

15 O 1/25

Verkündet am
[] durch Zustellung (§ 310 III ZPO)



als Urkundsbeamtin/er der
Geschäftsstelle

Landgericht Lübeck

Urteil

Im Namen des Volkes

In dem Rechtsstreit

[REDACTED]

- Kläger -

Prozessbevollmächtigte:

Rechtsanwälte **BK Verbraucherschutz Rechtsanwaltsgesellschaft mbH**, Viktoria-Luise-Platz 7, 10777 Berlin, Gz.: BKD-003914-IUS

gegen

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

- Beklagte -

Prozessbevollmächtigte:

[REDACTED]

wegen Ansprüche aus DSGVO wegen Datenverarbeitung

hat die 15. Zivilkammer des Landgerichts Lübeck durch den Vorsitzenden Richter am Landgericht [REDACTED] als Einzelrichter auf Grund der mündlichen Verhandlung vom 16.10.2025 für Recht erkannt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1, Abs. 3 Satz 1 DSGVO zu erteilen, welche personenbezogenen Daten des Klägers seit dem 01.04.2022

- durch die Software-Tools „Meta Business Tools“ erfasst wurden,

- nach Erfassung an die Server der Beklagten weitergeleitet wurden,

- dort gespeichert und anschließend verwendet wurden,

und weiterhin im Zusammenhang mit den so beauskunfteten Daten Auskunft zu jedem Datum gem. Art. 15 Abs. 1 lit. c., g. und h. DSGVO darüber zu erteilen,

- welchen Empfängern oder Kategorien von Empfängern die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,

- welche Herkunft die Daten haben.

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 bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers mit Hilfe der Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden.

3. Die Beklagte wird verurteilt, an den Kläger 5.500,00 Euro nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 11.10.2023, zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits trägt die Beklagtenseite.

6. Das Urteil ist wie vorläufig vollstreckbar, für die Klagepartei gegen Sicherheitsleistung in Höhe von 16.000,00 Euro und für die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags.

Der Streitwert wird auf 16.000,00 € festgesetzt.

Tatbestand

Die Beklagte ist Betreiberin des Netzwerkes „Facebook“. Dieses Netzwerk ermöglicht es den Nutzern, persönliche Profile zu erstellen und in dem Umfang ihrer so erstellten Präsenz in diesem Netzwerk mit anderen Nutzerinnen und Nutzern in Kontakt zu treten.

Die Beklagte ist ferner die Entwicklerin sog. „Meta Business Tools“, namentlich „Meta Pixel“, „App Events über Facebook-SDK“ und „Conversions API“ sowie „App Events API“ (nachfolgend genannt: „Business Tools“). Diese Business Tools werden von zahlreichen Drittunternehmen auf deren Webseiten, Servern oder Apps eingebunden. Betroffen sind insbesondere zahlreiche reichweitenstarke Webseiten und Apps in Deutschland, wie etwa zahlreiche große Nachrichtenseiten und -Apps (spiegel.de, bild.de, welt.de, faz.net, stern.de), große Reiseseiten und -Apps wie z.B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de, momondo.de), Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, aerzte.de, helios-gesundheit.de, jameda.de), Dating- und Erotikseiten (parship.de, amorelie.de, orion.de, lovescout24.de), aber auch Seiten mit Inhalten aus der Intimsphäre (krebshilfe.de, tfp-fertility.com (Samenbank), nie-wieder-alkohol.de, nvve.nl (Sterbehilfe in den Niederlanden mit deutschsprachigem Angebot)). Eine vollständige Übersicht der betroffenen Webseiten wurde und wird von der Beklagten nicht veröffentlicht. Nach - nicht substantiiert bestrittener - klägerischer Darstellung sind in Deutschland exemplarisch etwa die in Anlage K 4 gelisteten großen Webseiten nachweisbar betroffen.

Genereller Zweck dieser 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. Hierzu können von den Business Tools Daten an die Beklagte übermittelt werden. Im Einzelnen unterscheiden sich dabei die technischen Abläufe nach der Art der eingebundenen Tools.

Ist auf der von der Nutzerin oder dem Nutzer besuchten Seite das Business Tool „Meta Pixel“ bzw. auf der App das Business Tool „App Events“ eingebunden, stellt sich der Ablauf wie folgt dar: Sobald die Nutzerin oder der Nutzer die Webadresse oder URL eingegeben hat, kommuniziert der Browser der Nutzerin oder des Nutzers mit dem Server des Drittseitenanbieters, um die Inhalte der Seite zu laden (sog. HTTP-Anfrage). Sind auf dieser Seite Drittinhalte – wie die vorgenannten Business-Tools – eingebunden, weist der Server des Drittanbieters den Browser der Nutzerin oder des Nutzers an, auch mit den Servern der Beklagten zu kommunizieren, um diese eingebetteten Inhalte anzufragen. Der Browser der Nutzerin oder des Nutzers stellt hierauf eine weitere HTTP-Anfrage, nunmehr an die Server der Beklagten. Diese HTTP-Anfrage enthält dabei bestimmte standardisierte technische Informationen über das Gerät der Nutzerin bzw. des Nutzers, 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 et-

wa 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. Im weiteren Verlauf kann dann das derart aktivierte „Business-Tool“ 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“) an Meta übertragen, wobei Art und Umfang der übermittelten Daten davon abhängen, welches der vorgenannten Business Tools das Drittunternehmen integriert hat und wie es dieses Tool im Einzelnen einsetzt.

Ist auf der von der Nutzerin oder dem Nutzer besuchten Seite hingegen das Business Tool „Conversions API“ bzw. auf der App das Business Tool „App Events API“ (im folgenden: „API-Tools“) eingebunden, erfolgte keine weitere direkte HTTP-Abfrage an die Beklagte. Vielmehr wird das Business-Tool im Folgenden und unter im Einzelnen streitigen Umständen direkt auf dem Server des Drittanbieters aktiv und kann von dort die vorgenannten technischen Standarddaten sowie „weitere personenbezogene Daten“ an die Beklagte übermitteln.

Die vorgenannten Abläufe auf den Drittseiten erfolgen dabei unabhängig davon, ob die Nutzerin oder der Nutzer zu diesem Zeitpunkt die App von Instagram bzw. Facebook aktiviert hat. Für den durchschnittlichen Internetnutzer ist nicht erkennbar, ob die jeweils besuchte Webseite mit einem Meta Business Tool ausgestattet worden ist.

Die Nutzerinnen und Nutzer von Facebook können dabei über die dortigen Einstellmöglichkeiten innerhalb der Metasysteme (Rubrik „Meta Cookies auf anderen Apps und Webseiten“) Einfluss darauf nehmen, wie die derart bei der Beklagten eingehenden Daten weiterverwendet werden.

Die wie oben beschrieben bei der Beklagten eingehenden Daten werden von der Beklagten wie folgt - und teilweise in Abhängigkeit von den Einstellungen - weiterverarbeitet:

- mittels der eingehenden 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 In-

formation weiter an. Dieser Vorgang erfolgt (soweit die Daten überhaupt übertragen werden) unstreitig *immer* und insbesondere und *unstreitig* (vgl. Protokoll vom 16.10.2025, S. 9 in Zusammenschau mit der Klageerwiderung, dort Rn. 33 ff.) 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“.

Die Klägerseite selbst nutzt seit dem 13.4.2023 ausschließlich privat das Netzwerk Facebook unter dem Benutzernamen „[REDACTED]“. Die Klägerseite hat ausdrücklich ausgewählt, Meta's Nutzung von optionalen „Meta Cookies in anderen Apps und auf anderen Websites“ zuzustimmen.

Die Beklagte stellt ihren Nutzerinnen und Nutzern sog. „Self-Service“-Tools zur Verfügung, insbesondere das „Deine Aktivitäten außerhalb der Meta-Technologien“-Tool. Die Beklagte listet dabei zahlreiche, so auch gerichtsbekannte Einschränkungen auf, der die Auskünfte über dieses Tool unterliegen. Auszugsweise informiert die Beklagte ihre Nutzerinnen und Nutzer gerichtsbekannt wie folgt:

Hinweis: Unter „Aktivitäten außerhalb der Meta-Technologien“ siehst du nicht alle deine Aktivitäten. Zum Beispiel:

- **Deine jüngsten Aktivitäten sind in der Zusammenfassung nicht enthalten.** Es kann einige Tage dauern, bis deine Aktivitäten in „Aktivitäten außerhalb von Meta-Technologien“ angezeigt werden. Das jeweilige Datum in der Zusammenfassung deiner Aktivitäten gibt an, wann wir über diese Aktivität informiert wurden.
- **Wir erhalten mehr Einzelheiten und Aktivitäten, als du unter „Aktivitäten außerhalb von Meta-Technologien“ siehst.** Aus technischen Gründen und aus Gründen der Zuverlässigkeit zeigen wir nicht alle Aktivitäten, über die wir informiert wurden. Das betrifft unter anderem Informationen, die wir erhalten haben, während du nicht bei Facebook angemeldet warst, oder Situationen, in denen wir nicht überprüfen können, ob du auf einem bestimmten Gerät zuvor Facebook verwendet hast. Ebenso wenig zeigen wir Einzelheiten an, wie etwa den Artikel, den du zu deinem Einkaufswagen hinzugefügt hast.
- **Es kann vorkommen, dass wir aus technischen Gründen die Verknüpfung mit deinen Aktivitäten außerhalb von Meta-Technologien aufheben.** In diesem Fall werden dir keine Anzeigen in Zusammenhang mit den nicht mehr verknüpften Aktivitäten angezeigt.

Die Klägerseite forderte mit vorgerichtlichem Anwaltsschreiben vom 12.09.2023 (Anlage K 7) die Beklagte dazu auf, anzuerkennen, dass die Datenverarbeitung hinsichtlich Aktivitäten außerhalb des sozialen Netzwerkes ohne wirksame Einwilligung nicht zulässig sei, sich zu verpflichten, Daten auf Aufforderung zu anonymisieren oder zu löschen, anzuerkennen, dass eine vollständige Auskunft auf Aufforderung erteilt wird, es zu unterlassen, Daten zu verarbeiten, die Aktivitäten außerhalb des Netzwerkes betreffen und 5.000,00 € zu zahlen. Innerprozessual erteilte die Beklagte Auskunft mit Schreiben vom 06.06.2025 (Anlage B 9). Hinsichtlich des weiteren Inhalts wird auf die beiden Schreiben vollumfänglich Bezug genommen. Die Klägerseite behauptet, hierfür seien die mit dem Antrag zu 5. geltend gemachten Kosten entstanden.

Die Klägerseite behauptet, die Business Tools der Beklagten seien auf 30 - 40 % aller Webseiten weltweit und einer großen Zahl beliebter Apps aktiv. Nicht nur die „technischen Daten“, sondern auch umfangreiche „weiteren personenbezogenen Daten“ würden über die Meta Business-Tools immer und unabhängig davon, ob die Besucher hierin einwilligten oder nicht, an die Beklagte

übermittelt. Insbesondere auf die im Schriftsatz vom 17.12.2024, dort S. 17 ff. (Bl. 17 ff. d.A.) ausgeführten Fallbeispiele wird Bezug genommen. Erst dort werte die Beklagte aus, ob sie die rechtliche Befugnis hat, die empfangenen Daten zu verarbeiten. Die Daten würden von der Beklagten dann an die Mutterfirma in den USA sowie an weitere Firmen weitergegeben und im Meta-Konzern etwa zu Werbezwecken verwendet werden und zwar auch dann, wenn die Nutzer*innen hierin nicht einwilligen.

Die Klägerseite besuche regelmäßig Webseiten, auf denen Business Tools vorzufinden seien, insbesondere die Seiten "t-online.de", "finanzen.net", "docmorris.de". Sie fühle sich der Beklagten ausgeliefert und habe große Sorge, dass die Beklagte zu viel über sie wisse und habe Angst, dass mit Hilfe von KI eine Analyse ihrer Interessen, Reizthemen, Hoffnungen und Sorgen möglich wird, die genutzt werden kann, um sie zu manipulieren. Hinsichtlich des Klägervortrages hierzu im Einzelnen wird Bezug genommen auf die Replik vom 11. August 2025, dort S. 10 ff. (Bl. 177 ff. d.A.).

Die Klägerseite beantragt,

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1, Abs. 3 Satz 1 DSGVO zu erteilen, welche personenbezogenen Daten des Klägers seit dem 13.04.2023

- durch die Software-Tools „Meta Business Tools“ erfasst wurden,**
- nach Erfassung an die Server der Beklagten weitergeleitet wurden,**
- dort gespeichert und anschließend verwendet wurden,**

und weiterhin im Zusammenhang mit den so beauskunfteten Daten Auskunft zu jedem Datum gem. Art. 15 Abs. 1 lit. c., g. und h. DSGVO darüber zu erteilen,

- welchen Empfängern oder Kategorien von Empfängern die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,**
- welche Herkunft die Daten haben, inwieweit die Daten des Klägers für eine automatisierte Entscheidungsfindung einschließlich Profiling verwendet wurden und werden. Die Beklagte hat hierfür aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für die betroffene Person zu erteilen.**

2. Die Beklagte wird verpflichtet, die Daten gem. dem Antrag zu 1. nach Auskunftserteilung zu löschen.

3. 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 bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers mit Hilfe der Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden.

4. Die Beklagte wird verurteilt, an den Kläger eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 11.10.2023, zu zahlen.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, im Hinblick auf die Datenflüsse im Kontext des Einsatzes der Business Tools „Meta Pixel“ bzw. „App Events“ sei die oben beschriebene Erhebung und Übertragung der technischen Standarddaten an die Beklagte per HTTP-Abfrage der zeitgemäßen Nutzung des Internets immanent. Die Drittanbieter könnten zudem die Übermittlung der technischen Standarddaten per HTTP-Anfrage an die Beklagte „pausieren“ bis die Nutzer über Cookie-Banner ihre Einwilligung hierzu erteilt hätten. Im Hinblick auf alle eingesetzten Business-Tools behauptet die Beklagte, dass die Frage, welche Daten („technische Standarddaten“ und „weitere personenbezogene Daten“) *durch die Business-Tools selbst* an die Beklagte übermittelt würden, hinge davon ab, ob die Nutzerinnen und Nutzer diesbezüglich vorab zugestimmt hätten sowie von der Konfiguration der Einstellungen der Business-Tools bei den Drittanbietern. Die Drittfirmen hätten sich verpflichtet, diese Datenübertragungsfunktionen der Business Tools nur dann zu aktivieren, wenn sie zuvor eine Zustimmung der Nutzer*innen eingeholt hätten. Eine Kontrolle dahingehend, ob dies von den Drittfirmen auch umgesetzt worden sei, finde jedoch nicht statt. Es werde von der Beklagten jedoch überprüft, ob die übermittelten Daten besonders geschützte personenbezogene

Daten enthielten.

Die Beklagte behauptet, mit Hilfe der „Self-Service“-Tools könne die Klägerseite auf ihre personenbezogenen Daten im Zusammenhang mit der streitgegenständlichen Datenverarbeitung zugreifen und diese herunterladen. Die Beklagte meint, sie habe das Auskunftsbegehren mit ihrem Schreiben vom 6. Juni 2025 (Anlage B9) erfüllt.

Für den weiteren Parteivortrag wird auf den Inhalt der wechselseitigen Schriftsätze sowie insbesondere die Ausführungen in den mündlichen Verhandlungen Bezug genommen.

Entscheidungsgründe

I. Die Klage ist zulässig und im tenorierten Umfang begründet, im Übrigen unbegründet.

1. Die Klage ist zulässig.

a. Das Landgericht Lübeck ist in internationaler, sachlicher und örtlicher Hinsicht zuständig.

(1) Die internationale Zuständigkeit der deutschen Gerichtsbarkeit folgt aus Art. 79 Abs. 2 S. 2 DSGVO, nachdem die Klägerseite ihren gewöhnlichen Aufenthalt in Deutschland hat.

(a) Gemäß § 79 Abs. 2 DSGVO sind für Klagen gegen einen Verantwortlichen im Ausgangspunkt die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Nach S. 2 der Vorschrift können solche Klagen wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich – was vorliegend nicht der Fall ist - bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Sinn und Zweck dieser Zuständigkeitsregelung ist die Gewährleistung (und Erleichterung) eines effektiven Rechtsschutzes durch die betroffenenfreundliche Möglichkeit einer Klageerhebung am Aufenthaltsort, wobei damit nicht der „tatsächliche“, sondern der „gewöhnliche“ Aufenthaltsort gemeint ist, wie der Wortlaut der englischen Sprachfassung („habitual residence“) verdeutlicht (*Spindler/Dalby*, in: *Spindler/Schuster*, Recht der elektronischen Medien, 4. Aufl. 2019, DS-GVO Art. 79 Rn. 19).

Diese Voraussetzungen liegen vor. Die Beklagte ist Verantwortliche bzw. Auftragsverarbeitende im Sinne der DSGVO. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristi-

sche Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte hat vorliegend als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden, sodass sie insoweit als Verantwortliche im Sinne der DSGVO anzusehen ist (vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris; vgl. im Einzelnen auch unten); sie ist auch keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Die Klägerseite als betroffene Person hat ihren Wohnsitz in Steinburg im Kreis Herzogtum Lauenburg, sodass die deutsche Gerichtsbarkeit international zuständig ist.

(b) Es kann offenbleiben, ob Art 79 Abs. 2 DSGVO in seinem vorliegend eröffneten Anwendungsbereich die allgemeinen Zuständigkeitsvorschriften der EuGVVO verdrängt (in diesem Sinne etwa *Bergt* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 79 Rn. 15 m.w.N., Albrecht/Jotzo, Das neue Datenschutzrecht der EU, Teil 8: Rechtsbehelfe, Haftung und Sanktionen Rn. 29) oder die Vorschriften daneben anwendbar bleiben (in diesem Sinne wohl Gola/Heckmann/*Werkmeister*, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, DS-GVO Art. 79 Rn. 15). Denn auch nach den Vorschriften der EuGVVO ist keine abweichende ausschließliche Zuständigkeit im Sinne des Art. 24 EuGVVO begründet, sondern folgt die internationale Zuständigkeit der deutschen Gerichtsbarkeit vorliegend sowohl aus Art. 7 Nr. 1 lit. b) als auch Art. 18 Abs. 1 Alt. 2, Art. 17 Abs. 1 lit. c) EuGVVO (vgl. BGH, Urteil vom 29. Juli 2021 – III ZR 179/20 –, BGHZ 230, 347-389, Rn. 24). Nach Art. 18 EuGVVO kann ein Verbraucher gegen eine Vertragspartei, die ihre Tätigkeit auf den Mitgliedsstaat, in dem der Verbraucher seinen Wohnsitz hat, ausrichtet, vor dem Gericht seines Wohnsitzes Klage erheben.

Vorliegend nutzt die Klägerseite als Privatperson die Plattform der Beklagten, die dabei gewerblich handelt (EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 60, juris) und ihre Tätigkeit z.B. durch entsprechende Sprachoptionen auch speziell auf das Gebiet der Bundesrepublik und hier ansässige Nutzer ausgerichtet hat. Im Übrigen wäre aufgrund der Natur der Sache die Leistung der Beklagten, nämlich das Zurverfügungstellen der Nutzungs- und Kommunikationsmöglichkeiten, am Wohnsitz des Schuldners zu erbringen, so dass sich bereits aus Art. 7 Nr. 1 lit. b) 2. Spiegelstrich EuGVVO die internationale Zuständigkeit deutscher Gerichte ergibt.

(2) In sachlicher Hinsicht ist das erkennende Gericht gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG zuständig, nachdem der Wert des Streitgegenstandes 5.000,00 € übersteigt.

(3) Die örtliche Zuständigkeit des Landgerichts folgt sowohl aus § 44 Abs. 1 S. 2 BDSG als auch aus Art. 7 Nr. 1 lit. b) EuGVVO.

(a) Art. 79 Abs. 2 S. 1 DS-GVO regelt nur die internationale, nicht auch die örtliche Zuständigkeit (BR-Drs. 110/17, Anl., 111; Paal/Pauly/Frenzel, 3. Aufl. 2021, BDSG § 44 Rn. 1). Insoweit bestimmt § 44 Abs. 1 S. 2 BDSG, dass Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person auch bei dem Gericht des Ortes erhoben werden können, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Diese Voraussetzungen liegen vor, nachdem die Klägerseite ihren gewöhnlichen Aufenthalt im hiesigen Gerichtsbezirk hat.

(b) Im Übrigen folgt die örtliche Zuständigkeit auch aus Art. 7 Nr. 1 lit. b) EuGVVO, der – anders als die Art 17, 18 EuGVVO, die wie auch Art. 4 EuGVVO nur die internationale Zuständigkeit regeln – auch eine Regelung zur örtlichen Zuständigkeit enthält (*Geimer* in: Zöller, Zivilprozessordnung, 35. Aufl. 2022, Artikel 7 (Artikel 5 LugÜ), Rn. 1).

b. Der Antrag zu 2. ist unzulässig. Der Antrag ist nicht hinreichend bestimmt. In der Sache bezieht sich der Antrag auf eine unbestimmt große Zahl nicht näher benannter und dem Kläger auch nicht im Einzelnen bekannter Datenpunkte, mithin einer Gesamtheit von Datenpunkten unklarer Zahl. Die Benennung einer Gesamtheit von Gegenständen oder - hier - Datenpunkten unter Sammelbezeichnungen mag insoweit zwar in Einzelfällen zulässig sein, um den Anspruchstellern nicht unerfüllbare Vorgaben im Hinblick auf die Bestimmtheit aufzuerlegen. Mindestens erforderlich ist jedoch immer, dass die Sammelbezeichnung selbst derart bestimmt ist, dass sie sodann im Vollstreckungsverfahren eine klare Bestimmung der umfassten Gegenstände oder Datenpunkte zulässt. Dies ist hier nicht der Fall. Denn durch die Bezugnahme auf Ziff. 1 ist der Antrag beschränkt auf die dort aufgeführten Datenpunkte, die die Beklagte mit Hilfe der Meta Business Tools erfasst hat. Ob aber ein konkreter, bei der Beklagten etwaig noch gespeicherter Datenpunkt (z.B. die Email-Adresse, das Geburtsdatum etc. pp.) zuvor „mit Hilfe der Meta Business Tools“ erlangt wurde, dürfte regelmäßig alles andere als selbsterklärend sein - und wäre dann aufwändig im Vollstreckungsverfahren zu prüfen. Dies steht im Widerspruch zu dem Erfordernis einer unmissverständlichen Bezeichnung der Datenpunkte, die hier Gegenstand des Ausspruches sein sollen und droht aufwändige Rechtsstreitigkeiten ins Vollstreckungsverfahren zu verschleppen. Dies - und damit die hier von der Klägerseite entworfene Antragsformulierung - ist unzulässig.

c. Im Übrigen bestehen keine Bedenken hinsichtlich der Zulässigkeit der noch anhängigen Anträ-

ge. Insbesondere bestehen keine Bedenken gegen die Zulässigkeit des geltend gemachten Unterlassungsantrags.

(1) Die routinemäßig vorgetragenen Einwände der Beklagten im Hinblick auf die angebliche Unzulässigkeit des Rechtsschutzzieles teilt die Kammer nicht. Bei den vorgebrachten Einwänden handelt es sich letztlich nicht um ein rechtliches, sondern um rein rechtspolitisches Vorbringen, das von der irrigen Annahme ausgeht, die Beklagte habe grundsätzlich einen quasi naturgegebenen Anspruch auf ungestörte Anwendung der von ihr konzipierten „Business Tools“. Rechtlich gilt vielmehr das Gegenteil: Wenn die Beklagte Anwendungen auf den Markt bringt, mit denen sie jedoch keinen rechtskonformen Betrieb für alle Nutzer*innen sicherstellen kann, dann wird sie den Einsatz dieser „Tools“ jedenfalls dann unterlassen müssen, wenn sich die Betroffenen hiergegen rechtlich zur Wehr setzen. Dies kann dann auch bedeuten, dass die Beklagte die Tools insgesamt vom Markt nehmen und ihre Geschäftspraxis entsprechend jedenfalls im Anwendungsbeereich der DSGVO grundsätzlich ändern muss. Ein Rechtssatz dergestalt, dass Klagen unzulässig sind, wenn sie die Geschäftspraxis der Beklagten zu einschneidend berühren, ist der Rechtsordnung unbekannt.

(2) Nicht zu überzeugen vermag die Kammer auch das Argument, es handele sich bei dem gestellten Unterlassungsantrag letztlich um einen verkappten Leistungsantrag, da der eigentliche Schwerpunkt der Forderung der Klageseite darin liege, eine „aktive Handlung“ herbeizuführen, z. B. dass die Beklagte zukünftig technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten der Klagepartei zu implementieren habe (vgl. hierzu Landgericht Aachen, Urteil vom 26. Februar 2025, 12 O 53/24; Landgericht Oldenburg, Urteil vom 28. Oktober 2024, 5 O 2845/23; Landgericht Oldenburg, Urteil vom 28. Oktober 2024, 5 O 2937/23, Hervorhebung hinzugefügt). Dieses Vorbringen überzeugt die Kammer nicht. Die Klägerseite beantragt ein reines Unterlassen der Erhebung und Verarbeitung der streitgegenständlichen Daten. Dem kann die Beklagte auch tatsächlich durch ein reines Unterlassen nachkommen, etwa durch den Verzicht auf den Einsatz der Business-Tools. Die Notwendigkeit zu einem aktiven Tun in der Form von Umprogrammierungen o.ä. erwächst in keiner Weise aus dem Antrag der Klägerseite, sondern nur aus der ggf. bestehenden Intention der Beklagten, trotz eines ggf. bestehenden Unterlassungsanspruches mit der Verwendung der Tools fortzufahren - und hierzu Programmänderungen durchzuführen, die ihr dies möglicherweise erlauben könnten. Diese geschäftlich bedingte Intention der Beklagtenseite muss sich die Klägerseite nicht zurechnen lassen.

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

a. Der geltend gemachte Unterlassungsanspruch ist begründet, wobei die Kammer nach erneuter und eingehender Prüfung des sich laufend fortentwickelnden Vortrages der Parteien in diesem Verfahrenskomplex ihre bisherige differenzierende Würdigung der Rechtslage bezüglich „technischer Standarddaten“ und „sonstiger personenbezogener Daten“ aufgibt.

(1) Ein solcher Anspruch ergibt sich allerdings nicht aus Art. 17, 18 DSGVO oder aus sonstigen Bestimmungen der DSGVO (vgl. im Einzelnen nunmehr EuGH, Urteil vom 4. September 2025, C-655/23).

(2) Jedoch besteht ein Anspruch aus nationalem Recht. Insbesondere hat der Europäische Gerichtshof insoweit nunmehr klargestellt, dass die DSGVO einem derartigen Rückgriff auf nationale Anspruchsgrundlagen nicht entgegensteht (EuGH, a.a.O. Rn. 52). Bei der Zugrundelegung nationalen deutschen Rechts (hierfür u.a.: BeckOGK/T. Hermann, 1.11.2024, BGB § 823 Rn. 1285) folgt hier ein Unterlassungsanspruch aus § 1004 Abs. 1 S. 2 BGB analog, § 823 Abs. 1 BGB, Art. 2 Abs. 1 GG.

(a) Zunächst kann die Klägerseite verlangen, dass es die Beklagte unterlässt, die streitgegenständlichen Datenpunkte anlässlich des Besuchs der Klägerseite auf Drittseiten und -apps zu *erheben*.

(aa) Dabei legt die Kammer im ersten Schritt zu Grunde, dass davon auszugehen ist, dass die Klägerseite in der Vergangenheit auch individuell von der im Tatbestand generell geschilderten Datenerhebungspraxis der Beklagten betroffen war und insoweit auch eine Wiederholungsgefahr besteht – und zwar ohne dass es auf Klägerseite hierzu weiteren Vortrages zu einzelnen in der Vergangenheit besuchten Seiten bedarf.

Grundsätzlich 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 Busi-

ness 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 den oben beschriebenen Überwachungsmaßnahmen durch die eingesetzten Business-Tools betroffen war. Denn 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 ihren bzw. 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 haben kann, auf welchen Homepages zu welchem Zeitpunkt welche Business Tools der Beklagten enthalten waren. 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 Konstellation übertragbar. Denn auch hier findet die streitgegenständliche Überwachung der Nutzerinnen und Nutzer derart statt, dass diese bei dem Besuch von Drittseiten nicht nachvollziehen können, ob und welche sie betreffende 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 – alle bei ihr eingegangenen Daten weiterverarbeitet hat, muss es ihr unproblematisch möglich sein, in ihren Systemen vollständig und 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. Dass die Beklagte hiervon keinen Gebrauch macht und die Klägerseite nach wie vor und trotz Auskunftersuchen vollständig im Dunkeln darüber lässt, welche personenbezogenen Daten die Beklagte über die Klägerseite über die Business-Tools erfasst hat, kann nicht der Beklagten zum Vorteil gereichen.

Hieran ändern auch die von der Beklagten angeblich zur Verfügung gestellten „Selbstauskunfts-Tools nichts“. Schon aus den aus einer Vielzahl an Parallelverfahren gerichtsbekannten eigenen Auskünften der Beklagten zu den Einschränkungen des „Deine Aktivitäten außerhalb der Meta-Technologien“-Tools folgt unmissverständlich, dass dieses Angebot keinerlei tauglichen Weg bietet, um auch nur ansatzweise lückenlos die begehrten Auskünfte zu erhalten. Die von der Beklagten selbst formulierten Einschränkungen sind selbsterklärend und bedürften insoweit auch keiner weiteren Erläuterung („Hinweis: Unter „Aktivitäten außerhalb der Meta-Technologien“ siehst Du nicht alle deine Aktivitäten“, „Deine jüngsten Aktivitäten sind in der Zusammenfassung nicht enthalten“, „Wir erhalten mehr Einzelheiten und Aktivitäten, als du unter „Aktivitäten außerhalb von Meta-Technologien“ siehst“, „zeigen wir nicht alle Aktivitäten, über die wir informiert wurden.“). Nicht enthalten sind nach der Auskunft insbesondere auch solche Aktivitäten, *„wie wir erhalten haben, während du nicht bei Facebook angemeldet warst“* - mithin potentiell ganz erhebliche Datenmengen, die hier jedoch gerade streitgegenständlich sind.

(bb) Die Beklagte ist für die damit prozessual zu Grunde zu legende Datenerhebung über die 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). Der erforderliche Beitrag zur Datenverarbeitung kann dabei nach 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 damit selbst mit 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 Drittbetreibern erhoben und dann an

sie weitergeleitet werden. Denn sie ist jedenfalls - ggf. neben den Drittbetreibern - mitverantwortlich. Insoweit kann auf die folgenden Ausführungen des EuGH (Urteil vom 29. Juli 2019 - C-40/17) 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.(...)“.

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. Hieran ändert im Übrigen auch der weitere Vortrag der Beklagten zu den vertraglichen Abreden der Beklagten mit den Drittunternehmen nichts. Eine Abwälzung der Verantwortung per Vertrag auf Dritte steht nicht in Einklang mit der oben wiedergegebenen Rechtsprechung des EuGH. Der allein maßgebliche Begriff der Verantwortlichkeit knüpft nach der Rechtsprechung des EuGH daran an, ob rein tatsächlich „Einfluss auf die Mittel und Zwecke der Datenverarbeitung genommen wird“. Dies ist hier aus den angeführten Gründen der Fall und hieran ändern auch vertragliche Abreden mit den Drittanbietern nichts.

(cc) Die damit zu Lasten der Beklagten anzunehmende Verarbeitung auch individueller Daten der Klägerseite im Verantwortungsbereich jedenfalls auch der Beklagten über die streitgegenständlichen Business-Tools verletzte die Klägerseite auch in ihren absolut geschützten Rechten.

(i) Die oben aufgezeigte Praxis der Beklagten, über die streitgegenständlichen Tools personenbezogenen Daten auch der Klägerseite zu erheben, betrifft die Klägerseite in ihrem Recht auf informationelle Selbstbestimmung. Dieses unter den Bedingungen der modernen und von digitalen Systemen zutiefst geprägten Massengesellschaft essentielle Grundrecht schützt die Grundrechtsträger auch gegenüber Privaten in ihren Recht, selbst zu entscheiden, welche Daten an Dritte herausgegeben werden - und welche nicht.

(„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen mögli-

cher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“ (BVerfGE 65, 1 [43] = NJW 1984, 419). (BVerfG, Beschluss vom 6. November 2019 – 1 BvR 16/13 –, juris))

(ii) Die Praxis der Beklagten, von der nach den obigen Ausführungen auch anzunehmen ist, dass sie die Klägerseite individuell betroffen hat, ist auch rechtswidrig.

Gesichtspunkte, die diese Form der Datenerhebung rechtmäßig erscheinen lassen könnten, sind nicht vorgetragen und auch nicht ersichtlich. Insbesondere liegt kein Rechtfertigungsgrund nach Art. 6 Abs. 1 DSGVO vor. Eine Einwilligung des Klägers kann nicht festgestellt werden. Die Darlegungslast für eventuell vorliegende Einwilligungen liegt dabei schon nach allgemeinem Prozessrecht bei der Beklagtenseite. Diese müsste entsprechend vortragen, wann die Klägerseite bezogen auf welche Datenerhebungen in welcher Form und mit welchem prüffähigen Wortlaut eingewilligt hat. Derartiger Vortrag liegt schon deshalb nicht vor, weil die Beklagtenseite den Kläger – wie dargelegt – schon völlig im Dunkeln lässt, welche Daten sie überhaupt über die Business-Tools erhoben hat, so dass sie in sich konsequent auch nichts dazu vorträgt, inwiefern sie sich hierzu berechtigt erachtete. Wollte sich die Beklagte insoweit rechtskonform verhalten, müsste sie über geeignete Prozesse sicherstellen, dass in jedem Fall vor Beginn der Datenerhebung eine hierauf bezogenen Einwilligung der Nutzerinnen und Nutzer eingeholt würde und dies zum Zwecke des Nachweises auch derart digital dokumentiert würde, dass die Beklagte nachträglich den entsprechenden Nachweis führen könnte. Dass die Beklagte nach eigenem Vortrag keinerlei derartige Systeme vorhält, kann – erneut – nicht zu Lasten der Klägerseite gehen.

Nicht als Rechtfertigungsgrund zu überzeugen vermag insoweit auch das Vorbringen der Beklagten, es handle sich hierbei um eine jenseits von Meta-Produkten weit verbreitete Praxis und sei letztlich der aktuellen Funktionsweise „des Internets“ geschuldet. Zwar vermag die Kammer noch nachzuvollziehen, dass derartige Datenübermittlungen insbesondere technischer Standarddaten erforderlich sein möge 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, 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 weitschweifigem Vortrag der Beklagten irgendwie rekonstruierbar - grundsätzlich gerade nicht eingesetzt, um irgendwelche Inhalte auf Drittseiten anzubieten, sondern ausschließ-

lich 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 einzusetzen.

Wie bereits oben ausgeführt kann dem auch nicht überzeugend entgegengesetzt werden, dass von der Beklagten damit de facto die vollständige Einstellung der Business Tools verlangt würde und damit die dem Zivilprozess immanenten Grenzen überschritten würden. Die Argumentation läuft letztlich darauf hinaus, dass es möglich sein müsse, diese streitgegenständlichen Tools zu nutzen. DSGVO-konform gilt jedoch das Gegenteil: Sollte es tatsächlich nicht möglich sein, die allein im Interesse der Beklagten liegenden „Tools“ zu konzipieren, die keine Daten ohne dokumentierte Zustimmung erheben und weiterleiten, dann kann die Beklagte eben auch keine derartigen „Tools“ einsetzen. Dies im Verhältnis zwischen der Beklagten und einzelnen Klägern rechtlich umzusetzen, überschreitet auch nicht die Grenzen des Zivilrechts. Dass entsprechende Urteile als Rechtsreflex dann ggf. auf die ganze Geschäftspraxis der Beklagten ausstrahlen und diese in Frage stellen, ist der Rechtsordnung immanent. Ein Rechtssatz dahingehend, dass Zivilgerichte von Urteilen abzusehen hätten, wenn diese über den Einzelfall hinaus auch für andere Verhältnisse relevant sein könnten, ist naturgemäß inexistent.

(iii) 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. Aus den dargelegten Gründen hat das Gericht zu Grunde zu legen, dass bereits in der Vergangenheit entsprechende Rechtsverletzungen stattgefunden haben. Eine Wiederholungsgefahr ist damit schon nach allgemeinen Rechtsgrundsätzen indiziert.

Angesichts der sehr weiten Verbreitung dieser Tools auf zahllosen Apps und Seiten, ist zudem jedenfalls eine Erstbegehungsgefahr ohne das Erfordernis weiteren Vortrages des Klägers äußerst naheliegend. Allein schon der Umstand, dass die Tools auf den im unstreitigen Teils des Tatbestandes aufgeführten Seiten implementiert sind, begründet die naheliegende Gefahr, dass künftig auch der Kläger persönlich von den implementierten Tools betroffen sein kann. Untermauert wird diese Gefahr zuletzt mit den in Anlage K 4 aufgelisteten exemplarischen deutschsprachigen Websites, die ebenfalls die Business Tools implementiert haben sollen. Die Kammer stuft diesen Vortrag dabei auch als unstreitig ein, da die Beklagte diese Angaben jedenfalls nicht nachvollzieh-

bar bestritten hat Klar.

(b) 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.

(c) Nichts anderes gilt für den Anspruch, es zu unterlassen, die entsprechenden Datenpunkte so- dann zu speichern. Auf die obigen Ausführungen kann verwiesen werden. Insbesondere liegen auch hier *keinerlei Rechtfertigungsgründe* für die Speicherung der bei der Beklagten – über wel- ches Tool auch immer – eingegangenen Daten vor.

(aa) In Betracht käme insoweit allenfalls theoretisch zwar, dass die Nutzerinnen und Nutzer be- reits auf der Drittseite in einer dortig etwaig eingeholten Einwilligung auch der weiteren Speiche- rung der Daten in den Systemen der Beklagten zugestimmt haben könnten. Dies ist jedoch schon nach dem eigenen Vortrag der Beklagten nicht der Fall. Irgendwie gearteter Vortrag, dass bezüglich der weiteren Verarbeitung der Daten bei der Beklagten bereits eine Zustimmung durch die Drittseitenanbieter eingeholt wurde, fehlt zur Gänze.

(bb) Des Weiteren hat auch die Beklagte selbst keinerlei Einwilligung für die Speicherung der Da- ten in ihren Systemen eingeholt.

Eine derartige Einwilligung hat die Beklagte insbesondere schon nach dem eigenen, ausdrückli- chen Vortrag nicht über die Einstellung „Meta Cookies in anderen Apps und auf anderen Websei- ten“ eingeholt: „Zur Klarstellung: Meta beabsichtigt nicht, über die Einstellung „Meta Cookies in an- deren Apps und auf anderen Websites“ eine Einwilligung gem. Art. 6 Abs. 1 DSGVO für die Verar- beitung von Business Tools Daten einzuholen“ (Schriftsatz vom 10. Juni 2025, S. 24, = Bl. 98 d.A.).

Keine Einwilligung hat die Beklagte auch über die (weitere) Einstellungsmöglichkeit „Informationen von Werbepartnern zu deinen Aktivitäten“ eingeholt. Soweit der Kammer aus dem diffusen Vor- trag der Beklagten überhaupt noch nachvollziehbar, können die Nutzer in dieser Einstellung ledig- lich Einfluss darauf nehmen, ob ihre Daten „zum Zweck der Bereitstellung personalisierter Wer- bung“ genutzt werden dürfen – nicht aber eine Einwilligung für die grundsätzliche und dem denklogisch vorgelagerte Frage abgeben oder verweigern, *ob ihre Daten überhaupt von der*

Beklagten und egal zu welchem Zweck gespeichert werden dürfen. Nur dies ist aber Gegenstand aller hier anhängigen Verfahren im Kontext der Verwendung von Business Tools.

Insbesondere ist nochmals zu betonen, dass es zwischen den Parteien auch auf ausdrückliche Nachfrage im Termin zur mündlichen Verhandlung unstreitig blieb, dass die Beklagte einmal erhaltene Datenpunkte selbst dann zu Persönlichkeitsprofilen verarbeitet, wenn hierfür keine Einwilligung gegeben wurde – weshalb sie sich auch nicht auf Einwilligung berufe (vgl. Protokoll vom 16.10.2025, S. 8 ff.). Die Rechtswidrigkeit dieser Praktik ist mit Händen zu greifen.

(cc) Auch sonstige Rechtfertigungsgründe für die Speicherung der personenbezogenen Daten der Nutzerinnen und Nutzer, so auch der Klägerseite, liegen ersichtlich nicht vor. Nicht zu überzeugen vermag insbesondere 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. Auf die folgenden überzeugenden Ausführungen des Landgerichts Leipzig (LG Leipzig, Urteil vom 4. Juli 2025 – 5 O 2351/23 –, juris), die sich die Kammer zu eigen macht, wird Bezug genommen:

Der (...) Vortrag reicht indes nicht aus, um den strengen Anforderungen des EuGHs zu Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO gerecht zu werden. Die Beklagte erklärt nicht, wie personenbezogene Daten der Nutzer eingesetzt werden können, um den genannten Zwecken gerecht zu werden. Insofern wird bereits dem Erforderlichkeitskriterium des EuGHs nicht hinreichend Rechnung getragen. Zudem wird nicht klar, in welchem Umfang und auf welche Art und Weise personenbezogene Daten erhoben werden. Insofern kann das Gericht keine Überprüfung zur Angemessenheit der Datenverarbeitung vornehmen. Zu den sonstigen Rechtfertigungsgründen innerhalb von Art. 6 DSGVO wurde ebenfalls nicht hinreichend vorgetragen. Da es bereits an diesen Voraussetzungen fehlt, sind erst Recht die strengeren Anforderungen nach Art. 9 DSGVO nicht erfüllt. Im Übrigen verstößt das Vorgehen der Beklagten aus den gleichen Gründen gegen Art. 5 Abs. 2 DSGVO. Nach dem in dieser Vorschrift verankerten Grundsatz der Rechenschaftspflicht muss der Verantwortliche nachweisen können, dass die personenbezogenen Daten unter Einhaltung der in Art. 5 Abs. 1 DSGVO genannten Grundsätze erhoben und verarbeitet werden (EuGH, Ur. v. 4.10.2024, Az. C-446/21, NJW 2025, 207 Rn. 55). In Artikel 5 Abs. 1 DSGVO ist unter anderem der Grundsatz der Datenminimierung (lit. c) verankert, der bestimmt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (EuGH, a.a.O, NJW 2023, 2997).

(d) Das gleiche gilt im Übrigen für die weitere Verwendung der derart gespeicherten Datenpunkte. Auf die dortigen Ausführungen unter (c) kann zur Vermeidung von Wiederholungen verwiesen werden.

(e) Die Kammer hat im Übrigen noch erwogen, ob der geltend gemachte Unterlassungsantrag deshalb unbegründet sein könnte, weil ggf. denkbare Ausnahmetatbestände – insbesondere eine etwaige Einwilligung – nicht im Antrag aufgenommen sind (vgl. hierzu zuletzt etwa BGH, Urteil

vom 18.10.2015 – IV ZR 431/24 -, Juris Rn. 28 ff. für sog. „Schufa-Verfahren“). Die Kammer sieht vorliegend jedoch keine handhabbare Möglichkeit für die Klägerseite etwaige Ausnahmetatbestände mit der gebotenen Präzision (BGH, Urt. v. 18. 10. 2012 – I ZR 137/11 – Juris Rn. 21: *„so genau (...) werden, dass im Vollstreckungsverfahren erkennbar ist, welche konkreten Handlungen von dem Verbot ausgenommen werden“*) zu benennen. Denn hierfür wäre nicht ausreichend, als Ausnahmetatbestand das Vorliegen einer irgendwie gearteten Einwilligung zu benennen, da derart die regelmäßig streitige Frage ins Vollstreckungsverfahren getragen würde, ob eine etwaige Einwilligung überhaupt wirksam erteilt wurde – oder aber wegen der konkreten Fassung der notwendigen Aufklärungen und ihrer textlichen Gestaltung unwirksam sein könnte. Vielmehr wären konkrete Anforderungen an die Einwilligung zu formulieren – was vor dem Hintergrund der großen Vielfalt an denkbaren Gestaltungen von Einwilligungen in den Apps der Beklagten bzw. auf den Drittanbieterseiten schlicht nicht leistbar ist. Die Kammer erachtet es daher für prozessual überzeugender, diese Fragen nicht zum Gegenstand der Tenorierung werden zu lassen und es vielmehr der Beklagtenseite zuzumuten, im Falle der Vollstreckung aus dem vorliegenden Urteil trotz eventuellem Vorliegens einer Einwilligung den Weg einer Vollstreckungsgegenklage zu beschreiten.

b. Der Klägerseite steht des Weiteren auch ein Anspruch auf Schadensersatz aus Art. 82 DSGVO (aa.), nicht aber aus § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG (bb.) zu.

(1) Der Klägerseite steht ein Anspruch aus Art. 82 DSGVO in der zuerkannten Höhe zu.

(a) Die Kammer geht davon aus, dass die Klägerseite von der streitgegenständlichen Datenverarbeitung mittels der sog. Business Tools auch individuell - wenn auch nur teilweise - betroffen ist. Auf die obigen Ausführungen kann verwiesen werden.

(b) Die Verarbeitung der streitgegenständlichen technischen Standarddaten des Klägers durch die Beklagte erfolgte auch rechtswidrig. Auf die obigen Ausführungen wird Bezug genommen.

(c) Die Verarbeitung erfolgte auch schuldhaft, nämlich vorsätzlich.

(d) Der Klägerseite ist in Folge der rechtswidrigen und schuldhaften Datenverarbeitung durch die Beklagte auch ein Schaden entstanden.

Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schä-

den. Ein materieller Vermögensschaden wurde von der Klägerseite nicht vorgetragen. Sie beruft sich allein auf das Vorliegen eines immateriellen Schadens. Als Anknüpfungspunkte für einen immateriellen Schaden im Sinne des Art. 82 DSGVO sind nach der ständigen Rechtsprechung der Kammer die von der Klägerseite geschilderten Ängste und Sorgen, sowie die Verletzung des Rechts auf informationelle Selbstbestimmung bzw. der damit einhergehende Kontrollverlust an sich denkbar. Im Einzelnen:

(aa) Vorliegend kann ein Schaden im Sinne von Art. 82 DSGVO zum einen mit den geltend gemachten Ängsten und Sorgen der Klägerseite begründet werden.

Nachdem bis Ende 2023 weitgehend unklar war, ob bereits durch Datenschutzverstöße bedingte Ängste und Sorgen der betroffenen Personen einen hinreichenden Schaden im Sinne von Art. 82 DSGVO darstellen, hat der Gerichtshof der Europäischen Union erstmals mit Urteil vom 14. Dezember 2023 klargestellt, dass

„allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, einen „immateriellen Schaden“ im Sinne dieser Bestimmung darstellen kann.“ (EuGH, Urteil vom 14. Dezember 2023 – C-340/21 –, Juris).

Diese Rechtsprechung hat der Gerichtshof sodann mit Urteil vom 25. Januar 2024 vertieft und nochmals entschieden, dass

der Begriff „immaterieller Schaden“ eine Situation umfasst, in der die betroffene Person die begründete Befürchtung hegt – was zu prüfen Sache des angerufenen nationalen Gerichts ist –, dass einige ihrer personenbezogenen Daten künftig von Dritten weiterverbreitet oder missbräuchlich verwendet werden (EuGH, Urteil vom 25. Januar 2024 – C-687/21 –, Juris),

Dabei hat der Gerichtshof den nationalen Gerichten allerdings – insoweit einschränkend – die Aufgabe zugewiesen, zu prüfen, ob diese Befürchtung

„unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann.“ (EuGH, Urteil vom 14. Dezember 2023 – C-340/21 –, Juris).

Dies ist etwa dann nicht der Fall, wenn sich das Risiko der rechtswidrigen Datenweitergabe als rein hypothetisch erweist (EuGH, Urteil vom 25. Januar 2024 – C-687/21 –, Juris).

Ausdrücklich hat er sodann im nachfolgenden Urteil vom 21. Dezember 2023 im Hinblick auf den Grad der zu verlangenden Ängste oder Sorgen ausgesprochen, dass Art. 82 DSGVO keine Bagatellgrenze kennt:

„Somit kann nicht angenommen werden, dass über diese (...) Voraussetzungen hinaus für die Haftung nach Art. 82 I DS-GVO weitere Voraussetzungen aufgestellt werden dürfen, etwa die, dass der Nachteil spürbar oder die Beeinträchtigung objektiv sein muss. Folglich verlangt Art. 82 I DS-GVO nicht, dass nach einem erwiesenen Verstoß gegen Bestimmungen dieser Verordnung der von der betroffenen Person geltend gemachte „immaterielle Schaden“ eine „Bagatellgrenze“ überschreiten muss, damit dieser Schaden ersatzfähig ist (EuGH, Urteil vom 14. Dezember 2023 – C-340/21 -, Juris).

Wiederholt bemüht der Gerichtshof in diesem Zusammenhang hinsichtlich der Schadensintensität die Formel „so geringfügig er auch sein mag“ (EuGH, a.a.O.) und stellte zuletzt auch nochmals unmissverständlich klar, dass die schadensbegründenden Ängste und Sorgen nicht über bloße negative Gefühle, wie sie dem allgemeinen Lebensrisiko entsprechen, hinausgehen müssen (EuGH, Urteil vom 4. September 2025, C-655/23, Rn. 62)

Allerdings geht die Kammer dabei - auch dies in ständiger Rechtsprechung - davon aus, dass die derart begründeten Sorgen bzw. Ängste kausal auf die fragliche Rechtsgutverletzung rückführbar sein müssen (ausdrücklich bestätigt jetzt auch in EuGH, Urteil vom 4. September 2025, C-655/23, Rn. 62). Dies ist in der hier vorliegenden Konstellation von erheblicher Relevanz, weil die persönliche Betroffenheit von der streitgegenständlichen Datenverarbeitung nur in Bezug auf die Erhebung und Verarbeitung der technischen Standarddaten gegeben ist (vgl. oben). Hieraus folgt , dass auch die vorgetragenen Ängste und Sorgen in überzeugendem kausalen Zusammenhang gerade mit dieser spezifischen Verarbeitung stehen müssen. Durch dieses Erfordernis wird auch ausgeschlossen, dass jedwede diffuse Vorstellung der Klägerseite über das Geschäftsmodell der Beklagten unter dem Schlagwort der „Ängste und Sorgen“ schadensbegründend herangezogen werden können. Erforderlich ist daher, dass die Klägerseite zumindest eine laienhaft, näherungsweise zutreffende, Vorstellung davon gebildet hat, dass ihr Internetnutzungsverhalten in Bezug auf den Besuch von Drittseiten vermittels der „Business-Tools“ von der Beklagten in größerem Umfang nachverfolgt werden kann sowie, dass diese Vorstellung sodann zumindest mitursächlich für die geschilderten Ängste und Sorgen ist.

Ein derartiger Schaden liegt hier auf Seiten der Klagepartei vor. Der Kläger hat in der mündlichen Verhandlung hierzu nachvollziehbar ausgeführt, dass er, nachdem ihm die streitgegenständli-

chen Datenverarbeitungsvorgängen bei Facebook bewusst geworden waren, in Sorge über die Aufzeichnung höchstpersönlicher Daten aus seinem Internetnutzungsverhalten bei der Beklagten lebe.

Davon, dass diese – von der Beklagtenseite bestrittenen – Ängste tatsächlich vorliegen, ist das Gericht aufgrund der mündlichen Anhörung im Verhandlungstermin überzeugt. In der Rechtsprechung ist insoweit anerkannt, dass das Gericht im Rahmen der freien Würdigung des Verhandlungsergebnisses den Behauptungen und Angaben einer Partei i.S.v. § 141 ZPO unter Umständen auch dann glauben und sein Urteil hierauf stützen kann, wenn diese ihre Richtigkeit sonst nicht beweisen kann (vgl. z.B. BGH, Beschluss vom 24. Juni 2003 - VI ZR 327/02 -, NJW 2003, 2527; vgl. etwa auch KG Beschl. v. 5.9.2022 – 25 U 92/21, BeckRS 2022, 48732). So liegt es hier. Die Aussagen der Klägerseite erachtet das Gericht für glaubhaft. Dabei waren an die Glaubhaftigkeit der Angaben schon im Ansatz keine überstiegenen Anforderungen zu stellen. Denn schon im Ansatz liegt es mehr als Nahe, dass sich die Klägerseite nach Bekanntwerden des Verlustes ihrer Daten bei der Beklagten Sorgen um deren Verbleib und um deren Verwendung durch die hierfür Verantwortlichen macht. Für die Kammer liegt es insoweit nahe, dass sich faktisch jedermann, der davon erführe, dass seine Daten in der hier vorliegenden Art und Weise Gegenstand der Verarbeitung durch die Beklagte sind, sich über deren Verbleib und über deren weitere Verwendung Sorgen machen würde. Es nimmt daher wenig Wunder, dass dies auch bei der Klägerseite der Fall war. Dieser hat glaubhaft geschildert, dass ihn die Verwendung höchstpersönlicher Daten, wie insb. Gesundheitsdaten, erheblich störe. Eine Auslagerung seines Kommunikationsverhaltens weg von der Beklagten sei ihm aus beruflichen Gründen nicht möglich.

(bb) Zudem liegt ein Schaden unter dem Gesichtspunkt der Verletzung des Rechts auf informationelle Selbstbestimmung bzw. des reinen Kontrollverlustes vor.

Dabei geht die Kammer in ständiger Rechtsprechung davon aus, dass bereits der reine Kontrollverlust und damit die hieraus folgende Verletzung des Rechts auf informationelle Selbstbestimmung ausreicht, um einen Schaden zu begründen (vgl. zuletzt etwa ausführlich Urteil vom 4. Oktober 2024 - Az. 15 O 216/23 -, Juris) und sieht sich hierin auch durch die jüngste Entscheidung des Bundesgerichtshofes bestätigt (BGH, Urteil vom 18. November 2024 - IV ZR 10/24 -, Juris). Insoweit erachtet es die Kammer auch grundsätzlich nicht für ausgeschlossen, dass der Klägerin ein Schadensersatzanspruch insoweit zukommen könnte, als dass die Beklagte jedenfalls mithilfe der technischen Standarddaten rechtswidrig verarbeitet, gespeichert und weitergegeben hat, auf welchen Drittseiten sich die Klägerin aufgehalten hat (vgl. oben) und hierdurch einen Kontroll-

verlust über diese Daten bei der Klägerin bewirkt hat.

Allerdings hat die Kammer in ihrem Urteil vom 10. Januar 2025 (Az. 15 O 269/23) noch entschieden, dass zur Darlegung eines Schadens in Form des Kontrollverlusts grundsätzlich erforderlich ist, dass die Klägerseite darlegt und beweist, welche konkreten Datenpunkte in welcher numerischen Größenordnung hiervon betroffen sein sollen. Für die Feststellung eines Schadens (und auf nächster Stufe für die Bestimmung der Schadenshöhe) sei es von erheblicher Relevanz, ob die Beklagte im Verlauf mehrerer Jahre keine konkreten Daten verarbeitet hat (etwa weil auf den konkret von der Klägerseite besuchten Seiten zufälligerweise keine aktiven „Business Tools“ implementiert waren), nur einige Male den Besuch einer landläufigen Website verarbeitet hat, oder täglich duzende unterschiedliche und teilweise hochpersönlicher Internetbewegungen aufgezeichnet und rechtswidrig zu einem präzisen Persönlichkeitsprofil verarbeitet hat.

Die Kammer hat jedoch anlässlich der mündlichen Verhandlung in diesem Verfahren nochmals eingehend beraten und nunmehr im Lichte der jüngeren, hierzu ergangenen Rechtsprechung anderer Gerichte (insb. LG Mainz, Urteil vom 27. Juni 2025 - 3 O 29/24, GRUR-RS 2025, 16871; LG Leipzig Endurteil vom 4. Juli 2025 - 5 O 2351/23 -, GRUR-RS 2025, 15264; LG Ellwangen Urte. v. 9.4.2025 - 2 O 266/24, GRUR-RS 2025, 16870) sowie nachvollziehbarer Kritik an der bisherigen Ablehnung eines Schadens durch dieses Gericht (Niekrenz, Anmerkung zu LG Lübeck vom 10.01.2025 in: ZD 2025, 228) entschieden, dass unter Aufgabe der bisherigen Rechtsprechung ein Schaden in Form des Kontrollverlustes zu bejahen ist. In der Rechtsprechung des Bundesarbeitsgerichts ist etwa anerkannt, dass ein schadensbegründender Kontrollverlust auch dann vorliegt, wenn ein Arbeitgeber einen Arbeitnehmer durch eine Detektei im privaten Umfeld überwachen lässt (BAG Urteil vom 25. Juli 2024 - 8 AZR 225/23 -, NJW 2025, 100). Der Schaden liege in dieser Fallgestaltung „in dem durch die Überwachung erlittenen Kontrollverlust und insbesondere im Verlust der Sicherheit vor Beobachtung im privaten Umfeld“ - und zwar ohne dass es auf weiteren Vortrag ankomme, welche Daten genau erhoben worden seien (so wohl auch Ehmann/Selmayr/Nemitz, 3. Aufl., DS-GVO Art. 82 Rn. 17 Kühling/Buchner/Bergt, 4. Aufl., DS-GVO Art. 82 Rn. 18c). Diesen Erwägungen schließt sich die Kammer an. Sie sind auch auf den vorliegenden Fall zu übertragen, da das Wesen des vorliegenden Sachverhalts eben gerade nicht der Verlust der Kontrolle über einzelne oder eine Gesamtheit von konkret benennbarer Datenpunkte ist, sondern vielmehr darin liegt, dass die Klägerseite nicht ansatzweise mehr weiß und auch nicht wissen kann, welche und wieviele Daten die Beklagte aus ihrer Privat- und Intimsphäre über sie gesammelt hat und auch nicht weiß und wissen kann, was die Beklagte mit diesen Daten macht (i.d.S. auch LG Leipzig, Urteil vom 4. Juli 2025 - 5 O 2351/23 -, Rn. 72 ff., Juris).

(e) Der derart gefasste Schaden beruht auch kausal auf der von der Beklagten vorgenommenen rechtswidrigen Datenverarbeitung.

(f) Die Schadenshöhe schätzt die Kammer im Rahmen ihres Ermessens nach § 287 ZPO auf 5.500 EUR.

Im Rahmen der nach § 287 ZPO vorzunehmenden Schadensschätzung sind im Rahmen des Art. 82 DS-VGO allgemein die Art, Schwere, Dauer des Verstoßes, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der betroffenen personenbezogenen Daten in die Erwägung mit einzubeziehen.

Im Falle der mehrtägigen Überwachung einer Privatperson durch eine Detektei hat das Bundesarbeitsgericht einen Schadensersatzbetrag in Höhe von 1.500 EUR für angemessen erachtet (BAG Urteil vom 25. Juli 2024 - 8 AZR 225/23 -, NJW 2025, 100). Im Fall des Ausspähens persönlicher Daten im Rahmen einer verdeckten „Recherche“ hat das Oberlandesgericht Dresden einen Betrag von 5.000 EUR zuerkannt (OLG Dresden, Urteil vom 30. November 2021 - 4 U 1158/21 -, Juris). In den bereits entschiedenen Fällen, die mit dem hiesigen gleichgelagert waren, wurden Beträge zwischen 10.000 EUR (insb. LG Mainz, Urteil vom 27. Juni 2025 - 3 O 29/24, GRUR-RS 2025, 16871; LG Ellwangen Urte. v. 9.4.2025 – 2 O 266/24, GRUR-RS 2025, 16870) und 5.000 EUR zugesprochen (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264).

Daran gemessen erachtet die Kammer hier einen Schadensersatzbetrag von 5.500 EUR für angemessen. Es handelt sich bei dem festgestellten Datenschutzverstoß um eine schwere Verletzung des Rechts auf informationelle Selbstbestimmung, da das gesamte, höchstpersönliche Internetnutzungsverhalten betroffen ist (vgl. oben). Dabei handelt es sich auch nicht nur um eine punktuelle, zeitlich begrenzte rechtswidrige Maßnahme der Beklagten, sondern um einen sich über einen großen, mehrjährigen Dauerverstoß gegen grundlegende Rechte nach der DSGVO. Dieser Verstoß betraf auch Daten, die einen hohen Marktwert haben. Überzeugend führt hierzu das Landgericht Leipzig aus:

„(...) Für den Wert der Daten für die Beklagte hat das Gericht auf die Feststellungen des BKR-tA (Beschl. v. 2.5.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) zurückgegriffen. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der

Werbeeinnahmen einen Anteil i.H.v. 97 % ausmachte (BKartA a.a.O., Rn. 7). Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O., Rn. 53). Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon überzeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studien (siehe nur die Studie „Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?“, Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz; Infografik „Preis, den Erwachsene in den USA für personenbezogene Daten aufrufen würden (in US-Dollar)“, Statista mit Quelldaten von Morning ... Consult aus dem Jahr 2019, abgerufen unter <https://cdn.statcdn.com/Infographic/images/normal/18449.jpeg>). Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d.h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. [18b](#), beck-online).“ (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264, Rn. 85)

Hinzu kommt, dass die Klägerseite von der Beklagtenseite keine praktikablen Wege aufgezeigt bekommt, die Kontrolle über die von der Beklagten erlangten Daten wiederzuerhalten. Die Beklagte stellt der Klägerseite schon keine aussagekräftigen Informationsmöglichkeiten zur Seite, mit der diese verlässliche Kenntnis davon erlangen könnte, welche konkreten Daten die Beklagte über sie gespeichert hat (vgl. oben), und ist auch ersichtlich nicht zur nachvollziehbaren Löschung dieser Daten bereit.

Dabei bemisst die Kammer – Einzelrichter – den Schaden für den reinen Datenverlust auf 5.000 EUR. Hinzu kommen 500 EUR für die erlittenen Ängste und Sorgen (vgl. oben).

Soweit im Übrigen in der veröffentlichten Rechtsprechung den Meta-Nutzerinnen bzw. -Nutzern immer wieder vorgehalten wird, sie könnten auf die Nutzung der Meta-Produkte verzichten, überzeugt das das Gericht nicht ansatzweise. Sinn und Zweck der DSGVO ist es gerade, allen europäischen Bürgern ein einheitliches und hohes Datenschutzniveau bezüglich aller auf dem euro-

päischen Markt zugelassener Anwendungen, auch Social-Media-Produkten, zu gewährleisten. Die Argumentation, die Nutzer sollten eben auf diese Anwendungen verzichten, wenn dort Verletzungen des DSGVO stattfinden, führt diesen Regelungsansatz ersichtlich ad absurdum. Überzeugend führt hierzu auch das Landgericht Leipzig aus:

„Nicht anspruchsmindernd i.S.e. widersprüchlichen Verhaltens wirkt sich aus, dass der Kläger die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Die Beklagte nimmt im Bereich der Social-Media-Plattformen eine überragende marktübergreifende Stellung ein, welche bereits das Bundeskartellamt i.S.v. § 19a GWB festgestellt hat (BKartA, Beschl. v. 02.05.2022, Az. B6-27/21). Gerade für die Teilhabe am gesellschaftlichen Leben handelt es sich bei den Netzwerken der Beklagten mittlerweile um für den durchschnittlichen Bürger essenzielle Dienstleistungen (vgl. Erwägungsgründe Nr. 1, 3 zur VO 2022/2065), die faktisch nicht durch ein alternatives Netzwerk ersetzt werden können (zusammenfassend zu den Hintergründen siehe Mohr, EuZW 2019, 265 unter Bezugnahme auf die F.-Entscheidung des Bundeskartellamts vom 06.02.2019). Auch wenn der Nutzer Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, ist es ihm deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass der Kläger ihre Netzwerke DSGVOkonform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt der Kläger zum Ausdruck, dass ihm die Datenschutzverstöße der Beklagten nicht egal sind, sondern er eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es dem Kläger hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, sein Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden (vgl. Paal, ZfDR 2023, 325).“ (LG Leipzig Endurteil vom 4. Juli 2025 – 5 O 2351/23 -, GRUR-RS 2025, 15264, Rn. 95)

Auch diese Ausführungen macht sich die Kammer zu eigen.

(2) Ein darüberhinausgehender Anspruch ergibt sich nicht aus der Verletzung des allgemeinen Persönlichkeitsrechts, § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG. Denn der Regelung des Art. 82 DSGVO kommt insoweit zur Überzeugung der Kammer eine Sperrwirkung zu. Überzeugend führt hierzu das Landgericht Nürnberg-Fürth aus:

„Zwar ist die Kontrolle über die eigenen Daten, etwa bei Fragen der Speicherung, über das Recht auf informationelle Selbstbestimmung gewährleistet, welches eine Ausprägung des allgemeinen Persönlichkeitsrechts darstellt, und wird im Rahmen der mittelbaren Drittwirkung als sonstiges Recht vom Schadensersatzanspruch des § 823 Abs. 1 BGB geschützt (Grüneberg, BGB, 82. Auflage, § 823 Rn. 132). Jedoch ist durch Art. 82 DSGVO eine einheitliche und abschließende Anspruchsgrundlage für Schadensersatz bei personenbezogenen Daten geschaffen worden, die gegenüber dem nationalen Recht vorrangig

ist (OLG Frankfurt vom 30.03.2023, Az. 16 U 22/22, juris Rn. 58f.). Dafür spricht schon ErwGr. 9 DSGVO, der von der Schaffung eines einheitlichen Schutzniveaus in der Union ausgeht. Der angestrebten Vollharmonisierung würde es entgegenlaufen, wenn in den nationalen Rechtsordnungen unterschiedliche zusätzliche Schadensersatzansprüche vorhanden wären, so dass der DSGVO insoweit eine Sperrwirkung zukommt. Dem steht auch nicht entgegen, dass ErwGr. 146 S. 3 DSGVO erklärt, dass der Schadensersatz nach DSGVO unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten gilt. Demnach bleiben zwar weitere Schadensersatzansprüche grundsätzlich erhalten (Ehmann/Selmayr/Nemitz, DS-GVO, 3. Auflage, Art. 82 Rn. 11). Dazu zählt auch der allgemeine Schadenersatzanspruch des deutschen Rechts auf Grundlage von § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG (Verletzung des allgemeinen Persönlichkeitsrechts), der weiterhin anwendbar bleibt (Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, Art. 82 DSGVO Rn. 32). Dies bedeutet aber nicht, dass Schadensersatzansprüche, die gerade mit DSGVO-Verstößen begründet werden, mit anderen Anspruchsgrundlagen als Art. 82 DSGVO verfolgt werden könnten. Dies dürfte daher im Übrigen auch der Einordnung von DSGVO – Normen als Schutzgesetz im Sinne von § 823 Abs. 2 BGB entgegenstehen (Borges/Keil, Big Data, 1. Auflage, § 7 Haftung für Daten und Analysen Rn. 267).“ (LG Nürnberg-Fürth: Urteil vom 28.11.2024 - . 6 O 5782/23 -).

Dem schließt sich die Kammer an. Überzeugend sind die obigen Ausführungen insbesondere auch deshalb, weil der Schadensersatzanspruch aus § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG in seiner Genese überhaupt erst entwickelt wurde, um Betroffene über das vom Bundesverfassungsgericht zuerkannte Grundrecht auf informationelle Selbstbestimmung vor intransparenter Verarbeitung oder Nutzung seiner personenbezogenen Daten zu schützen, mithin eine im deutschen Recht ansonsten bestehende Rechtsschutzlücke zu schließen (vgl. hierzu insb. auch BeckOGK/T. Hermann, 1.11.2024, BGB § 823 Rn. 1285). Eine derartige Rechtsschutzlücke besteht nach Gültigkeit des Art. 82 Abs. 1 DSGVO jedoch nicht mehr, da dieser den Anspruch erhebt, sämtliche materiellen und immateriellen Schäden zu schließen. Es muss daher im Anwendungsbereich des Art. 82 DSGVO zum Ersatz immaterieller Schäden nicht mehr auf den Anspruch auf Geldentschädigung zurückgegriffen werden, der sich aus dem Schutzauftrag der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergibt (a.a.O., Rn. 1287).

c. Der Zinsanspruch folgt aus §§ 288 BGB.

d. Die Klägerseite kann von der Beklagten keine Freihaltung von den geltend gemachten vorgerichtlichen Rechtsanwaltskosten verlangen. Die Beklagtenseite hat bereits die Entstehung derartiger Kosten bestritten (Schreiben vom 10.06.2025, Bl. 162 d.A). Beweismittel zur Entstehung

derartiger Kosten fehlen jedoch. Ein richterlicher Hinweis auf diesen Umstand war nicht erforderlich, da nur Nebenforderungen betroffen sind.

e. Die Auskunftsklage ist ebenfalls weitgehend begründet. Die Klägerseite kann von der Beklagten die begehrte Auskunft – mit Ausnahme der Auskunft nach Art. 15 Abs. 1 h DSGVO - verlangen.

a. Der Klägerseite als von den Datenverarbeitungsprozessen der Beklagten Betroffene steht grundsätzlich der Auskunftsanspruch des Art. 15 DSGVO zu. Durch die detailhafte wenn auch sprachlich wenig glückliche Umschreibung der begehrten Auskunft hat die Klägerseite insbesondere auch die erforderliche Präzisierung ihres Anspruches (vgl. BeckOK DatenschutzR/Schmidt-Wudy, 53. Ed. 1.8.2025, DS-GVO Art. 15 Rn. 47) vorgenommen.

b. Inhaltlich kann die Klägerseite aus Art. 15 Abs. 1 DSGVO nicht lediglich abstrakte Umschreibungen einer etwaigen allgemeinen Handhabe verlangen. Vielmehr verpflichtet Art. 15 Abs. 1 DSGVO die Verantwortliche zur präzisen Auskunft über die konkret bei ihr verarbeiteten personenbezogenen Daten (unstr., vgl. etwa BeckOK DatenschutzR/Schmidt-Wudy, 53. Ed. 1.8.2025, DS-GVO Art. 15 Rn. 50-52.3). Der Anspruch gem. Art. 15 Abs. 1 DSGVO umfasst dabei die folgenden Informationsansprüche:

Zum einen Auskunft über alle Arten verarbeiteter Informationen, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist (BGH, Urteil vom 15. Juni 2021 - VI ZR 576/19 -, BeckRS 2021, 16831). Konkret gewendet bedeutet dies, dass die Beklagte nicht abstrakt-generalisierende Informationen über ihre Datenverarbeitungspraxis schuldet, sondern - wie auch der Rückschluss zu Art. 15 Abs. 3 DSGVO erkennen lässt - konkrete Auflistungen, welche konkreten Informationen der Beklagten über Drittseitenbesuche und Besuche von Apps der Beklagten vorliegen.

Auskunft verlangen kann die Klägerseite des Weiteren darüber, ob die Daten an welche Dritte weitergegeben wurden (Art. 15 Abs. 1 c)) und ob und ggf. wie die Daten für automatisierte Entscheidungsfindungen verwandt wurden (Art. 15 Abs. 1 h)).

Geschuldet ist des Weiteren auch eine Information über etwaige Datentransfers in Drittstaaten, Art. 15 Abs. 2 DSGVO (vgl. hierzu BeckOK DatenschutzR/Schmidt-Wudy, 53. Ed. 1.8.2025, DS-GVO Art. 15 Rn. 81, 82: „Verlangt jedoch der Betroffene die Auskunft, ob ein Datentransfer in Drittstaaten erfolgt, so hat der Verantwortliche diesbezüglich die Pflicht zur Auskunft nach Art. 15 Abs. 2, (...)“). Soweit das Landgericht Kiel insoweit entscheiden hat, ein solches

Recht bestehe nicht im Falle einer Übermittlung auf der Grundlage eines Angemessenheitsbeschlusses gemäß Art. 45 DSGVO – wie im Falle der USA – (LG Kiel Urt. v. 10.10.2024 – 6 O 274/23, GRUR-RS 2024, 48755, Rn. 37) folgt die Kammer dem nicht. Vielmehr erscheint der Kammer der Regelung des Art. 15 Abs. 2 DSGVO denklogisch immanent, dass der Verpflichtete in jedem Fall Auskunft erteilen muss, ob und in welchen Drittstaat Daten übertragen wurden. Denn eine sinnvolle Auseinandersetzung, ob die vom Landgericht Kiel erkannte Ausnahme greift und ggf. welche weitergehende Auskunftsrechte über spezifische Garantien dem Betroffenen zustehen könnten, kann zwischen den Parteien überhaupt nur dann geführt werden, wenn der Betroffene überhaupt erfahren hat, dass und wohin seine Daten übermittelt wurden. Die ausdrücklich in Art. 15 Abs. 2 DSGVO normierten Auskunftsansprüche setzen damit die Grundinformation über einen Datentransfer zwingend voraus.

c. Soweit die Beklagte hiergegen einwendet, sie habe den Auskunftsanspruch bereits erfüllt, ist dies fernliegend. Erfüllt werden kann der Auskunftsanspruch gem. Art. 15 DSGVO entweder durch die Übermittlung der entsprechenden Information oder durch Negativauskunft (BeckOK DatenschutzR/Schmidt-Wudy, 53. Ed. 1.8.2025, DS-GVO Art. 15 Rn. 50-52.3). Nichts hiervon ist hier erfolgt. Im Einzelnen:

(1) Soweit sich die Beklagte darauf beruft, die Klägerseite könne die begehrten Informationen „auf einfachem Wege“ über die angebotenen Self-Service Tools abrufen, entspricht dies offenkundig nicht der Wahrheit. Dass dennoch immer wieder in zahlreichen Verfahren derart vorgetragen wird, erstaunt und dürfte deutlich im Widerspruch zur Wahrheitspflicht im deutschen Prozessrecht stehen.

(a) Schon aus den eigenen Auskünften der Beklagten zu den Einschränkungen des „Deine Aktivitäten außerhalb der Meta-Technologien“-Tools folgt unmissverständlich, dass dieses Angebot keinerlei tauglichen Weg bietet, um auch nur ansatzweise lückenlos die begehrten Auskünfte zu erhalten. Die von der Beklagten selbst formulierten Einschränkungen sind selbsterklärend und bedürften insoweit auch keiner weiteren Erläuterung („Hinweis: Unter „Aktivitäten außerhalb der Meta-Technologien“ siehst Du nicht alle deine Aktivitäten“, „Deine jüngsten Aktivitäten sind in der Zusammenfassung nicht enthalten“, „Wir erhalten mehr Einzelheiten und Aktivitäten, als du unter „Aktivitäten außerhalb von Meta-Technologien“ siehst“, „zeigen wir nicht alle Aktivitäten, über die wir informiert wurden.“). Nicht enthalten sind nach der Auskunft insbesondere auch solche Aktivitäten, *„wie wir erhalten haben, während du nicht bei Facebook angemeldet warst“* - mithin potentiell ganz erhebliche Datenmengen, die hier jedoch gerade streitgegenständlich sind.

(b) Soweit in den übermittelten Schriftsätzen und Unterlagen daneben noch mehr oder weniger klar auf weitere „Tools“ verwiesen wird, führt auch dies nicht weiter. Insbesondere die Tools „Zugriff auf deine Informationen“ und „Deine Informationen herunterladen“ betreffen nach den dortigen Ausführungen lediglich den Einstellungsverlauf und den von den Nutzerinnen und Nutzern selbst erstellten Content („Wenn Du eine Kopie von allem möchtest, was du auf Instagram geteilt hast“), nicht aber die hier streitgegenständlichen Informationen über Drittseitenbesuche außerhalb der Meta-Apps.

(c) Soweit insoweit abweichende Rechtsprechung anderer Gerichte besteht (etwa Urteil des Landgerichts Kiel vom 10. Oktober 2024, Az. 6 O 274/23, Juris: „Zudem kann der Kläger über die von der Beklagten zur Verfügung gestellten „Self-Service“-Tools jederzeit ohne Weiteres selbst auf die von ihm begehrten Informationen zugreifen.“) ist dies der Kammer nur damit erklärlich, dass in diesem Verfahren augenscheinlich aufgrund des dortigen Vortrages kein Anlass bestand, sich näher mit der Funktionsweise der Tools zu befassen. Tatsächlich und aus den oben ausgeführten Gründen bieten die Tools keine Möglichkeit des auch nur näherungsweise lückenlosen Zugriffs auf die streitgegenständlichen Informationen.

(2) Des Weiteren kann sich die Beklagte auch weitgehend nicht auf Erfüllung durch Ihr Schreiben vom 6. Juni 2025 berufen.

Das Begehren 1 gemäß dem vorgenannten Schreiben wurde schon deshalb nicht erfüllt, weil die Beklagte dort lediglich auf die vorgenannten Selbstbedienungs-Tools verweist. Auf die obigen Ausführungen wird Bezug genommen. Dasselbe gilt für Begehren 3.

In der Antwort auf Begehren 2 wird zwar eine Liste an Empfängern vorgelegt. Aus der Liste erschließt sich jedoch nicht ansatzweise, welche Daten an diese Empfänger jeweils weitergegeben worden sein sollen.

Abzuweisen war die Klage allerdings im Hinblick auf den Auskunftsanspruch gem. Art. 15 Abs. 1 h). Denn jedenfalls insoweit liegt eine unmissverständliche Negativauskunft in dem Schreiben vom 30. Juni 2025 vor, der den Anspruch erfüllt: „Meta hat keine Verarbeitung in Bezug auf die personenbezogenen Daten Ihres Kunden festgestellt, die in den Anwendungsbereich von Art. 22 Abs. 1 DSGVO fällt.“

(3) Auch innerprozessual wurde der Auskunftsanspruch nicht weiter erfüllt.

f. Das Gericht ist sich im Übrigen darüber im klaren, dass die obigen Ausführungen in der Gesamtschau mit sich bringen, dass im Ergebnis faktisch jeder und jedem Facebook- bzw. Instagramnutzerin oder -nutzer die hier zuerkannten Unterlassungs- und Schadensersatzansprüche zustehen dürften – und zwar ohne dass es hierfür weiteren Vortrages zum individuellen Nutzungsverhalten bedarf. Prozessual betrachtet ist dies jedoch lediglich die rechtliche Konsequenz aus dem Umstand, dass die Beklagte ihrer sekundären Darlegungslast hinsichtlich der Frage nicht nachkommt, welche konkreten personenbezogenen Daten sie von den Nutzerinnen und Nutzern über die von ihr konzipierten Business Tools erhebt und verarbeitet. Käme sie rechtskonform ihrer Pflicht nach, dazu vorzutragen, welche Daten sie von den einzelnen Nutzerinnen und Nutzern erhalten und verarbeitet hat (wozu sie nach Art. 15 DSGVO ohnehin verpflichtet ist), könnte sie eine deutlich individuellere Prüfung der geltend gemachten Ansprüche erreichen. Dass sie hiervon keinen Gebrauch macht, obgleich ihr eine entsprechende Darlegung zweifelsfrei möglich wäre, kann nicht zur Rechtlosstellung der Klägerseite und zum vollständigen Leerlaufen der einschlägigen Regelungen der DSGVO führen (i.d.S. auch und mit überzeugender Begründung LG Leipzig, Urteil vom 4. Juli 2025 – 5 O 2351/23 –, juris).

II.

Die Entscheidung über die Kosten folgt aus § 92 Abs. 2 Nr. 1.

III.

Die vorläufige Vollstreckbarkeit richtet sich nach §§ 709 S. 1 und S. 2.

IV.

Den Gebührenstreitwert hat die Kammer mit 16.000,00 € festgesetzt.

1. Der Bemessung des Gebührenstreitwertes hat die Kammer im Ausgangspunkt gemäß § 48 Abs. 1 S. 1 GKG die für die Zuständigkeit des Prozessgerichts oder die Zulässigkeit des Rechtsmittels geltenden Vorschriften der §§ 3, 6-9 ZPO über den Wert des Streitgegenstands zu Grunde gelegt. In der konkreten Streitsache ist ferner zu berücksichtigen, dass verfahrensgegenständlich eine Mehrzahl von Anträgen ist und die Streitigkeiten je nach Antrag zum Teil als vermögensrechtlich und zum Teil als nichtvermögensrechtlich zu qualifizieren sind.

Ob ein Rechtsstreit vermögens- oder nichtvermögensrechtlicher Natur ist, bestimmt sich nach dem Zweck des jeweiligen Klageantrages. Ist der Klageantrag unmittelbar auf eine vermögens-

werte Leistung gerichtet, handelt es sich stets um einen vermögensrechtlichen Streit. Ferner sind Ansprüche als vermögensrechtlich zu qualifizieren, die auf vermögensrechtlichen Beziehungen beruhen bzw. ihnen entstammen, sowie solche Ansprüche, die im Wesentlichen der Wahrung wirtschaftlicher Belange dienen. In allen anderen Fällen ist das Rechtsverhältnis entscheidend, aus dem der geltend gemachte Anspruch hergeleitet wird (vgl. *Elzer* in: Toussaint, Kostenrecht, 53. Aufl. 2023, GKG § 48 Rn. 7 m.w.N.).

Für die Fälle nichtvermögensrechtlicher Streitigkeiten bestimmt § 48 Abs. 2 S. 1 GKG, dass der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen zu bestimmen ist, wobei die Grenzen gemäß §§ 34 Abs. 1, 48 Abs. 2 S. 2 GKG bei 500 € und 1 Mio. € liegen. Im Grundsatz kann in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei einer nichtvermögensrechtlichen Streitigkeit und mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Wert von 5.000 € ausgegangen werden (vgl. etwa BGH, Beschluss vom 17. November 2015 – II ZB 8/14 –, Rn. 13, juris). Bei der Bemessung darf ferner das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (vgl. BGH Beschluss vom 28.1.2021 – III ZR 162/20 –, GRUR-RS 2021, 2286 Rn. 9 m.w.N.).

2. Hieran gemessen hat die Kammer den Streitwert auf insgesamt 16.000,00 € festgesetzt.

a. Den Streitwert des Auskunftsantrages beziffert die Kammer mit 500,00 €.

b. Den Löschantrag zu 2. beziffert die Kammer mit 5.000 EUR.

c. Der als Antrag zu 3. gestellte Antrag auf Unterlassung betrifft eine nichtvermögensrechtliche Streitigkeit. Die Kammer hat für diesen Unterlassungsantrag einen Gebührenstreitwert von 5.000,00 € festgesetzt.

Wie oben ausgeführt, ist der Streitwert des Unterlassungsantrags als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses zu ermitteln, unter Berücksichtigung der jeweiligen Umstände des Einzelfalls, § 48 Abs. 2 S. 1 GKG. Nach der Rechtsprechung des Bundesgerichtshofs kann in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei einer nichtvermögensrechtlichen Streitigkeit und mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Wert von 5.000 € ausgegangen werden (BGH, Beschluss vom 17. November 2015 - II ZB 8/14, WM 2016, 96 Rn. 13). Die Klägerseite betont u.a. in ihrer Klage wie schwerwiegend der Eingriff der Beklagten, dies insbesondere mit Blick auf das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts sei. Den Anspruch auf immaterielles Schmerzensgeld beziffert sie selbst mit 5.000,00 €, wobei sie ausdrücklich betont, dass

es sich ihrer Auffassung nach dabei um einen Mindestbetrag handelt.

Die Kammer setzt daher, insbesondere aufgrund fehlender konkreter Anhaltspunkte für einen höheren oder geringeren Wert, dem Gedanken der allgemeinen Wertvorschrift des § 23 Abs. 3 S. 2 RVG folgend, für den Unterlassungsantrag einen Wert von 5.000,00 € an.

d. Der Antrag zu 3. betrifft eine vermögensrechtliche Streitigkeit; der Streitwert ergibt sich aus dem der Klägerseite zuerkannten immateriellen (Mindest-)Ersatzbetrag in Höhe von 5.500,00 €.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung kann das Rechtsmittel der Berufung eingelegt werden. Die Berufung ist nur zulässig, wenn der Wert des Beschwerdegegenstands 600 Euro übersteigt oder das Gericht des ersten Rechtszuges die Berufung im Urteil zugelassen hat.

Die Berufung ist binnen einer Notfrist von **einem Monat** bei dem

Schleswig-Holsteinischen Oberlandesgericht
Gottorfstraße 2
24837 Schleswig

einzulegen.

Die Frist beginnt mit der Zustellung der vollständigen Entscheidung, spätestens mit Ablauf von fünf Monaten nach der Verkündung der Entscheidung.

Die Berufung muss mit Schriftsatz durch eine Rechtsanwältin oder einen Rechtsanwalt eingelegt werden. Die Berufungsschrift muss die Bezeichnung der angefochtenen Entscheidung und die Erklärung enthalten, dass Berufung eingelegt werde.

Die Berufung muss binnen zwei Monaten mit Anwaltsschriftsatz begründet werden. Auch diese Frist beginnt mit der Zustellung der vollständigen Entscheidung.

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 Lübeck
Am Burgfeld 7
23568 Lübeck

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 genann-

ten 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 Erstatteinreichung 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.



Vorsitzender Richter am Landgericht