

Landgericht Augsburg

Az.: 082 O 262/24



IM NAMEN DES VOLKES

In dem Rechtsstreit

[REDACTED]

- Klägerin -

Prozessbevollmächtigte:

Rechtsanwälte **BRR Automotive Rechtsanwaltsgesellschaft mbH**, Viktoria-Luise-Platz 7,
10777 Berlin, Gz.: DTS-000453-23

gegen

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

- Beklagte -

Prozessbevollmächtigte:

[REDACTED]

wegen Datenverarbeitung

erlässt das Landgericht Augsburg - 8. Zivilkammer - durch die Richterin am Landgericht [REDACTED]
als Einzelrichterin am 28.03.2025 aufgrund der mündlichen Verhandlung vom 13.01.2025 folgen-
des

Endurteil

1. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, zu unterlassen, auf Dritt-Webseiten und -Apps außerhalb des sozialen Netzwerks „Instagram“ der Beklagten folgende personenbezogene Daten der Klägerin mit Hilfe von Business Tools zu erheben, an

die Server der Beklagten weiterzugeben, die Daten auf den Servern der Beklagten zu speichern und anschließend zu verwenden:

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

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

sowie folgende personenbezogene Daten der Klägerin

b) auf Webseiten

- die URLs der Webseiten samt ihrer Unterseiten
- der Zeitpunkt des Besuchs
- der „Referrer“ (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),
- die von der Klägerin auf der Webseite angeklickten Buttons

sowie

- weitere von der Beklagten „Events“ genannte Daten, die die Interaktionen der Klägerin auf der jeweiligen Webseite dokumentieren

c) in mobilen Dritt -Apps

- der Name der App sowie
- der Zeitpunkt des Besuchs

- die von der Klägerin in der App angeklickten Buttons sowie
 - die von der Beklagten „Events“ genannte Daten, die die Interaktionen der Klägerin in der jeweiligen App dokumentieren.
2. Die Beklagte wird verurteilt, bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, die über die aktuelle Speicherung hinausgehende Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO der unter 1. a), b) und c) aufgeführten, seit dem 25.05.2018 von der Beklagten verarbeiteten personenbezogenen Daten bis zur Erfüllung des Löschungs- bzw. Anonymisierungsanspruchs gemäß Ziffer 3. zu unterlassen, insbesondere diese Daten nicht an Dritte zu übermitteln.
 3. Die Beklagte wird verurteilt, sämtliche seit dem 25.05.2018 bei der Beklagten gespeicherten personenbezogenen Daten gemäß Ziffer 1. a) einen Monat nach rechtskräftigem Abschluss des Verfahrens vollständig zu löschen und der Klägerin die Löschung zu bestätigen sowie sämtliche seit dem 25.05.2018 bei der Beklagten gespeicherten personenbezogenen Daten gemäß Ziffer 1. b) und c) einen Monat nach rechtskräftigem Abschluss des Verfahrens vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.
 4. Die Beklagte wird verurteilt, an die Klägerin 5.000,00 € nebst Zinsen hieraus in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 03.05.2024 zu zahlen.
 5. Die Beklagte wird verurteilt, die Klägerin von vorgerichtlichen Rechtsanwaltskosten ihrer Prozessbevollmächtigten in Höhe von 627,13 € freizustellen.
 6. Im Übrigen wird die Klage abgewiesen.
 7. Von den Kosten des Rechtsstreits haben die Klägerin 6 % und die Beklagte 94 % zu tragen.
 8. Das Urteil ist vorläufig vollstreckbar, für die Klägerin jedoch nur gegen Sicherheitsleistung in Höhe von 8.000,00 €. Die Klägerin kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in gleicher Höhe leistet.

Beschluss

Der Streitwert wird auf 8.000,00 € festgesetzt.

Tatbestand

Die Klägerin verfolgt datenschutzrechtliche Ansprüche.

Die Klägerin nutzt seit dem 22.10.2017 privat das von der Beklagten betriebene soziale Netzwerk „Instagram“ unter dem Benutzernamen „[REDACTED]“. Die Nutzung kostet kein Geld. Die Beklagte generiert Umsatz, indem sie Werbetreibenden die Möglichkeit bietet, gegen Entgelt Anzeigen für ein Publikum auf Instagram zu präsentieren. Dem Nutzer wird bei Nutzung des Netzwerks personalisierte Werbung angezeigt, die auf seinen Interessen basiert, welche die Algorithmen der Beklagten u.a. aus den bei der Registrierung angegebenen Daten (Benutzername, E-Mail-Adresse, Telefonnummer, Alter, Interessen, Hobbies), den Aktivitäten des Nutzers auf Instagram und seinen dort gepflegten sozialen Kontakten („On-Platform“-Daten) extrahieren. Dies wird von der Klägerin nicht beanstandet.

Die Beklagte hat verschiedene sog. „Business Tools“ entwickelt, die von den jeweiligen Betreibern auf Dritt-Webseiten und -Apps eingebunden werden und unter deren Nutzung ebenfalls Daten der Nutzer an die Beklagte versendet werden („Off-site“-Daten):

1. „Meta Pixel“ für Webseiten und „App Events über Facebook-SDK“ für Apps: Einfügen eines einfachen Skripts im Code der Webseiten und Apps. Dies wird vom technisch durchschnittlich versierten Nutzer nicht bemerkt. Der Code kann bei Unterbinden der Cookie-Setzung oder Nutzung des Inkognito-Modus unterbunden oder erschwert werden. Er lief im Zeitpunkt der Klageerhebung nach Recherchen der Prozessbevollmächtigten des Klägers beispielsweise auf großen Nachrichtenseiten und -Apps (z.B. [spiegel.de](https://www.spiegel.de), [bild.de](https://www.bild.de), [welt.de](https://www.welt.de), [faz.net](https://www.faz.net), [stern.de](https://www.stern.de)), großen Reiseseiten und -Apps (z.B. [tripadvisor.de](https://www.tripadvisor.de), [hrs.de](https://www.hrs.de), [holidaycheck.de](https://www.holidaycheck.de), [kayak.de](https://www.kayak.de), [momondo.de](https://www.momondo.de)), Seiten und Apps, die medizinische Hilfe bieten (z.B. [apotheken.de](https://www.apotheken.de), [shop-apotheke.de](https://www.shop-apotheke.de), [docmorris.de](https://www.docmorris.de), [aerzte.de](https://www.aerzte.de), [helios-gesundheit.de](https://www.helios-gesundheit.de), [jameda.de](https://www.jameda.de)), Dating- und Erotikseiten ([parship.de](https://www.parship.de), [amorelie.de](https://www.amorelie.de), [orion.de](https://www.orion.de), [lovescout24.de](https://www.lovescout24.de)), Seiten mit Inhalten aus der innersten Intimsphäre ([krebshilfe.de](https://www.krebshilfe.de), [tfp-fertility.com](https://www.tfp-fertility.com) [Sa-

menbank], nie-wieder-alkohol.de, nvve.nl [Sterbehilfe in den Niederlanden]). Welche Webseiten in der Vergangenheit den „Meta Pixel“ genutzt haben, kann vom Kläger und seinen Prozessbevollmächtigten nicht nachvollzogen werden.

2. Seit 2021 „Conversions API“ für Webseiten und „App Events API“ für Apps: Einbindung eines Skripts auf den Servern der Webseiten- und App-Betreiber. Dadurch erfolgt die Erfassung der Daten nicht mehr auf dem Rechner des Nutzers und kann auch vom technisch versierten Nutzer nicht bemerkt oder abgeschaltet werden. Er kann auch durch Nichtzulassen von Cookies, Nutzen des Inkognito-Modus oder eines VPN nicht umgangen werden. Welche Webseiten und Apps diese Tools nutzen, kann vom Kläger und seinen Prozessbevollmächtigten nicht nachvollzogen werden.

Die Beklagte gibt in einem Performance Leitfaden auf Seite 23 an: „Die Conversions API ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben.“ In der Fußnote 12 wird ausgeführt: „Opt-Out Nutzer*innen sind Personen, die der Tracking-Einwilligung von Facebook/Instagram auf Mobilgeräten ab iOS 14.5 nicht zugestimmt haben.“

Diese Art von Tools, die von vielen Unternehmen angeboten werden, werden durch Millionen von größeren und kleineren Organisationen auf der ganzen Welt genutzt, um z.B. ihre Reichweite zu verbessern, Menschen zu erreichen, die ihre Produkte oder Dienstleistungen nutzen oder sich dafür interessieren könnten und um die Effektivität ihrer Werbekampagnen zu analysieren. Die Verwendung dieser Technologien ist im Zeitalter des heutigen Internet allgegenwärtig und integraler Bestandteil der alltäglichen Internetnutzung.

Die Beklagte kann einen Nutzer identifizieren, nachdem das Drittunternehmen die Informationen des Nutzers übermittelt hat, soweit die übermittelten Informationen mit den der Beklagten bekannten Informationen des Nutzers übereinstimmen. Jeder Nutzer ist für die Beklagte zu jeder Zeit individuell erkennbar, sobald er sich auf den Dritt-Webseiten bewegt oder eine App benutzt hat, auch wenn er nicht beim Netzwerk der Beklagten eingeloggt ist. Dabei ist jeder einzelne Klick und jede Texteingabe auf den Dritt-Webseiten und -Apps für die Beklagte nachverfolgbar. Sie weiß, welche Webseiten und Unterwebseiten der Nutzer besucht hat, was er angeklickt, gesucht und gekauft hat. Die Nachverfolgung der Aktivitäten auf Webseiten und Apps in Form von Aufrufen einer Seite, Klicks auf Artikel oder Buttons, Tastatureingaben und Ausfüllen eines Formulars oder Absenden eines Suchbefehls, das In-den-Warenkorb-Legen und Kaufen eines Artikels, bezeichnet die Beklagte als „Events“.

Die Daten sendet die Beklagte ausnahmslos weltweit in Drittstaaten, insbesondere die USA. Dort wertet sie die Daten in für den Nutzer unbekanntem Maß aus, gibt die Daten - ohne den Nutzer hiervon zu informieren - an Dritte, die sie allgemein bezeichnet als Werbetreibende und Audience Network-Publisher, Partner, die die Analysedienste der Beklagten nutzen, Partner, die Waren und Dienstleistungen anbieten, integrierte Partner, Anbieter für Messlösungen, Anbieter für Marketinglösungen, Dienstleister, externe Forscher, und Behörden weiter. Dabei übermittelt die Beklagte ohne Einwilligung der Nutzer keine Informationen an Werbetreibende, die Nutzer persönlich identifizieren.

Die Einstellungen der Beklagten in ihrem sozialen Netzwerk sehen folgende Auswahlmöglichkeiten für die Nutzer vor:

Nutzer können die Nutzung von optionalen Cookies erlauben, indem sie folgende Einstellung aktivieren: „Optionale Cookies: Unsere Cookies in anderen Apps und auf anderen Webseiten: Wir verwenden Cookies in Apps und auf Websites von anderen Unternehmen, die Meta-Technologien nutzen. Mithilfe dieser Cookies können andere Unternehmen Informationen über deine Aktivitäten in ihren Apps und auf ihren Websites mit uns teilen.“ Die Einstellung kann jederzeit geändert werden. Der Kläger hat diese Einstellung ausgewählt. Falls ein Nutzer sich entscheidet, die Nutzung der optionalen Meta Cookies auf Drittwebseiten nicht zu erlauben, wird die Beklagte die über Cookies oder ähnliche Technologien erhobenen Daten dieses Nutzers nicht für bestimmte Datenverarbeitungsvorgänge verwenden, insbesondere nicht für die Datenverarbeitung zur Bereitstellung personalisierter Werbung, sondern nur für begrenzte Zwecke, nach ihren Angaben: Sicherheits- und Integritätszwecke, z.B. Sicherheit von Kindern, Bekämpfung potenzieller krimineller Aktivitäten, Hassrede, Sicherheitsbedrohungen wie Hackerangriffe und Cyberspionage.

Nutzer können die Werbeanzeigen auf Instagram über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ kontrollieren, in der es heißt:

„Sollen wir Informationen von Werbepartnern zu deinen Aktivitäten verwenden, um die Werbung anzuzeigen?

Ja, meine Werbung mithilfe dieser Informationen relevanter machen.

Wir zeigen dir Anzeigen, die - basierend darauf, was dir bereits gefällt - relevanter für dich sind.

Nein, meine Werbung nicht mithilfe dieser Informationen relevanter machen.

Wir verwenden für die Auswahl von Werbeanzeigen, die du siehst, weniger Informa-

tionen über dich, weshalb sie wahrscheinlich eher für andere Personen interessant sind.“

Bei der zweiten handelt es sich um die Standardeinstellung. Die Auswahl kann jederzeit geändert werden. In der Datenschutzrichtlinie heißt es hierzu: „Nutzung von Informationen von Partnern, Anbietern und anderen Dritten, um die Werbeanzeigen, die du siehst, auf dich zuzuschneiden: Wenn wir dir Werbung auf Meta-Produkten zeigen, verwenden wir mit deiner Zustimmung Informationen, die Partner, Anbieter und andere Dritte uns bezüglich Aktivitäten außerhalb der Meta-Produkte bereitstellen und die wir mit dir verknüpft haben [...]“

Wird die Funktion deaktiviert, schreibt die Beklagte: „Wir verwenden für die Auswahl von Werbeanzeigen weniger Informationen über dich“ und „Einige Informationen werden unabhängig von deiner Auswahl anonymisiert und zur Verbesserung unserer Produkte verwendet“.

Die Klägerin hat über diese Einstellung keine Einwilligung erteilt.

Auch wenn der Nutzer die beiden Optionen verneint hat und bevor seine Einwilligung zu Cookies auf der Dritt-Webseite eingeholt wird, werden die Daten, dass der individualisierte Nutzer die Dritt-Webseite aufgerufen hat, an die Beklagte übersandt. Dabei handelt es sich um eine HTTP-Anfrage, bei der durch den Browser automatisch die technischen Standarddaten gesendet werden, um Meta Pixel zu laden (Datum, Uhrzeit, IP-Adresse, URL der Webseite, die den Server anruft, Betriebssystem des Gerätes, Art und Softwareversion des Browsers, Sprache, Verwendung und Parameter eines Touchscreens).

In ihren AGB hat sich die Beklagte ausbedungen, dass sie das zur Steuerung von Werbezwecken erstellte Persönlichkeitsprofil auch zu nicht werberelevanten Zwecken genutzt werden kann. In ihren AGB geht sie davon aus, dass sie die App-, Browser- und Geräteinformationen und Informationen von Partnern, Anbietern und Dritten dauerhaft und uneingeschränkt auch ohne Einwilligung vornehmen kann, nämlich zur Erfüllung eines Vertrages, einer rechtlichen Verpflichtung, zum Schutz wesentlicher Interesse, zur Wahrung öffentlicher Interessen sowie für berechnigte Interessen der Beklagten.

Seit dem 30.10.2023 bietet die Beklagte eine Abonnementoption an, die es Nutzern ermöglicht, ein monatliches Abonnement abzuschließen, um Instagram ohne Werbung zu nutzen. Solange der Nutzer ein Abonnement abgeschlossen hat, werden seine Daten nicht für Werbung verwendet.

Die Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien“ erlaubt den Nutzern, eine Zusammenfassung der mit ihren Konten verknüpften Informationen über die neuesten Aktivitäten auf

Webseiten und Apps von Drittunternehmen zu kontrollieren und abzurufen. Nicht enthalten sind: die jüngsten Aktivitäten innerhalb der vorhergehenden Tage. Die Beklagte erhält auch mehr Einzelheiten und Aktivitäten, als der Nutzer sehen kann. Die Beklagte schreibt hierzu: „Aus technischen Gründen und aus Gründen der Zuverlässigkeit zeigen wir nicht alle Aktivitäten, über die wir informiert wurden. Das betrifft unter anderem Informationen, die wir erhalten haben, während du nicht bei Instagram angemeldet warst, oder Situationen, in denen wir nicht überprüfen können, ob du auf einem bestimmten Gerät zuvor Instagram verwendet hast. Ebenso wenig zeigen wir Einzelheiten an, wie etwa den Artikel, den du zu deinem Einkaufswagen hinzugefügt hast.“ Der Kläger ist nur sehr selten in seinem Browser auf dem Netzwerk der Beklagten eingeloggt.

Die Beklagte bietet die Funktion „Zugriff auf deine Informationen“ und „Deine Informationen herunterladen“ an, mit dem die Nutzer eine Kopie ihrer Informationen für ihr Konto herunterladen können, einschließlich der Informationen über Aktivitäten außerhalb von Instagram, die die Beklagte von Drittunternehmen erhält.

In der Einstellung können die Nutzer auch bestimmte Aktivitäten „trennen“, d.h. frühere künftige Informationen über Aktivitäten auf den Webseiten oder Apps von ihrem Konto zu trennen. Aktivitäten von den ausgewählten Apps und Webseiten werden nicht mehr in dem Konto gespeichert. Die sog. „UID“, die dem Nutzer zugeordnet ist, wird durch eine „SID“, die nur einer Gruppe von ähnlichen Nutzern zugeordnet ist, ersetzt. Die Beklagte behält sich vor, weiterhin die „UID“ zu nutzen, wenn dies aus „Sicherheitsgründen“ erforderlich ist. Über die Einstellung „künftige Aktivitäten verwalten“ können Nutzer eine Verknüpfung mit künftigen Aktivitäten aufheben, d.h. Informationen, die Unternehmen und Organisationen zu den Interaktionen des Nutzers an die Beklagte übermitteln, werden zukünftig nicht mehr verknüpft. Entscheidet sich der Nutzer hierfür, löscht die Beklagte auch die früheren Aktivitäten des Nutzers.

Mit Schreiben vom 10.07.2023 wurde die Beklagte aufgefordert, Auskunft zu erteilen, die Daten zu löschen oder eine Einwilligung vorzulegen sowie ein Schmerzensgeld in Höhe von 5.000 € zu zahlen (Anlage K3).

Die Klägerin forderte die Beklagte mit Schriftsatz vom 01.10.2024 erneut zur Auskunftserteilung nur an die Klägerin unmittelbar auf. Hinsichtlich des Inhalts des Auskunftsbegehrens wird auf Seiten 42 bis 45 des Schriftsatzes vom 01.10.2024 Bezug genommen. Die Beklagte antwortete hierauf mit Schreiben vom 22.11.2024 (Anlage B11).

Die Klägerin behauptet, sie surfe regelmäßig auf Webseiten, auf denen die streitgegenständlichen Business Tools integriert seien. Sie macht geltend, sie könne nicht angeben, auf welchen mit einem solchen Business Tool versehenen Seiten sie in den letzten Jahren aktiv war, da sie nicht wisse, was genau sie seit 2018 auf welchen Webseiten und Apps getan habe, und nicht wisse, auf welchen Webseiten und Apps die Business Tools integriert waren. Bei Erfüllung eines etwaigen Auskunftsanspruchs nach Art. 15 DSGVO werde das Onlineverhalten der Klägerin innerhalb des Verfahrens öffentlich gemacht, was die Klägerin zum Schutz ihrer Intimsphäre vermeiden wolle. Sie gibt an: Sie beschäftige sich mit sensiblen Themen im Monat wie folgt: 20 Stunden: finanzielle Themen: Online-Banking, Handel von Aktien und Kryptowährung, Recherche zum Immobilienkauf, Kreditkonditionen und Anlagemöglichkeiten; 5 Stunden: gesundheitliche Themen, regelmäßige Nutzung von Online-Apotheken, Portale der Ärztevermittlung und zur Terminbuchung, Recherche zu Krankheitssymptomen; 1 Stunde: politische Themen wie Migration, Klimawandel, Genderdebatte, aktuelles Kriegsgeschehen; rechtliche Themen; Datingseiten. Dar- aus könne auf die finanzielle Situation, die Kreditwürdigkeit, Gesundheit und Sexualleben sowie sexuelle Orientierung, politische Einstellungen und Wahlprioritäten geschlossen werden.

Die Business Tools der Beklagten seien auf 30 - 40 % aller Webseiten weltweit und einer großen Zahl beliebter Apps aktiv.

Die Beklagte spioniere das Privatleben sämtlicher Nutzer, die bei einem ihrer Netzwerke „Facebook“ oder „Instagram“ angemeldet sind, aus. Deren digitale Bewegungen auf Webseiten oder mobilen Apps, d.h. im gesamten Internet würden rechtswidrig aufgezeichnet. Dies betreffe Daten aus der Privat- und der Intimsphäre der Nutzer. Die Klägerin könne sich beim Aufrufen von Webseiten oder Apps nie sicher sein, ob die Beklagte „mitlese“ oder was sie tue. Sie habe die Kontrolle darüber verloren, was die Beklagte mit den Daten mache, was sie über die Klägerin wisse und mit wem sie dieses Wissen teile. Dies belaste die Klägerin sehr.

Die Klägerin meint, die Verarbeitung der personenbezogenen Daten der Klägerin sei seit dem 25.05.2018 rechtswidrig gewesen. Ein Unterlassungsanspruch ergebe sich unmittelbar aus Art. 17 DS-GVO, jedenfalls aber aus nationalem Recht gemäß § 823 Abs. 1 i.V.m. § 1004 BGB. Ein Verpflichtungsanspruch gemäß Klageantrag zu 3. ergebe sich unmittelbar aus Art. 6, 9 DS-GVO, da die Beklagte kein Recht zur weiteren Datenverarbeitung habe, zudem als vertragliche Nebenpflicht aus § 242 BGB und als Nebenpflicht aus Art. 15 DS-GVO (da die Klägerin ggf. zukünftige Auskunft über die Verarbeitung der Daten begehre, dürften diese vor Erfüllung des Auskunftsanspruchs nicht von der Beklagten manipuliert werden) und aus Art. 18 Abs. 1 lit. b), Abs. 2 DS-GVO, § 823 Abs. 1 i.V.m. § 1004 BGB. Die nationalen Vorschriften seien aufgrund der Öff-

nungsklausel des Erwägungsgrundes 146 S. 4 DS-GVO neben der DS-GVO anwendbar. Ein Lösungsanspruch bestehe gemäß Art. 17 DS-GVO. Die von der Beklagten angebotene Pseudonymisierung gemäß Art. 4 Nr. 5 DS-GVO sei gemäß Erwägungsgrund 26 der DS-GVO nicht mit einer Löschung gleichzusetzen, da sie jederzeit wieder individualisiert werden könnten. Zumindest bestehe ein Anspruch auf vollständige Anonymisierung der Daten, der sich als Minus ebenfalls aus Art. 17 Abs. 1 DS-GVO ergebe. Die von der Beklagten als Trennung bezeichnete Pseudonymisierung genüge nicht, da sie nachträglich wieder rückgängig gemacht werden könne. Der Antrag sei gemäß § 259 ZPO zulässig. Ein Schadensersatzanspruch bestehe gemäß Art. 82 DS-GVO sowie § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG wegen der Verletzung des Rechts auf informationelle Selbstbestimmung als Ausformung des Allgemeinen Persönlichkeitsrechts. Es liege ein schwerer Eingriff in die informationelle Selbstbestimmung der Klägerin vor. Mit den Business Tools sei die vollständige Ausspähung und Überwachung des Privatlebens der Klägerin möglich. Die Klägerin habe das Gefühl, im Privatleben vollständig von der Beklagten überwacht zu werden. Sie fühle sich der Marktmacht der Beklagten ausgeliefert; lösche sie die Apps der Beklagten, verliere sie große Teile der sozialen Kontakte über Social Media. Sie zögere teilweise beim Besuch von Webseiten und der Nutzung von Apps, weil sie nicht genau wisse, inwieweit sie dabei von der Beklagten getrackt werde. Sie befürchte, dass die Informationen genutzt werden, um sie zu manipulieren.

Die Klägerin beantragte mit ihrer Klageschrift vom 16.01.2024 zunächst:

1. Es wird festgestellt, dass bei rechtskonformer Auslegung des Nutzungsvertrages der Parteien zur Nutzung des Netzwerks "Instagram" unter dem Benutzernamen „[REDACTED]“ abweichend von den Regelungen des Nutzungsvertrags die Verarbeitung von folgenden personenbezogenen Daten, die die Beklagte auf Dritt webseiten und –Apps außerhalb der Netzwerke der Beklagten verarbeitet und im Zuge dessen mit dem obigen Nutzeraccount der Klagepartei verknüpft hat, in folgendem Umfang seit dem 25.05.2018 nicht zulässig war:

a) auf besuchten Dritt -Webseiten und -Apps die personenbezogenen Daten, die der Identifizierung der Klagepartei dienen, ob direkt oder in gehashter Form übertragen,

d.h.

- E-Mail der Klagepartei

- Telefonnummer der Klagepartei

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

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b) auf Dritt-Webseiten

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

c) in mobilen Dritt-Apps

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

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungs-

fall bis zu zwei Jahren, zu unterlassen, ohne wirksame Einwilligung der Klagepartei auf Drittseiten – und Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten gem. des Antrags zu 1. zu verarbeiten, solange im Einzelfall kein Rechtfertigungsgrund gem. Art. 6 Abs 1 b – e DSGVO vorliegt.

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

4. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, der aber mindestens 1.000,00 Euro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 08.08.2023, zu zahlen.

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

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

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

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 25.05.2018 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weiterge-

geben hat, unter Benennung dieser Dritten,

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

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

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

sowie auf zweiter Stufe (Stufenklage):

8. Die Beklagte wird verurteilt, an die Klagepartei materiellen und immateriellen Schadensersatz aufgrund der Verarbeitung der gem. des Antrags zu 6. beauskunfteten Daten, dessen Höhe in das Ermessen des Gerichts gestellt wird, und dessen Mindestsumme nach erfolgter Auskunftserteilung konkretisiert wird, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 08.08.2023, zu zahlen

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

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

Die Klägerin beantragt mit Schriftsatz vom 01.10.2024 zuletzt:

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

"Instagram" unter dem Benutzernamen „[REDACTED]“ der Beklagten die Erhebung mit Hilfe der Meta Business Tools, die Weitergabe an die Server der Beklagten, die dortige Speicherung und anschließende Verwendung von folgenden personenbezogenen Daten nicht gestattet:

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

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

sowie folgende personenbezogene Daten der Klagepartei

b) auf Webseiten

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

sowie

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

c) in mobilen Dritt -Apps

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

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

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

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

5. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 1.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 08.08.2023, zu zahlen.

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

Die Beklagte beantragt,

die Klage abzuweisen,

den Rechtsstreit gemäß § 348 Abs. 3 ZPO auf die Kammer zu übertragen.

Die Beklagte erklärt, der vorrangige Zweck der Business Tools sei es, Drittunternehmen bei der Integration von Meta Produkten zu unterstützen, die Effektivität ihrer Werbeanzeigen zu messen und Personen zu erreichen, die ihre Produkte oder Dienstleistungen nutzen oder an diesen interessiert sein könnten. Die Drittunternehmen könnten sich dazu entscheiden, Kundendaten in Form von „event data“ mit der Beklagten zu teilen, d.h. Daten zur Aktivität auf der Webseite oder der App des Drittunternehmens. Zudem könnten die Drittunternehmen entscheiden, bestimmte Daten mit der Beklagten zu teilen, z.B. um auf Instagram Werbeanzeigen für ihre eigenen Kunden zu schalten.

Sie gehe davon aus, dass - obwohl die Klageseite den relevanten Verarbeitungszweck nicht konkretisiere - sich der Antrag der Klageseite auf die Verarbeitung der durch die Business Tools erhalten personenbezogenen Daten zum Zweck der Anzeige von personalisierter Werbung auf Instagram beziehe, die die Beklagte als „streitgegenständliche Datenverarbeitung“ bezeichnet.

Sie meint, die Drittunternehmen, die sich für die Nutzung der Business Tools auf ihren Webseiten und Apps entschieden haben und die Daten erheben und an die Beklagte übermitteln, seien die maßgeblich Verantwortlichen für die Installation und Nutzung der Business Tools, die Offenlegung von Informationen über die Business Tools für die Besucher, die Erhebung und Übermittlung der Daten auf Basis einer Rechtsgrundlage. Die Pflicht, die notwendigen Informationen zur Verfügung zu stellen sowie die erforderliche Einwilligung von den Besuchern der Webseite oder App einzuholen, obliege den Drittunternehmen und nicht der Beklagten. Sie macht geltend, die Klägerin lege nicht dar, dass die von ihr aufgeführten Webseiten und Apps diese Pflichten verletzt hätten.

Nachdem ein Drittunternehmen die personenbezogenen Daten des Nutzers erhoben und mithilfe der Business Tools an die Beklagte übermittelt habe, hänge die Frage, ob die Beklagte die Daten für die „streitgegenständliche Datenverarbeitung“ nutze, maßgeblich von den Einstellungen des

Nutzers ab. Entscheide sich ein Nutzer, optionale Cookies nicht zu erlauben, verwende die Beklagte „für bestimmte Verarbeitungszwecke“ keine über Cookies und ähnliche Technologien erhobenen Daten, einschließlich für die „streitgegenständliche Datenverarbeitung“. Selbst wenn ein Nutzer die Verwendung der optionalen Cookies auf anderen Webseiten und Apps erlaube, müsse der Nutzer dennoch ausdrücklich über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ in die „streitgegenständliche Datenverarbeitung“ einwilligen. Sie gibt hierzu an, dass sie die „streitgegenständliche Datenverarbeitung“ lediglich dann vornehme, wenn der Nutzer ausdrücklich über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ in die „streitgegenständliche Datenverarbeitung“ gemäß Art. 6 Abs. 1 lit. a. DSGVO einwillige. Habe der Nutzer nicht über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ eingewilligt, nehme die Beklagte für diesen Nutzer keine „streitgegenständliche Datenverarbeitung“ vor. Da die Klägerin nicht in die streitgegenständliche Datenverarbeitung eingewilligt habe, nehme die Beklagte diese nicht vor.

Zu der Seite 23 ihres Performance Leitfadens mit dem Inhalt: „Die Conversions API ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben.“ erklärt die Beklagte: Es handele sich dabei um ein Produkt, dass der Messung der Effektivität von Werbekampagnen diene. Die Aussage habe keinen Bezug zur Datenverarbeitung zur Bereitstellung personalisierter Werbung und sei daher für die Klageanträge in diesem Verfahren nicht relevant.

Sie trägt weiter vor: Soweit die Klägerin andere Verarbeitungszwecke außerhalb der Datenverarbeitung zur Bereitstellung personalisierter Werbung angreifen wolle, die in Bezug zu den Daten der Klägerin stehen, die die Beklagte (angeblich) über die Business Tools erhalten habe, spezifiziere die Klägerin keine Verarbeitungszwecke, so dass die Beklagte keine Darlegungslast treffe, bzgl. irgendwelcher anderen Datenverarbeitungen oder deren Rechtsgrundlagen auszuführen. Es sei der konkrete Verarbeitungszweck, der eine Ermittlung der Rechtsgrundlage eines Verantwortlichen bedinge. Ohne Identifizierung des konkreten streitgegenständlichen Verarbeitungszwecks sei es nicht möglich, eine Bewertung der Rechtsgrundlage zu ermöglichen. Die Klage sei unbestimmt und unsubstantiiert. Daher könne die Beklagte das Begehren der Klägerin nur interpretieren und bezeichne dies als „streitgegenständliche Datenverarbeitung“ bzw. „Datenverarbeitung zur Bereitstellung personalisierter Werbung“. Die Klägerin wolle sich nach dem Verständnis der Beklagten gegen die angebliche Verarbeitung personenbezogener Daten zum Zwecke der Bereitstellung personalisierter Werbung auf Instagram wenden. Die anderen Zwecke, zu denen die Beklagte die Daten verarbeite, die über die Business-Tools erhalten werden, seien in der Datenschutzrichtlinie offengelegt und würden von der Beklagten nicht bestritten. Z.B. nutze die Beklagte

die Daten, um die Sicherheit und die Integrität von ihren Servern zu schützen, etwa um die Systeme vor bössartigen Angriffen zu schützen, bei denen die Business Tools zur Verbreitung von Spam, Scraping oder anderen Cyberattacken missbraucht werden könnten, z.B. Überforderung der Server, Versand missbräuchlicher Informationen. Hierfür benötige die Beklagte keine Einwilligung. Obwohl die Klägerin diese anderen Zwecke kenne, versäume es die Klägerin zu spezifizieren, gegen welche zusätzlichen Verarbeitungszwecke er sich wenden wolle, und Argumente darzulegen, weshalb die Datenverarbeitung der Beklagten für den jeweiligen Zweck gemäß Art. 6 DS-GVO unzulässig wäre. Da die Klägerin nicht ausführe, welche Verarbeitungszwecke sie angreifen wolle, könne die Beklagte sich nicht hinsichtlich spezifischer Rechtsgrundlagen für irgendwelche Verarbeitungszwecke verteidigen.

Die Beklagte bestreitet, dass ihre Business Tools auf mindestens 30 - 40 % aller Webseiten weltweit aktiv seien. Die Klägerin habe keinerlei zuverlässige Methode zur Bestimmung oder Herkunft dieser Prozentsätze angegeben habe.

Sie meint, über die Einstellung „Deine Aktivitäten außerhalb von Meta-Technologien“ könnte der Nutzer eine Zusammenfassung der von Drittunternehmen geteilten Informationen über die Aktivitäten abrufen, einschließlich der Namen der Webseiten und Apps.

Sie habe auf das Auskunftsverlangen der Klägerin gemäß Art. 15 DSGVO geantwortet. Sie habe auf die Funktionen „Zugriff auf deine Informationen“, „Deine Informationen herunterladen“ und „Deine Aktivitäten außerhalb der Meta-Technologien“ hingewiesen. Sie habe die Klägerin über die Identität einzelner, bestimmter Empfänger informiert. Sie habe bestätigt, dass keine Verarbeitung festgestellt werden konnte, die in den Anwendungsbereich des Art. 22 Abs. 1 DS-GVO fällt. Im Übrigen überschreite das Auskunftsverlangen den Umfang von Art. 15 DS-GVO, insoweit die Klägerin Auskunft verlange, auf welchen Webseiten und Apps die Business Tools aktiv sind.

Sie macht geltend, die Klägerin habe nicht dargelegt noch Beweis angetreten, dass sie überhaupt relevante Webseiten oder Apps Dritter besucht habe. Sie habe jedoch über die Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien“ Zugang zu derartigen Informationen. Die Beklagte bestreitet mit Nichtwissen, dass die Klägerin eine der genannten Webseiten besucht hat. Sie weist darauf hin, dass die Prozessbevollmächtigten die Klägerin ausdrücklich angewiesen haben, keine Beweise bzgl. Webseiten und Apps vorzulegen, unter dem Vorwand, angeblich die privaten Informationen nicht preisgeben zu wollen. Dies sei inkonsistent mit der Behauptung, die Beklagte erhalte diese Informationen über die Business Tools.

Sie meint, Art. 17 DS-GVO sehe ein Recht auf Löschung vor, gewähre jedoch dem unmissver-

ständlichen Wortlaut nach keinen Anspruch auf Unterlassung. Für den Fall, dass das Gericht einer anderen Auffassung sein sollte, beantragt sie, das Verfahren gemäß § 148 ZPO analog auszusetzen, bis der EuGH über eine Vorlagefrage des BGH, Beschluss vom 26.09.2023, Az. VI ZR 97/22, entschieden hat. Nationales Recht sei nicht anwendbar, da die DS-GVO das Datenschutzrecht der EU vollständig harmonisiere und die Mitgliedstaaten nationales Recht nicht zur Interpretation oder Erweiterung der Betroffenenrechte anwenden dürften. Kapitel 3 der DS-GVO enthalte kein Recht auf eine Unterlassungsklage.

Der Klageantrag zu 3. sei unzulässig, da er eine außerprozessuale Bedingung enthalte. Zudem gebe es dafür keine rechtliche Grundlage. Art. 15 DS-GVO verpflichte den Verantwortlichen nicht dazu, die personenbezogenen Daten von Betroffenen für den Fall des hypothetischen und zukünftigen Auskunftersuchens zu speichern.

Die DS-GVO verleihe kein Recht auf Anonymisierung von Daten.

Der Klägerin sei kein Schaden entstanden. Er verstehe die streitgegenständliche Datenverarbeitung falsch, die Beklagte spioniere und überwache nicht. Die von ihr angegebenen Ängste und Befürchtungen seien subjektive Empfindungen in Bezug auf potenzielle Ereignisse, deren Eintritt unwahrscheinlich sei.

Die Beklagte könne den Erhalt des vorgerichtlichen Schreibens nicht bestätigen. Sie habe keine Aufzeichnungen über den Erhalt des vorgerichtlichen Anwaltsschreibens. Die Klägerin habe bereits auf die in dem Schreiben geforderten Informationen über das Self-Service-Tool zugreifen können. Das Schreiben habe offenbar lediglich der Klagevorbereitung gedient und sei deshalb als solches nicht erstattungsfähig.

Die Klägerin repliziert, es sei allein Sache der Klägerin zu entscheiden, welchen Streitgegenstand das Verfahren haben solle. Die Verarbeitung der im Klageantrag zu 1. benannten personenbezogenen Daten solle vollumfänglich unterbunden werden, nicht nur hinsichtlich des Anteils zur Anzeige personalisierter Werbung.

Die DS-GVO konstituiere eine Verbotssystematik mit einem Rechtfertigungsvorbehalt. Die Beklagte müsse die Rechtfertigung für ihre Datenverarbeitung vorweisen können. Es sei nicht Sache des Klägers vorzutragen, welche - nur der Beklagten bekannten - Verarbeitungszwecke er konkret angreifen wolle. Die Behauptung von „Sicherheits- und Integritätszwecken“ sei pauschal. Mangels verständlicher Rechtfertigung sei die Verarbeitung der benannten Daten immer rechts-

widrig.

Die Schaltfläche „Informationen zu Aktivitäten von Werbepartnern“ ermögliche lediglich, auszuwählen, ob aufgrund der Daten „relevantere Werbung“ angezeigt wird. Ob die Daten für Werbeanzeigen verwendet werden oder nicht, habe jedoch nichts damit zu tun, ob die Datensammlung stattfinde oder nicht. Die Schaltflächen „Optionale Cookies erlauben“ und „Informationen über Aktivitäten von Werbepartnern“ würden keine taugliche Einwilligung i.S.d. Art. 6 Abs. 1 lit. a DS-GVO darstellen. Sie sei nicht freiwillig, informiert und hinreichend bestimmt erfolgt. Jedenfalls sei eine Einwilligung mit Erhebung der Klage offensichtlich widerrufen worden. Über die Business Tools zeichne die Beklagte zunächst unterschiedslos die Daten aller Nutzer auf. Erst nachdem die Daten an die Server der Beklagten geschickt worden seien, werte die Beklagte aus, ob sie die rechtliche Befugnis habe, die - bereits verarbeiteten - Daten zu verarbeiten. In dem Zeitpunkt, in dem die Beklagte prüfe, ob eine Einwilligung des Nutzers vorliege, seien daher bereits mehrere rechtfertigungsbedürftige Datenverarbeitungsvorgänge erfolgt: Abgleich der auf der Webseite ermittelten Datensätzen mit den bei der Beklagten hinterlegt, Speicherung der Daten auf den Servern der Beklagten. Die Beklagte habe dadurch die alleinige Datenhoheit und entscheide, wie sie die Daten auf ihren Servern sortiere, verwerte und filtere.

Die allgemeine Lebenserfahrung spreche dafür, dass die Klägerin regelmäßig Webseiten besuche, auf denen die Business Tools der Beklagten eingebunden seien. Es sie an der Beklagten, die Auskunft zu erteilen habe, welche Daten der Klägerin sie verarbeitet habe und weiter verarbeite. Die Klägerin habe nicht in den vergangenen Jahren protokolliert, wann sie auf welchen Webseiten und Apps was getan habe. Zudem wisse sie nicht, wann und wo sie hierbei von der Beklagten ausspioniert worden sei. Sie habe vor der Mandatierung ihrer Prozessbevollmächtigten kein Bewusstsein dafür gehabt, dass die Beklagte ihre Aktionen außerhalb von Instagram aufzeichne. Sie habe deshalb jegliche Kontrolle über ihre Daten verloren. Sie könne nie sicher wissen, welche Daten die Beklagte verarbeitet und gespeichert habe, wie das Profiling der Beklagten funktioniere und mit welchen Dritten die Daten der Klägerin geteilt wurden. Die Beklagte sei gemäß Art. 15 DS-GVO verpflichtet, der Klägerin mitzuteilen, auf welchen Drittseiten und -Apps sie ihre Klicks und Texteingaben durch die Business Tools aufzeichne.

Das Gericht hat die Klägerin persönlich angehört. Hinsichtlich des Ergebnisses der persönlichen Anhörung wird Bezug genommen auf das Protokoll der öffentlichen Sitzung vom 13.01.2025.

Hinsichtlich des weiteren Sach- und Streitstandes wird zur Ergänzung des Tatbestandes Bezug genommen auf die Schriftsätze der Klägerseite vom 16.01.2024, 01.10.2024, 10.12.2024, 02.01.2025, 10.02.2025, der Beklagtenseite vom 26.07.2024, 25.11.2024, 20.12.2024, 23.12.2024, jeweils nebst Anlagen, sowie das Protokoll der öffentlichen Sitzung vom 13.01.2025.

Entscheidungsgründe

I.

Eine Vorlage des Rechtsstreits an die Kammer zur Entscheidung über eine Übernahme erfolgt nicht, da die Gründe des § 348 Abs. 3 S. 1 ZPO nicht gegeben sind.

Die Sache weist keine besonderen Schwierigkeiten tatsächlicher oder rechtlicher Art auf (Nr. 1). Der Sachverhalt ist zwischen den Parteien weitgehend unstreitig und beschränkt sich trotz des Umfangs der Schriftsätze auf die gleichförmige Datenverarbeitung der Beklagten auf Drittwebseiten und -Apps. Rechtlich kann auf allgemeine Grundsätze zur Zulässigkeit von Klageanträgen sowie bei Prüfung der Begründetheit auf die Rechtsprechung von BGH und EuGH abgestellt werden.

Die Rechtssache hat keine grundsätzliche Bedeutung (Nr. 2). Es handelt sich um eine von deutschlandweit hundert bis tausenden Klagen, deren abschließende Entscheidung nach Durchlaufen der Landgerichte voraussichtlich erst durch OLG-, BGH- oder EuGH-Rechtsprechung erfolgen wird.

II.

Die Klage ist weit überwiegend zulässig.

1.

Das Landgericht Augsburg ist gemäß Art. 79 Abs. 2 S. 2, Art. 82 Abs. 6 DS-GVO, § 44 Abs. 1 S. 2 BDSG, § 1 ZPO i.V.m. §§ 71 Abs. 1, 23 GVG international, örtlich und sachlich zuständig.

2.

Der Klageantrag zu 1. ist unzulässig.

Gemäß § 256 Abs. 1 ZPO kann auf Feststellung des Nichtbestehens eines Rechtsverhältnisses Klage erhoben werden, wenn der Kläger ein rechtliches Interesse daran hat, dass das Rechtsverhältnis durch richterliche Entscheidung alsbald festgestellt werde.

Ein Feststellungsinteresse besteht nur, wenn dem subjektiven Recht des Klägers eine gegenwärtige Gefahr der Unsicherheit dadurch droht, dass der Beklagte es ernstlich bestreitet oder er sich eines Rechts gegen den Kläger berühmt, und wenn das erstrebte Urteil infolge seiner Rechtskraft geeignet ist, diese Gefahr zu beseitigen. Ein Feststellungsinteresse besteht nur, wenn dasselbe Ziel nicht durch einen einfacheren Weg erreicht werden kann. Ist dem Kläger eine Klage auf Leistung möglich und zumutbar und erschöpft sie das Rechtsschutzziel, fehlt dem Kläger grundsätzlich das Feststellungsinteresse, weil er im Sinne einer besseren Rechtsschutzmöglichkeit den Streitstoff in einem Prozess klären kann (Greger in Zöller, ZPO, § 256, Rn. 12, 14 m.w.N.).

Im vorliegenden Fall besteht kein Feststellungsinteresse.

Die Klägerin begehrt bzgl. der Datenverarbeitung, auf die sich ihr Feststellungsantrag bezieht, für die Vergangenheit bereits Löschung und Schadensersatz sowie für die Zukunft die Unterlassung der Datenverarbeitung. Eine über die geltend gemachten Leistungsanträge hinaus bestehende Rechtsunsicherheit ist nicht zu erkennen. Die bereits gestellten Leistungsanträge erschöpfen das Rechtsschutzziel der Klägerin bzgl. der streitgegenständlichen Datenverarbeitung.

3.

Im Übrigen sind die Klageanträge zulässig, insbesondere hinreichend bestimmt.

III.

Die Klage ist im Übrigen überwiegend begründet.

1.

Die Klägerin hat einen Unterlassungsanspruch gegen die Beklagte.

Es kann dahinstehen, ob sich auch für eine Unterlassungsklage ohne Löschantrag und eine

Datenverarbeitung in der Zukunft ein Unterlassungsanspruch unmittelbar aus Art. 17, Art. 18, Art. 4 Nr. 3 DS-GVO oder einer sonstigen Bestimmung der DS-GVO ergibt (EuGH-Vorlage des BGH, Beschluss vom 26.09.2023, Az. VI ZR 97/22, GRUR 2023, 1724, Rn. 17 - 21, m.w.N.).

Die Klägerin hat jedenfalls einen Unterlassungsanspruch wegen Verstoßes gegen die DS-GVO und wegen Verletzung des allgemeinen Persönlichkeitsrechts der Klägerin gemäß § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 2 GG, § 823 Abs. 2 S. 1 BGB i.V.m. Art. 6 DS-GVO, jeweils i.V.m. § 1004 Abs. 1 S. 2 BGB analog.

a)

Die Vorschriften des nationalen Rechts zu Unterlassungsansprüchen sind insoweit jedenfalls neben der DS-GVO anwendbar.

Das Gericht geht davon aus, dass diese Frage unter Heranziehung allgemeiner Grundsätze und der neuesten Rechtsprechung des EuGH keiner weiteren Klärung bedarf (so aber noch EuGH-Vorlage des BGH, Beschluss vom 26.09.2023, Az. VI ZR 97/22, GRUR 2023, 1724, dritte Vorlagefrage, Rn. 28 ff., m.w.N.).

Gemäß Art. 288 Abs. 1 AEUV hat die Verordnung allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat. Der Anwendungsvorrang des Europarechts ist allgemein anerkannt (Ruffert in Calliess/Ruffert, EUV/AEUV, Art. 1 AEUV, Rn. 16 f., m.w.N.). Zwar ergibt sich daraus und aus der unmittelbaren Geltung der Verordnung zugleich ihr uneingeschränkter Vorrang vor nationalem Recht. Dies hat jedoch nicht zur Folge, dass nationale Vorschriften, die denselben Sachverhalt betreffen, überhaupt nicht mehr zur Anwendung kommen. Es bedeutet lediglich, dass den Regelungen der Verordnung entgegenstehendes oder inhaltsgleiches nationales Recht unanwendbar oder das nationale Recht unionsrechtskonform auszulegen ist (Ruffert in Calliess/Ruffert, EUV/AEUV, Art. 1 AEUV, Rn. 18, 21, 24, m.w.N.; Sydow in Sydow/Marsch, DS-GVO, Einleitung, Rn. 8 f., m.w.N.).

Die DS-GVO enthält keinen ausdrücklichen Unterlassungsanspruch. Die Regelungen der DS-GVO stellen aber auch keinen abschließenden und jedweden anderen Anspruch ausschließenden Katalog der Rechte des Betroffenen gegen den Verantwortlichen dar. Eine andere Sichtweise würde den Zielen der DS-GVO widersprechen, wohingegen die Gewährung eines nationalen Anspruchs auf Unterlassung den Zielen und dem Regelungsgehalt der DS-GVO nicht entgegensteht.

Zwar hat der Ordnungsgeber mitgeteilt: Um ein gleichmäßiges und hohes Datenschutzniveau

für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden (Erwägungsgrund 10). Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie - in den Mitgliedstaaten - gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Falle ihrer Verletzung (Erwägungsgrund 11). Damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern können, beseitigt werden, ist eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten für die Verantwortlichen vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten gewährleistet (Erwägungsgrund 13).

Jedoch heißt es auch: Die DS-GVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DS-GVO). Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DS-GVO). Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten (Erwägungsgrund 1).

Gemäß Art. 79 Abs. 1 DS-GVO hat jede betroffene Person unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Art. 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche, wenn sie der Ansicht ist, dass die ihr aufgrund der DS-GVO zustehenden Rechte infolge einer nicht im Einklang mit der DS-GVO stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Das Unionsrecht ist, ebenso, wie es den Einzelnen Pflichten auferlegt, auch dazu bestimmt, ihnen Rechte zu verleihen, die Teil ihres rechtlichen Besitzstands werden, wobei der EuGH insoweit betont, dass solche Rechte u. a. aufgrund von Verpflichtungen entstehen, die dem Einzelnen

wie auch den Mitgliedstaaten und den Organen der Union auferlegt werden. Jede Verpflichtung, die einer natürlichen oder juristischen Person auferlegt wird, hat nämlich in der Regel die damit verbundene Wirkung, einer anderen Person ein Recht zu gewähren. Außerdem steht fest, dass jedes Recht, das einem Einzelnen durch das Unionsrecht verliehen wird, mit einem Rechtsbehelf einhergeht, der gerade auf die Durchsetzung dieses Rechts abzielt, wobei es in Ermangelung spezifischer unionsrechtlicher Vorschriften, die diesem Zweck dienen, Sache der Mitgliedstaaten ist, die Achtung der in Rede stehenden Rechte im Rahmen von Rechtsbehelfen des innerstaatlichen Rechts sicherzustellen. Aus der Rechtsprechung des EuGH geht nämlich eindeutig hervor, dass die nationalen Gerichte die Rechte schützen müssen, die das Unionsrecht dem Einzelnen verleiht. Unter diesen Umständen sollte die Durchsetzung der Rechte, die Personen aus der DSGVO herleiten können, in Ermangelung ausdrücklicher Bestimmungen des Unionsrechts, die diesem Zweck dienen, im Rahmen der von den Mitgliedstaaten vorgesehenen Rechtsbehelfe sichergestellt werden können (Generalanwalt beim EuGH, Schlussantrag vom 25.04.2024, Rs. C-21/23, GRUR-RS 2024, 8646, Rn. 63, 64, 66 m.w.N.).

Zum eventuell erschöpfenden Charakter der Rechtsbehelfe, die das Unionsrecht für den Schutz der Rechte vorsieht, die seine Normen Einzelpersonen gewähren, gilt Folgendes: Der EuGH hat entschieden, dass eine durch das Unionsrecht umfassend harmonisierte Haftungsregelung dennoch neben einer alternativen Haftungsregelung nach nationalem Recht bestehen kann, die auf demselben Sachverhalt und derselben Grundlage beruht, sofern diese alternative Regelung das harmonisierte System nicht beschädigt und dessen Ziele und praktische Wirksamkeit nicht beeinträchtigt. Allein der erschöpfende Charakter eines im Unionsrecht vorgesehenen Systems von Rechtsbehelfen reicht daher nicht aus, um die Möglichkeit eines Mitgliedstaats auszuschließen, im nationalen Recht einen alternativen Rechtsbehelf vorzusehen, der sich auf dasselbe Recht stützt, sofern bestimmte Bedingungen erfüllt sind (Generalanwalt beim EuGH, Schlussantrag vom 25.04.2024, Rs. C-21/23, GRUR-RS 2024, 8646, Rn. 70 m.w.N.).

Konkret für die DS-GVO gilt nach neuester Rechtsprechung des EuGH Folgendes: Bei der Auslegung einer unionsrechtlichen Vorschrift sind nicht nur ihr Wortlaut, sondern auch ihr Kontext und die Ziele zu berücksichtigen, die mit der Regelung, zu der sie gehört, verfolgt werden. Zum Wortlaut der Bestimmungen der DS-GVO ist festzustellen, dass in keiner dieser Bestimmungen ausdrücklich ausgeschlossen wird, dass ein Betroffener eine Unterlassungsklage erheben kann. Zum Regelungszusammenhang ist darauf hinzuweisen, dass diese Verordnung in ihrem Kapitel II materielle Bestimmungen enthält, die unter anderem die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5) und die Voraussetzungen für die Rechtmäßigkeit der Verarbeitung (Art. 6) umfassen und die uneingeschränkte Achtung insbesondere des in Art. 16 I AEUV und Art.

8 der Charta verankerten Grundrechts der betroffenen Personen auf Schutz personenbezogener Daten sicherstellen sollen. Zwar enthalten die Bestimmungen des Kapitels VIII DS-GVO keine spezielle Öffnungsklausel, die es den Mitgliedstaaten ausdrücklich erlaubt, einem Betroffenen gegenüber einem Unternehmen, das angeblich gegen die materiellen Bestimmungen dieser Verordnung verstößt, die Möglichkeit einzuräumen, auf Unterlassung dieses Verstoßes zu klagen. Aus dem Wortlaut und dem Kontext der Bestimmungen dieses Kapitels VIII ergibt sich jedoch, dass der Unionsgesetzgeber mit dem Erlass dieser Verordnung keine umfassende Harmonisierung der Rechtsbehelfe, die bei einem Verstoß gegen die Bestimmungen der DS-GVO zur Verfügung stehen, vornehmen und insbesondere nicht ausschließen wollte, dass Betroffene eines mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten auf der Grundlage des nationalen Rechts unter dem Gesichtspunkt des Verbots der Vornahme dieser Geschäftspraktiken Klage erheben können. Diese Auslegung wird durch die mit der DS-GVO verfolgten Ziele bestätigt. Insbesondere aus dem 10. Erwägungsgrund dieser Verordnung geht nämlich hervor, dass bei der Verarbeitung personenbezogener Daten ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen gewährleistet und die Hemmnisse für den Verkehr personenbezogener Daten in der Union beseitigt werden sollen. Im 11. Erwägungsgrund der Verordnung heißt es außerdem, dass ein wirksamer Schutz dieser Daten die Stärkung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen erfordert, die personenbezogene Daten verarbeiten und darüber entscheiden, ebenso wie – in den Mitgliedstaaten – gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten sowie gleiche Sanktionen im Fall ihrer Verletzung. Dem 13. Erwägungsgrund der Verordnung zufolge ist, damit in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, beseitigt werden, eine Verordnung erforderlich, die für die Wirtschaftsteilnehmer Rechtssicherheit und Transparenz schafft, natürliche Personen in allen Mitgliedstaaten mit demselben Niveau an durchsetzbaren Rechten ausstattet, dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter vorsieht und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten und gleichwertige Sanktionen in allen Mitgliedstaaten gewährleistet. Die Möglichkeit für den Betroffenen, bei den Zivilgerichten Klage auf Unterlassung eines von diesem Unternehmen angeblich begangenen Verstoßes gegen die materiellen Bestimmungen der DS-GVO zu erheben, lässt diese Ziele nicht nur unberührt, sondern kann die praktische Wirksamkeit dieser Bestimmungen sogar verstärken und damit das mit dieser Verordnung angestrebte hohe Schutzniveau der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten verbessern. Denn zum einen hat eine Unterlassungsklage, die von einem Betroffenen gegen ein Unternehmen unter dem Gesichtspunkt des

Verbots der Vornahme dieser Geschäftspraktiken wegen eines behaupteten Verstoßes gegen die materiellen Bestimmungen der DS-GVO erhoben wird, keinerlei Einfluss auf das in Kapitel VIII dieser Verordnung vorgesehene Rechtsbehelfssystem oder auf das Ziel, in der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen zu gewährleisten und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, zu beseitigen. Insbesondere ist durch eine Koexistenz der von der DS-GVO selbst und dem nationalen Recht vorgesehenen Rechtsbehelfen keine Gefahr für die einheitliche Durchsetzung der DS-GVO zu befürchten. Aus den Art. 77–80 DS-GVO ergibt sich, dass diese Verordnung weder eine vorrangige oder ausschließliche Zuständigkeit vorsieht noch einen Vorrang der Beurteilung der genannten Behörde oder des genannten Gerichts zum Vorliegen einer Verletzung der durch die Verordnung verliehenen Rechte. Folglich wirkt sich die Erhebung einer Unterlassungsklage durch einen Betroffenen des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten bei den Zivilgerichten nicht auf das durch Kapitel VIII DS-GVO geschaffene Rechtsbehelfssystem aus. Außerdem wird durch das in Art. 267 AEUV vorgesehene Vorabentscheidungsverfahren gewährleistet, dass die materiellen Bestimmungen der DS-GVO, die die Aufsichtsbehörde und die auf der Grundlage der Art. 77–80 DS-GVO angerufenen Gerichte auf der einen Seite und die von einem Betroffenen unter dem Gesichtspunkt des Unterlassungsbegehrens angerufenen Gerichte auf der anderen Seite möglicherweise auf den gleichen Verstoß anwenden, einheitlich ausgelegt werden. Drittens wird die Verwirklichung des Ziels, in der Union ein gleichmäßiges Datenschutzniveau für die betroffenen Personen zu gewährleisten und Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten, zu beseitigen, nicht dadurch gefährdet, dass den Betroffenen die Möglichkeit eingeräumt wird, sich unter Anwendung des nationalen Rechts auf die materiellen Bestimmungen der DS-GVO zu berufen. Selbst wenn einzelne Mitgliedstaaten diese Möglichkeit nicht vorsähen, würde dies nämlich nicht zu einer Fragmentierung der Umsetzung des Datenschutzes in der Union führen, weil die materiellen Bestimmungen der DS-GVO für alle Verantwortlichen iSv Art. 4 Nr. 7 DS-GVO gleichermaßen verbindlich sind und ihre Einhaltung durch die in dieser Verordnung vorgesehenen Rechtsbehelfe sichergestellt wird. Zum anderen ist zum Ziel der Gewährleistung eines wirksamen Schutzes der betroffenen Personen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten und zur praktischen Wirksamkeit der materiellen Bestimmungen der DS-GVO festzustellen, dass eine Unterlassungsklage unbestreitbar zur Einhaltung dieser Bestimmungen und damit dazu beiträgt, die Rechte der betroffenen Personen zu stärken und ihnen ein hohes Schutzniveau zu gewährleisten. Im Übrigen kann sich eine Unterlassungsklage für die Gewährleistung dieses Schutzes als besonders wirksam erweisen, da sie es ermöglicht, zahlreiche Verletzungen der Rechte der von der Verarbeitung ihrer personenbezogenen Daten betroffenen Personen zu verhindern. Nach alledem sind die

Bestimmungen der DS-GVO dahin auszulegen, dass sie einer nationalen Regelung nicht entgegenstehen, die – neben den Eingriffsbefugnissen der zur Überwachung und Durchsetzung dieser Verordnung zuständigen Aufsichtsbehörden und den auf die DS-GVO gestützten Rechtsschutzmöglichkeiten der betroffenen Personen – die Befugnis einräumt, wegen Verstößen gegen die DS-GVO gegen den Verletzer im Wege einer Unterlassungsklage vor den Zivilgerichten vorzugehen (vgl. EuGH (Große Kammer), Urteil vom 04.10.2024, Rs. C-21/23, NJW 2025, 33, Rn. 52 - 73). Die Entscheidung des EuGH erging zu einer wettbewerbsrechtlichen Unterlassungsklage. Kann aber ein Wettbewerber Verstöße gegen die DS-GVO mittels Unterlassungsklage nach nationalem Recht geltend machen, so muss dies erst recht für die von der Verletzung der DS-GVO betroffene Person gelten.

b)

Die Voraussetzungen des Unterlassungsanspruchs sind erfüllt.

aa)

Der Verstoß gegen ein Schutzgesetz i.S. des § 823 Abs. 2 S. 1 BGB begründet – soweit Wiederholungsgefahr besteht – einen Unterlassungsanspruch entsprechend § 1004 Abs. 1 BGB. Demnach ist derjenige, der gegen ein den Schutz eines anderen bezweckendes Gesetz i.S. des § 823 Abs. 2 S. 1 BGB verstößt, dem anderen entsprechend § 1004 Abs. 1 BGB zur Unterlassung verpflichtet (BGH, Beschluss vom 26.09.2023, Az. VI ZR 97/22, GRUR 2023, 1724, Rn. 26; BGH, Urteil vom 17.07.2008, Az. I ZR 219/05, GRUR 2008, 996, Rn. 12, 13).

(1)

Schutzgesetz i.S. des § 823 Abs. 2 S. 1 BGB ist jede Rechtsnorm, die zumindest auch dazu dienen soll, den Einzelnen oder einzelne Personenkreise gegen die Verletzung eines bestimmten Rechtsguts zu schützen (BGH, Urteil vom 17.07.2008, Az. I ZR 219/05, GRUR 2008, 996, Rn. 15).

Bei Art. 6 DS-GVO handelt es sich nach dem oben Gesagten um ein Schutzgesetz im Sinne des § 823 Abs. 2 S. 1 BGB.

(2)

Mit der streitgegenständlichen Datenverarbeitung hat die Beklagte gegen Art. 5 Abs. 1, Art. 6 DS-GVO verstoßen.

(a)

Der zeitliche (Art. 99 Abs. 2 DS-GVO) und räumliche (Art. 3 Abs. 1 DS-GVO) Anwendungsbereich der Datenschutz-Grundverordnung ist eröffnet. Die Verordnung ist auch sachlich anwendbar (Art. 2 Abs. 1 DS-GVO).

(b)

Die Beklagte hat personenbezogene Daten der Klägerin verarbeitet.

Datenverarbeitung ist gemäß Art. 4 Nr. 2 DSGVO jeder Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben
- das Erfassen
- die Organisation
- das Ordnen
- die Speicherung
- die Anpassung
- die Veränderung
- das Auslesen
- das Abfragen
- die Verwendung
- die Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung
- der Abgleich
- die Verknüpfung
- die Einschränkung
- das Löschen oder die Vernichtung

Das ist vorliegend der Fall.

Die Beklagte hat nicht bestritten, dass sie personenbezogene Daten der Klägerin auf Webseiten und Apps mittels ihrer Business Tools von Drittunternehmen erhalten, diese gespeichert und zu mehreren Zwecken verarbeitet hat. Sie hat lediglich bestritten, dass sie diese Daten zu dem Zweck der Bereitstellung personalisierter Werbung nutzt.

Die Verarbeitung liegt daher erstens in der Erhebung personenbezogener Daten der Nutzer, wenn diese Nutzer Websites oder Apps aufrufen und dort gegebenenfalls Informationen eingeben, indem sie sich registrieren oder Online-Bestellungen aufgeben, zweitens in der Verknüpfung

dieser Daten mit dem jeweiligen Nutzerkonto des sozialen Netzwerks und drittens in der Verwendung dieser Daten (EuGH, Urteil vom 04.07.2023, Rs. C-252/21, Rn. 71, zit. nach juris).

Die Klägerin hat in ihrer persönlichen Anhörung folgende Webseiten und Apps angegeben, die sie besucht habe, auf denen die Business Tools installiert waren: idealo, preisvergleich, ikea, otto, adidas, shop-apotheke, docmorris, jameda, paypal.

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

Es ist auch davon auszugehen, dass weitere personenbezogene Daten der Klägerin auf anderen Webseiten und Apps von der Beklagten verarbeitet wurden und werden. Es kann dahinstehen, ob von der Klägerin verlangt werden kann, sich auch noch an weitere Webseiten und Apps zu erinnern, die sie in den letzten Jahren genutzt hat. Denn jedenfalls ist ihr die Recherche nicht möglich, ob auf diesen die Business Tools der Beklagten installiert waren oder sind. Demgegenüber ist es der Beklagten unschwer möglich, in ihrem Datenbestand zu sehen, welche Daten von welchen Drittwebseiten und -Apps sie verarbeitet hat. Es ist auch im Übrigen nach allgemeiner Lebenserfahrung davon auszugehen, dass die Klägerin weitere Webseiten und Apps genutzt hat, auf denen die Business Tools der Beklagten installiert waren. Die Beklagte hat hierzu selbst vortragen, solche Tools würden durch Millionen von größeren und kleineren Organisationen auf der ganzen Welt genutzt und seien allgegenwärtig und integraler Bestandteil der alltäglichen Internetnutzung.

Auch für den Einwand der Beklagten, dass es sich teilweise um mit der Eigenart des Internets verbundene Daten handelt, ist der Anwendungsbereich eröffnet, dessen sich der Verordnungsgeber bewusst war, indem er feststellte: Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren (Erwägungsgrund 30).

Dabei ist Gegenstand dieses Verfahrens offensichtlich nach den Anträgen und dem Vortrag der Klägerin jegliche Verarbeitung jeglicher personenbezogener Daten zu jeglichen Zwecken und nicht nur die Verarbeitung der von der Beklagten erhobenen und bei ihr gespeicherten Daten zu dem Zweck der Anzeige personalisierter Werbung.

Der Streitgegenstand wird bestimmt durch das Rechtsschutzbegehren (Antrag), in dem sich die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt (Anspruchsgrund), aus dem der Kläger die begehrte Rechtsfolge herleitet (§ 253 II Nr. 2 ZPO). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören. Vom Streitgegenstand werden damit alle materiell-rechtlichen Ansprüche erfasst, die sich im Rahmen des gestellten Antrags aus dem zur Entscheidung unterbreiteten Lebenssachverhalt herleiten lassen (BGH, Urteil vom 18.11.2024, VI ZR 10/24, NJW 2025, 298, Rn. 17).

Es ist daher nicht relevant, dass die Beklagte bewusst versucht, den Streitgegenstand und damit auch ihren Vortrag auf einzelne Teilaspekte ihrer Datenverarbeitung zu verkürzen.

(c)

Die Beklagte ist ab dem Zeitpunkt der Erfassung der Daten der Klägerin durch die streitgegenständlichen Business Tools Verantwortliche im Sinne der DS-GVO.

Verantwortlicher ist gemäß Art. 4 Nr. 7 DS-GVO u.a. eine juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche, Art. 26 Abs. 1 DS-GVO. Ungeachtet der Einzelheiten einer Vereinbarung zwischen den gemeinsam Verantwortlichen kann die betroffene Person ihre Rechte im Rahmen der DS-GVO bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Die Beklagte hat die streitgegenständlichen Business Tools, mit denen die Daten der Klägerin auf den Webseiten und Apps von Drittanbietern erfasst werden, selbst hergestellt und zum Zwecke der Erhebung und Übermittlung der Daten den Drittanbietern zur Verfügung gestellt. Sie hat daher über die Zwecke und Mittel der Datenverarbeitung mitentschieden und ist damit Verantwortliche (vgl. EuGH, Urteil vom 29.07.2019, Rs. C-40/17, MMR 2019, 579, Rn. 76 - 81).

(d)

Die Datenverarbeitung war nicht rechtmäßig.

Bei Verstößen gegen die Vorschriften der Art. 5–11 DS-GVO, mithin des zweiten Kapitels der Datenschutz-Grundverordnung, die Grundsätze für die Verarbeitung von Daten aufstellen, liegt zu-

gleich eine unrechtmäßige Datenverarbeitung vor (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 24, m.w.N.).

Gemäß Art. 5 Abs. 1 a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz). Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (Rechenschaftspflicht), Art. 5 Abs. 2 DS-GVO.

Gemäß Art. 6 Abs. 1 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der dort genannten Bedingungen erfüllt ist. Die Beklagte hat jedoch keinen Rechtfertigungsgrund substantiiert vorgetragen.

Daneben ist auch der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 c) DS-GVO verletzt (vgl. mit ausführlicher Begründung zum streitgegenständlichen Sachverhalt: EuGH, Urteil vom 04.10.2024, Rs. C-446/21, GRUR-RS 2024, 26053, Rn. 49 - 65).

(3)

Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr ist gegeben. Der begangene Verstoß der Beklagten begründet die tatsächliche Vermutung für seine Wiederholung (BGH, Urteil vom 17.07.2008, Az. I ZR 219/05, GRUR 2008, 996, Rn. 32). Sie hat auf das außergerichtliche Schreiben der Klägerin nicht reagiert. Im gerichtlichen Verfahren macht sie weiterhin die Berechtigung der Datenverarbeitung geltend.

bb)

Zugleich stellt die von der Beklagten vorgenommene Datenverarbeitung einen Eingriff in das allgemeine Persönlichkeitsrecht in der Ausprägung des Rechts auf informationelle Selbstbestimmung gemäß § 823 Abs. 1 i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG, das dem Einzelnen die Befugnis gibt, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, dar, was einen Unterlassungsanspruch begründet (vgl. BGH, Beschluss vom 26.09.2023, Az. VI ZR 97/22, GRUR 2023, 1724, Rn. 26; BGH, Urteil vom 15.09.2015, Az. VI ZR 175/14, NJW 2016, 789).

Der Eingriff ist auch rechtswidrig, da das durch Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK gewährleistete Interesse der Klägerin am Schutz ihrer Persönlichkeit und ihrer Daten das Gewinnerzielungsinteresse der Beklagten überwiegt.

Für die Wiederholungsgefahr gilt das oben Gesagte.

2.

Die Klägerin hat gemäß Art. 18 Abs. 1 b) DS-GVO das Recht, von der Beklagten die Einschränkung der Verarbeitung der bisher erhobenen und bei ihr gespeicherten Daten zu verlangen, da die Verarbeitung nach dem oben Gesagten unrechtmäßig ist und die Klägerin zunächst die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt.

Dies hat gemäß Art. 18 Abs. 2 DS-GVO zur Folge, dass die personenbezogenen Daten - von ihrer Speicherung abgesehen - nur mit Einwilligung der Klägerin oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedsstaates verarbeitet werden.

Einen Ausnahmefall hat die Beklagte nicht geltend gemacht.

3.

Die Klägerin hat gemäß Art. 17 Abs. 1 d) DS-GVO das Recht, von der Beklagten zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und die Beklagte ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, da nach dem oben Gesagten die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

Nach ihrer Wahl ist die Beklagte bzgl. der personenbezogenen Daten in Ziff. 1 b) und c) als Minus zur Löschung zur Anonymisierung der Daten berechtigt.

4.

Die Klägerin hat einen Anspruch auf Ersatz eines immateriellen Schadens in Höhe von 5.000,00 € gemäß Art. 82 Abs. 1 DS-GVO.

Gemäß Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen.

Nach der Rechtsprechung des EuGH erfordert ein Schadensersatzanspruch i.S.d. Art. 82 Abs. 1 DS-GVO einen Verstoß gegen die Datenschutz-Grundverordnung, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden

und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind. Die Darlegungs- und Beweislast für diese Voraussetzungen trifft die Person, die auf der Grundlage von Art. 82 Abs. 1 DS-GVO den Ersatz eines (immateriellen) Schadens verlangt. Nicht nachzuweisen hat die betroffene Person im Rahmen eines Schadensersatzanspruchs nach Art. 82 I DS-GVO ein Verschulden des Verantwortlichen. Art. 82 DS-GVO sieht vielmehr eine Haftung für vermutetes Verschulden vor, die Exkulpation obliegt nach Art. 82 Abs. 3 DS-GVO dem Verantwortlichen (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 21, m.w.N.).

a)

Wie oben bereits festgestellt, hat die Beklagte gegen Art. 5 Abs. 1, Art. 6 Abs. 1 DS-GVO verstoßen, indem sie die personenbezogenen Daten des Klägers unrechtmäßig verarbeitet hat.

b)

Der Begriff des „immateriellen Schadens“ ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DS-GVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren. Dabei soll nach Erwägungsgrund 146 S. 3 DS-GVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der DS-GVO reicht nach der Rechtsprechung des EuGH jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – iSe eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich. Es ist nicht erforderlich, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat. Jedoch ist die betroffene Person verpflichtet, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle bedeutet nicht, dass eine Person, die von einem Verstoß gegen die Datenschutz-Grundverordnung betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden iSv Art. 82 dieser Verordnung darstellen. Allerdings kann schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert. Im ersten Satz des 85. Erwägungsgrundes der DS-GVO heißt es, dass „(e)ine Verletzung des Schutzes personenbezogener Daten ... – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen (kann), wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung,

Identitätsdiebstahl oder -betrug, finanzielle Verluste ... oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person“. Aus dieser beispielhaften Aufzählung der „Schäden“, die den betroffenen Personen entstehen können, geht nach der Rechtsprechung des Gerichtshofs hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen Verlust der Kontrolle („the mere loss of control“, „la simple perte de contrôle“) über ihre eigenen Daten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte. Freilich muss auch insoweit die betroffene Person den Nachweis erbringen, dass sie einen solchen – das heißt in einem bloßen Kontrollverlust als solchem bestehenden – Schaden erlitten hat. Ist dieser Nachweis erbracht, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 28 - 31, m.w.N.).

Der Betroffene, der Ersatz des immateriellen Schadens verlangt, muss folglich geltend machen (und ggf. nachweisen), dass der Verstoß gegen die Datenschutz-Grundverordnung negative Folgen für ihn gehabt hat, die einen immateriellen Schaden darstellen. Für eine ordnungsgemäße Darlegung muss das Gericht nach allgemeinen Grundsätzen anhand des Parteivortrags beurteilen können, ob die gesetzlichen Voraussetzungen der an eine Behauptung geknüpften Rechtsfolgen erfüllt sind. Ein Sachvortrag zur Begründung eines Anspruchs ist demnach bereits dann schlüssig und erheblich, wenn die Partei Tatsachen vorträgt, die in Verbindung mit einem Rechtsatz geeignet und erforderlich sind, das geltend gemachte Recht als in der Person der Partei entstanden erscheinen zu lassen. Die Angabe näherer Einzelheiten ist nicht erforderlich, soweit diese für die Rechtsfolgen nicht von Bedeutung sind. Das Gericht muss nur in die Lage versetzt werden, aufgrund des tatsächlichen Vorbringens der Partei zu entscheiden, ob die gesetzlichen Voraussetzungen für das Bestehen des geltend gemachten Rechts vorliegen (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 33 - 34, m.w.N.).

Diesen Darlegungserfordernissen hat das Vorbringen der Klägerin Genüge getan.

Sie hat dargelegt, die o.g. Webseiten besucht zu haben. Zudem ist nach dem oben Gesagten davon auszugehen, dass die Beklagte auch eine Vielzahl weiterer Daten von anderen Webseiten und Apps verarbeitet hat.

Weiter hat die Klägerin im Rahmen ihrer persönlichen Anhörung mitgeteilt: Sie habe festgestellt,

dass sehr viele Daten gesammelt werden auf Seiten, von denen ihr das nicht bewusst gewesen sei. Es sei ihr klar, dass der Algorithmus, wenn sie auf Instagram oder Facebook sei und dort etwas anklicke, das erfasse und ihr entsprechende andere Sachen vorschlage. Dass aber sehr persönliche Daten gesammelt werden, finde sie nicht schön. Das betreffe gerade Sachen wie politische Themen. Sie gehe auch auf Apothekenseiten, wo sie Medikamente bestelle. Das habe die Beklagte gar nichts anzugehen. Man könne daraus vielleicht auch gesundheitliche Rückschlüsse ziehen. Sie wisse nicht, wofür die Daten verwendet werden. Sie mache sich dann Gedanken, was sie suche und auf welche Seiten sie gehe. Sie frage sich, warum das so wichtig sei, diese Daten zu sammeln. Es koste sie viel Zeit. Sie versuche, sämtliche Cookies abzulehnen. Teilweise sei das uferlos. Es beschäftige sie extrem. Sie könne es aber nicht vermeiden. Sie nutze das Internet beruflich und privat. Woher solle sie wissen, wo noch Daten gesammelt werden? Sie frage sich, wie sie bestimmen könne, was gesammelt werde, wie sicher es sei und wie die Daten dann weiter verwendet würden. Sie erteile doch keine pauschale Einwilligung übergreifend für alle Seiten. Sie würde gern selbst mitbestimmen, vor allem, wenn es um sensible Themen gehe wie politische Dinge. Sie sollte auch ein Mitspracherecht haben, was weitergegeben wird. Sie habe versucht, die Einstellungen der Beklagten durchzulesen. Es sei sehr undurchsichtig gewesen. Es sei ein Riesenwust gewesen. Sie verstehe nicht, warum die Beklagte über ihren Geldtransfer Bescheid wissen müsse. Sie frage sich, welche Daten gesammelt werden. Sie frage sich, wo sie Informationen herbekomme, wo die Business Tools installiert seien. Sie könne es gar nicht selektieren.

Dieses Vorbringen genügt sowohl hinsichtlich des eingetretenen Kontrollverlustes bezüglich seiner oben genannten Daten als auch hinsichtlich der sich hieraus entwickelnden besonderen Befürchtungen und Bemühungen den Anforderungen an einen hinreichend substantiierten Klagevortrag.

c)

Der Schaden in Form des Kontrollverlustes ist auch kausal auf die Datenschutzverletzung der Beklagten zurückzuführen. Die Beklagte hat über mehrere Jahre rechtswidrig eine Vielzahl auf Webseiten und Apps erhobene Daten des Klägers gespeichert und verarbeitet. Auf welchen Webseiten und Apps die Business Tools der Beklagten installiert waren, ist für den Kläger nicht nachvollziehbar, gleiches gilt für die bei der Beklagten vorhandenen Daten. Die Beklagte hat damit den Kontrollverlust über die Daten des Klägers hervorgerufen.

d)

Zu einem etwaigen Ausschluss der Haftung nach Art. 82 Abs. 3 DS-GVO hat die Beklagte nicht vorgetragen.

e)

Die Datenschutz-Grundverordnung enthält keine Bestimmung über die Bemessung des aus Art. 82 Abs. 1 DS-GVO geschuldeten Schadensersatzes. Die Bemessung richtet sich vielmehr entsprechend dem Grundsatz der Verfahrensautonomie nach den innerstaatlichen Vorschriften über den Umfang der finanziellen Entschädigung. In Deutschland ist somit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden. Die innerstaatliche Verfahrensautonomie bei der Ermittlung des nach Art. 82 DS-GVO zu ersetzenden Schadens unterliegt freilich mehreren aus dem Unionsrecht folgenden Einschränkungen. Die Modalitäten der Schadensermittlung dürfen bei einem unter das Unionsrecht fallenden Sachverhalt nicht ungünstiger sein als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz). Auch dürfen sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz). In Anbetracht der Ausgleichsfunktion des in Art. 82 DS-GVO vorgesehenen Schadensersatzanspruchs, wie sie in Erwägungsgrund 146 S. 6 DS-GVO zum Ausdruck kommt, ist eine auf Art. 82 DS-GVO gestützte Entschädigung in Geld als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DS-GVO dagegen nicht erfüllen. Folglich darf nicht die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, und ob der Verantwortliche vorsätzlich gehandelt hat, berücksichtigt werden. Im Ergebnis soll die Höhe der Entschädigung zwar nicht hinter dem vollständigen Ausgleich des Schadens zurückbleiben, sie darf aber auch nicht in einer Höhe bemessen werden, die über den vollständigen Ersatz des Schadens hinausginge. Ist der Schaden gering, ist daher auch ein Schadensersatz in nur geringer Höhe zuzusprechen. Dies gilt auch unter Berücksichtigung des Umstandes, dass der durch eine Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung. Bei Ausübung seines Schätzungsermessens hat das Gericht zu beachten: Ist nach den Feststellungen des Gerichts allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten gegeben, weil weitere Schäden nicht nachgewiesen sind, hat der Tatrichter bei der Schätzung des Schadens insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten (vgl. Art.

9 | DS-GVO) und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Weiter hat er die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle in den Blick zu nehmen (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 93 - 100, m.w.N.).

Bei der Bemessung des immateriellen Schadensersatzes ist vorliegend insbesondere zu berücksichtigen:

Die Beklagte verarbeitet seit mehreren Jahren personenbezogene Daten in nicht erkennbarem Umfang, wobei nach der allgemeinen Lebenserfahrung zur Internetnutzung und der oben genannten Annahme einer weiten Verbreitung der Business Tools davon auszugehen, dass die Daten einen weiten Bereich der privaten Lebensgestaltung der Klägerin umfassen. Der Umfang der bei der Beklagten gespeicherten Daten ist auch nach mehreren Auskunftsverlangen der Klägerin vollkommen unklar und kann aufgrund der erheblichen Einschränkungen (nur Angabe der Webseite, nur Daten, bei denen die Klägerin gleichzeitig auf Facebook eingeloggt war, nur Daten der letzten Monate) auch über die von der Beklagten zur Verfügung gestellte Funktion nicht annähernd erfasst werden. Der EuGH hat hierzu festgestellt: Die Verarbeitung ist besonders umfassend, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Online-Aktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von der Beklagten aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird (Urteil vom 04.07.2023, Rs. C-252/21, Rn. 118).

Hervorzuheben ist, dass die Beklagte sich für die Rechtmäßigkeit der massiven Datenerhebung, -speicherung und -verarbeitung auf keinerlei Rechtsgrundlage, insbesondere nicht auf eine Einwilligung der Klägerin beruft, die Klägerin somit nicht aufgrund ihrer Account-Einstellungen jedenfalls mit der Datenverarbeitung der Beklagten rechnen musste.

Mit den Webseiten shop-apotheke, docmorris und jameda sind auch nach Art. 9 Abs. 1 DS-GVO besonders geschützte Gesundheitsdaten erfasst (EuGH, Urteil vom 04.10.2024, Rs. C-21/23, MMR 2024, 1022).

Demgegenüber ist zu berücksichtigen, dass die Klägerin - unter Darlegung nachvollziehbarer Gründe - bewusst von der Geltendmachung eines Auskunftsanspruchs nach Art. 15 DS-GVO abgesehen und daher das Ausmaß der Daten für das Gericht im Unklaren gelassen hat.

Wenngleich die Beklagte sich das Recht zur Weitergabe der Daten vorbehalten hat, ist eine solche nicht vorgetragen.

Nach alledem hält das Gericht einen Betrag in Höhe von 5.000,00 € für angemessen.

Auch bei der Beurteilung einer Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts nach den nationalen Rechtsvorschriften des § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, Art. 2 Abs. 1 GG (vgl. BGH, Urteil vom 12.03.2024, Az. VI ZR 1370/20, NJW 2024, 2836, Rn. 69 ff.) wäre dieser Betrag angemessen.

5.

Die Klägerin hat einen Anspruch auf Freistellung von den vorgerichtlichen Rechtsanwaltskosten in Höhe von 627,13 € aus Art. 82 Abs. 1 DS-GVO, § 249 Abs. 1, 257 S. 1 BGB.

Die Kosten der Rechtsverfolgung und deshalb auch die Kosten eines mit der Sache befassten Rechtsanwalts gehören, soweit sie zur Wahrnehmung der Rechte erforderlich und zweckmäßig waren, grundsätzlich zu dem wegen einer unerlaubten Handlung zu ersetzenden Schaden. Dabei ist maßgeblich, wie sich die voraussichtliche Abwicklung des Schadensfalls aus der Sicht des Geschädigten darstellt. Ist die Verantwortlichkeit für den Schaden und damit die Haftung von vornherein nach Grund und Höhe derart klar, dass aus der Sicht des Geschädigten kein vernünftiger Zweifel daran bestehen kann, dass der Schädiger ohne weiteres seiner Ersatzpflicht nachkommen werde, so wird es grundsätzlich nicht erforderlich sein, schon für die erstmalige Geltendmachung des Schadens gegenüber dem Schädiger einen Rechtsanwalt hinzuzuziehen. In derart einfach gelagerten Fällen kann der Geschädigte grundsätzlich den Schaden selbst geltend machen, so dass sich die sofortige Einschaltung eines Rechtsanwalts nur unter besonderen Voraussetzungen als erforderlich erweisen kann, wenn etwa der Geschädigte aus Mangel an geschäftlicher Gewandtheit oder sonstigen Gründen wie etwa Krankheit oder Abwesenheit nicht in der Lage ist, den Schaden selbst anzumelden. Nach diesen Maßstäben kann im vorliegenden Fall ein materiell-rechtlicher Kostenerstattungsanspruch aus Art. 82 Abs. 1 DS-GVO für die anwaltliche Tätigkeit nicht verneint werden. Dabei ist auch zu berücksichtigen, dass zum Zeitpunkt des anwaltlichen Schreibens eine Vielzahl von Rechtsfragen in Zusammenhang mit der DS-GVO weder durch den Gerichtshof noch durch die nationalen Gerichte geklärt war (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24, NJW 2025, 298, Rn. 78 - 80, m.w.N.).

Das ist vorliegend der Fall. Die Klägerin richtete sich gegen ein im Ausland ansässiges Unternehmen auf der Grundlage europäischer Vorschriften. Es war daher notwendig, dass sie sich anwaltlicher Hilfe bediente. Im Zeitpunkt des Anwaltsschreibens waren auch noch nicht dem Diesel- oder Scraping-Sachverhalt ähnlich viele Verfahren in Masse geltend gemacht, vorgerichtlich abgelehnt und gerichtlich anhängig, so dass eine außergerichtliche Klärung nicht von vornherein aussichtslos war.

Ausweislich des als Anlage K3 vorgelegten Schreibens vom 10.07.2023, dessen Erhalt die Beklagte nicht substantiiert bestritten hat (sie gibt nur an, sie habe keine Aufzeichnungen, es existiert allerdings ein Antwortschreiben der Beklagtenseite) waren Gegenstand des außergerichtlichen Schreibens teilweise auch die nun abschließend mit der Klage verfolgten Ansprüche, so dass die Rechtsanwaltsgebühren, soweit inhaltlich identisch und schließlich erfolgreich (Löschung, Schmerzensgeld), aus 6.000,00 € (siehe sogleich zum Streitwert unter V.) zu berechnen sind und daher eine 1,3-Geschäftsgebühr zzgl. Auslagen und Mehrwertsteuer, somit 627,13 € betragen.

6.

Der Zinsanspruch hinsichtlich des Schadensersatzes ergibt sich aus §§ 291, 288 Abs. 1, 187 Abs. 1 analog BGB.

Das erst- und einmalige anwaltliche Aufforderungsschreiben stellt keine Mahnung im Sinne des § 286 Abs. 1 BGB. Die einseitige Bestimmung eines Erklärungs- oder Zahlungsziels fällt nicht unter § 286 Abs. 2 Nr. 1 BGB (BGH, Urteil vom 25.10.2007, Az. III ZR 91/07, NJW 2008, 50).

Als Rechtshängigkeitsbeginn wurde gemäß § 189 ZPO die Verteidigungsanzeige vom 02.05.2024 herangezogen, da kein vorheriger Zustellnachweis zur Akte gelangt ist.

V.

Die Streitwertfestsetzung in Höhe von insgesamt 8.000,00 € beruht auf §§ 63 Abs. 2 S. 1, 39 Abs. 1, 40, 48 Abs. 1 S. 1, Abs. 2 S. 1 GKG.

Die Klägerin gab bei Klageerhebung den Streitwert wie folgt an:

- | | |
|------------------------------|---|
| 1. Feststellungsanspruch | 5.000,00 € |
| 2. Unterlassung Erhebung | 5.000,00 € |
| 3. Unterlassung Verarbeitung | 5.000,00 € |
| 4. Schadensersatzanspruch | 1.000,00 € (in Absprache mit dem Rechtsschutzversicherer, angemessen seien tatsächlich mindestens 5.000,00 €) |

Das Gericht hält folgende Streitwerte für angemessen:

- | | |
|------------------------|----------|
| 1. Feststellungsantrag | 500,00 € |
|------------------------|----------|

Da dieser keine über die weiteren Anträge hinaus gehende Bedeutung hat.

2. Unterlassungsanspruch zukünftige Datenerhebung 5.000,00 €

Entsprechend dem für die bisherige Verletzung begehrten Schadensersatzanspruch.

3. Unterlassung Verarbeitung 500,00 €

Geringeres Interesse, da die Klägerin sich gerade gegen die ursprüngliche und weitere Datenverarbeitung richtet und bisher ausdrücklich von der klageweisen Durchsetzung eines Auskunftsanspruchs abgesehen hat. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftersuchen reagieren zu können (Erwägungsgrund 64 zur DS-GVO).

4. Verpflichtung Löschung und Anonymisierung 1.000,00 €

5. Zahlungsanspruch 1.000,00 €

Die zwischenzeitlich fallengelassenen Hilfsanträge sind gemäß § 45 Abs. 1 S. 2 GKG nicht zu berücksichtigen. Nebenforderungen sind gemäß § 43 Abs. 1 GKG nicht zu berücksichtigen.

VI.

1.

Ausgehend von dem genannten Streitwert ergeht die Kostenentscheidung gemäß §§ 91 Abs. 1, 92 Abs. 1 ZPO.

2.

Die Entscheidung über die vorläufige Vollstreckbarkeit ergeht für den Kläger gemäß § 709 ZPO und für die Beklagte gemäß §§ 708 Nr. 11, 711 ZPO.

3.

Die Zwangsmittellandrohung beruht auf § 890 ZPO. Ausreichend ist die Angabe der Art und des Höchstmaßes (Musielak/Voit/Lackmann, ZPO, § 890, Rn. 17).

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht Augsburg
Am Alten Einlaß 1
86150 Augsburg

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem vierten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, 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, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen

- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:

- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils

geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

[REDACTED]

Richterin am Landgericht

Verkündet am 28.03.2025

gez.

[REDACTED], JAng

Urkundsbeamtin der Geschäftsstelle



Für die Richtigkeit der Abschrift
Augsburg, 28.03.2025

[REDACTED], JAng

Urkundsbeamtin der Geschäftsstelle