8 O 439/23

Landgericht Siegen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

des Herrn [redacted]

Klägers,

Prozessbevollmächtigte: Rechtsanwälte BK Automotive Baumeister & Kollegen Verbraucherkanzlei , Viktoria-Luise-Platz 7, 10777 Berlin,

gegen

die Meta Platforms Ireland Ltd., vertreten durch Herrn Rick Kelley (Director), 4 Grand Canal Sqare, Grand Canal Harbour, Dublin, Irland,

Beklagte,

Prozessbevollmächtigte: [redacted],

hat die 8. Zivilkammer des Landgerichts Siegen
auf die mündliche Verhandlung vom 04.09.2025
durch den Vorsitzenden Richter am Landgericht Dr. [redacted] als Einzelrichter

für Recht erkannt:

1. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis

zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten – und Apps außerhalb der Netzwerke der Beklagten die folgenden personenbezogenen Daten der Klagepartei mit Hilfe der Meta Business Tools zu erheben, an die Server der Beklagten weiterzugeben, die Daten dort zu speichern und anschließend zu verwenden:

- die URLs der von der Klägerpartei besuchten Webseiten samt ihrer Unterseiten;

- die Namen der von der Klägerseite genutzten Apps;

- den Zeitpunkt des Besuchs der jeweiligen Webseite bzw. App.

2. Die Beklagte wird verurteilt, an den Kläger 5.000,00 € nebst Zinsen hieraus in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 05.09.2023 zu zahlen.

3. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten seiner Prozessbevollmächtigten in Höhe von 627,13 € freizustellen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits haben der Kläger zu 38 % und die Beklagte zu 62 % zu tragen.

6. Das Urteil ist vorläufig vollstreckbar. Für die klagende Partei im Hinblick auf die Vollstreckung des Tenors unter Ziffer 1 gegen Sicherheitsleistung in Höhe von 600 € und im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages. Der klagenden Partei bleibt nachgelassen, die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung

Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrages leistet.

Der Streitwert wird auf 12.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten um datenschutzrechtliche Unterlassungs-, Löschungs- und Schadensersatzansprüche.

Die klagende Partei nutzt seit dem 26.11.2008 das von der Beklagten betriebene soziale Netzwerk Facebook mit der E-Mail-Adresse [redacted] wobei die Beklagte bis zum 21.07.2021 noch unter „Facebook Ireland Ltd." firmierte. Seit seiner Registrierung nutzte der Kläger das Netzwerk zu privaten Zwecken. Als Gegenleistung für die Nutzung des Netzwerks fordert die Beklagte kein Geld. Der Klagepartei wird bei Nutzung des Netzwerks Werbung angezeigt, die auf ihren Interessen basiert, welche die Algorithmen der Meta Ltd. aus den Tätigkeiten der Klagepartei in Facebook sowie den sozialen Kontakten, die sie in Facebook pflegt, extrahieren können. Wahlweise können die Nutzer seit November 2023 ein Abo-Modell wählen, bei dem sie gegen Zahlung einer monatlichen Gebühr die Anzeige von Werbung abschalten können.

Die Beklagte ist Entwicklerin der sog. „Meta Buisness Tools", namentlich „Meta Pixel", „App Events über Facebook-SDK" und „Conversions API" sowie „App Events API". Diese Meta Business Tools stellt sie Webseitenbetreibern und App-Anbietern zur Verfügung, die diese auf ihrer Webseite bzw. in ihrer App integrieren können. Dazu müssen die Webseitenbetreiber und die Hersteller der App die Nutzungsbedingungen der Beklagten für die Business Tools akzeptieren. Unter anderem ist darin unter „3. Besondere Bestimmungen für die Nutzung bestimmter Business-Tools“ folgendes geregelt:

„c. Du sicherst zu und gewährleistest, dass du einen stabilen und hinreichend auffälligen Hinweis für Nutzer bezüglich dem Erfassen, Teilen sowie der Verwendung der Business-Tool-Daten bereitgestellt hast, der mindestens folgende Angaben enthalten muss: i. Für Websites: Einen eindeutigen und auffälligen Hinweis auf jeder Seite der Website, auf der unsere Pixel genutzt werden. Ein solcher Hinweis hat auf eine klare Erläuterung zu verlinken, die besagt, (a) dass Dritte, einschließlich Meta, möglicherweise Cookies, Web Beacons und sonstige Speichertechnologien nutzen, um Informationen von deinen Websites und anderen Stellen im Internet zu erfassen oder zu erhalten, und diese Informationen dann für die Bereitstellung von Messlösungen, das Anzeigen-Targeting und die Auslieferung von Anzeigen verwenden, (b) wie Nutzer sich für ein Opt-out bezüglich der Erfassung und

Verwendung von Informationen für das Anzeigen-Targeting entscheiden können und (c) wo Nutzer auf einen Mechanismus zugreifen können, um eine solche Auswahl zu treffen (z. B. durch Bereitstellung von Links zu http://www.aboutads.info/choices und http://www.youronlinechoices.eu/). ii. Für Apps: Einen eindeutigen und auffälligen Link, der in deinen App-Einstellungen oder in jeder Datenrichtlinie und aus jedem Store bzw. von jeder Website aus, in der/dem deine App vertrieben wird, leicht zugänglich ist. Dieser Link muss auf eine klare Erläuterung verlinken, die besagt, (a) dass Dritte, einschließlich Meta, möglicherweise Informationen von deiner App und anderen Apps erfassen bzw. erhalten und diese Informationen dann für die Bereitstellung von Messlösungen und das Anzeigen-Targeting und die Auslieferung von Anzeigen verwenden, und (b) wie und wo Nutzer sich für ein Opt-out bezüglich der Erfassung und Verwendung von Informationen für das Anzeigen-Targeting entscheiden können.

d. In Rechtsordnungen, in denen für das Speichern von Cookies oder sonstigen Informationen auf dem Gerät eines Endnutzers und das Zugreifen auf diese eine informierte Einwilligung erforderlich ist (wie u. a. in der Europäischen Union), musst du in nachprüfbarer Weise sicherstellen, dass ein Endnutzer alle erforderlichen Einwilligungen erteilt, bevor du Meta-Business-Tools nutzt, um Meta das Speichern von Cookies oder sonstigen Informationen auf dem Gerät des Endnutzers und den Zugriff auf diese zu ermöglichen. (Vorschläge zur Implementierung von Einwilligungsmechanismen findest du in unserer Ressource zur Cookie-Einwilligung.).“

Wegen der weiteren Einzelheiten und des inhaltss der Business Tool Nutzungsbedingungen wird auf die Anlage B5 (Bl.604 ff. d. A.) Bezug genommen

Genereller Zweck der Meta Business Tools ist es unter anderem, die Effektivität von Werbeanzeigen von Drittunternehmen auf den von Meta angebotenen Plattformen wie Instagram oder Facebook zu erhöhen und zu messen. Sobald eine Nutzerin oder ein Nutzer des Netzwerkes Instagram bzw. Facebook die Homepage einer Firma, welche derartigen Business Tools einsetzt, besucht, übermitteln die Drittfirmen über die derart eingebundenen Business Tools insbesondere die folgenden Daten an die Beklagte - und zwar unabhängig davon, ob die Nutzerin oder der Nutzer zu diesem Zeitpunkt die App von Instagram oder Facebook aktiviert hat:

- immer jedenfalls solche technischen Daten, die der Beklagten mit einer Wahrscheinlichkeit von über 99 % eine Identifizierung der jeweiligen Nutzerin bzw. des jeweiligen Nutzers innerhalb der Metasysteme erlaubt (im Folgenden: „technische Standarddaten“), sowie das Datum, dass und wann die fragliche Drittseite mit diesen technischen Parametern aufgesucht wurde. Technische

Standarddaten in diesem Sinne sind etwa die mit dem Nutzergerät verknüpfte IP-Adresse, das Betriebssystem des Geräts, die Art des verwendeten Browsers (z. B. Chrome, Firefox, Safari, usw.), dessen Softwareversion, die vom Kunden verwendete Sprache und ob das Gerät des Kunden einen Touchscreen hat und die Parameter dieses Touchscreens;

- unter im Einzelnen streitigen Umständen weitere Daten (im Folgenden „weitere personenbezogene Daten“), insbesondere zur aktuellen und zurückliegenden Aktivität auf der Homepage wie etwa Klicks auf einzelne Artikel oder Buttons, Tastatureingaben, Formulareingaben etc. (sog. „event data“), - wobei Art und Umfang der übermittelten Daten davon abhängt, welches der vorgenannten Business Tools das Drittunternehmen integriert hat und wie sie dieses Tool im Einzelnen einsetzen.

Für den durchschnittlichen Internetnutzer ist nicht erkennbar, ob die jeweilige Webseite mit einem Meta Business Tool ausgestattet worden ist. Die Nutzerinnen und Nutzer von Facebook können dabei über die dortigen Einstellmöglichkeiten Einfluss darauf nehmen, wie die derart bei der Beklagten eingehenden Daten weiterverwendet werden. In der Rubrik Einstellungen können die Nutzerinnen und Nutzer entscheiden, ob sie den Einsatz von „Meta Cookies auf anderen Apps und Webseiten“ erlauben. Die über die Business Tools von den Apps und Homepages an die Beklagten übertragenen Daten werden von der Beklagten wie folgt - und teilweise in Abhängigkeit von dem Vorliegen der in den Einstellungen abgegebenen Einwilligung - weiterverarbeitet:

- mittels der übertragenen technischen Standarddaten wird - soweit, wie ganz regelmäßig, möglich (vgl. oben) - eine bereits von Meta erfasste Person identifiziert. Der Umstand des Besuchs der die Daten übertragenden Homepage bzw. App sowie der entsprechende Zeitpunkt wird sodann dem personenbezogenen Profil dieser Person zugeordnet und gespeichert und reichert dieses Persönlichkeitsprofil entsprechend um diese personenbezogene Information weiter an. Dieser Vorgang erfolgt unstreitig immer und insbesondere und ausdrücklich unstreitig (vgl. Protokoll vom 4.9.2025, Bl. 2230 d. A.) auch dann, wenn die betroffene Person einer Datenübertragung an die Beklagte gegenüber dem Drittanbieter nicht zugestimmt und in die Datenverarbeitung auch gegenüber der Beklagten nicht eingewilligt hat.

- auch die weiteren personenbezogenen Daten werden jedenfalls dann gespeichert und mit den sonstigen gegebenenfalls vorhandenen Daten über den jeweiligen Nutzer zu einem personenbezogenen Profil verbunden, wenn die Nutzerin bzw. der Nutzer in den Einstellungen ihre Zustimmung zur Nutzung „optionaler Cookies“ erteilt hat (vgl. oben). Hat sie diese Zustimmung nicht erteilt, verwendet die Beklagte die Daten für nicht näher bezeichnete „bestimmte Verarbeitungsvorgänge“ nicht und im Übrigen nur „für eingeschränkte Zwecke, wie Sicherheits- und Integritätszwecke“,

einschließlich „zum Zwecke der Überwachung von versuchten Angriffen auf die Systeme von Meta“.

Mit Schreiben ihrer Prozessbevollmächtigten vom 07.08.2023 wandte sich die klagende Partei an die Beklagte und machte Auskunfts-, Löschungs- und Schadensersatzansprüche geltend. Es wurde eine Zahlungsfrist bis zum 04.09.2023 gesetzt. Wegen des weiteren Inhalts wird auf die Anlage K3 (Bl. 197 ff. d. A.) verwiesen. Eine Zahlung durch die Beklagte erfolgte nicht.

Der Kläger behauptet, ihm stünden die gelten gemachten Ansprüche zu, weil die Beklagte illegal Daten verarbeite. Sie spioniere das Privatleben sämtlicher Nutzer von „Facebook“ und „Instagram“ aus. Dies geschehe, indem sie durch ihre „Business Tools“ alle Bewegungen ihrer Nutzer aufzeichne, die diese auf Webseiten oder Apps von Drittanbietern unternehmen würden. Dadurch werde die gesamte Internetpräsenz der Betroffenen gegen deren Willen rechtswidrig aufgezeichnet. Durch die Verwendung der „Business Tools“ werde das Verhalten der Nutzer nicht nur in den sozialen Netzwerken der Beklagten, sondern auch auf Drittwebsites und -Apps analysiert. Die so erworbenen Informationen würden illegal an die Beklagte weitergegeben und von dieser verarbeitet. Die „Business Tools“ seien von den Betreibern der Webseiten und Apps auf deren Netzwerken eingebunden worden, um höhere Werbeeinnahmen zu generieren. Zusätzlich habe die Beklagte weitere Techniken entwickelt (sog. „digitaler Fingerabdruck“), um die Nutzer bzw. deren Verhalten im Internet weitreichend identifizieren und nachverfolgen zu können. Auf zahlreichen Websites würden diese „Business Tools“ der Beklagten im Hintergrund laufen. Eine Liste solcher Webseiten seien den zur Akte gereichten Anlagen K2 (Bl. 185 ff. d.A.), dem Anlagenkonvolut K13 (Bl. 1015 ff. d.A.) sowie der Anlage K14 (Bl. 1017 ff. d.A.) zu entnehmen. Das Nutzerverhalten jedes einzelnen Nutzers, so auch das Nutzungsverhalten des Klägers, werde detailliert aufgezeichnet. Die entsprechenden Daten würden von der Beklagten weltweit in unsichere Drittstaaten weitergeleitet, insbesondere in die USA. Entgegen der Behauptung der Beklagten würden die Daten nicht nur für den Zweck verarbeitet, benutzerdefinierte Werbung auf ihren Plattformen bereitzustellen. Die Beklagte würde die „Business Tools“ vielmehr dazu einsetzen, Daten des Klägers auf Drittwebseiten und -Apps zu erlangen und diese dann weiterzuverarbeiten. Der Kläger habe einer solchen Datenverarbeitung gem. Art. 6 Abs. 1 lit. a DSGVO nicht zugestimmt. Seit dem 25.05.2018 werde der Kläger von der Beklagten überwacht, die seine persönlichen Daten durch die Nutzung der „Business Tools“ rechtswidrig sammele und verarbeite. Die Beklagte könne ihre Verantwortung auch nicht auf Drittunternehmer abwälzen. Diese nutzten gerade die von der Beklagten entwickelten und zur Verfügung gestellten Technologien. Der Kläger habe das Gefühl, im Privatleben ständig durch

die Beklagte überwacht zu werden. Die umfangreiche Datenerhebung der Beklagten im gesamten Internet sei durch keine der in Art. 6-9 DSGVO normierten Rechtsgrundlagen gedeckt. Es liege auch keine wirksame Einwilligung gem. Art. 6. Abs. 1 lit. a, b DSGVO vor. Auch eine Rechtfertigung der Beklagten nach Art. 6 Abs. 1 lit. c-f DSGVO komme nicht in Betracht. Dem Kläger stünden aufgrund der illegalen Datenverarbeitung die beantragten Feststellungs- und Unterlassungsansprüche zu. Weiterhin stünde ihm auch der mit dem Klageantrag zu 5 geltend gemachte Anspruch auf eine Geldentschädigung in Höhe von mindestens 5.000,00 € zu. Bei deren Bemessung sei ein anderer Maßstab anzulegen als bei den sogenannten „Datenleck-Fällen“. In diesen Fällen haben Dritte (Hacker) die Daten der Nutzer abgegriffen. Hier gestalte sich die Konstellation anders als bei den „Datenleck“-Fällen, da die Beklagte die Daten ihrer Nutzer sogar selbst ausspioniere und alle Bewegungen ihrer Nutzer im Internet überwache.

Der Kläger hat seine Anträge mit Schriftsatz vom 14.08.2024 geändert und teilweise zurückgenommen und beantragt zuletzt, wie folgt zu erkennen:

> **1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks ”Facebook” unter der E-Mail-Adresse [redacted] die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem 25.05.2018 nicht gestattet:**
>
> **a) auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der**
>
> **Klagepartei, ob direkt oder in gehashter Form übertragen, d. h. E-Mail der Klagepartei, Telefonnummer der Klagepartei, Vorname der Klagepartei, Nachname der Klagepartei, Geburtsdatum der Klagepartei, Geschlecht der Klagepartei, Ort der Klagepartei, Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID” genannt), IP-Adresse des Clients, User-Agent des Clients (d. h. gesammelte Browserinformationen), interne Klick-ID der Meta Ltd., interne Browser-ID der Meta Ltd., Abonnement-ID, Lead-ID, anon_id, die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid“ genannt) sowie folgende personenbezogene Daten der Klagepartei**
>
> **b) auf Webseiten die URLs der Webseiten samt ihrer Unterseiten der Zeitpunkt des Besuchs der „Referrer“ (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist), die von der Klagepartei auf der Webseite angeklickten Buttons sowie weitere von**

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

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

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

3. Die Beklagte wird verpflichtet, sämtliche unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits verarbeiteten personenbezogenen Daten ab sofort unverändert am gespeicherten Ort zu belassen, d. h. insbesondere diese erst zu löschen, wenn die Klagepartei sie hierzu auffordert, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, und diese bis zu diesem Zeitpunkt nicht zu verändern, intern nicht weiter zu verwenden, und nicht an Dritte weiterzugeben.

4. Die Beklagte wird verpflichtet, sämtliche gem. dem Antrag zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten der Klagepartei auf ihre Aufforderung hin, spätestens jedoch sechs Monate nach rechtskräftigem Abschluss des Verfahrens, vollständig zu löschen und der Klagepartei die Löschung zu bestätigen sowie sämtliche gem. dem Antrag zu 1 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren.

5. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, der aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 05.09.2023, zu zahlen.

6. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 973,66 Euro freizustellen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, der Feststellungsantrag sei mangels Rechtsschutzinteresses schon unzulässig. Im Übrigen sei die Klage unbegründet, weil die behauptete illegale Datenverarbeitung nicht stattfinde. Die Beklagte würde die streitgegenständliche Datenverarbeitung nur vornehmen, wenn der Nutzer ausdrücklich über die Einstellungen in die Datenverarbeitung gem. Art. 6 Abs. 1 lit. a DSGVO eingewilligt habe. Der Kläger habe dies nicht getan, dementsprechend würde auch keine Datenverarbeitung erfolgen. Unabhängig davon verkenne die Klägerseite aber auch die Funktionsweise der von der Beklagten verwendeten „Business Tools“. Die Verwendung dieser Technologien sei nicht rechtswidrig und viele andere Unternehmen würden vergleichbare Tools nutzen. Zudem sei nicht die Beklagte, sondern die Drittunternehmen, die die „Business Tools“ nutzten, die richtigen Verantwortlichen. Die Drittunternehmen würden die „Business Tools“ in ihre Webseiten und Apps integrieren und mit deren Hilfe die Daten erheben und an die Beklagte übermitteln. Damit unterliege es auch diesen Drittunternehmen ihre Nutzer über die Datenerhebung und die Datenübermittlung an die Beklagte zu belehren. Der Klageantrag zu. 4 sei abzuweisen, weil schon keine Datenverarbeitung vorliege. Darüber hinaus bestünde aber auch eine Rechtsgrundlage für den Fall einer Datenverarbeitung. Die Datenverarbeitung verstoße nicht gegen Art. 6 oder 9 DSGVO. Der Kläger habe schon nicht ausreichend dargetan, dass er Webseiten oder Apps Dritter besucht habe bzw. welche Webseiten und Apps er konkret genutzt habe. Darüber hinaus verleihe der Anspruch aus Art. 17 DSGVO kein Recht auf Anonymisierung. Der mit dem Klageantrag zu 5 geltend gemachte Schmerzensgeldanspruch aus Art. 82 DSGVO sei mangels Datenverstoßes ebenfalls zurückzuweisen. Der Kläger habe nicht nachgewiesen, dass ihm ein tatsächlicher Schaden entstanden sei, der auf einem Verstoß beruhe. Eine reine Abschreckungswirkung begründe noch nicht einen Anspruch aus Art. 82 DSGVO und die behaupteten psychischen Beeinträchtigungen genügten ebenfalls nicht, um einen solchen Anspruch zu rechtfertigen. Auch ein Schadensersatzanspruch nach § 823 Abs. 1 BGB wegen der Verletzung des Allgemeinen Persönlichkeitsrechts bestehe nicht.

Hinsichtlich der weiteren Einzelheiten des Sach- und Streitstands wird auf die Schriftsätze der Parteien nebst Anlagen Bezug genommen.

Entscheidungsgründe

I.

Die Klage ist mit Ausnahme der Anträge zu 1) und 4) zulässig und im tenorierten Umfang begründet. Im Übrigen ist die Klage unbegründet.

1.

Der nach Klageänderung und teilweiser Klagerücknahme noch anhängige Teil der Klage ist mit Ausnahme der Anträge zu 1) und 4) zulässig.

Das Landgericht Siegen ist international, sachlich und örtlich zuständig.

Die internationale Zuständigkeit deutscher Gerichte folgt zum einen aus Art. 18 Abs. 1 Alt. 2. EuGVVO. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Sitz hat, oder aber vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO Verbraucher und hat seinen Wohnsitz in Siegen, sodass die deutschen Gerichte international zuständig sind. Die internationale Zuständigkeit ergibt sich im Übrigen auch aus Art. 79 Abs. 2 Satz 1 DSGVO.

Das Landgericht Siegen ist nach §§ 23 Nr. 1, 71 Abs. 1 GVG auch sachlich und nach Art. 17 Abs. 1 lit c., Art. 18 Abs. 1 Alt. 2 EuGVVO örtlich zuständig.

2.

Der Klageantrag zu 1. ist bereits unzulässig, weil das erforderliche Rechtsschutzbedürfnis sowie das nach § 256 Abs. 1 ZPO vorausgesetzte Feststellungsinteresse der Klageseite fehlt.

a)

Das Rechtsschutzbedürfnis für eine Feststellungsklage liegt nur dann vor, wenn dasselbe Ziel nicht durch einen „einfacheren und billigeren Weg“ erreicht werden kann, wie z.B. durch eine Leistungsklage (BGH Urt. v. 1.7.1974 – VIII ZR 68/73, BeckRS 1974, 31125977). Ist eine Leistungsklage möglich, dann fehlt der Klageseite das Rechtsschutzinteresse an der Erhebung einer Feststellungsklage.

Im hiesigen Fall ist eine Leistungsklage möglich. Aufgrund des Vorrangs der Leistungsklage fehlt es dementsprechend an dem für die Feststellungsklage erforderlichen Rechtsschutzinteresse. Denn mit dem Klageantrag zu 3. macht der Kläger einen Unterlassungsanspruch, der einen solchen Leistungsantrag enthält, gestützt auf genau die gleiche Behauptung einer unrechtmäßigen Datenverarbeitung, geltend. Ein Interesse des Klägers daran, eine Klärung derselben Frage im Rahmen

eines Feststellungantrags gemäß dem Klageantrag zu 1. herbeizuführen, ist nicht ersichtlich.

b)

Der Klageantrag zu 1. ist auch deshalb unzulässig, weil er die Voraussetzungen des § 256 Abs. 1 ZPO nicht erfüllt. Dieser normiert, dass eine Feststellungsklage nur hinsichtlich der Feststellung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses erhoben werden kann und nur dann, wenn der Kläger ein rechtliches Interesse daran hat, dass das Rechtsverhältnis durch richterliche Entscheidung alsbald festgestellt wird.

Für dieses Feststellungsinteresse ist gerade nicht ausreichend, wenn lediglich ein allgemeines Klärungsinteresse besteht, vielmehr ist es nur gegeben, wenn dem Recht oder der Rechtslage des Klägers eine gegenwärtige Gefahr der Unsicherheit droht und das erstrebte Urteil geeignet ist, diese Gefahr zu beseitigen (st Rspr, vgl. BGH Beschl. v. 2.11.2022 – IV ZR 39/22, BeckRS 2022, 43298 Rn. 13; BGH, Urteil vom 12.10.2021 – EnZR 43/20 –, NZBau 2022, 167, Rn. 20 mwN). Das Feststellungsinteresse fehlt entsprechend, wenn durch die begehrte Feststellung der Streit nicht endgültig beendet wird, weil dies nur mit einem Leistungs- oder Unterlassungstitel möglich ist. Nur dadurch wird die Vollstreckung ermöglicht, mehrfache Prozesse vermieden und die Kostenlast des Beklagten verringert (Anders, in: Anders/Gehle, ZPO, 83. Auflage, 2025, § 256, Rn. 41 mwN). Vorliegend beantragt der Kläger festzustellen, dass die streitgegenständliche Datenverarbeitung seit dem 25.05.2018 rechtswidrig war. Der Kläger ist hier aber durchaus in der Lage, eine Unterlassungsklage oder Klage auf Löschung zu erheben (vgl. auch LG Stuttgart, Endurteil vom 24.10.2024 – 12 O 170/23, GRUR-RS 2024, 36702, Rn. 27), was er durch die Klageanträge zu 3. und zu 4. auch getan hat. Es ist nicht ersichtlich, warum der Feststellungsantrag zusätzlich zulässig sein sollte und der Kläger führt hierzu auch nichts Näheres aus. Weiterhin hat der BGH ausdrücklich klargestellt, dass es sich bei der Frage der Rechtswidrigkeit bzw. Unzulässigkeit eines bestimmten Verhaltens um eine abstrakte Rechtsfrage ohne Bezug zu einem konkreten Rechtsverhältnis handelt und dahingehende Feststellungsbegehren nicht unter § 256 Abs. 1 ZPO fallen (BGH, Urteil vom 20. April 2018 – V ZR 106/17, NJW 2018, 3441 Rn. 13).

3.

Der Klageantrag zu 4., mit welchem eine Löschung / Anonymisierung der im Klageantrag zu 1. benannten Daten verlangt wird, ist hingegen unzulässig. Es fehlt an der nach § 259 ZPO notwendigen Besorgnis der Leistungsverweigerung.

Voraussetzung für die Zulässigkeit des Antrags ist insoweit die begründete Erwartung des Gläubigers, dass sich der Schuldner der rechtzeitigen Leistung entziehen werde, was in der Regel begründet ist, wenn der Schuldner den Anspruch ernsthaft bestreitet. Diese besondere Prozessvoraussetzung für eine Klage gemäß § 259 ZPO ist vom Kläger darzulegen und gegebenenfalls zu beweisen (vgl. Zöller, ZPO, 33. Auflage, § 259 Rn. 5).

Hier hat die Beklagte mehrfach ihre Bereitschaft zur Löschung derjenigen Daten, welche ihr von Drittunternehmen übermittelt wurden, erklärt. Es wurde insoweit vorgetragen, dass die Beklagte den Nutzern ihrer Dienste Einstellungsmöglichkeiten biete, um die von Drittunternehmen geteilten Informationen über Aktivitäten von ihrem Facebook-Konto zu trennen und die Konten jederzeit vollständig zu löschen. Mit der Option „Frühere Aktivitäten löschen“ biete die Beklagte eine Möglichkeit an, frühere Aktivitätsdaten von Dritten, die mit einem Facebook-Konto verknüpft waren, vollständig von diesem zu lösen und dadurch die identifizierende Verbindung aufzuheben. Auch existiere mit der Option „Zukünftige Aktivitäten trennen“ ein Werkzeug, um die Speicherung zukünftiger Verbindungen zu verhindern.

Hierbei handelte es sich um die Bereitschaft zur Löschung im Sinne des Art. 17 DSGVO.

Insoweit wird der Begriff der Löschung im Sinne dieser Vorschrift maßgeblich durch den erwünschten Erfolg bestimmt. Gleichgültig ist, auf welche Art und Weise dieser Erfolg im Einzelnen herbeigeführt wird. Alle technischen Möglichkeiten können herangezogen werden, um die Unbrauchbarmachung zu erreichen. Entscheidend ist, dass weder der Verantwortliche noch ein Dritter auf vorhandene personenbezogene Daten zugreifen und diese auslesen oder verarbeiten kann. Auf eine nur theoretische Möglichkeit der Rekonstruktion von Daten kommt es dabei nicht an (vgl. BeckOK, Datenschutzrecht, Stand: 01.08.2023, Art. 17 DSGVO Rn. 55).

Personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO erfordern eine identifizierte oder identifizierbare natürliche Person. Durch das hier durch die Beklagte in Aussicht gestellte „Trennen“ der Aktivitäten würde jeglicher Bezug zu einer identifizierbaren natürlichen Person aufgehoben, was als Unbrauchbarmachen im Sinne des Art. 17 DSGVO zu klassifizieren ist.

Der Kläger hat auch nicht hinreichend vorgetragen, dass die Beklagte tatsächlich nicht gewillt ist, die ihn betreffenden Daten entsprechend der vorgenannten Vorschriften zu löschen. Der dahingehende Vortrag des Klägers, die Beklagte stelle insoweit lediglich die Möglichkeit einer „Pseudonymisierung“ in Aussicht, vermag kein abweichendes Ergebnis zu rechtfertigen. So wurde bereits nicht konkret dargelegt, weswegen es der Beklagten nach der durchgeführten Aufhebung der Verbindung der Datenbestände mit dem Profil, welche eine Identifizierung des Klägers gerade erst möglich macht, problemlos möglich sein soll, die persönliche Verbindung zum Kläger

wiederherzustellen. In dieser Hinsicht ergibt sich nach der Auffassung der Kammer auch nichts Abweichendes aus dem Erwägungsgrund Nr. 26 der DSGVO. Dass weiterhin zusätzliche Informationen existieren würden, welche im Sinne der Legaldefinition des Art. 4 Nr. 5 DSGVO eine erneute Verknüpfung der Datenbestände für eine Identifizierbarkeit möglich machen würden, ist nicht vorgetragen.

Daneben weist die vom Kläger verlangte Anonymisierung der Daten keinen eigenständigen Anwendungsbereich auf und kann nicht als aliud anstelle einer Löschung verlangt werden.

Diesbezüglich führt auch die mit einer Anonymisierung verbundene vollständige Aufhebung des Personenbezugs dazu, dass mangels Identifizierbarkeit keine personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO mehr vorliegen. Des Weiteren ergibt sich aus dem Wortlaut des Art. 4 Nr. 1 DSGVO, dass die Verordnung eine Löschung der Daten nicht denklogisch mit einer vollständigen Vernichtung des Bestandes gleichsetzt. Dementsprechend kann die Anonymisierung lediglich als Unterfall der Löschung ohne eigenständige Bedeutung angesehen werden (vgl. auch Stürmer, ZD 2020, 626 – 631).

Dass die Beklagte bereit ist, die Identifizierbarkeit vorhandener personenbezogener Daten des Klägers in geeigneter Weise aufzuheben, folgt auch daraus, dass sie sich gegen den Klageantrag zu 3. verteidigt, mit dem der Kläger verlangt, seine Daten – zunächst - unverändert am gespeicherten Ort zu belassen.

II.

Die Klage ist im tenorierten Umfang begründet, im Übrigen unbegründet.

1.

Der geltend gemachte Unterlassungsanspruch ist im tenorierten Umfang begründet,

im Übrigen unbegründet.

a) Soweit die Klägerseite ihren Unterlassungsantrag auf die nachfolgend aufgeführten Datenpunkte aus dem klägerischen Antrag bezieht, ist die Klage unbegründet.

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

- interne Browser-ID der Meta Ltd.
- Abonnement –ID
- Lead-ID
- anon_id

- die Advertising ID des Betriebssystems Android (von der Meta Ltd. „madid“ genannt)
sowie aus Webseiten:
- 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 der jeweiligen Webseite dokumentieren
sowie aus mobilen Dritt-Apps:
- 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

Die Kammer schließt sich insoweit der dazu ergangenen Rechtsprechung des LG Lübeck (Urteil vom 10.01.2025 - 15 O 269/23) an. Das LG Lübeck hat dazu folgendes ausgeführt:

„Dabei kann dahinstehen, ob sich der geltend gemachte Unterlassungsanspruch aus Art. 17, 18 DSGVO oder aus sonstigen Bestimmungen der DSGVO ergibt, oder aber aus § 1004 Abs. 1 S. 2 BGB analog, § 823 Abs. 1 BGB, Art. 2 Abs. 1 GG oder ob die DSGVO keine Unterlassungsansprüche der hier erforderlichen Art kennt und dennoch den Rückgriff auf nationales Recht sperrt. Hierzu im Einzelnen:

(a) Für den letztgenannten Fall wäre die Klageabweisung selbsterklärend, da unter dieser Hypothese schon mangels tauglicher Anspruchsgrundlage der klägerischen Anspruch entfiele.

(b) Auch unter der Annahme der Möglichkeit des Rückgriffs auf § 1004 Abs. 1 S. 2 BGB analog, § 823 Abs. 1 BGB, Art. 2 Abs. 1 GG käme im Ergebnis kein Anspruch in Betracht. Voraussetzung für das Entstehen eines Anspruches wäre nämlich in diesem Fall jedenfalls, dass die geltend gemachte Rechtsgefährdung - hier die behauptete Verarbeitung gerade der vorgenannten personenbezogenen Datenpunkte durch die Beklagte – hinreichend nahe bevorsteht (Wiederholungs- oder zumindest Erstbegehungsgefahr, vgl. etwa MüKoBGB/Raff, 9. Aufl. 2023, BGB § 1004 Rn. 295-297). Dabei genügt nicht schon die bloße Möglichkeit einer Beeinträchtigung; die Besorgnis muss auf Tatsachen und nicht nur auf subjektiven Befürchtungen beruhen. Dabei kann allerdings zugunsten des Anspruchstellers vermutet werden, dass sich eine vorausgegangene Verletzung wiederholen wird (a.a.O., Rn. 300). Eine derartige hinreichende hinreichend nahe Gefahr vermag die Kammer nicht zu Grunde zu legen. Die Kammer legt dabei ihrer Entscheidung zu Grunde, dass die oben im Einzelnen aufgeführten Datenpunkte keine „technischen Standarddaten“ im obigen Sinne darstellen, sondern es sich vielmehr um „sonstige personenbezogene Daten“ gemäß obiger Definition handelt. Derartige Daten werden von der Beklagten über die streitgegenständlichen Business-Tools jedoch gerade nicht in jedem Fall des Besuches einer Website oder der Nutzung einer App erhoben,

weitergeleitet und verarbeitet. Vielmehr hängt es unter anderem - dies auch unstreitig - von der Art des eingesetzten Business Tools sowie dessen Konfiguration durch den Drittseitenbetreiter ab, ob und welche Daten insoweit erhoben und an die Beklagte übermittelt werden. Entsprechend obläge es nach allgemeinen zivilprozessualen Regelungen der Klägerseite unter dem Gesichtspunkt der Wiederholungsgefahr, darzulegen, welche konkreten Apps oder Websites sie in der Vergangenheit aufgesucht bzw. genutzt hat, welche Art Business Tool dort eingesetzt wurde und welche konkreten Datenpunkte der von der Klägerseite aufgeführten Art dort abgegriffen und an die Beklagte übermittelt wurden.“

Derartiger Vortrag fehlt in allen am 4.9.2025 von der Kammer verhandelten Verfahren gegen die Beklagte fast vollständig. Zwar hat der Kläger noch vorgetragen, regelmäßig die Seiten Wahlomat, Westfalenpost, Spiegelonline, Paypal und idealo zu nutzen. Vortrag dazu, ob dort und welche von der Klägerseite bemühten Datenpunkte abgegriffen und an die Beklagte übertragen wurden, findet sich jedoch nicht. Gleiches gilt im Übrigen sinngemäß für die Anforderungen an eine evtl. bestehende Erstbegehungsgefahr. Es liegt auch kein einlassungsfähiger Vortrag dahingehend vor, dass die Klägerseite in hinreichender zeitlicher Nähe eine konkrete Seite aufsuchen wird, die gerade die von der Klägerseite aufgezählten Datenpunkte ohne seine Einwilligung abrufen könnte.

Der Klägerseite wird dadurch die Rechtsdurchsetzung nicht in unangemessener Weise erschwert (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Dabei hat die Kammer insbesondere berücksichtigt, dass es der Klägerseite naturgemäß nicht möglich sein dürfte, substantiiert vorzutragen, wann in der Vergangenheit auf welcher Seite welche Datenpunkte abgegriffen wurden (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Die Kammer sieht insoweit jedoch keine unzumutbare Erschwernis für die Klägerseite (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Insbesondere hätte es der Klägerseite freigestanden, im Wege der Stufenklage gegen die Beklagte vorzugehen um in erster Stufe per Auskunftsanspruch Gewissheit darüber zu erlangen, welche konkreten Datenpunkte aus welcher Quelle von der Beklagten erfasst wurden(so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Auf diese Weise hätte sodann auf zweiter oder dritter Stufe konkret überprüft werden können, ob und inwieweit eine Wiederholungsgefahr bestehen kann (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Dies würde den Rechtsstreit im Übrigen auch auf konkrete und der Logik des Zivilprozesses entsprechende Tatsachen- und Rechtsfragen zurückführen, anstatt des hier von der Klägerseite angestrebten Weges, gleichsam allgemeinverbindlich das Geschäftsmodell der Beklagten fast ohne konkreten Einzelfallbezug zum Kläger zur Prüfung zu stellen - ein Unterfangen, für welches der Zivilprozess nicht das

geeignete Instrumentarium vorsieht (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

b)

Nichts anderes gilt im Übrigen, wenn unterstellt würde, dass der DSGVO selbst ein Unterlassungsanspruch, sei es aus Art. 17, 18 DSGVO oder aus sonstigen Bestimmungen der DSGVO, zu entnehmen ist. Denn wie auch immer ein derartiger Anspruch im Einzelnen dogmatisch fundiert und ausgestaltet sein könnte, so wäre doch in jedem Fall zur Überzeugung der Kammer erforderlich, dass - wie auch im deutschen Recht - eine irgendwie greifbare Erstbegehungs- oder Wiederholungsgefahr angenommen werden kann. Dies ist aber aus den vorgenannten Gründen nicht der Fall.

c)

Eine Aussetzung des Verfahrens zwecks Abwartens auf die Entscheidung des EuGH über die vom BGH aufgeworfenen Fragen (BGH, Beschl. v. 26.9.2023 – VI ZR 97/22 (OLG Frankfurt in Darmstadt) ist insoweit nicht angezeigt, da der klägerische Anspruch unter jeder denkbaren Prämisse ausscheidet (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

2.

Soweit die Klägerseite hingegen begehrt, dass die Beklagte es unterlassen soll, über

die streitgegenständlichen Business - Tools auf Drittseiten und -apps zu erheben, wann die Klägerseite welche Websites besucht hat bzw. welche Apps sie benutzt hat, und diese Daten sodann an sich selbst zu übertragen, dort zu speichern und zu verwenden, ist die Klage begründet (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

a) Der Anspruch ergibt sich aus Art. 17, 18 DSGVO oder aus sonstigen Bestimmungen der DSGVO, jedenfalls aber aus § 1004 Abs. 1 S. 2 BGB analog, § 823 Abs. 1 BGB, Art. 2 Abs. 1 GG (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

112 (b) Aus dem generellen Regelungsziel der DSGVO folgt, dass die Rechtsordnung grundsätzlich eine Möglichkeit für von rechtswidrigen Datenverarbeitungsvorgängen betroffenen Personen gegeben sein muss, gegen diese per Unterlassungsklage vorzugehen (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Insoweit führt der EuGH in seiner Entscheidung vom 4. Oktober 2024 - Az C-21/23 - aus, dass generelles Regelungsziel der DSGVO ist, den Betroffenen im europäischen Rechtsraum ein hohes Schutzniveau zu gewährleisten und die praktische Wirksamkeit der DSGVO sicherzustellen:

„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 DSGVO festzustellen, dass (…) eine von einem Mitbewerber des mutmaßlichen Verletzers von Vorschriften zum Schutz personenbezogener Daten erhobene Unterlassungsklage zwar nicht diesem Ziel dient, sondern einen lauteren Wettbewerb sicherstellen soll; sie trägt jedoch unbestreitbar zur Einhaltung dieser Bestimmungen und damit dazu bei, die Rechte der betroffenen Personen zu stärken und ihnen ein hohes Schutzniveau zu gewährleisten (vgl. in diesem Sinne Urteil vom 28. April 2022, Meta Platforms Ireland, CEU:C:2022:322, Rn. 74). (…) Im Übrigen könnte sich eine solche Unterlassungsklage eines Mitbewerbers, ähnlich wie Klagen von Verbänden zur Wahrung von Verbraucherinteressen, 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.“ (a.a.O,.Rn. 46 ff.).

Vor diesem Hintergrund ist die Kammer davon überzeugt, dass in jedem Fall sichergestellt sein muss, dass drohende Rechtsbeeinträchtigungen aufgrund von Verletzungen der DSGVO auch in Wege der Unterlassungsklage abgewendet werden können (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Ob sich dies aus der DSGVO selbst ergibt oder über die insoweit mögliche Anwendung nationalen Rechts, kann vorliegend offenbleiben, weil bei der Zugrundelegung nationalen deutschen Rechts (hierfür u.a.: BeckOGK/T. Hermann, 1.11.2024, BGB § 823 Rn. 1285; so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23) ein Unterlassungsanspruch aus § 1004 Abs. 1 S. 2 BGB analog, § 823 Abs. 1 BGB, Art. 2 Abs. 1 GG folgt und die Klägerseite zunächst verlangen kann, dass es die Beklagte unterlässt, die vorgenannten Datenpunkte auf Drittseiten und -apps zu erheben. Die generelle Praxis der Beklagten, immer und auch ohne Einwilligung jedenfalls solche technischen Standarddaten, die der Beklagten mit einer Wahrscheinlichkeit von über 99 % eine Identifizierung der jeweiligen Nutzerin bzw. des jeweiligen Nutzers innerhalb der Metasysteme erlaubt, sowie das Datum, dass und wann die fragliche Drittseite mit diesen technischen Parametern aufgesucht wurde, über die Business Apps zu erheben, beeinträchtigt die Betroffenen in ihrem Recht auf informationelle Selbstbestimmung (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Dieses unter den Bedingungen der modernen und von digitalen Systemen zutiefst geprägten Massengesellschaft essentielle Grundrecht schützt die Grundrechtsträger auch gegenüber Privaten in ihrem Recht, selbst zu entscheiden, welche Daten an Dritte herausgegeben werden - und welche nicht (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

Die Praxis der Beklagten ist auch rechtswidrig. Gesichtspunkte, die diese spezifische Form der Datenverarbeitung durch die Beklagte rechtmäßig erscheinen lassen

könnten, sind nicht vorgetragen und auch nicht ersichtlich. Insbesondere liegt kein Rechtfertigungsgrund nach Art. 6 Abs. 1 DSGVO vor. Vor allem eine Einwilligung der Betroffenen für diese Form der Datenverarbeitung ist, wie zwischen den Parteien unstreitig, nicht gegeben. Vielmehr erfolgt diese Datenerhebung in jedem Fall und unabhängig davon, ob die Betroffenen hierin bei Aufruf der fraglichen Website oder App eingewilligt haben oder nicht. Diesbezüglich überzeugt das Vorbringen der Beklagten, es handele sich hierbei um eine jenseits von Meta-Produkten weit verbreitete Praxis und letztlich der aktuellen Funktionsweise „des Internets“ geschuldet, in jeglicher Hinsicht nicht. Zwar vermag die Kammer noch nachzuvollziehen, dass derartige Datenübermittlungen insbesondere technischer Standarddaten erforderlich sein mögen um etwa eingebettete Funktionalitäten von Drittanbietern ordnungsgemäß laden und darstellen zu können - wobei auch insoweit nach der Konzeption der DSGVO an sich vorab eine Zustimmung eingeholt werden muss (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23), andernfalls eben auf die eingebettete Funktionalität kein Zugriff aufgebaut werden kann. Vor allem aber erschließt sich der Kammer vorliegend nicht, was dieser technische Umstand mit der hier streitgegenständlichen Implementierung der Business Tools zu tun haben soll. Denn diese werden von den Drittfirmen und der Beklagten - soweit aus dem langatmigem Vortrag der Beklagten irgendwie rekonstruierbar - grundsätzlich gerade nicht eingesetzt um irgendwelche Inhalte auf Drittseiten anzubieten, sondern ausschließlich um das Nutzungsverhalten der Nutzerinnen und Nutzer zu Werbezwecken zu erfassen. Würde die Beklagte diese Tools nicht anbieten, wären die angesteuerten Websites aus Nutzerinnen- und Nutzersicht völlig unverändert nutzbar. Nachteile ergäben sich ausschließlich für die Beklagte selbst, nämlich für ihr Bemühen, im eigenen geschäftlichen Interesse in massenhaftem Umfang Persönlichkeitsprofile zu erstellen um diese kommerziell für Werbezwecke und andere, wenig transparente Zwecke einzusetzen.

b)

Die Beklagte ist für die Datenerhebung der von ihr konzipierten Business Tools auch verantwortlich i.S.d. Art. 4 Nr. 7 DSGVO. „Verantwortlicher“ i.S. d. DSGVO ist insoweit jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hierfür genügt es nach gängiger Rechtsprechung des EuGH auch, dass die fragliche Person aus Eigeninteresse Einfluss auf die Mittel und Zwecke der Datenverarbeitung nimmt (BeckOK DatenschutzR/Spoerr, 50. Ed. 1.8.2024, DS-GVO Art. 26 Rn. 18-25; LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Der erforderliche Beitrag zur Datenverarbeitung kann dabei nach der Rechtsprechung des EuGH bereits in der Ermöglichung der Erhebung der Daten und der Einflussnahme auf die Kategorien der Daten, welche erhoben werden sollen, liegen. Hiernach hat die Kammer keine

Zweifel an der Verantwortlichkeit jedenfalls auch der Beklagten, da diese die von ihr entwickelten Business-Tools zur Verfügung stellt, die hier zugrunde gelegte Datenerhebung auch ohne Einwilligung der Beklagten damit selbst konfiguriert hat und die ihr von den Drittanbietern übermittelten Daten auch nach eigenem Vortrag selbst und zum eigenen wirtschaftlichen Vorteil nutzt. Die Beklagte kann dem auch nicht überzeugend entgegenhalten, dass die Daten letztlich von den Drittwebseitenbetreibern erhoben und dann an sie weitergeleitet werden. Denn sie ist jedenfalls - ggf. neben den Drittwebseitenbetreibern - mitverantwortlich. Insoweit kann auf die folgenden Ausführungen des EuGH (Urteil vom 29. Juli 2019 - C-40/17 - , Juris) verwiesen werden:

„Mit der Einbindung eines solchen Social Plugins in ihre Website hat Fashion ID im Übrigen entscheidend das Erheben und die Übermittlung von personenbezogenen Daten der Besucher dieser Seite zugunsten des Anbieters dieses Plugins, im vorliegenden Fall Facebook Ireland, beeinflusst, die ohne Einbindung dieses Plugins nicht erfolgen würden. Unter diesen Umständen und vorbehaltlich der insoweit vom vorlegenden Gericht vorzunehmenden Nachprüfungen ist davon auszugehen, dass Facebook Ireland und Fashion ID über die Mittel, die dem Erheben personenbezogener Daten der Besucher der Website von Fashion ID und deren Weitergabe durch Übermittlung zugrunde lagen, gemeinsam entschieden haben.(…) Folglich ist Fashion ID für die Vorgänge des Erhebens personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung gemeinsam mit Facebook Ireland als verantwortlich im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 anzusehen“.

Der in dem Urteil des EuGH behandelte Sachverhalt lässt sich dabei mit dem hiesigen vergleichen. Denn auch hier werden Daten durch ein „Tool“ der Beklagten, nämlich ein Business-Tool, welches eine Drittseite installiert hat, an die Beklagten weitergeleitet.

c)

Zuletzt stellt die sich hieraus ergebende Rechtsverletzung der von den Business Tools Betroffenen auch konkret für die Klägerpartei eine hinreichend konkrete und unmittelbare Bedrohung dar, dem sie mit einem individuellen Unterlassungsanspruch begegnen kann. Zwar gilt auch hier - wie oben - im Ansatzpunkt, dass die Klägerseite konkret geltend machen muss, dass die geltend gemachte Rechtsverletzung hinreichend nahe und für sie selbst bevorsteht (Wiederholungs- oder zumindest Erstbegehungsgefahr, vgl. etwa MüKoBGB/Raff, 9. Aufl. 2023, BGB § 1004 Rn. 295-297; LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Im Unterschied zu oben ist dies für die hier behandelte Rechtsverletzung anzunehmen. Denn, wie ausgeführt und im Unterschied zu oben, hängt hier die Datenerhebung nicht von weiteren

Parametern und Einstellungen ab, sondern erfolgt automatisch und in jedem Fall eines Seiten- oder Appaufrufs und völlig unabhängig von der Einwilligung des Klägers. Die Rechtsverletzung droht damit in jedem Fall bei einem Seiten- oder Appaufruf, welche das Business-Tool implementiert hat. Angesichts der sehr weiten Verbreitung dieser Tools auf zahllosen Apps und Seiten, ist diese Gefahr ohne das Erfordernis weiteren Vortrages des Klägers als bewiesen anzusehen. Allein schon der Umstand, dass die Tools auf den in der Anlage K2 aufgeführten Seiten implementiert sind, begründet die naheliegende Gefahr, dass künftig auch der Kläger persönlich von den implementierten Tools betroffen sein kann. Denn in der Anlage K 2 sind 466 exemplarische deutschsprachige Websites aufgelistet, die nach dem Vortrag der Klägerseite ebenfalls die Business Tools implementiert haben sollen. Die Kammer stuft diesen Vortrag dabei auch als unstreitig ein, da die Beklagte diese Angaben jedenfalls nicht nachvollziehbar bestritten hat, sondern lediglich diffus anmerkte, hierfür gebe es „keine Anhaltspunkte“ (Klageerwiderung, S. 40, Rn. 70 = Bl. 500 d.A.) - eine nicht einlassungsfähige Randbemerkung die ersichtlich offenlässt, ob die Beklagte insoweit mit Nichtwissen bestreiten möchte - was wohl unzulässig wäre - oder möglicherweise lediglich die Mühen scheut, die Angaben zu überprüfen und es daher dabei belässt, unüberprüfte Zweifel anzudeuten - was zivilprozessual ebenso möglich wie folgenlos wäre (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23).

d)

Des Weiteren kann die Klägerseite auch verlangen, dass es die Beklagte unterlässt die derart erhobenen Datenpunkte auf ihre eigenen Server zu übertragen. Auf die obigen Ausführungen kann insoweit vollumfänglich verwiesen werden. Auch dieser Vorgang erfolgt immer und unabhängig davon, ob die Betroffenen hierin eingewilligt haben oder nicht.

e)

Nichts Anderes und in erster Linie gilt für den Anspruch, es zu unterlassen, die entsprechenden Datenpunkte sodann zu speichern und weiter zu verwenden. Insbesondere ist nochmals zu betonen, dass es zwischen den Parteien auch auf ausdrückliche richterliche Nachfrage im Termin zur mündlichen Verhandlung unstreitig blieb, dass die Beklagte die fraglichen Datenpunkte selbst dann dem Persönlichkeitsprofil der Betroffenen hinzufügt, wenn hierfür keinerlei Einwilligung gegeben wurde. Die Rechtswidrigkeit dieser Praktik liegt ohne weiteres auf der Hand und ist auch in keiner Weise mit dem eigenen Vortrag der Beklagtenseite zu vereinbaren, sie stütze sich hinsichtlich der vorgenommenen Datenverarbeitung auf die ihr gegenüber abgegebene Einwilligung der Nutzer - welche ja gerade nicht

vorliegt (vgl. oben). Nicht zu überzeugen vermag insoweit im Übrigen auch der Verweis der Beklagten auf nicht weiter erläuterte „Sicherheits- und Integritätszwecke“. Der Vortrag ist weitgehend unklar, wird auch nicht verständlich erläutert und ist ersichtlich nicht einlassungsfähig und damit unbeachtlich. Um es nochmal deutlich auf den Punkt zu bringen, das massenhafte, im Verborgenen, weil ohne Einwilligung (siehe oben) Speichern von Daten verstößt eklatant gegen den Grundsatz der Datensparsamkeit und stellt im Prinzip eine ausgeklügelte Form der in Europa gegen Grundrechte verstoßenden Vorratsdatenspeicherung dar (vgl. dazu EuGH, Urteil vom 20.09.2022 - C-793/19 und C-794/19).

f)

Nichts Anderes würde im Übrigen gelten, wenn als Anspruchsgrundlage nicht deutsches Recht, sondern ein aus der DSGVO hergeleiteter Anspruch zu Grunde zu legen wäre (so auch LG Lübeck, Urteil vom 10.01.2025 - 15 O 269/23). Eine Aussetzung des Verfahrens kam daher nicht in Betracht. Insbesondere erscheint es der Kammer nach der jüngsten Entscheidung des EuGH ausgeschlossen, dass es weder einen DSGVO-rechtlich fundierten noch einen nationalen Anspruch geben könnte.

3.

Der Klageantrag zu 3. ist unbegründet.

Es ist bereits nicht ersichtlich, auf welche Rechtsgrundlage der Kläger einen Anspruch auf unveränderte Speicherung der bereits erhobenen Daten stützen möchte. Aus Art. 17 DSGVO folgt dem ausdrücklichen Wortlaut her lediglich ein Recht auf Löschung von Daten. Es ist nicht ersichtlich, dass das vom Kläger verfolgte Rechtsschutzziel auf dieser Grundlage verfolgt werden könnte. Folglich kommt dem klägerischen Begehren am ehesten der Anspruch auf Einschränkung der Verarbeitung aus Art. 18 DSGVO nahe. Diesbezüglich sieht Art. 18 DSGVO aber die vom Kläger gewählte Formulierung des Antrags (Daten zunächst belassen, dann aber auf Aufforderung löschen) nicht vor mit der Folge, dass mangels entsprechender Anspruchsgrundlage kein Anspruch besteht.

4.

Der Kläger hat ferner gegen die Beklagte einen Anspruch auf Schadensersatz nach Art. 82 DSGVO. Nach der Rechtsprechung des Gerichtshofes erfordert ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DSGVO 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 (EuGH, Urteil vom 4. Oktober 2024 – C-507/23 –, juris Rn. 24; BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 21 jeweils m. w. N.).

a)

Die Beklagte hat, wie bereits erläutert, eklatant gegen die DSGVO verstoßen, indem sie personenbezogene Daten der klagenden Partei ohne Rechtsgrundlage verarbeitete.

b)

Der Kläger hat dadurch auch einen immateriellen Schaden erlitten. Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren. Dabei soll nach ErwG 146 Satz 3 DSGVO 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 Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen

Verstoß) erforderlich. Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DSGVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat. Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DSGVO verpflichtet ist, 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 im Sinne von Art. 82 dieser Verordnung darstellen. Schließlich hat der Gerichtshof in seiner jüngeren Rechtsprechung unter Bezugnahme auf den Erwägungsgrund 85 DSGVO klargestellt, dass 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 DSGVO 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 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 (BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 28 ff. m. w. N. zur Rechtsprechung des EuGH). Nach diesen Maßstäben liegt es in diesem Fall auf der Hand, dass der kläger einen solchen Kontrollverlust erlitten hat. Die Beklagte hat personenbezogene Daten der klagenden Partei über die streitgegenständlichen Meta Business Tools ohne eine Einwilligung erhoben und bei sich gespeichert. Nach Einlassung der Beklagtenseite kann der Nutzer des sozialen Netzwerkes gerade nicht über die Ablehnung der Nutzungsbedingungen oder Einstellungen seiner Privatsphäre eine Datenerhebung und Datenverarbeitung der Beklagten ausschließen. Selbst eine Ablehnung der Cookies der Drittwebseite führt insbesondere nicht zu einem Ausschluss der Datenerhebung der Beklagten, wie sie selbst einräumt. Es spielt insoweit keine Rolle, dass „nur“ http-Daten des Nutzers erhoben werden. Nach Überzeugung des Gerichts ist aus dem Umstand, dass eine Datenverarbeitung durch die Beklagte bereits mit Aufruf der Drittwebseite, auf der sich ein Business Tool der Beklagten befindet, stattfindet und nicht von Seiten des Nutzers ausgeschlossen werden kann, eine unzulässige Datenverarbeitung gegeben. Die Beklagte nimmt eine Datenverarbeitung ungeachtet einer Zustimmung vor. Dabei spielt es auch keine Rolle, dass es sich nur um „automatisch“ generierte Daten, wie http-Daten handelt.

Insoweit geht die Kammer davon aus, dass die Klägerseite von der streitgegenständlichen Datenverarbeitung mittels der sog. Business Tools auch individuell – wenn auch nur teilweise - betroffen ist. Dazu bedurfte es auch keines substantiierteren Vortrages zu einzelnen besuchten Webseiten. Vielmehr ist das Maß der Substantiierungspflicht von der jeweiligen Zumutbarkeit im Einzelfall abhängig. Die Pflicht zur Substantiierung findet ihre Grenzen in dem subjektiven Wissen der Partei und der Zumutbarkeit weiterer Ausführungen (vgl. etwa Mertins, Substantiierung im Zivilprozess, NJ 2009, 441 unter Verweis auf BGH, Urteil vom 27.11.1985 - IV a ZR 97/84 -, NJW 1986, 1162). Die Kammer schließt hieraus, dass es vorliegend der Klägerseite grundsätzlich nicht zumutbar ist, näher zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten und mit Business Tools der Beklagten versehenen Homepages vorzutragen und dass es entsprechend grundsätzlich ausreichend ist, wenn sie vorträgt, dass jede Instagram bzw. Facebook-Nutzerin bzw. jeder Instagram- bzw. Facebook-Nutzer mit erheblicher

Wahrscheinlichkeit von Überwachungsmaßnahmen durch die eingesetzten Business-Tools betroffen war. Zum einen kann schon naturgemäß niemand mit vertretbarem Aufwand rekonstruieren, welche Homepages zu welchem Zeitpunkt er oder sie in der Vergangenheit besucht hat und auch ist niemand verpflichtet entsprechende Verlaufsprotokolle in seinen Rechnern vorzuhalten. Zum anderen wäre der Klägerseite aber auch selbst dann, wenn dieses Wissen vorhanden wäre, kein substantiierterer Vortrag möglich, da die Klägerseite keinen auch nur ansatzweise vollständigen Überblick darüber hat, auf welchen Homepages zu welchem Zeitpunkt welche Business Tools der Beklagten enthalten waren. Faktisch wäre die Klägerseite entsprechend gezwungen, ihr gesamtes Internetnutzungsverhalten offen zu legen - was gerichtlicherseits zu verlangen ersichtlich im eklatanten Widerspruch zum Normzweck der DSGVO stünde. Entsprechend hat im Übrigen auch das Bundesverfassungsgericht zu der Frage entschieden, wie substantiiert im Verfassungsbeschwerdeverfahren wegen der Verletzung des Rechts auf informationelle Selbstbestimmung durch geheimdienstliche Maßnahmen vorzutragen ist. Wörtlich führte das Bundesverfassungsgericht dort aus:

„Zur Begründung der Möglichkeit eigener und gegenwärtiger Betroffenheit durch eine

gesetzliche Ermächtigung zu heimlichen Maßnahmen, bei der die konkrete Beeinträchtigung zwar erst durch eine Vollziehung erfolgt, die Betroffenen in der Regel aber keine Kenntnis von Vollzugsakten erlangen, reicht es aus, wenn die Beschwerdeführenden darlegen, mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt zu werden (vgl. BVerfGE 155, 119 <160 Rn. 75>). (…) Für die Wahrscheinlichkeit eigener Betroffenheit spricht eine große Streubreite der Überwachungsmaßnahme, wenn die Maßnahme also nicht auf einen tatbestandlich eng umgrenzten Personenkreis zielt, insbesondere, wenn sie auch Dritte in großer Zahl zufällig erfassen kann (BVerfGE 162, 1 <53 Rn. 98>).“ (BVerfG, Beschluss vom 08.10.2024 - 1 BvR 1743/16, 1 BvR 2539/16 -, BeckRS 2024, 30241, Rn. 89).

Diese Grundsätze sind zur Überzeugung der Kammer auf die hier vorliegende Frage übertragbar. Denn auch hier findet die streitgegenständliche Überwachung der Nutzerinnen und Nutzer derart statt, dass diese bei dem Besuch von Drittseiten nicht nachvollziehen ob und welche sie betreffender Daten an Meta gelangen und was dort mit diesen Daten geschieht. Zudem weisen die Maßnahmen unstreitig eine sehr große Streubreite auf, zielen nicht auf einen begrenzten Personenkreis ab und erfassen potentiell und zufällig eine sehr große Zahl an Personen. Die Verteidigungsmöglichkeiten der Beklagten werden hierdurch auch nicht unzumutbar beschnitten. Denn da diese - unstreitig – die empfangenen Daten weiterverarbeitet hat, müsste es ihr möglich sein, in ihren Systemen vollständig und nachvollziehbar darlegbar zu überprüfen, ob die Klägerseite möglicherweise und entgegen aller

Wahrscheinlichkeit gar nicht betroffen war - und dies sodann vortragen und ggf. unter Beweis stellen können.

Für das hier vorliegende Verfahren folgt hieraus zwar nicht, dass die Kammer generell zu Grunde legen kann, dass die Klägerseite von allen streitgegenständlichen Datenverarbeitungsvorgängen der Beklagten auch individuell betroffen ist. Denn, wie bereits oben erörtert, besteht eine große Wahrscheinlichkeit der individuellen Betroffenheit nur bzgl. der Erhebung der technischen Standarddaten. Hinsichtlich der darüberhinausgehenden sonstigen personenbezogenen Daten besteht eine derartige hinreichende Wahrscheinlichkeit nicht, da die Erfassung dieser Datenpunkte stark davon abhängig ist, welche konkreten Seiten besucht werden, welche Business Tools auf diesen eingebunden sind, wie diese konfiguriert sind und welche Einwilligungen von den Drittseitenbetreibern mit welchen Folgen bei ausbleibender Einwilligung eingeholt werden. Soweit die Klägerseite ihre individuelle Betroffenheit auch mit diesen Datenpunkten begründen möchte, müsste sie daher - wie bereits oben ausgeführt - den Weg über die Stufenklage mit Auskunftsklage auf erster Stufe gehen. Deswegen besteht lediglich im Hinblick auf die Verarbeitung der technischen Standarddaten und die dadurch gegebene individuelle Betroffenheit der Klägerseite ein Schadensersatzanspruch. Die dafür erforderliche haftungsbegründende Kausalität liegt vor. Gerade die Datenerhebung auf den Drittwebseiten bzw. Apps führte zu der Datenspeicherung bei der Beklagten, die seitens der klagenden Partei nicht verhindert werden kann. Ein immaterieller Schaden in Form des Kontrollverlusts ist somit gegeben.

c)

Der immaterielle Schaden beträgt der Höhe nach insgesamt 5.000,00 €. Art und Umfang des Schadensersatzanspruchs richten sich nach den nationalen Vorschriften in §§ 249 ff. BGB und § 287 ZPO i.V.m. den europarechtlichen Vorgaben des haftungsbegründenden Tatbestands in Art. 82 DSGVO.

Hinsichtlich der Kriterien nach denen die Höhe eines Schadens zu bemessen ist enthält die DSGVO keine Bestimmung. Insbesondere können aufgrund des unterschiedlichen Zwecks der Vorschriften nicht die in Art. 83 DSGVO genannten Kriterien herangezogen werden. 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. Allerdings

unterliegt die Ermittlung des Schadens unionsrechtlichen Einschränkungen. Die Modalitäten der Schadensermittlung dürfen bei einem - wie im Streitfall - 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 DSGVO vorgesehenen Schadenersatzanspruchs, wie sie in Erwägungsgrund 146 Satz 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld als "vollständig und wirksam" anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO dagegen nicht erfüllen. Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen hat. 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. Ist nach den Feststellungen des Gerichts allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten – wie hier – 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 Abs. 1 DSGVO) 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 etwa durch Entfernung einer Veröffentlichung aus dem Internet (inkl. Archiven) oder Änderung des personenbezogenen Datums (z.B. Rufnummernwechsel; neue Kreditkartennummer) in den Blick zu nehmen. Als Anhalt für einen noch effektiven Ausgleich könnte in den Fällen, in denen die Wiedererlangung der Kontrolle mit verhältnismäßigem Aufwand möglich wäre, etwa der hypothetische Aufwand für die Wiedererlangung der Kontrolle dienen. Dabei haben die nationalen Gerichte nach der Rspr. des EuGHs in Ermangelung eigener europäischer Regelungen zur Bestimmung der Höhe des Anspruchs nach Art. 82 DSGVO die bestehenden nationalen Vorschriften im Lichter der Äquivalenz und Effektivität des Unionsrechts anzuwenden (EuGH, NJW 2024, 2599 Rn. 27). Soweit es der EuGH ausschließt,

dass im Rahmen der Ausgleichsfunktion des Schadensersatzanspruchs i.S.v. Art. 82 DSGVO ein möglicher Vorsatz des Verantwortlichen oder der Grad der Schwere des Verstoßes berücksichtigt wird, gibt er jedoch auch zu erkennen, dass der Schadensersatz der Höhe nach den konkret erlittenen Schaden vollständig ausgleichen muss (EuGH, a.a.O., NJW 2024, 2599 Rn. 29). Mit Blick auf den Vergleich physischer, materieller und immaterieller Schäden stellt der EuGH auf den 146. Erwägungsgrund der DSGVO ab und weist insoweit darauf hin, dass der Begriff des Schadens im Sinne der Rechtsprechung des EuGH auf eine Art und Weise weit ausgelegt werden sollte, die den Zielen dieser Verordnung in vollem Umfang entspricht mit der Folge, dass die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten sollten (EuGH NJW 2024, 2599 Rn. 36). Weiterhin führt er aus, dass durch die nationalen Vorschriften zur Umsetzung des immateriellen Schadensersatzanspruchs die Ausübung der durch das Unionsrecht verliehenen Rechte, insbesondere der DSGVO, nicht unmöglich gemacht oder übermäßig erschwert werden darf (EuGH, NJW 2024, 2599 Rn. 34.). Damit bringt der EuGH zum Ausdruck, dass an der deutschen Rechtsprechung, die bislang immateriellen Schadensersatz bei Persönlichkeitsrechtsverletzungen grundsätzlich nur höchst ausnahmsweise und insgesamt lediglich in geringem Umfang zugesprochen hat, bei der Anwendung der DSGVO nicht festgehalten werden darf (so auch Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18a; Ehmann/Selmayr/Nemitz, 3. Aufl. 2024, DS-GVO Art. 82 Rn. 38). Daraus folgt nicht zuletzt, dass trotz der Beschränkung auf den bloßen Ausgleich der erlittenen Nachteile, die Höhe des Schmerzensgeldes über die in der nationalen Rechtsprechungspraxis etablierten Beträge aus Schmerzensgeldtabellen hinausgehen kann (so auch Kühling/Buchner/Bergt, 4. Aufl. 2024, DSGVO Art. 82 Rn. 18d m.w.N.). Ein „Sich-Einfügen“ in die bisherige nationale Rechtsprechungspraxis stünde geradezu im Widerspruch zur europarechtsautonomen Auslegung des Schadensersatzanspruchs gem. Art. 82 DSGVO. Soweit andere Gerichte teilweise auf nationale Schadensersatzansprüche wie § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG zurückgreifen, um die erweiterten Schutzkategorien dieser Ansprüche einbeziehen zu können (Genugtuung und Prävention) – letztlich um die vermeintlichen Restriktionen des EuGHs mithilfe dieser Ansprüche dogmatisch zu umgehen – ist dieses Vorgehen ob der oben genannten Gründe redundant. Der EuGH betont nämlich, dass der Schadensersatzanspruch nach Art. 82 DSGVO neben den Sanktionen des Art. 83 DSGVO ebenfalls geeignet sein muss, die Einhaltung der Vorschriften der DSGVO sicherzustellen (EuGH NJW 2024, 1561 Rn. 62).

Die Höhe des Schadensersatzanspruchs ist nach der nationalen Vorschrift des § 287 ZPO zu schätzen. Nach § 287 Abs. 1 S. 1 ZPO entscheidet das Gericht nach

Würdigung aller Umstände nach freier Überzeugung. Hierbei handelt es sich um das Einfallstor für die o.g. europarechtlichen Vorgaben. Nach § 287 Abs. 1 S. 2 ZPO steht es schließlich im Ermessen des Gerichts, ob es im Rahmen der Schadensbemessung eine Beweisaufnahme durchführt. Anknüpfungspunkte für die Bemessung eines immateriellen Schadensersatzanspruchs muss hier vordergründig der auf der Klägerseite eingetretene Verlust der Daten sein. Dieser ist hinsichtlich des unterschiedlichen grundrechtlich garantierten Schutzniveaus der betroffenen Daten zu differenzieren. Dies gilt insbesondere, wenn besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO betroffen sind (OLG Dresden, Urt. v. 10.12.2024, Az. 4 U 808/24, ZD 2025, 221 Rn. 20). Zudem sind vor allem der Umfang der gesammelten Daten und die Dauer des Verstoßes zwischen der Verletzungshandlung zu berücksichtigen. Hierbei handelt es sich um Kategorien zur Feststellung der Schadenstiefe bzw. -intensität, die nicht gleichzusetzen sind mit dem Grad der Schwere des Verstoßes, den der EuGH für nicht berücksichtigungsfähig erklärt (EuGH, a.a.O., NJW 2024, 2599 Rn. 26). Darüber hinaus kann die Möglichkeit des Betroffenen an der Wiedererlangung seiner Daten bzw. der Kontrolle über diese eine Rolle spielen (OLG Dresden, a.a.O., ZD 2025, 221, Rn. 20). Weiterhin hat die Kammer bei der Schadensschätzung auch bezüglich dem Wert der personenbezogenen Daten einen entsprechenden Anknüpfungspunkt beigemessen. Hierfür ist auf den Wert personenbezogener Daten für die Beklagte – soweit dieser geschätzt werden konnte – abgestellt worden, zudem auf den allgemeinen Wert personenbezogener Daten auf dem hierfür relevanten legalen oder auch illegalen Markt. Die Berücksichtigung des Wertes der Daten für den Verletzer wird jedenfalls im Bereich der kommerziellen Nutzung auch in der Literatur gefordert (Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 82 Rn. 31, m.w.N.).

Für das Ausmaß und den Umfang der betroffenen Daten wird auf die bisherigen Ausführungen verwiesen. Dasselbe gilt für die Grundrechtssensibilität der betroffenen Daten. Den Wert der Daten für die Beklagte hat das Gericht auf der Grundlage der Feststellungen des BKartA (Beschl. v. 02.05.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) geschätzt. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der Werbeeinnahmen einen Anteil i.H.v. 97 % ausmachte (BKartA a.a.O., Rn. 7). Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O.,

Rn. 53). Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon überzeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studien (siehe nur die Studie "Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?", Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz). Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d.h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18b, beck-online).

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

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

Schadensschätzung nach § 287 ZPO, bei der die Freiheit der richterlichen Überzeugungsbildung zusätzlich erweitert wird. Insofern wäre es dem Gericht freigestellt gewesen, auf eine informatorische Anhörung des Klägers zu verzichten. Auch die vorliegend durchgeführte Anhörung des Klägers hat nach Überzeugung der Kammer gerade keinen weiteren Erkenntnisgewinn erbracht, der über die Mitteilung des Kontrollverlusts und der Verunsicherung, was die Beklagte mit den massenhaft gesammelten Daten beabsichtigt zu tun, hinausgeht. Grund hierfür ist, dass es gerade das Problem der klägerischen Partei und auch des Gerichts ist, festzustellen, was konkret die Beklagte mit den Daten vorhat bzw. was sie bereits jetzt unternimmt. Da dies bis zuletzt nicht bekannt wird, kann sich die Erwartung oder Befürchtung des Klägers nicht auf ein bestimmtes Verhalten konkretisieren. Dies kann und darf ihm nicht zum Nachteil gereichen. Soweit – wie im vorliegenden Fall – die vorgetragene spezifische Betroffenheit nicht über das Maß der allgemeinen Betroffenheit hinausgeht und sich damit keine Schadensvertiefung aus dem klägerischen Vortrag ableiten lässt, kann sich das Gericht allein auf die allgemeine Beeinträchtigung des Durchschnittsbetroffenen i.S.d. DSGVO beziehen. Die Kammer hat daher ohne auf das jeweilige subjektive Empfinden des konkreten Klägers abstellen zu müssen, eine durchschnittliche, aufgeklärte und verständige betroffene Person zu Grunde gelegt, und deren Betroffenheit als Maßstab für einen Mindestschaden herangezogen.

Die Mindestbeeinträchtigung ist ohne das Hinzutreten weiterer Umstände bereits besonders schwerwiegend und hebt sich maßgeblich von den sog. Scraping-Fällen ab, in denen ein Mindestschaden i.H.v. 100 € für den bloßen Kotrollverlust für angemessen erachtet wird (siehe nur OLG Dresden, a.a.O., ZD 2025, 221 Rn. 20 m.w.N.). Anders als in den Scraping-Fällen ist die Quantität und Qualität der streitgegenständlichen Daten um ein Vielfaches größer, sodass der Mindestschaden weitaus höher einzustufen ist. Die Datenverarbeitung durch die Beklagte stellt nach der Rspr. des EuGHs per se einen schweren Eingriff in die durch Art. 7 und 8 GrCh gewährleisteten Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten dar (EuGH NJW 2025,207 Rn. 63), der nicht gerechtfertigt ist. Die Verletzung dieser Grundrechte wird auch durch den Durchschnittsbetroffenen i.S.d. DSGVO als erhebliche Beeinträchtigung im o.g. Sinne wahrgenommen. Der aufgeklärte und verständige Durchschnittsbetroffenen i.S.d. DSGVO wird sich der Bedeutung und Tragweite der über ihn gesammelten Daten bewusst, denn er kennt die Relevanz von personenbezogenen Daten innerhalb einer digitalisierten Gesellschaft und Wirtschaft (s.o. zur Wahrnehmung der Gesellschaft hinsichtlich der Werthaltigkeit von Daten). Der Kontrollverlust über nahezu sämtliche Daten seiner Online-Nutzungsaktivitäten bedeutet für ihn eine dauerhafte und nicht ohne Weiteres zu beseitigende negative Beeinflussung, die sich nach außen hin in unterschiedlichen Sorgen und Ängsten manifestiert. In jedem Falle setzt sich der Nutzer gezwungener Maßen mit dem Verlust der personenbezogenen

Daten auseinander und wird hierdurch in Bezug auf sein weiteres Verhalten bei der Nutzung des Internets dauerhaft beeinflusst.

Das Gericht erachtet anhand der obigen Ausführungen in der Gesamtschau einen Betrag i.H.v. insgesamt 5.000 € für einen angemessenen Schadensersatz. Dieser Betrag ergibt sich, wenn man für jedes Jahr der Datenschutzverletzung der vorliegenden Art und des dadurch erlittenen Kontrollverlustes einen Betrag von 1.000,00 € je Jahr, gerechnet ab dem Inkrafttreten der DSGVO am 25. Mai 2018 bis zur außergerichtlichen Inanspruchnahme der Beklagten im Jahr 2023 ansetzt. Dies ergibt vorliegend einen Betrag von 5.000 €, da der Kläger bereits bei Inkrafttreten der DSGVO am 25. Mai 2018 Nutzer der Beklagten war. Insofern war zu berücksichtigen, dass zur Überzeugung des Gerichts nicht festgestellt werden konnte, dass im Rahmen der streitgegenständlichen Datenverarbeitung besondere Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO verarbeitet wurden. Die klagende Partei hat insofern in ihrer Anhörung zwar glaubhaft angegeben, teilweise auch Webseiten zu besuchen, auf denen Gesundheitsinformationen geteilt werden und aus dessen Besuch sich Rückschlüsse über die gesundheitliche Situation ihrer Familie ergeben können. Konkrete Angaben hat der Kläger auf Anraten seines Prozessbevollmächtigten jedoch nicht gemacht. Dementsprechend kann nicht festgestellt werden, ob auf diesen unbekannten Webseiten die Meta Business Tools integriert waren und ob dementsprechend die Beklagte Daten i.S.d. Art. 9 DSGVO verarbeitet hat. Auch sonst konnte die klagende Partei nicht den Nachweis erbringen, dass die Beklagte im konkreten Fall über die streitgegenständlichen Meta Business Tools besondere Kategorien personenbezogener Daten verarbeitet. Soweit die klagende Partei behauptet, die Beklagte wisse, welche politische Gesinnung sie habe, welche sexuelle Orientierung oder welchen Gesundheitszustand, blieb dies zu unkonkret. Entscheidend für die Bemessung nach Jahren ist aber, dass die Meta Business Tools seit mehreren Jahren genutzt werden, um heimlich, also auch ohne Einwilligung, personenbezogene Daten der klagenden Partei zu verarbeiten. Da dies nicht jedem Nutzer der Beklagten geläufig sein dürfte, der Kläger glaubhaft dargelegt hat, dass es ihm nicht geläufig war, darf dieser Umstand der Ungewissheit der Beklagten, die es auch im vorliegenden Verfahren nicht eingesehen hat, die vom Kläger ohne Einwilligung gespeicherten Daten offen zu legen, nicht im Rahmen der Bemessung des Schadensersatzes zum Vorteil gereichen. Außerdem ist zu berücksichtigen, dass ein weiter Empfängerkreis besteht. Die Beklagte teilt die von ihr erhobenen personenbezogenen Daten der klagenden Partei mit Werbetreibenden und Audience Network-Publishern, mit Partnern, die die Analysedienste der Beklagten nutzen, integrierten Partnern, Anbietern für Messlösungen, Anbietern für Marketinglösungen, allen möglichen Dienstleistern und externen Forschern. Eine Änderungsmöglichkeit der personenbezogenen Daten besteht offensichtlich nicht. Zudem ist der Aufwand, dem Kontrollverlust entgegenzuwirken, vergleichsweise hoch, was allein schon daran deutlich wird, dass die Klägerin vorliegend Klage

erheben musste, um eine weitere Erhebung der personenbezogenen Daten durchzusetzen.

Zum Vergleich ist in der Rechtsprechung wegen Ausspähung durch Einschaltung eines Detektivbüros einen Schadensersatzanspruch i.H.v 5.000 € für angemessen erachtet worden (OLG Dresden, Urt. v. 30.11.2021, Az. 4 U 1158/21, NZG 2022, 335). Die Reichweite der im hiesigen Verfahren betroffenen Daten geht über das Maß in dem Verfahren vor dem OLG Dresden hinaus, da nach dem als zugestanden anzusehenden klägerischen Vortrag dessen gesamtes im digitalen Bereich stattfindendes Privatleben dauerhaft und nicht nur auf einzelne Aspekte begrenzt aufgezeichnet wurde und immer noch wird. Seit dem Inkrafttreten der DSGVO handelt es sich bei dem als zugestanden anzusehenden Vorgehen der Beklagten um einen solch weitgehenden Verstoß, der den Rahmen der bisher bekannten Fälle bei weitem überschreitet, sodass der Mindestbetrag von 1000,00 € für jedes Jahr der Datenschutzverletzung ohne Darlegung einer besonderen individuellen Betroffenheit erforderlich, aber auch angemessen ist. Die Kammer ist sich dabei der Tatsache bewusst, dass das Zusprechen eines Betrags i.H.v. 1.000 € je Jahr ohne das Erfordernis der spezifischen Darlegung einer über das gerichtlich festgestellte Maß der Mindestbeeinträchtigung hinausgehenden Intensität praktisch bedeutet, dass eine Vielzahl von Nutzern der Beklagten ohne größeren Aufwand Klage erheben kann. Dem stehen jedoch keine durchgreifenden Bedenken gegenüber, denn diese Form der privaten Rechtsdurchsetzung ist nach dem Willen des europäischen Gesetzgebers und der Rechtsprechung des EuGHs nach den obigen Ausführungen gerade bezweckt und dient in Form des sog. Private Enforcement dazu, die Einhaltung der Vorschriften der DSGVO und damit deren Effektivität zu gewährleisten. Zudem ist angesichts der bezogen auf Deutschland vorgetragenen Anzahl von Klagen, die durch die Prozessbevollmächtigten des Klägers bislang erhoben worden sind, keine existenzgefährdende Wirkung auf die Beklagte zu befürchten. Denn im Hinblick auf die Höhe der bereits erörterten jährlichen Erlöse der Beklagten mit Werbung geht es, selbst wenn alle Klage erfolgreich sein sollten, insgesamt betrachtet um Beträge, die die Beklagte ohne weiteres bedienen kann.

Dass der Kläger auch nach Kenntniserlangung über die Datenverarbeitung nach wie vor die von der Beklagten angebotenen Dienste in Anspruch nimmt, wirkt sich nicht anspruchsmindernd aus. Aufgrund der überragenden marktübergreifenden Stellung der Beklagten auf Social-Media-Plattformen ist es dem Nutzer, auch wenn er Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass der Kläger ihre Netzwerke DSGVO-konform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt der Kläger zum Ausdruck, dass ihm die Datenschutzverstöße der Beklagten nicht egal

sind, sondern er eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es dem Kläger hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, sein Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden. Dementsprechend scheidet auch ein Mitverschulden des Geschädigten i.S.v. § 254 BGB aus, wobei für den Schadensersatzanspruch nach Art. 82 DSGVO umstritten ist, ob lediglich unter den Voraussetzungen von Art. 82 Abs. 3 DSGVO ein Ausschluss der Haftung in Betracht kommt (siehe Kühling/Buchner/Bergt DS-GVO Art. 82 Rn. 59 m.w.N. auch zur Gegenansicht).

Der Zinsanspruch folgt aus § 286 Abs. 1, § 288 Abs. 1 BGB. Durch die erfolglos gebliebene Zahlungsaufforderung befand sich die Beklagte ab dem 05.09.2023 Verzug. Antragsgemäß waren Zinsen ab dem 05.09.2023 zuzusprechen.

5.

Die klagende Partei hat einen Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten in Höhe von 627,13 € aus Art. 82 DSGVO. 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. Daher kann sich auch aus Art. 82 DSGVO unter diesen Voraussetzungen ein Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten ergeben (BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 79 f.). Es erscheint gerade im Hinblick darauf, dass zum Zeitpunkt des vorgerichtlichen Tätigwerdens eine Vielzahl von Rechtsfragen in Zusammenhang mit Art. 82 DSGVO noch ungeklärt waren, aus Sicht der Klägerin höchst nachvollziehbar, sich zur Durchsetzung ihrer Ansprüche eines Rechtsanwalts zu bedienen (vgl. auch BGH, Urteil vom 18. November 2024 – VI ZR 10/24 –, juris Rn. 80). Der Höhe nach berechnen sich die Gebühren nach einem Gegenstandswert von bis zu 6.000,00 €. Insofern gilt, dass die allein begründeten vorgerichtlich geltend gemachten Auskunfts-, sowie Löschungsansprüche jeweils mit 500 € zu berücksichtigen sind. Hinzuzurechnen ist der ebenfalls geltend gemachte Schadensersatzanspruch; in Höhe der tatsächlich berechtigten 5.000,00 €. Unter Berücksichtigung einer 1,3 Geschäftsgebühr gem. §§ 2, 13 RVG, Nr. 2300 VV RVG, der Auslagenpauschale gem. Nr. 7002 VV RVG, sowie 19% Umsatzsteuer ergibt sich so ein Betrag i.H.v. 627,13 €.

III.

Die Entscheidung über die Kosten folgt aus §§ 92 Abs. 1, 269 III 2 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 Satz 1, 2, § 708 Nr. 11, 711 ZPO.

IV.

Den Gebührenstreitwert setzt die Kammer endgültig auf 12.000,00 € fest.

Die Streitwertentscheidung beruht auf §§ 3, 5 Halbsatz 1 ZPO i.V.m. § 48 Abs. 1 Satz 1, Abs. 2 Satz 1 GKG. Den Streitwert für nichtvermögensrechtliche Ansprüche bestimmt das Gericht gemäß § 48 Abs. 2 Satz 1 GKG unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache sowie der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen; er kann im Einzelfall von dem in § 23 Abs. 3 Satz 2 Halbsatz 2 RVG vorgesehenen Regelstreitwert von 5.000,00 € erheblich abweichen. Dabei sind insbesondere das Interesse des Klägers und seine zu besorgende wirtschaftliche sowie persönliche Beeinträchtigung zu berücksichtigen. Zu berücksichtigen sind zudem die Stellung der Parteien sowie Art und Umfang der begehrten Handlung. Die Wertangaben in der Klageschrift sind für das Gericht nicht bindend; ihnen kommt aber, wenn sie nicht offensichtlich unzutreffend sind, ein erhebliches Gewicht zu (vgl. OLG Hamm, Urteil vom 15.08.2023 – 7 U 19/23, GRUR 2023, 1791 [1807 Rn. 258 f.] m.w.N.).

1. Der Streitwert für den Antrag zu Ziffer 1) ist gemäß § 3 ZPO und § 48 Abs. 2 Satz 1 GKG auf 500,00 € festzusetzen, da dieser keine über die weiteren Anträge hinausgehende Bedeutung hat.
2. Der Unterlassunganspruch bezüglich zukünftiger Datenerhebung wurde mit 5.000,00 € festgesetzt und entspricht dem für die bisherige Verletzung begehrten Schadensersatzanspruch.
3. Der Antrag zu 3 auf Unterlassung der Verarbeitung wurde auf 500,00 € festgesetzt, da insoweit ein geringeres Interesse vorliegt, weil sich der Kläger gerade gegen die ursprüngliche und weitere Datenverarbeitung richtet und bisher ausdrücklich von der klageweisen Durchsetzung eines Auskunftsanspruchs abgesehen hat.
4. Der unzulässige Antrag zu 4 auf Verpflichtung zur Löschung und Anonymisierung wurde mit 1.000,00 € festgesetzt.
5. Der Zahlungsanspruch wurde auf 5.000,00 € festgesetzt.
6. Die zwischenzeitlich fallengelassenen Hilfsanträge waren gemäß § 45 Abs. 1 S. 2 GKG nicht zu berücksichtigen. Nebenforderungen waren gemäß § 43 Abs. 1 GKG nicht zu berücksichtigen.

Dr. [redacted]