorien zur Feststellung der Schadenstiefe bzw. -intensität, die nicht gleichzusetzen sind mit dem Grad der Schwere des Verstoßes, den der EuGH für nicht berücksichtigungsfähig erklärt (EuGH, a.a.O., NJW 2024, 2599 Rn. 26). Darüber hinaus kann die Möglichkeit des Betroffenen an der Wiedererlangung seiner Daten bzw. der Kontrolle über diese eine Rolle spielen (OLG Dresden, a.a.O., ZD 2025, 221, Rn. 20).

Weiterhin hat das Gericht bei der Schadensschätzung für den Wert der personenbezogenen Daten einen entsprechenden Anknüpfungspunkt festgelegt. Hierfür hat es auf den Wert personenbezogener Daten für die Beklagte – soweit dieser geschätzt werden konnte – abgestellt, zudem auf den allgemeinen Wert personenbezogener Daten auf dem hierfür relevanten legalen oder auch illegalen Markt. Die Berücksichtigung des Wertes der Daten für den Verletzer wird jedenfalls im Bereich der kommerziellen Nutzung auch in der Literatur gefordert (Simitis/Hornung/Spiecker *gen. Döhmann*, Datenschutzrecht, DS-GVO Art. 82 Rn. 31, m.w.N.).

(2) Für das Ausmaß und den Umfang der betroffenen Daten wird auf die Ausführungen weiter oben verwiesen, auch für die Grundrechtssensibilität der betroffenen Daten. Hinzutritt, dass es aufgrund des bis zum Schluss der mündlichen Verhandlung bestehenden Schweigens der Beklagten zur streitgegenständlichen Datenverarbeitung aussichtslos erscheint, dass der Kläger konkrete Kenntnis davon erhält, ob er die Kontrolle der Daten durch Löschung o.ä. wiedererlangen könnte. Zudem ist über die Geständnisfiktion hinaus rein tatsächlich nicht feststellbar, ob und in welchem Umfang die Daten bereits an Dritte weitergegeben wurden und eine Datensicherung auch aus diesem Grund ausgeschlossen ist.

Erschwerend kommt hinzu, dass sogar wenn der Kläger in Bezug auf die Erhebung und Verarbeitung von Daten zu Zwecken personalisierter Werbung die von der Beklagten vorgesehene Einwilligung abgegeben hätte, diese unwirksam gewesen wäre, da die allgemeine und unterschiedslose Sammlung von Daten u.a. gegen den Grundsatz der Datenminimierung verstößt und die unbegrenzte Speicherung personenbezogener Daten zu Zwecke der zielgerichteten Werbung unverhältnismäßig ist (siehe nur EuGH, a.a.O., NJW 2025, 207 Rn. 58 ff.).

Für den Wert der Daten für die Beklagte hat das Gericht auf die Feststellungen des BKartA (Beschl. v. 02.05.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) zurückgegriffen. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der Werbeeinnahmen einen Anteil i.H.v. 97 % ausmachte (BKartA a.a.O., Rn. 7). Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O., Rn. 53). Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon überzeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und

dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studien (siehe nur die Studie "Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?", Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz; Infografik "Preis, den Erwachsene in den USA für personenbezogene Daten aufrufen würden (in US-Dollar)", Statista mit Quelldaten von Morning Consult aus dem Jahr 2019, abgerufen unter <https://cdn.statcdn.com/Infographic/images/normal/18449.jpeg>).

Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d.h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. Kühling/Buchner/*Bergt*, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18b, beck-online).

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

(a) Nach der Rechtsprechung des BGH ist es dem Tatgericht nach der nationalen Norm des § 286 ZPO grundsätzlich erlaubt, "allein aufgrund des Vortrags der Parteien und ohne Beweiserhebung festzustellen, was für wahr und was für nicht wahr zu erachten ist" (BGH, Beschl. v. 27.09.2017, Az. XII ZR 48/17, NJW-RR 2018, 249). Obwohl diese Rechtsprechung konkret auf die Überzeugungsbildung des Tatgerichts anhand einer informatorischen Anhörung abzielt, ist sie darüber hinaus auch so zu verstehen, dass das Gericht frei darin ist, seine Überzeugung nach § 286 ZPO jenseits der Strengbeweismittel zu bilden. Dies gilt insbesondere im Falle der

Schadensschätzung nach § 287 ZPO, bei der die Freiheit der richterlichen Überzeugungsbildung zusätzlich geweitet ist. Insofern war es dem Gericht freigestellt, auf eine informatorische Anhörung des Klägers – so wie sie die meisten anderen Gerichte bislang vorgenommen haben – zu verzichten. Bei einer Anhörung des Klägers wäre nach Überzeugung des Gerichts gerade kein weiterer Erkenntnisgewinn zu erwarten gewesen, der über die Mitteilung des im Allgemeinen eher diffusen Gefühls des Datenverlusts und der Verunsicherung hinausgeht. Grund hierfür ist, dass es gerade das Problem der klägerischen Partei und auch des Gerichts ist, festzustellen, was konkret die Beklagte mit den Daten vorhat bzw. was sie bereits jetzt unternimmt. Da dies bis zuletzt nicht bekannt wird, kann sich die Erwartung oder Befürchtung des Klägers nicht auf ein bestimmtes Verhalten konkretisieren. Dies kann und darf ihm nicht zum Nachteil gereichen.

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

Die Kammer konnte daher ohne auf das jeweilige subjektive Empfinden des konkreten Klägers abstellen zu müssen, eine durchschnittliche, aufgeklärte und verständige betroffene Person zu Grunde legen, und deren Betroffenheit als Maßstab für einen Mindestschaden zu nehmen.

(4) Die Mindestbeeinträchtigung ist ohne das Hinzutreten weiterer Umstände bereits besonders schwerwiegend und hebt sich maßgeblich von den sog. Scraping-Fällen ab, in denen ein Mindestschaden i.H.v. 100 EUR für den bloßen Kontrollverlust für angemessen erachtet wird (siehe nur OLG Dresden, a.a.O., ZD 2025, 221 Rn. 20 m.w.N.). Anders als in den Scraping-Fällen ist die Quantität und Qualität der streitgegenständlichen Daten um ein Vielfaches größer, sodass der Mindestschaden weitaus höher einzustufen ist. Die Datenverarbeitung durch die Beklagte stellt nach der Rspr. des EuGHs per se einen schweren Eingriff in die

durch Art. 7 und 8 GrCh gewährleisteten Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten dar (EuGH, a.a.O., NJW 2025, 207 Rn. 63), der nicht gerechtfertigt ist.

Die Verletzung dieser Grundrechte wird auch durch den Durchschnittsbetroffenen i.S.d. DSGVO als erhebliche Beeinträchtigung im o.g. Sinne wahrgenommen. Der aufgeklärte und verständige Durchschnittsbetroffene i.S.d. DSGVO wird sich der Bedeutung und Tragweite der über ihn gesammelten Daten bewusst, denn er kennt die Relevanz von personenbezogenen Daten innerhalb einer digitalisierten Gesellschaft und Wirtschaft (s.o. zur Wahrnehmung der Gesellschaft hinsichtlich der Werthaltigkeit von Daten). Der Kontrollverlust über nahezu sämtliche Daten seiner Online-Nutzungsaktivitäten bedeutet für ihn eine dauerhafte und nicht ohne Weiteres zu beseitigende negative Beeinflussung, die sich nach außen hin in unterschiedlichen Sorgen und Ängsten manifestiert. In jedem Falle setzt sich der Nutzer gezwungenermaßen mit dem Verlust der personenbezogenen Daten auseinander und wird hierdurch in Bezug auf sein weiteres Verhalten bei der Nutzung des Internets dauerhaft beeinflusst.

Das Gericht erachtet anhand der obigen Ausführungen in der Gesamtschau einen Betrag i.H.v. 5.000 EUR für einen angemessenen Schadensersatz. Zum Vergleich hat das OLG Dresden in einer Entscheidung wegen Ausspähung durch Einschaltung eines Detektivbüros einen Schadensersatzanspruch i.H.v. 5.000 EUR für angemessen erachtet (OLG Dresden, Urf. v. 30.11.2021, Az. 4 U 1158/21, NZG 2022, 335). Die Reichweite der im hiesigen Verfahren betroffenen Daten geht über das Maß in dem Verfahren vor dem OLG Dresden hinaus, da nach dem als zugestanden anzusehenden klägerischen Vortrag dessen gesamtes im digitalen Bereich stattfindendes Privatleben dauerhaft und nicht nur auf einzelne Aspekte begrenzt aufgezeichnet wurde und immer noch wird. Seit dem Inkrafttreten der DSGVO handelt es sich bei dem als zugestanden anzusehenden Vorgehen der Beklagten um einen solch weitgehenden Verstoß, der den Rahmen der bisher bekannten Fälle bei weitem überschreitet, sodass der Mindestbetrag ohne Darlegung einer besonderen individuellen Betroffenheit mit dem des OLG Dresden in dem o.g. Verfahren gleichgesetzt werden kann.

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

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

Nicht anspruchsmindernd i.S.e. widersprüchlichen Verhaltens wirkt sich aus, dass der Kläger die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Aufgrund der überragenden marktübergreifenden Stellung der Beklagten auf Social-Media-Plattformen (s.o.) ist es dem Nutzer, auch wenn er Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, ist es ihm deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass der Kläger ihre Netzwerke DSGVO-konform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt der Kläger zum Ausdruck, dass ihm die Datenschutzverstöße der Beklagten nicht egal sind, sondern er eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es dem Kläger hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, sein Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden (vgl. Paal, ZfDR 2023, 325).

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

e) Der Kläger hat des Weiteren einen Anspruch auf Verzugszinsen aus der Schadensersatzforderung gem. §§ 286 Abs. 1, 288 Abs. 1 BGB. Durch die vorgerichtliche Zahlungsaufforderung vom 28.03.2024 (Anl. K 3) mit Fristsetzung bis zum 18.04.2024 befand sich die Beklagte in Verzug, sodass Zinsen wie beantragt ab dem 26.04.2024 zuzusprechen waren.

4. Der Kläger kann von der Beklagten Freistellung seiner vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 EUR verlangen, Art. 82 Abs. 1 DS-GVO, §§ 249 Abs. 1, 257 S. 1 BGB.

Außergerichtlich wurde u.a. ein Schmerzensgeldanspruch i.H.v. 5.000 EUR geltend gemacht. Der Klageantrag wurde später lediglich mit einem Betrag i.H.v. mindestens 1.500 EUR beziffert. Soweit das Gericht dennoch auf einen Schmerzensgeldbetrag i.H.v. 5.000 EUR erkennt, erfasst der Schadensersatzanspruch nach Art. 82 DSGVO als weitere materielle Schadensposition auch die Kosten, die durch die außergerichtliche Beauftragung eines Rechtsanwalts angefallen sind (BGH, Urt. v. 18.11.2024, Az. VI ZR 10/24, GRUR 2024, 1910 Rn. 79). Die außergerichtliche Vertretung durch einen Rechtsanwalt war im damaligen Zeitpunkt erforderlich und zweckmäßig. Insbesondere war zur damaligen Zeit nicht absehbar, dass die Beklagte jegliche vorgerichtliche Einigung ablehnte. Im Übrigen handelt es sich um einen äußerst komplexen Sachverhalt, dessen außergerichtliche Geltendmachung dem Kläger allein nicht zuzumuten war. Damit waren die außergerichtlichen Kosten in jedem Fall auf Grundlage eines Streitwerts i.H.v. mindestens 5.000 EUR gerechtfertigt. Der geltend gemachte Betrag i.H.v. 367,23 EUR war demgemäß nach § 308 ZPO begrenzt auf diese Höhe zuzusprechen.

III. Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus § 709 S. 1 ZPO.

IV. Der Streitwert wird nach §§ 63 Abs. 2, 39 Abs. 1, 40, 43 Abs. 1, 48 Abs. 2 Satz 1, 48 Abs. 1 S. 1 GKG i.V.m. §§ 3 ff. ZPO auf 8.000 EUR festgesetzt und setzt sich wie folgt zusammen:

- Auskunft: 2.000 EUR
- Löschung: 1.000 EUR
- Entschädigung: 5.000 EUR

In bürgerlichen Rechtsstreitigkeiten richten sich die Gebühren nach den für die Zuständigkeit des Prozessgerichts geltenden Vorschriften, also u.a. den §§ 3 bis 9 ZPO, § 48 Abs. 1 S. 1 GKG. Nach § 48 Abs. 2 S. 1 GKG ist in nichtvermögensrechtlichen Streitigkeiten der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen zu bestimmen. Unterschieden wird für die Bewertung zwischen vermögensrechtlichen und nichtvermögensrechtlichen Streitigkeiten. Vermögensrechtliche Streitigkeiten, also solche, die aus einem vermögensrechtlichen Rechtsverhältnis hergeleitet oder jedenfalls auf

eine vermögenswerte Leistung gerichtet sind, werden gem. § 48 Abs. 1 GKG nach den prozessualen Wertvorschriften der §§ 3 bis 9 ZPO bewertet, für nichtvermögensrechtliche Streitigkeiten enthält das GKG eigenständige Wertvorschriften.

Vermögensrechtliche Streitigkeiten sind solche, die sich auf Vermögensrechte beziehen. Auf Vermögenswerte beziehen sich aber nicht nur alle unmittelbar auf eine vermögenswerte Leistung gerichtete Ansprüche (z. B. auf Entschädigung in Geld wegen einer Persönlichkeitsrechtsverletzung), sondern auch aus nicht vermögensrechtlichen Rechtsverhältnissen hergeleitete, nicht auf eine vermögenswerte Leistung (z.B. auf Unterlassung) gerichtete Ansprüche, deren Verfolgung in wesentlicher Weise auch der Wahrung wirtschaftlicher Belange dient (BeckOK KostR/*Toussaint*, 47. Ed. 01.10.2024, GKG § 48 Rn. 18).

Zu den allgemeinen Grundsätzen der Wertberechnung gehört es, für die Bewertung auf das Interesse des jeweiligen Antragstellers – hier des Klägers als „Angreifer“ - abzustellen.

1. Der Streitwert für die Klage auf Auskunft war dabei auf 2.000 EUR festzusetzen.

Üblicherweise wird das Angriffsinteresse des Klägers bei der Auskunftsklage durch den Leistungsanspruch bestimmt, zu dessen Durchsetzung die Auskunft benötigt wird, wobei dann dieser zunächst nach § 3 ZPO zu schätzen ist. Dies geschieht nach objektiven Anhaltspunkten, wobei anhand des Tatsachenvortrags des Klägers danach zu fragen ist, welche Vorstellungen er sich vom Wert des Leistungsanspruchs oder dessen Abwehr bei Klageeinreichung gemacht hat. Zu bewerten ist das Interesse des Klägers unter wirtschaftlichen Gesichtspunkten, wobei auch zu berücksichtigen ist, ob der Leistungsanspruch nach den festgestellten Verhältnissen überhaupt oder allenfalls in geringerer Höhe in Betracht kommt. In einem zweiten Schritt ist eine Quote zu bilden, deren Höhe davon abhängt, inwieweit der Kläger für die Geltendmachung des Leistungsanspruchs auf die begehrte Auskunft angewiesen ist (BeckOK KostR/*Toussaint*, 47. Ed. 01.10.2024, GKG § 48 Rn. 21.2). Der Auskunftsanspruch soll für den Betroffenen Transparenz schaffen und ihm das für die Durchsetzung seines Rechts, selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen zu können, notwendige Wissensfundament an die Hand geben. Der Auskunftsanspruch ist seiner Natur nach ein Instrument zur Durchsetzung der weiteren Betroffenenrechte wie Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) oder Schadensersatz nach Art. 82 DSGVO (VGH Baden-Württemberg, Beschl. v. 30.10.2024, Az. 2 S 560/24, ZGI 2024, 277, Rn. 13, unter Verweis auf BVerwG Urt. v. 16.09.2020, Az. 6 C 10/19 Rn. 19).

Vorliegend geht es dem Kläger jedoch nicht darum, mit der Auskunft eine Leistungsklage vorzubereiten, sondern prioritär darum, Informationen zu erhalten, welche Daten von ihm, auch aus der Privat- und Intimsphäre, die den besonderen Kategorien des Art. 9 Abs. 1 DSGVO unterfallen, beim Aufsuchen von Webseiten und Apps erfasst, weitergeleitet und verwendet wurden, sodann Informationen über Herkunft und Empfänger sowie über Zweck und Umfang der Verarbeitung der Daten zu bekommen. Der Kläger möchte durchsetzen, dass die bisher über die Business Tools erfassten personenbezogenen Daten umfassend beauskunftet werden.

Für die Höhe des Gebührenstreitwerts kommt es nicht auf den quantitativen Umfang der Auskunft an, sondern worüber Auskunft verlangt wird. Hier geht es nicht wie bei den Scraping-Fällen um vom Nutzer selbst eingegebene und übermittelte Daten bei der Registrierung und im persönlichen Profil, sondern um Angaben über das Surfverhalten und Online-Aktivitäten eines Nutzers in erheblichem Umfang. Das Interesse an einer Beauskunftung, mit der in Erfahrung gebracht werden soll, inwieweit persönliche Nutzerdaten erhoben und weitergegeben wurden und werden, kann vorliegend mit 2.000 EUR angesetzt werden, also dem Vierfachen des Gebührenstreitwerts der Auskunftsklagen in den Scraping-Fällen (vgl. beispielhaft OLG Dresden, Beschl. v. 31.07.2023, Az. 4 W 396/23). Auf den Auffangwert des § 52 Abs. 2 GKG soll nach dem OLG Dresden (Urt. v. 26.7.2022, Az. 18 U 24/22) bei einer Klage auf Datenauskunft soll grundsätzlich nicht abgestellt werden, da dieser Wert für Auskunftsansprüche aus reinem Informationsinteresse als deutlich übersetzt anzusehen sei. Dennoch ist es vorliegend nicht gerechtfertigt, lediglich einen Wert i.H.v. 500 EUR anzusetzen, da das Persönlichkeitsrecht des Klägers bei Erfassung seines Surfverhaltens hier stärker beeinträchtigt worden ist und die Auskunft, welche Daten hierbei erhoben, verarbeitet und weitergegeben wurden, eine größere Bedeutung für den Betroffenen hat, als bei einer Auskunft über die persönlichen Daten in den Scraping-Fällen. Dort mag es angemessen eingeordnet sein, den Wert eines im Wege eines Annexantrags geltend gemachten Auskunftsanspruchs im Zusammenhang mit Leistungs- und Unterlassungsanträgen wegen (behaupteter) Rechtsverletzungen durch die Betreiber von sozialen Netzwerken mit nicht mehr als 500 EUR festzusetzen (LG Karlsruhe, Beschl. v. 05.07.2023, Az. 10 W 5/23, ZD 2023, 746 Rn. 10 ebenso etwa LG Bonn, Urt. v. 07.06.2023, Az. 13 O 126/22; LG Bamberg, Urt. v. 06.06.2023, Az. 42 O 782/22).

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

3. In Bezug auf den Antrag gerichtet auf Zahlung eines Schadensersatzanspruchs war der Gebührenstreitwert daran zu bemessen, welcher Betrag unter Zugrundelegung des klägerischen Tatsachenvortrags angemessen erscheint (Anders/Gehle/Gehle, 83. Aufl. 2025, ZPO Anh. § 3 Rn. 99). Insoweit wird auf die obigen Ausführungen des Gerichts zur Begründetheit der Klage verwiesen.

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

Rechtsbehelfsbelehrung:

Gegen die Festsetzung des Streitwertes findet die **Beschwerde** statt, wenn der Wert des Beschwerdegegenstands 200 EUR übersteigt oder wenn die Beschwerde in dieser Entscheidung zugelassen wurde.

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

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

Die Beschwerde ist bei dem

Landgericht Leipzig
Harkortstraße 9
04107 Leipzig

einzulegen.

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

Die Beschwerde kann auch als elektronisches Dokument eingereicht werden. Das elektroni-

sche Dokument muss für die Bearbeitung durch das Gericht gemäß §§ 2 und 5 der Elektronischer-Rechtsverkehr-Verordnung (ERVV) geeignet sein.

Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht. Rechtsbehelfe, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument einzureichen. Das elektronische Dokument muss

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

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

[Redacted Signature]

Richterin am Landgericht

[Redacted Signature]

[Redacted Signature]

Richter

Richterin am Landgericht

verhindert wegen Urlaubs.

[Redacted Signature]