



Landgericht Leipzig

Zivilkammer

Aktenzeichen: **05 O 2351/23**

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

[REDACTED]

- Kläger -

Prozessbevollmächtigte:

BRR Automotive Rechtsanwaltsgesellschaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin,
Gz.: DTS-003033-IUS

gegen

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

- Beklagte -

Prozessbevollmächtigte:

[REDACTED]

wegen Feststellung, Unterlassung und Schadensersatz

hat die 5. Zivilkammer des Landgerichts Leipzig durch

Präsident des Landgerichts [REDACTED]

Richterin am Landgericht [REDACTED]

Richter [REDACTED]

auf Grund der mündlichen Verhandlung vom 20.05.2025 am 04.07.2025

für Recht erkannt:

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks

„Facebook“ unter der E-Mail-Adresse [REDACTED] die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem [REDACTED] nicht gestattet:

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

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

sowie folgende personenbezogene Daten der Klagepartei

b) auf Websites

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

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

c) in mobilen Dritt-Apps

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

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an

ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten gem. des Antrags zu 1. zu verarbeiten.

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 01.09.2023 zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 540,50 EUR freizustellen.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits trägt die Beklagte.

7. Das Urteil ist gegen Sicherheitsleistungen i.H.v. 20.000 EUR vorläufig vollstreckbar.

Beschluss:

Der Streitwert wird auf insgesamt 14.000 EUR festgesetzt.

Tatbestand

Der Kläger begehrt im Zusammenhang mit der Verwendung von sog. Business Tools neben der Feststellung rechtswidriger Datenverarbeitung von der Beklagten Unterlassung und 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 Facebook unter der E-Mail-Adresse [REDACTED]. 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 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 zu Werbezwecken 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 zu Werbezwecken geteilten Informationen über Aktivitäten von dem jeweiligen Facebook-Konto in Bezug auf die Schaltung von personalisierter Werbung trennen lassen und/oder die künftigen Verknüpfungen zwischen dem Facebook-Konto und den von Drittunternehmen geteilten Informationen über Aktivitäten in Bezug auf die Schaltung von personalisierter Werbung ausschalten.

Die Beklagte geriert sich gemäß der von ihr verwendeten Vertragsbedingungen als Inhaberin der Rechte, das Verhalten ihrer Nutzer nicht nur bei Nutzung ihrer eigenen Produkte und Dienstleistungen zu analysieren, sondern darüber hinaus auch auf einer Vielzahl von Websites und Apps. Die Einrichtung eines Kontos im Netzwerk der Beklagten setzt voraus, dass der Nutzer den Nutzungsbedingungen (aktuelle 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 K3, S. 96 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 Werbetreibenden und „Audience Network-Publishern“, 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-
seiten 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 (par-
ship.de, amorelie.de, orion.de, lovescout24.de), sowie Seiten mit Inhalten aus der innersten In-
timosphäre (krebshilfe.de, tfp-fertility.com (Samenbank), nie-wieder-alkohol.de, nvve.nl (Sterbe-
hilfe; 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 persönli-
che und höchstpersönliche Daten zur Gesundheit, zur politischen Einstellung, zur Weltan-
schauung, 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 nachverfolg-
bar. Diese weiß, welche Seiten- und Unterseiten wann besucht wurden, was dort angeklickt,
gesucht oder gekauft wurde (vgl. Beispiele der Seiten niewiederalkohol.de, shop-apothe-
ke.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 Beklagte anhand der im Antrag zu 1 aufgeführten perso-
nenbezogenen 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 Fingerprin-
tings 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-Set-
zung von Drittanbietern stückweise unterbinden und auch die Ausführung von Skriptanwen-
dungen 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 un-
bestrittenen 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, selbständig 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.

Um einen möglichst umfangreichen Datensatz zu erhalten, ermutigt die Beklagte Websitesbetreiber dazu, ihr möglichst viele Informationen der Websitesbesucher zu übermitteln. Die Websitesbetreiber haben ebenfalls ein Interesse daran, der Beklagten alle verfügbaren Informationen über die jeweiligen Nutzer zu übersenden. Denn je mehr Daten der Beklagten zur Verfügung stehen, desto besser gelingt die Kundenakquise. Die Beklagte bewirbt ihr Geschäftsmodell offensiv 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 -verarbei-

tung 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 05.09.2024, Seiten 12 bis 35 Bezug genommen.

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 03.08.2023 machte die Klagepartei Ansprüche auf Auskunft nach Art. 15 DSGVO, Löschung nach Art. 17 DSGVO und Schmerzensgeld vorgerichtlich unter Fristsetzung bis 31.08.2023 gegenüber der Beklagten geltend. 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, die Verarbeitung der über die „Meta Business Tools“ erlangten personenbezogenen Daten durch die Beklagte sei 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 5.000 EUR zu beziffern.

Der Kläger hat mit der Replik vom 05.09.2024 die ursprünglichen Anträge aus der Klageschrift unter Ziff. 1 und 2 abgeändert. Darüber hinaus hatte der Kläger vormals hilfsweise im Wege der Stufenklage beantragt, die Beklagte für den Fall, dass dem Antrag unter Ziff. 1 nicht entsprochen wird, zur Auskunftserteilung über die von ihr verarbeiteten personenbezogenen Da-

ten, zur Löschung nach erfolgter Auskunftserteilung und zum Schadensersatz aufgrund der Verarbeitung der beauskunfteten Daten zu verurteilen. Schließlich hatte der Kläger hilfsweise beantragt, die Beklagte auch für den Fall, dass dem Antrag unter Ziff. 1 und 3 entsprochen wird, zur Löschung bzw. Anonymisierung sämtlicher unter Antrag Ziff. 1 genannter Daten zu verurteilen.

Der Kläger beantragt zuletzt:

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks

„Facebook“ unter der E-Mail-Adresse [REDACTED] die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem [REDACTED] nicht gestattet:

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

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

sowie folgende personenbezogene Daten der Klagepartei

b) auf Websites

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

c) in mobilen Dritt-Apps

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

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an

ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und –Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten gem. des Antrags zu 1. zu verarbeiten.

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 5.000,00 EUR beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinsatz seit dem 01.09.2023, zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 1.054,10 EUR freizustellen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte meint, die Datenerhebung auf Drittwebsites- und Apps sei rechtmäßig. Sie benötige insofern keine Rechtsgrundlage. Vielmehr 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.

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 solche 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 einfache 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 überwiegend Erfolg.

I. Die Klage ist vollumfänglich zulässig.

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

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

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

bb) Die Beklagte ist nach dem tatsächlichen Vortrag der Klägerseite ebenfalls Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die streitgegenständlichen Business Tools. Insoweit wird auf die zutreffenden Ausführungen des LG Stuttgart verwiesen (Urt. v. 24.10.2024, Az. 12 O 170/23,

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

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

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

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

3. Soweit die Anträge aus der Klageschrift vom 10.10.2023 mit der Replik vom 05.09.2024 teil-

weise geändert wurden, ist dies zulässig.

a) 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 ZPO § 264 Rn. 6 unter dem Stichwort eines „*unzutreffend formulierten Klageantrags*“, siehe auch OLG Dresden, Urt. v. 1. 12. 2010, Az. 1 U 475/10, NJW-RR 2011, 924, 927).

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

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

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

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

Die aus dem in der Klage vorgetragenen Sachverhalt abgeleitete rechtliche Beziehung ist die Beziehung zwischen dem Kläger und der Beklagten, welche sich aus dem Nutzungsvertrag

bei der Nutzung des Netzwerks "Facebook" unter der E-Mail-Adresse [REDACTED] ergibt. Insoweit erstreckt sich der Feststellungsantrag auf die Frage, ob es der Beklagten anhand der Ausgestaltung dieses Vertrags – in den AGB – gestattet ist, die im Antrag unter Ziff. 1 genannten personenbezogenen Daten seit dem [REDACTED] zu verarbeiten.

In diesem Zusammenhang nicht erforderlich war es für den Kläger vorzutragen, welche Daten konkret gespeichert wurden. Es reichte aus, für die Datenkategorien Sammelbezeichnungen zu verwenden. Dies folgt daraus, dass eine nähere Bestimmung der einzelnen Datensätze der Klägerseite aufgrund des fehlenden Vortrags der Beklagten im Rahmen ihrer sekundären Darlegungslast bis zuletzt nicht erfolgt ist. Da der Kläger selbst keinen Einblick in die von der Beklagten verarbeiteten Daten hat, muss es ihm zur Gewährung eines effektiven Rechtsschutzes prozessual gestattet sein, seinen Vortrag auf die ihm bekannten Umstände zu beschränken. Diesem Erfordernis wurde durch die Aufzählung der einzelnen Datenkategorien hinreichend Rechnung getragen.

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

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

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

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

Es kann insoweit eine Parallele zur zulässigen Feststellung einer Schadensersatzpflicht „dem Grunde nach“ bei nicht abgeschlossenen Schadensentwicklungen gezogen werden. In diesen Fällen reicht bereits die entfernte Möglichkeit, dass weitere Folgeschäden aus demselben (abgeschlossenen) haftungsbegründenden Ereignis zu erwarten sind, aus, um ein Feststellungsinteresse zu begründen (BGH, Urt. v. 15.7. 1997, Az. VI ZR 184/96, NJW 1998, 160). Der Sachvortrag zur Wahrscheinlichkeit gehört dabei zur materiellen Klagebegründung (Thomas/Putzo/Seiler, § 256 ZPO, Rn. 14). Dies muss erst recht im hier vorliegenden Fall gelten, bei dem das haftungsbegründende Verhalten noch nicht abgeschlossen ist, sondern weiter fort dauert, indem die streitgegenständliche Datenverarbeitung weiter stattfindet. Kann in einem Schadensersatzprozess zulässigerweise die Feststellung begehrt werden, dass die Beklagtenseite verpflichtet ist, sämtliche materiellen und immateriellen Schäden aus einem bestimmten (Unfall-)Ereignis auszugleichen, so ist die hier vorliegende Feststellungsklage das Pendant hierzu. Bei der Feststellung der Schadensersatzverpflichtung ist das haftungsbegründende Ereignis abgeschlossen und liegt vollständig in der Vergangenheit; anders im hier vorliegenden Fall: die Schadenszufügung hat noch kein Ende gefunden. Dem Kläger verbleibt in dieser Konstellation nur die Möglichkeit, feststellen zu lassen, dass der Nutzungsvertrag die Form der Datenerhebung, deren Zulässigkeit sich aber die Beklagte berührt, nicht erlaubt ist.

Aus Sicht des Gerichts ist es im hiesigen Fall nach dem Sachvortrag der Klägerseite wahrscheinlich, dass dem Kläger weitere Ansprüche wegen der streitgegenständlichen Datenverarbeitung bereits jetzt zustehen oder zustehen werden. Da der Kläger gegenwärtig noch nicht alle bisherigen und künftigen Datenschutzverstöße und deren konkrete Handlungsformen benennen kann, wäre er bei der Ablehnung eines Feststellungsinteresses gezwungen, für jeden weiteren klageweise geltend gemachten Anspruch, der seinen Ursprung in der hier streitgegenständlichen Datenverarbeitung hat, die Rechtswidrigkeit der Datenverarbeitung erneut darzulegen und ggfs. zu beweisen. Insofern wäre er einem erheblichen Prozessrisiko ausgesetzt. Es würde zudem eine Mehrbelastung der Gerichte bedeuten. Dies kann durch eine vorgreifliche Feststellungsklage – und allein durch diese – verhindert werden. Der Kläger befürchtet nach seinem Sachvortrag, dass die Beklagte die von ihr gesammelten Daten an Dritte weitergibt oder bereits weitergegeben hat (siehe nur Klageschrift, S. 12 f., Bl. 12 f. d. Akte) und sie somit weitere potenziell rechtswidrige Handlungen verübt. Diese Befürchtungen hat die Beklagte nicht ausgeräumt. Insbesondere hat sie durch ihre fehlende prozessuale Erklärung zu den klägerischen Behauptungen zur Überzeugung des Gerichts zu erkennen gegeben, dass sie trotz prozessualer Wahrheitspflicht einen intransparenten Umgang mit Nutzerdaten auch gegenüber dem Gericht praktiziert. Schließlich ist es dem Kläger unbenommen, auch in Zukunft einen weiteren immateriellen Schaden, der aus der fortdauernden Rechtsverletzung resultiert, geltend zu machen. Der Unterlassungstitel bietet insoweit lediglich die Möglichkeit, als Grundlage zur Festsetzung von Ordnungsmitteln gem. § 890 ZPO herangezogen zu werden. Er ist jedoch gerade keine Grundlage für weitere Schadensersatzansprüche und damit nicht äquivalent.

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

Die Beklagte berührt sich bis zuletzt auch prozessual mit der Aussage, die Datenverarbeitung, so wie sie im Antrag unter Ziff. 1 dargestellt wird, werde von ihr nicht vorgenommen, da der Kläger eine Einwilligung in die Datenverarbeitung nicht abgegeben habe. Darüber hinaus erklärt sie jedoch im Widerspruch zu der ersten Aussage, dass sie personenbezogene Daten, welche sie von Drittunternehmen über die Business Tools erhalten hat, zu anderen Zwecken rechtmäßig verarbeitet (siehe zuletzt Schriftsatz vom 09.05.2025, S. 12 = Bl. 973 d. Akte). Die Beklagte setzt demnach das von der Klägerseite zur rechtlichen Prüfung vorgelegte Verhalten bewusst oder unbewusst fort. Insofern bedarf es einer gerichtlichen Klärung.

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

b) Der Feststellungsantrag ist hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO. Soweit die Beklagte meint, dass der Kläger konkret vortragen müsse, welche Websites und Apps Dritter die Business Tools nutzen, kann dies nicht überzeugen. Der Kläger hat mit der Anlage „Liste häufig besuchter Websites in Deutschland mit Meta Pixel“ (Bl. 201 d. klägerischen Anlagenhefts) hinreichend dargelegt, dass die Vielzahl der von einem nicht näher bestimmten Internetnutzer regelmäßig aufgerufenen Websites die Business Tools der Beklagten nutzt. Bei der Liste der Websites handelt es sich um einen Querschnitt von Websites, von denen ein Internetnutzer im Regelfall mindestens eine Seite pro Tag aufruft. Die Websites bilden sämtliche Kategorien der Internetnutzung ab (Nachrichten, Politik, Gesundheit, Sexualität, Religion, Finanzen usw.). Es kann nach allgemeiner Lebenserfahrung unterstellt werden, dass Internetnutzer Websites aus der dargelegten Liste aufrufen. Würde das Gericht im Rahmen der Darlegungslast dem Kläger abverlangen, dass er jede von ihm besuchte Website der letzten Jahre im Sinne eines Browserverlaufs offenlegen müsste, würde der Sinn einer auf die Verletzung von Datenschutzvorschriften gestützten Klage ad absurdum geführt werden, da es gerade das klägerische Ziel ist, die Erhebung von personenbezogenen Daten durch die Beklagte zu verhindern, und damit auch Informationen über den eigenen Browserverlauf – soweit nur der Beklagten bekannt – vor anderen geheim zu halten.

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

4. Auch der Unterlassungsantrag ist zulässig. Dem Kläger stehen keine einfacheren Mittel zur Verfügung, die streitgegenständliche Datenverarbeitung zu verhindern. Soweit die Beklagte in ihren Einstellungen ermöglicht, dass eine Trennung der Schnittstelle zwischen den Business Tools und dem Nutzerkonto des Klägers möglich ist, beschränkt sich dies allein auf die Zwecke der Bereitstellung personalisierter Werbung. Stets beziehen sich die Ausführungen der Beklagten auf die "streitgegenständliche Datenverarbeitung", wobei sie diese abweichend von dem gerichtlich festgelegten Streitgegenstand der Datenverarbeitung durch die Business

Tools im Allgemeinen nur auf die Datenverarbeitung zu Werbezwecken beschränkt (siehe hierzu insbesondere Klageerwiderung vom 23.05.2025, S. 19, Bl. 291 d. Akte). Die Beklagte spricht deshalb in diesem Zusammenhang von durch "Werbepartner[n] bereitgestellte Informationen" (Klageerwiderung vom 23.05.2025, S. 22, Bl. 294 d. Akte). Darüber hinaus findet die Datenverarbeitung weiterhin dauerhaft unstreitig zu Integritäts- und Sicherheitszwecken statt. Zudem ist unstreitig, dass die Datenerhebung und -verarbeitung innerhalb der Business Tools und die Weiterleitung der Daten an die Beklagte in jedem Fall praktiziert wird.

II. Die Klage ist überwiegend begründet.

1. Der Feststellungsantrag hat in der Sache Erfolg.

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

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

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

In seiner Entscheidung vom 4.7.2023 hat der EuGH (a.a.O. = NJW 2023, 2997) die Anforderung

rungen an die Rechtfertigung einer Datenverarbeitung nach den o.g. Vorschriften präzisiert. Er führt wie folgt aus:

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

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

6. Art. 6 I UAbs. 1 Buchst. c der VO (EU) 2016/679 ist dahin auszulegen,

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

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

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

„Desgleichen wird das vorlegende Gericht nach Maßgabe von Art. 6 Abs. 1 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 erhoben 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 26.11.2024, S. 48, Bl. 522 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. 4.10.2024, Az. C-446/21, NJW 2025, 207 Rn. 55). In Artikel 5 Abs. 1 DSGVO ist unter anderem der Grundsatz der Datenminimierung (lit. c) verankert, der bestimmt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (EuGH, a.a.O, NJW 2023, 2997).

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).

2. Der Kläger hat einen Unterlassungsanspruch aus Art. 17 DSGVO i.V.m. Art. 79 DSGVO. Obwohl die Vorschrift dem Wortlaut nach lediglich ein Recht auf Löschung beinhaltet, kann der Kläger aus Art. 17 DSGVO i.V.m. Art. 79 DSGVO auch einen Unterlassungsanspruch herleiten. *"Aus der Verpflichtung zur Löschung von Daten ergibt sich implizit zugleich die Verpflichtung, diese Daten künftig nicht wieder zu speichern."* (LG Berlin II, Urt. v. 11.04.2025, Az. 58 O 72/24, S. 8, amtlicher Ausdruck, mitgeteilt durch die Klägerseite; einen Unterlassungsanspruch aus Art. 17 DSGVO ebenfalls herleitend OLG Düsseldorf, Urt. v. 05.10.2023, 16 U 127/22, GRUR-RS 2023, 28156 und BeckOK DatenschutzR/Worms, 52. Ed. 1.11.2024, DS-GVO Art. 17 Rn. 77a). Materielle Voraussetzung des Anspruchs ist die konkrete Gefahr einer rechtswidrigen Verarbeitung personenbezogener Daten.

a) 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 Funktionswei-

se der Business Tools, der Übertragung der personenbezogenen Daten und der Erstellung von Nutzerprofilen – dem Urteil als unstreitig zugrunde zu legen. Die Beklagte ist dem klägerischen Vortrag in nicht erheblicher Weise entgegengetreten. Der Vortrag der Beklagten 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 handele, die nach der Eigenart des Internets stets erhoben und verarbeitet werden, kann dies nicht verfangen. Auch diese Daten fallen unter den Anwendungsbereich der DSGVO. Der Verordnungsgesetzgeber war sich dessen bewusst und stellte in Erwägungsgrund 30 fest, dass natürlichen Personen unter Umständen Online-Kennungen wie IP-Adressen, Cookie-Kennungen oder andere Identifikatoren zugeordnet werden können, die mit ihrem Gerät, Softwareanwendungen, Tools oder Protokollen zusammenhängen. Im Übrigen geht die Datenverarbeitung der Beklagten über diese technischen Standarddaten weit hinaus.

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

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

d) Die Androhung des Ordnungsmittels beruht auf § 890 Abs. 2 ZPO. Der Rückgriff auf die na-

tionale Vorschrift ist erforderlich, da die DSGVO mit der Sanktionsnorm in Art. 83 DSGVO keine äquivalente Regelung bereithält, die gleichermaßen geeignet ist, den Unterlassungstitel zur Gewährung effektiven Rechtsschutzes durchzusetzen (so auch LG Landau, Versäumnisurteil vom 26.02.2024, Az. 2 O 239/23, S. 13, amtlicher Ausdruck, mitgeteilt durch die Klägerseite).

3. 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. 4.5.2023, 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 un-

terschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche 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 Schadensbemessung berücksichtigt werden. Im Gegenzug gibt der EuGH den nationalen Gerichten jedoch vor, dass die Höhe des geschuldeten immateriellen Schadensersatzes „seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung“ (zum Ganzen EuGH, Ur. v. 20.6.2024, 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. Döhmman*, 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. 2.5.2022, 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 Zugschnitt 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 Wer-

bung 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. 4.10.2024, 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. 27.9.2017, 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. 4. 2004, Az. C-456/01 P und C-457/01 P, GRUR Int 2004, 631, Rn. 35; Urt. v. 8.10.2020, 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 Scra-

ping-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, Urt. 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. 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). Auch wenn der Nutzer 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 03.08.2023 (Anl. K 3) befand sich die Beklagte in Verzug, sodass Zinsen ab dem 01.09.2023 zu zahlen sind.

4. Der Kläger kann von der Beklagten teilweise Freistellung seiner vorgerichtlichen Rechtsanwaltskosten i.H.v. 540,50 EUR verlangen, Art. 82 Abs. 1 DS-GVO, §§ 249 Abs. 1, 257 S. 1 BGB.

Der Schadensersatzanspruch nach Art. 82 DSGVO umfasst 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.

Zu berücksichtigen war jedoch, dass die außergerichtlichen Kosten allein auf der Grundlage des Streitwerts des Schadensersatzanspruchs i.H.v. 5.000 EUR bemessen werden können. Für die weiteren Ansprüche käme lediglich ein Verzugsschadensersatzanspruch (§§ 280 Abs. 1 und 2, 286 BGB) in Betracht. Die hier geltend gemachten Kosten der Erstmahnung sind jedoch insoweit nicht ersatzfähig (siehe nur BGH, Urt. v. 12.5.2016, Az. IX ZR 208/15, NJW-RR 2017, 124 Rn. 20). Entgegen der Rechtsauffassung des Klägers war die Beklagte auch nicht vorher in Verzug geraten.

Ausgehend davon belaufen sich die ersatzfähigen außergerichtlichen Kosten auf 540,50 EUR. Nach § 60 Abs. 1 RVG ist für die Vergütung das bisherige, bis zum 31.5.2025 geltende Gebührenrecht anzuwenden, wenn der unbedingte Auftrag zur Erledigung derselben Angelegenheit i.S.d. § 15 RVG vor dem Inkrafttreten einer Gesetzesänderung, d.h. vor dem 1.6.2025 erteilt worden ist.

III. Die Kostenentscheidung beruht auf § 92 Abs. 2 Nr. 1 ZPO. Der Kläger unterliegt lediglich

mit einem Teilbetrag der eingeklagten außergerichtlichen Kosten. Dieser Betrag ist jedenfalls als Unterliegen mit weniger als zehn Prozent anzusetzen (vgl. OLG Köln, Urt. v. 2.9.2022, Az. 20 U 266/21 NJOZ 2022, 1325 Rn. 56). Nichts Anderes ergibt sich aus der Regelung in § 45 Abs. 1 S. 2 GKG hinsichtlich der vor der Entscheidung des Gerichts zurückgenommenen Hilfsansprüche.

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

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 insgesamt 14.000 EUR festgesetzt und setzt sich wie folgt zusammen:

- Unterlassung: 4.000 EUR
- Feststellung: 5.000 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. 1.10.2024, 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 Feststellung war auf 4.000 EUR festzusetzen.

Den Antrag auf Unterlassung mit einem Streitwert für die Gebühren an Hand eines Auffangwertes festzusetzen, ist auch im Rahmen der Festsetzung nach § 48 Abs. 2 GKG vom Ansatz her sachgerecht.

Da auch § 48 Abs. 2 GKG die Bewertung in das (freie) Ermessen des Gerichts stellt, besteht im Ergebnis kein Unterschied zur prozessualen Auffangvorschrift des § 3 ZPO (BeckOK *KostR/Toussaint*, 47. Ed. 1.10.2024, GKG § 48 Rn. 36). Dies führt dazu, dass für nichtvermögensrechtliche Streitigkeiten auch im Prozessrecht, wenn es also um den Zuständigkeits- oder Beschwerdewert geht, auf die Kriterien des § 48 Abs. 2 GKG zurückgegriffen wird (BeckOK *KostR/Toussaint*, 47. Ed. 1.10.2024, GKG § 48 Rn. 37). Vielfach wird daher vorgeschlagen, auf den anwaltsgebührenrechtlichen Auffangwert des § 23 Abs. 3 Satz 2 RVG – 5.000 EUR – zurückzugreifen und diesen im Ergebnis zum Regelstreitwert für nichtvermögensrechtliche Streitigkeiten zu machen. Von dieser Grundlage geht auch das Oberlandesgericht Dresden bei der Festsetzung des Streitwerts bei Unterlassungsbegehren in Bezug auf Daten aus, meint jedoch, da der Auffangwert nach Maßgabe des Einzelfalles zu erhöhen oder zu vermindern ist, in den Scraping-Fällen den Streitwert auf 3.500 EUR herabsetzen zu müssen (OLG Dresden, Beschl. v. 31.7.2023 – 4 W 396/23, BeckRS 2023, 21123 Rn. 10).

Bei der Bemessung des Wertes in den Scraping-Fällen hat das Oberlandesgericht Dresden berücksichtigt, dass die Sicherung der Daten, die im Internet eine weite Verbreitung finden, für den Kläger eine Bedeutung hat. Andererseits ist aber bei der Schwere der Beeinträchtigung in Blick zu nehmen, dass es sich um Daten aus der Sozialsphäre gehandelt und er bestimmte Daten in Kenntnis der öffentlichen Zugänglichkeit preisgegeben hat. Er kann das soziale Netzwerk der Beklagten nicht ohne Mitteilung von bestimmten Daten nutzen, die für alle Nutzer des Internets zugänglich sind – wie Name, Geschlecht und Nutzer-ID – und er hat dies in Kauf genommen. Bei der (geringeren) Schwere des Vorwurfes wurde vom Oberlandesgericht Dresden in den Scraping-Fällen für die Herabsetzung des Streitwertes berücksichtigt, dass die Beklagte nicht durch aktives Tun die Daten in unzulässiger Weise verarbeitet hat, sondern vielmehr die von den Nutzern öffentlich gestellten Daten von Dritten in unzulässiger Weise mittels automatisierter Verfahren massenhaft abgeschöpft wurden und der Vorwurf des Klägers dahin

zielt, dass die Beklagte keine Vorsorge dagegen getroffen hat.

Noch darunter hat der Bundesgerichtshof den Wert der Unterlassungsanträge in den Scraping-Fällen auf insgesamt 1.500 EUR festgesetzt (BGH, Beschl. v. 10.12.2024, Az. VI ZR 7/24, GRUR-RS 2024, 37952 Rn. 15).

Der BGH hat bei der Festsetzung des Streitwertes für Unterlassungsanträge in den Scraping-Fällen folgende Maßstäbe vorangestellt: Maßgeblich bei einem Unterlassungsantrag nach bereits erfolgter Verletzungshandlung ist das Interesse des Anspruchstellers an der Unterbindung weiterer gleichartiger Verstöße, welches maßgeblich durch die Art des Verstoßes, insbesondere nach seiner Gefährlichkeit und Schädlichkeit für den Inhaber des verletzten Rechts, bestimmt wird. Allerdings kann auch anderen, von der bereits erfolgten Verletzungshandlung unabhängigen Faktoren – etwa dem Grad der Wahrscheinlichkeit künftiger Zuwiderhandlungen – Rechnung zu tragen sein (vgl. BGH, Urt. v. 12.05.2016, Az. I ZR 1/15, NJW 2017, 814 Rn. 33 ff. m.w.N). Das Gefährdungspotential ist dabei allein mit Blick auf das konkrete Streitverhältnis zu bestimmen. Für generalpräventive Erwägungen ist bei der Bewertung eines zivilrechtlichen Unterlassungsanspruchs ebenso wenig Raum (BGH, a.a.O., NJW 2017, 814 Rn. 42 m.w.N) wie für eine Orientierung an einem etwaigen (Gesamt-)Schaden unter Einbeziehung anderer Betroffener (vgl. BGH, Beschl. v. 30.11.2004, Az. VI ZR 65/04, juris, Rn. 2; OLG Hamm, Urt. v. 15. August 2023, Az. 7 U 19/23, juris, Rn. 277). Schließlich darf das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (BGH, Beschl. v. 26.11.2020, Az. III ZR 124/20, K&R 2021, 127 Rn. 11, zusammenfassend BGH, Beschl. v. 10.12.2024, Az. VI ZR 7/24, GRUR-RS 2024, 37952 Rn. 14).

Für die Festsetzung im konkreten Fall führt der BGH aus: *„Der Kläger selbst hat seinen Zahlungsanspruch auf Ersatz des bereits eingetretenen Schadens auf 1.000 EUR beziffert. Der Senat hat hierzu in einem weiteren Parallelverfahren näher ausgeführt, dass er auch eine Bemessung in der Größenordnung von 100 EUR für den bloßen Kontrollverlust von Rechts wegen nicht beanstanden würde (Urteil vom 18. November 2024 – VI ZR 10/24, juris Rn. 100). Seinen Antrag auf Feststellung hinsichtlich etwaiger zukünftiger Schäden hat auch der Kläger mit 500 EUR bewertet; dies erscheint angesichts der absehbaren Schwierigkeiten beim Nachweis der Ursächlichkeit künftiger Schäden auch sachgerecht. Die Verletzungshandlung liegt bereits fünf Jahre zurück, ohne dass es bislang jenseits des bloßen Kontrollverlustes zum Eintritt nachweisbarer Schäden oder einer weiteren Verletzungshandlung gekommen wäre; die Beklagte hat die Suchbarkeitsfunktion in der dem Streitfall inmitten stehenden Ausgestaltung viel-*

mehr zwischenzeitlich deaktiviert. Beide Unterlassungsanträge nehmen ihren Ausgangspunkt in derselben Verletzungshandlung und hängen in der Sache eng zusammen.“ (BGH, a.a.O., Rn. 15).

Der vorliegende Sachverhalt ist nach den Behauptungen und der Darstellung des Klägers, die für die Wertfestsetzung maßgebend sind, vollständig anders gelagert. Vorliegend möchte der Kläger unterbinden, dass die Beklagte sein Nutzungsverhalten als Teil seines Privatlebens nicht weiter überwacht und die Ergebnisse der Überwachung wirtschaftlich verwertet, in dem sie an Dritte für den Nutzer des Netzwerks der Beklagten nicht mehr kontrollierbar weitergegeben werden. Insoweit von einem Auffangstreitwert von 5.000 EUR auszugehen und entsprechend den bisher erfolgten Streitwertangaben der Prozessbevollmächtigten in einer Vielzahl von Fällen von einem auf 4.000 EUR abgesenktem Streitwert auszugehen, ist sachgerecht.

Es bestehen noch keine ausreichenden Anhaltspunkte dafür, dass das Interesse eines Anspruchstellers an der Unterbindung weiterer gleichartiger Verstöße der Beklagten geringer ausfallen würde, wenn er die Verfahrenskosten selbst zu tragen hätte, und er diese nicht von einer Rechtsschutzversicherung getragen bekommt – auch wenn ggf. die überwiegend bei den bundesdeutschen Gerichten anhängigen Verfahren gegen die Beklagte im Zusammenhang mit Verstößen gegen die DSGVO von einem Rechtsschutzversicherer finanziert werden. Insoweit kann auch nicht darauf abgestellt werden, dass derjenige, der die Kosten eines auf Unterlassung gerichteten Verfahrens zu tragen hat, das Interesse an der Unterlassung – realistischer – mit einem weitaus geringeren Betrag beziffern würde.

2. Der Streitwert für den Antrag auf Feststellung war auf 5.000 EUR festzusetzen. Unter Berücksichtigung der Ausführungen unter Ziff. 1 und der Ausführungen zur Zulässigkeit der Feststellungsklage ist bei diesem Antrag von einem Mehr an Rechtsschutzinteresse im Vergleich zur Unterlassungsklage auszugehen, da sich die Feststellung sowohl auf die Zukunft als auch die Vergangenheit erstreckt und eine Vielzahl von möglichen weiteren Ansprüchen gegen die Beklagte vorbereiten kann. Das Gericht erachtet es deshalb für sachgerecht, in diesem Fall den Regelstreitwert ohne Abzug anzusetzen.

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.

5. Die zwischenzeitlich fallengelassenen Hilfsanträge sind gemäß § 45 Abs. 1 S. 2 GKG ebenfalls nicht zu berücksichtigen.

Rechtsbehelfsbelehrung:

Gegen die Festsetzung des Streitwertes findet die **Beschwerde** statt, wenn der Wert des Beschwerdegegenstands 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 elektronische Dokument muss für die Bearbeitung durch das Gericht gemäß §§ 2 und 5 der Elektronischer-Rechtsverkehr-Verordnung (ERVV) geeignet sein.

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

1. mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein und gemäß § 4 ERVV übermittelt werden, wobei mehrere elektronische Dokumente nicht mit einer gemeinsamen qualifizierten elektronischen Signatur übermittelt werden dürfen, oder
2. von der verantwortenden Person signiert und auf einem der sicheren Übermittlungswege,

die in § 130a Abs. 4 der Zivilprozessordnung abschließend aufgeführt sind, eingereicht werden.

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



Präsident des Landgerichts



Richterin am Landgericht



Richter