Oberlandesgericht Dresden

Zivilsenat

Aktenzeichen: **2 U 967/25**
Landgericht Chemnitz, 1 O 1825/24

IM NAMEN DES VOLKES

ENDURTEIL

In dem Rechtsstreit

[redacted]

- Kläger und Berufungskläger -

Prozessbevollmächtigte:
BK Baumeister & Kollegen Verbraucherkanzlei, Viktoria-Luise-Platz 7, 10777 Berlin,
Gz.: BKD-018798-24

gegen

Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2 K5, Irland
vertreten durch d. Director

- Beklagte und Berufungsbeklagte -

Prozessbevollmächtigte:
[redacted]

wegen illegaler Datenverarbeitung gem. § 42 Abs. 2 BDSG (kein "Datenleck"-Fall)

hat der 2. Zivilsenat des Oberlandesgerichts Dresden durch

Präsident des Oberlandesgericht[redacted]
Richter am Oberlandesgericht[redacted]
Richterin am Oberlandesgericht[redacted]

aufgrund der mündlichen Verhandlung vom 27.05.2026 am 10.06.2026

für Recht erkannt:

I. Auf die Berufung des Klägers wird das Urteil des Landgerichts Chemnitz vom 31.07.2026 (1 O 1825/25) unter Zurückweisung der weitergehenden Berufung abgeändert und wie folgt neu gefasst:

1. Die Beklagte wird verurteilt, Auskunft darüber zu erteilen, welche durch die Meta Business Tools erlangten personenbezogenen Daten die Beklagte seit dem 12.10.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Instagram“ unter dem Benutzername[redacted]s Klägers verknüpft hat,

a) auf Dritt-Webseiten und Dritt-Apps die personenbezogenen Daten, die der Identifizierung des Klägers dienen, ob direkt oder in gehashter Form übertragen, das heißt,
- E-Mail des Klägers
- Telefonnummer des Klägers
- Vorname des Klägers
- Nachname des Klägers
- Geburtsdatum des Klägers
- Geschlecht des Klägers
- Ort des Klägers
- Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID“ genannt)
- IP-Adresse des Clients
- User-Agent des Clients (das heißt gesammelte Browserinformation)
- interne Klick-ID der Meta Ltd.
- interne Browser-ID der Meta Ltd.
- Abonnement-ID
- Lead-ID und
- anon-ID

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten des Klägers,

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

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

außerdem für jedes erhobene Datum,

- ob und wenn ja, welche konkreten personenbezogenen Daten des Klägers die Beklagte seit dem 12.10.2018 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben

hat unter Benennung dieser Dritten,

- ob und wenn ja, welche konkreten Daten des Klägers die Beklagte seit dem 12.10.2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat,
- 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 und die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für die betroffene Person zu erteilen.

2. Die Beklagte wird verpflichtet, die vorstehend unter Nummer 1 aufgeführten Daten 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, die vorstehend unter Nummer 1 aufgeführten personenbezogenen 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 1.500,00 Euro nebst Zinsen i.H.v. fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 10.01.2025 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

II. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

III. Dieses Urteil ist vorläufig vollstreckbar, hinsichtlich des Unterlassungsanspruchs (I.3.) gegen Sicherheitsleistung in Höhe von 1.000,00 EUR und hinsichtlich des Auskunftsanspruchs (I.1.) und des Löschungsanspruchs (I.2.) jeweils gegen Sicherheitsleistung in Höhe von 500,00 EUR. Wegen des sonstigen vollstreckungsfähigen Inhalts des Urteils kann jede Partei die Vollstreckung durch Sicherheitsleistung in Höhe von 110 Prozent des gegen sie vollstreckbaren Betrags abwenden, wenn nicht die Gegenseite vor der Vollstreckung Sicherheit in Höhe von 110 Prozent des zu vollstreckenden Betrags leistet.

IV. Die Revision wird zugelassen.

Beschluss:

Der Streitwert der 1. Instanz wird unter Abänderung der Wertfestsetzung im erstinstanzlichen Urteil auf 7.000,00 EUR festgesetzt.

Gründe:

I.

Die Parteien streiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch sogenannte „Business-Tools“ der Beklagten über Verstöße gegen die DSGVO und dar-

aus resultierende Auskunfts-, Unterlassungs-, Löschungs- und Schadensersatzansprüche.

Die Beklagte, bis Oktober 2021 unter „Facebook Ireland Ltd." firmierend, ist Betreiberin des sozialen Netzwerks „Instagram", welches der Kläger seit dem 12.10.2018 unter dem Benutzernamen [redacted] ausschließlich privat genutzt hat. Am 30.03.2026 hat der Kläger sein Instagram-Konto selbst deaktiviert. Die Nutzung der Plattform ist - abgesehen von der frei wählbaren Möglichkeit eines Abo-Modells, die der Kläger nicht gewählt hat - kostenfrei. Geschäftsmodell der Beklagten ist es u.a., ihren werbetreibenden Kunden gegen Entgelt zielgerichtete personalisierte Werbung zu ermöglichen.

Mit der Registrierung bei dem von der Beklagten betriebenen sozialen Netzwerk stimmen Nutzer – so auch der Kläger – diesbezüglichen Nutzungsbedingungen der Beklagten zu (vgl. Anlage B 2, Stand: 15.01.2024). Dort wird bereits auf Seite 1 ausdrücklich auf Regelungen verwiesen, wie die Beklagte Informationen verwendet, um Werbeanzeigen und andere kommerzielle und werbliche Inhalte zu zeigen, für deren Bewerbungen Unternehmen und Organisationen bezahlen. Des Weiteren sind in das Nutzungsverhältnis eine „Datenschutzrichtlinie" (Anlage K 3) sowie eine nicht vorgelegte „Cookie-Richtlinie" einbezogen.

Die Beklagte verarbeitet personenbezogene Daten ihrer Nutzer, die bei Nutzung ihrer Netzwerke erfasst werden (sog. „On-platform"-Daten), insbesondere Informationen, die der Nutzer bei der Registrierung und Erstellung eines Profils bereitstellt, z.B. Name, E-Mail-Adresse, Telefonnummer; außerdem Informationen über Aktivitäten des Nutzers auf der jeweiligen Plattform, z.B. von Nutzer erstellte Beiträge, gesendete und empfangene Nachrichten, angesehene Inhalte, Zeitpunkt, Dauer und Häufigkeit der Nutzeraktivität sowie sonstige Interaktionen; darüber hinaus App-, Browser- und Geräteinformationen, genutzte Software, Identifikatoren des Geräts zur Unterscheidung von Geräten anderer Nutzer, Signale von dem Gerät, Informationen zur Netzwerkverbindung des Geräts einschließlich IP-Adresse und standortbezogene Informationen; überdies Informationen über Kontakte, z.B. Freunde und Follower des Nutzers und deren Nutzungsverhalten innerhalb der Netzwerke der Beklagten sowie schließlich auch Informationen über den Nutzer, basierend auf der Aktivität anderer Nutzer (vgl. Anlage K 3, S. 5 ff.).

Darüber hinaus bietet die Beklagte Dritten, nämlich werbetreibenden Kunden, im geschäftlichen Verkehr die Nutzung ihrer Meta-Business-Tools an, die von diesen Geschäftspartnern auf zahlreichen Webseiten, Servern oder Apps eingebunden werden und mit denen diese Kunden durch die Teilung bestimmter Daten mit der Beklagten nach Maßgabe der Nutzungs-

bedingungen „die Leistung ihrer Produkte und Dienstleistungen besser verstehen und messen“ und gleichzeitig „Personen, die diese nutzen oder daran Interesse haben, besser erreichen und ihnen einen besseren Service […] bieten“ können (vgl. Anlage B 3, Seite 3). Zu diesen Tools gehören die Applikationen Meta Pixel, Conversions API, App-Events über Facebook-SDK, Offline-Conversions und App-Events API, mit denen Programmierschnittstellen für die Datenerhebung und -übertragung beim Besuch von Webseiten oder der Nutzung von Apps geschaffen worden sind. Die übermittelten Daten ermöglichen es der Beklagten, die Informationen unmittelbar oder mittels eines Algorithmus einem bestimmten Nutzer zuzuordnen.

Die von der Beklagten angebotenen Tools werden – für den Nutzer nicht oder nicht ohne weiteres erkennbar – in zahlreichen reichweitenstarken Internetseiten eingebettet, dazu zählen etwa Nachrichtenseiten (z.B. spiegel.de, bild.de, welt.de, faz.net, sueddeutsche.de, stern.de, mdr.de), Webseiten von Reiseanbietern (z.B. tripadvisors.de, hrs.de, holiday-check.de, airbnb.de), Shoppingportale (z.B. ebay.de, otto.de, kaufland.de, zalando.de, ikea.com, autoscout24.de), Webseiten zu Finanzthemen (z.B. comdirect.de, ing.de, commerzbank.de, paypal.com), Webseiten und Apps, die Informationen zu Gesundheitsfragen bzw. medizinischen Themen bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, aerzte.de, jameda.de), Dating- und Erotikseiten (z.B. parship.de, lovescout.de) sowie zu zahlreichen anderen Themen (z.B. kicker.de, sport1.de, dhl.de, gutefrage.net, linkedin.com; vgl. insgesamt Anlagen K 1, K 4, K 5).

Über die vorgenannten Business Tools erhält die Beklagte sog. „Off-platform“-Daten, die sie über die zuvor dargestellten „On-platform“-Daten hinaus verarbeitet. Zu den Informationen, welche die Beklagte über Meta Business Tools von Drittanbietern erhält, gehören sog. „Kontaktinformationen“, mit denen Einzelpersonen identifiziert werden können, z.B. Namen, E-Mail-Adressen, Telefonnummern, in „gehashter“ (verschlüsselter) Form und außerdem sog. „Event-Daten“ mit Informationen über Nutzeraktionen auf Dritt-Webseiten, z.B. das Aufrufen einer Seite, die Installation von Apps oder der Kauf von Produkten (vgl. Anlage B 5 unter Ziff. 1. a. i. und ii.).

Diesen Tools liegen die Folgenden Nutzungs- und Datenverarbeitungsbedingungen zugrunde: „Nutzungsbedingungen für Meta-Business-Tools“, Stand 25.04.2023, (Anlage B 5), „Parameter für Kund*innen-Informationen“ (Anlage K 14) sowie die Aufstellung „Unzulässige Informationen“ (Anlage B 6) dazu, welche Informationen Drittunternehmen mit der Beklagten teilen dürfen.

Im Rahmen der zugehörigen Nutzungsbedingungen verpflichtet die Beklagten ihre Kunden, welche die Business Tools nutzen möchten, in nachprüfbarer Weise sicherzustellen, dass ein Endnutzer alle erforderlichen Einwilligungen erteilt, bevor die Tools genutzt werden, um der Beklagten das Speichern von Cookies oder sonstigen Informationen auf dem Gerät des Endnutzers und den Zugriff hierauf zu ermöglichen (vgl. Anlage B 5, S. 4) und verlangt deshalb von ihren Kunden eine Zusicherung, dass sie über eine Rechtsgrundlage für die Offenlegung und Verwendung von mittels Business Tools erhobenen Daten verfügen und auch im Übrigen alle datenschutzrechtlichen Vorschriften einhalten (vgl. Anlage B 5, S. 2).

Nach Eingang der durch die Business Tools erhobenen Daten auf den Servern der Beklagten werden diese ausgelesen und automatisiert mit den bei ihr bereits hinterlegten Datensätzen abgeglichen. Ist der Beklagten in Auswertung der übertragenen Datensätze eine Zuordnung des Anwenders zu einem bei ihr registrierten Nutzer möglich, hängt deren weitere Verwendung davon ab, welche Auswahlentscheidung diesbezüglich in den Einstellungen des betreffenden Profils hinterlegt ist.

Einzelne Einstellungen geben dem privaten Nutzer zur Kontrolle der Nutzung der Daten von Drittwebseiten und -Apps durch die Beklagte die Möglichkeit, sogenannte optionale Cookies in anderen Apps und auf anderen Webseiten zu teilen bzw. das Setzen solcher Cookies nicht zu erlauben (Anlage B 7, insb. Seite 9 ff.) bzw. über die Einstellung „Informationen von Werbepartnern zu Aktivitäten verwenden, um Werbung anzuzeigen“ zu entscheiden (Anlage B 7, Seite 14 ff.). So kann die voreingestellte Verwendung optionaler Cookies deaktiviert oder – unabhängig davon – die Erlaubnis erteilt werden, Informationen von Werbepartnern zu Aktivitäten zu verwenden, um Werbung anzuzeigen. Erfolgt die Zustimmung zur Nutzung der Daten zum Zwecke der Anzeige personalisierter Werbung nicht, nutzt die Beklagte die auf Drittwebseiten und -Apps erhobenen Daten nicht, um dem Nutzer relevante Werbung anzuzeigen.

Der Kläger hat in den Einstellungen eine Erlaubnis zur Verwendung von Informationen zur Anzeige personalisierter Werbung nicht erteilt (vgl. die Beklagte, S. 125 dA LG).

Ausweislich ihrer Datenschutzrichtlinie werden die mittels Business Tools übermittelten Daten von der Beklagten aber – in eingeschränktem Umfang – zu anderen Zwecken verarbeitet, gespeichert und genutzt, etwa zum Schutz der Sicherheit und Integrität ihrer Server sowie auch zur Messung der Effektivität von Werbekampagnen. Dies erfolgt unabhängig von den vorgenannten Einstellungen. Der Nutzer kann durch die Deaktivierung der vorgenannten Einstellungen auch nicht verhindern, dass die Beklagte über Dritte generierte Daten überhaupt erhält.

Nutzer von Instagram haben außerdem die Möglichkeit, sich in den Einstellungen, dort unter „Deine Aktivitäten außerhalb von Meta-Technologien“, eine Zusammenfassung der mit ihrem Konto verknüpften Informationen über ihre Aktivitäten, die Drittunternehmen mit der Beklagten geteilt haben, in eingeschränktem Umfang anzeigen zu lassen („Self-Service-Tools“). Darüber hinaus besteht dort die Möglichkeit, die von Drittunternehmen geteilten Daten von ihrem Nutzerkonto zu trennen und – bezogen auf konkrete Drittunternehmen – eine Verknüpfung von Informationen für die Zukunft auszuschließen. Gelöscht werden die Daten hierdurch nicht. Die vorgenannte Einstellung kann auch nicht verhindern, dass die Beklagte weiterhin Daten von Drittunternehmen erhält; es wird lediglich keine Verknüpfung mit dem Nutzerkonto mehr vorgenommen.

Der Kläger hat mit seiner Klage in erster Instanz zuletzt einen Auskunftsantrag, einen Löschungsantrag, einen Unterlassungsantrag und einen Anspruch auf immaterielle Entschädigung geltend gemacht und außerdem die Erstattung vorgerichtlicher Anwaltskosten verlangt. Insbesondere hat er beanstandet, dass nach Übertragung der Daten an die Beklagte mittels Business Tools, die auf dem Rechner des Nutzers oder den Servern von Webseiten und App-Betreibern laufen, ein Abgleich erfolge, durch den die Beklagte ermitteln könne, wessen personenbezogene Daten sie durch Business Tools gesammelt, an ihre Server übertragen lassen und bereits verarbeitet habe. Hiervon sei er betroffen, weil er viele Webseiten und Apps nutze, auf denen Meta Business Tools vorzufinden seien; er surfe durchschnittlich mehrere Stunden in der Woche über einen Browser im Internet und verbringe mindestens eine Stunde täglich in Apps (S. 31, 274 dA LG). Die Daten des Klägers verarbeite die Beklagte automatisch ohne jede Unterscheidung genauso wie die Daten aller anderen Nutzer auch. Der Kläger habe keine hinreichende Kenntnis darüber, welche seiner personenbezogenen Daten mittels Business Tools an die Beklagte übermittelt und von ihr verarbeitet würden. Die Beklagte gebe ihm keine Möglichkeit, diese Datenverarbeitung zu beenden, die stets stattfinde und nicht berücksichtige, ob der Kläger hierin eingewilligt habe oder nicht oder ob er seinen Account weiterbetreibe oder lösche. Die Beklagte, welche die Darlegungs- und Beweislast bzgl. einer Rechtfertigung und Einwilligung nach Art. 6 DSGVO trage, habe bisher nur Screenshots von Schaltflächen zur „Einwilligung in die Verarbeitung für personenbezogene Werbung“ vorgelegt und auf unbenannte „Dritte“ verwiesen, mit denen sie angeblich Verträge abgeschlossen habe, die diese Dritten dazu verpflichteten, wirksame Einwilligungen bei dem Nutzer einzuholen. Dieser Vortrag sei unsubstantiiert und nicht einlassungsfähig. Weitere konkrete Rechtfertigungsgründe könne die Beklagte nicht für sich in Anspruch nehmen. Soweit sie Sicherheitsaspekte anführe, bleibe ihr Vortrag vage. Zudem sei sie spätestens bei der Verarbeitung auf ihren eigenen

Servern, also nach der Übertragung durch Business Tools, nicht mehr „gemeinsam Verantwortliche" im Sinne von Art. 26 DSGVO mit Drittbetreibern und könne sich auf eine gegenüber diesen erteilte Einwilligung nicht berufen. Die außergerichtlich mit anwaltlichem Schreiben vom 02.07.2024 (Anlage K 7) geltend gemachten Ansprüche habe die Beklagte nicht erfüllt.

Die Beklagte ist der Klage entgegengetreten. Sie hat bestritten, von Dritt-Webseiten oder -Apps stammende personenbezogene Daten des Klägers in rechtswidriger Weise zu verarbeiten; vielmehr entspreche ihr Vorgehen den Vorschriften der DSGVO. Sie hat insbesondere in Abrede gestellt, dass konkrete Off-Plattform-Daten des Klägers verarbeitet oder ihm individuell zugeordnet worden seien. Die Beklagte hat weiter behauptet, Art und Umfang der Verarbeitung von Off-Plattform-Daten hingen von den jeweiligen technischen Implementierungen der Meta Business Tools durch die Drittunternehmen sowie von den Entscheidungen und Einstellungen der Nutzer ab. Zudem hat sie geltend gemacht, dass Off-Plattform-Daten – abhängig von der jeweiligen Konstellation – nicht oder nur zu bestimmten Zwecken verarbeitet würden. Eine persönliche Betroffenheit des Klägers hat sie in Abrede gestellt.

Wegen des weiteren Vorbringens der Parteien und der in 1. Instanz gestellten Anträge wird auf die erstinstanzlichen Feststellungen in dem angefochtenen Urteil Bezug genommen.

Mit Urteil vom 31.07.2025 hat das Landgericht die Klage abgewiesen. Der Antrag, mit dem die Löschung verlangt wird, sei mangels der gemäß § 259 ZPO notwendigen Besorgnis der Leistungsverweigerung unzulässig, die übrigen Anträge unbegründet. Die begehrten Auskünfte seien bereits mit außergerichtlichem Schreiben vom 25.04.2025 (Anlage B 8) erteilt worden. Der Antrag auf Schadensersatz sei unbegründet, weil es an einem Schaden des Klägers - etwa durch einen „Kontrollverlust" oder eine emotionale Beeinträchtigung - fehle. Zudem habe er auch keinen Verstoß der Beklagten gegen die DSGVO nachgewiesen. Aus diesem Grund habe er auch keinen Unterlassungsanspruch gegen die Beklagte. Mit Beschluss vom 03.09.2025 hat das Landgericht einen Tatbestandsberichtungsantrag des Klägers zurückgewiesen.

Hiergegen wendet sich der Kläger mit seiner Berufung, mit der er die erstinstanzlich gestellten Anträge vollumfänglich weiterverfolgt. Der Löschungsantrag sei angesichts des Bestreitens des Anspruchs durch die Beklagte zulässig und auch begründet. Hinsichtlich des geltend gemachten Auskunftsanspruchs verkenne das erstinstanzliche Gericht, dass keine Erfüllung eingetreten sei. Der Antrag auf Unterlassen der künftigen Datenverarbeitung sei begründet; die Nennung einzelner vom Kläger aufgesuchter Webseiten sei entgegen der Auffassung des erstinstanzlichen Gerichts nicht notwendig und auch nicht möglich. Der auf Zahlung immateri-

ellen Schadensersatzes gerichtete Antrag sei nach Art. 82 DSGVO begründet. Entgegen der Auffassung des Landgerichts bestreite die Beklagte nicht, personenbezogene Daten des Klägers mithilfe ihrer Business Tools auf Drittwebseiten und -Apps erfasst zu haben und weiterhin zu erfassen, diese an ihre Server weiterzuleiten, dort zu speichern und weiterzuverarbeiten. Sie bestreite lediglich, dass sie die Weiterverarbeitung zum Zwecke der Bereitstellung personalisierter Werbung vornehme. Soweit das Landgericht konkreten Vortrag zu einzelnen Verarbeitungsvorgängen vermisse, komme es darauf nicht an. Streitgegenständlich seien abstrakte Voreinstellungen und die Funktionsweise der Business Tools gegenüber dem Kläger hinsichtlich der Erfassung und Weiterleitung personenbezogener Daten durch die Business Tools sowie der erstmaligen Speicherung und anschließenden Weiterverarbeitung der empfangenen Daten auf den Servern der Beklagten. Die Beklagte habe keinerlei Recht, ihre Softwaretools im Internet so auszurichten, dass eine unüberschaubare Vielzahl von Datenpunkten des Klägers gesammelt werde, mit deren Hilfe es möglich sei, ein umfassendes Persönlichkeitsprofil über sie zu erstellen. Die Beklagte verarbeite unstreitig Daten ihrer Nutzer, auch wenn sich diese mit den von der Beklagten bereitgestellten Einstellungsmöglichkeiten gegen die Verwendung ihrer Daten zum Zwecke der Bereitstellung personalisierter Werbung entschieden hätten. Die Datenverarbeitung geschehe umfassend und ohne hinreichenden Rechtfertigungsgrund; sie betreffe außerdem auch höchstpersönliche Daten im Sinne von Art. 9 DSGVO. Die Anwendung der Business Tools auf den Kläger bewirke einen Kontrollverlust über seine Daten, der darin liege, dass er nicht wisse, was die Beklagte über ihn weiß und weitergibt. Dies führe zu erheblicher Unsicherheit. Deswegen sei ein Anspruch auf immateriellen Schadensersatz begründet und in Höhe von mindestens 5.000,00 EUR angemessen. Auch ein Anspruch auf die Freistellung von vorgerichtlichen Rechtsanwaltskosten stehe ihm zu, dabei handele es sich um einen aus dem DSGVO-Verstoß der Beklagten resultierenden Schaden.

Der Kläger zuletzt beantragt,

> das Urteil des Landgerichtes Chemnitz vom 31.07.2025 abzuändern und neu zu fassen wie folgt:
>
> 1. Die Beklagte wird verurteilt, Auskunft darüber zu erteilen, welche durch die „Meta Business Tools“ erlangten personenbezogenen Daten die Beklagte seit dem 12.10.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Instagram“ unter dem Benutzernamen [redacted] des Klägers verknüpft hat,
>
> a) auf Dritt-Webseiten und Dritt-Apps die personenbezogenen Daten, die der Identifizierung des Klägers dienen, ob direkt oder in gehashter Form übertragen, das heißt,
> - E-Mail des Klägers
> - Telefonnummer des Klägers

- Vorname des Klägers
- Nachname des Klägers
- Geburtsdatum des Klägers
- Geschlecht des Klägers
- Ort des Klägers
- Externe IDs anderer Werbetreibender (von der Meta Ltd. „external_ID“ genannt)
- IP-Adresse des Clients
- User-Agent des Clients (das heißt gesammelte Browserinformation)
- interne Klick-ID der Meta Ltd.
- interne Browser-ID der Meta Ltd.
- Abonnement-ID
- Lead-ID und
- anon-ID

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten des Klägers,

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

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

außerdem für jedes erhobene Datum,

- ob und wenn ja, welche konkreten personenbezogenen Daten des Klägers die Beklagte seit dem 12.10.2018 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat unter Benennung dieser Dritten,
- ob und wenn ja, welche konkreten Daten des Klägers die Beklagte seit dem 12.10.2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat,
- 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 und die Tragweite und angestrebte Auswirkung einer solchen Verarbeitung für die betroffene Person zu erteilen.

2. Die Beklagte wird verpflichtet, die Daten gemäß des Antrags 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 gemäß des Antrags zu 1. 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 31.07.2024, zu zahlen.

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

Die Beklagte beantragt,

die Berufung zurückzuweisen.

Sie verteidigt das angefochtene Urteil und hält die Klageanträge überwiegend für zu unbestimmt und damit unzulässig. Der Nutzer müsse in die Datenverarbeitung zur Bereitstellung personalisierter Werbung gemäß Art. 6 Abs. 1 lit. a DSGVO über die Schaltfläche „Informationen über Aktivitäten von Werbepartnern“ einwilligen. Sie sei auf eine Datenquelle beschränkt, nämlich auf die von Werbepartnern übermittelten Aktivitäten eines Nutzers außerhalb der Plattform Instagram. Eine Datenverarbeitung zur Bereitstellung personalisierter Werbung erfolge nur, wenn ein Nutzer eine solche Einstellung erteilt habe. Anderenfalls könne eine solche Datenverarbeitung nicht erfolgen, was die Beklagte nach erfolgtem Abgleich zur Feststellung, ob der Nutzer in ihren sozialen Netzwerken registriert sei, ermittle. Dies gelte auch für den Kläger, der eine solche Einwilligung nicht erteilt habe. Wenn ein Nutzer über Einstellmöglichkeiten innerhalb der Metasysteme optionale „Meta-Cookies auf anderen Apps und Webseiten“ nicht erlaube, werde keine Datenverarbeitung zur Bereitstellung personalisierter Werbung für diesen Nutzer vorgenommen bzw. würden „für bestimmte Verarbeitungsvorgänge“ keine über Cookies und ähnliche Technologien erhobenen Daten, einschließlich der streitgegenständlichen Datenverarbeitung verwendet. In diesem Fall nutze die Beklagte nur eingeschränkt Daten, die über Cookies und ähnliche Technologien erhoben wurden, und zwar für eingeschränkte Zwecke, wie Sicherheits- und Integritätszwecke, einschließlich Zwecke der Überwachung von versuchten Angriffen auf die Systeme der Beklagten, wie z.B. durch die forcierte Überlastung ihrer Webseite. Die Beklagte stütze sich nicht für jeden Verarbeitungszweck auf eine Einwilligung, da dies auch gesetzlich nicht erforderlich sei. Mangels konkreter Darlegung, welchen Verarbeitungszweck der Kläger angreifen möchte, könne sie hierauf auch nicht konkret erwidern.

Ferner übermittelten Drittunternehmen Daten über die Aktivitäten einer Person auf deren Web-

seite oder App über die streitgegenständlichen Business Tools nur dann an die Beklagte, wenn diese Person tatsächlich mit einem Drittunternehmen interagiere, das eines der streitgegenständlichen Business Tools nutze. Diese Drittunternehmen seien über die Nutzungsbedingungen für Business Tools verpflichtet, alle Offenlegungen vorzunehmen sowie Rechte und Genehmigungen einzuholen, bevor sie Business-Tools-Daten an die Beklagte weitergäben. Die Beklagte habe darüber hinaus eine formelle „Art. 26 DSGVO-Vereinbarung“ mit Drittunternehmen getroffen („Vertragszusatz“, vgl. Anlage B 9), die diese verpflichte, eine Einwilligung hinsichtlich der Platzierung nicht notwendiger Cookies einzuholen. Die Implementierung von Cookie-Bannern und die Einholung der Einwilligungen liege daher in erster Linie in der Verantwortung der Drittunternehmen. Hinsichtlich der gerügten Übermittlung von sog. technischen Standarddaten, z.B. über http-Anfragen, würden von Drittunternehmen sowohl bei Meta Pixel als auch bei der Conversions-API Technologien eingesetzt, die sicherstellen sollen, dass keine Daten an die Beklagte übertragen werden, bis eine Einwilligung eingeholt worden sei; hierüber habe die Beklagte auch informiert (vgl. Anlagen B 16, B 17, B 18). Mangels Zugriffs auf die Drittwebseiten und -Apps kontrolliere die Beklagte nicht, ob die Business Tools richtig installiert seien, dies stünde allein in der Verantwortung der Drittunternehmen. Nur diese hätten die Möglichkeit, ihren Code dementsprechend zu konfigurieren und sicherzustellen, dass der Browser der Person oder der Server des Drittunternehmens eine http-Anfrage erst dann ausführe, wenn die Person ihre Einwilligung zu nicht notwendigen Cookies erteilt habe. Um den Schutz besonders sensibler Daten zu gewährleisten, habe die Beklagte Maßnahmen implementiert, die dazu dienen sollen, den Erhalt und die Nutzung potenziell sensibler Daten zu verhindern. Hierzu gehöre die Kategorisierung der Datenquellen mit erweiterten Datenbeschränkungen und die automatisierte Blockierung und Filterung vor oder bei Empfang der Ereignisdaten, bevor diese Daten in den Werbesystemen von Meta gespeichert oder verwendet würden. Dem Kläger habe es daher oblegen, konkret darzulegen, welche Webseiten er besucht habe und unter Beweis zu stellen, dass über diese Webseiten Daten an die Beklagte übermittelt würden, ohne dass zuvor die Einwilligung des Klägers eingeholt worden sei. Auf eine etwaige Beweisnot, auch mit Blick auf die angebliche Unzumutbarkeit, den gesamten Browserverlauf öffentlich zu machen, könne sich der Kläger nicht berufen; eine sekundäre Darlegungslast treffe die Beklagte nicht. Auch die vom Kläger vorgelegte Liste der angeblich meistbesuchten Webseiten in Deutschland genüge nicht. Vielmehr habe die Beklagte einige der Webseiten dieser Liste überprüft und festgestellt, dass sie zum Zeitpunkt der Überprüfung keine Business Tools verwendet hätten.

In der Berufungsinstanz hat sich die Beklagte zudem näher dazu erklärt, worin ihre Nutzung der erhobenen Daten zu „Sicherheits- und Integritätszwecken“ bestehe. Danach würden diese

in begrenztem Umfang genutzt, um Sicherheitsbedrohungen einschließlich „Hacking“ von Benutzerkonten, automatisiertem „Scraping“ und Verbreitung von Malware zu verhindern, um Nutzer, die Infrastruktur, das Netzwerk, die Systeme und die Öffentlichkeit vor Gefahren zu schützen, u. a. vor Manipulationen der öffentlichen Debatte, kriminellen Aktivitäten sowie Kontakten „risikobehafteter erwachsener Akteure“ mit Minderjährigen, und um Probleme in ihren Systemen zu erkennen und zu beheben. Zur Erfüllung dieser Zwecke sei die auf einen kleinen Prozentsatz der mittels Business Tools übertragenen Informationen beschränkte Datenverarbeitung unerlässlich. Wegen sich ständig ändernder Techniken feindlicher Akteure könnten weder die Kategorien von Sicherheitsangriffen noch die relevanten Datenkategorien oder Methoden der Datenverarbeitung vollständig aufgelistet oder beschrieben werden. Aufgrund der Komplexität der Prozesse und der vielfältigen Faktoren, die bei der Untersuchung potenziell schwerwiegender oder böswilliger Aktivitäten eine Rolle spielten, seien Aufbewahrungsfristen für Daten, die in Sicherheits- und Integritätsuntersuchungen angewendet würden, schwer präzise zu definieren. Im Allgemeinen betrage die Speicherdauer bis zu 90 Tage; im Einzelfall könne sich jedoch auch eine längere Aufbewahrung für eine ordnungsgemäße Untersuchung erforderlich machen. Maximale Aufbewahrungsfristen würden durch einen umfassenden, funktionsübergreifenden Prüfprozess festgelegt, der verschiedene Elemente berücksichtige, etwa die Art des spezifischen Sicherheits- und Integritätsproblems, das die Beklagte behandele.

Wegen weiterer Einzelheiten wird auf die Schriftsätze der Parteien verwiesen.

II.

Die form- und fristgerecht eingelegte und begründete Berufung des Klägers ist zulässig und teilweise begründet. Seine Klage, für die die internationale Zuständigkeit deutscher Gerichte gemäß Art. 18 Abs. 1 EuGVVO sowie gemäß Art. 79 Abs. 2 Satz 2 DSGVO gegeben ist, ist zulässig und zum Teil begründet.

1. Der Antrag zu Ziffer 1 in der im Termin geänderten Fassung, mit dem der Kläger Auskunft verlangt, ist zulässig und begründet.

a) Maßgeblich ist die vom Kläger im Termin gestellte Antragsfassung. Die Einwilligung der Beklagten in die darin liegende Änderung der Klage ist anzunehmen, weil sie sich in der mündlichen Verhandlung auf den geänderten Antrag eingelassen hat (§§ 263, 267 ZPO). Jedenfalls ist die Klageänderung sachdienlich.

b) Der auf die Verarbeitung mittels Business Tools beschränkte Auskunftsanspruch ist zulässig und insbesondere hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO).

Ein Antrag ist hinreichend bestimmt, wenn er den Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung des Urteils ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 18.11.2024, VI ZR 10/24, Rn 52, juris).

Diesem Maßstab genügt der Antrag. Der Kläger hat die personenbezogenen Daten, über deren Verarbeitung und Verknüpfung er Auskunft begehrt, hinreichend genau bezeichnet. Die Bezugnahme auf „Dritt-Webseiten“ und „Dritt-Apps“ steht dem nicht entgegen. Der Auskunftsantrag umfasst ersichtlich alle Dritt-Webseiten und Dritt-Apps, auf denen ein Business Tool der Beklagten integriert ist; die Aufzählung einzelner Dritt-Webseiten und Dritt-Apps ist nicht erforderlich (ebenso OLG Hamm, Urteil vom 09.03.2026, I-8 U 13/25, Rn. 59, juris). In zeitlicher Hinsicht soll die Auskunft den Zeitraum ab dem 12.10.2018 - dem Zeitpunkt der Einrichtung des Nutzerkontos - bis zum Schluss der letzten mündlichen Verhandlung erfassen.

c) Der Antrag ist auch begründet.

aa) Der Auskunftsanspruch ist gemäß Art. 15 DSGVO entstanden. Die Beklagte ist Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO (dazu (1)), der Kläger hat Anspruch auf Auskunft über die in Art. 15 Abs. 1 und Abs. 2 DSGVO aufgeführten Daten (dazu (2)) und sein Antrag ist nicht rechtsmissbräuchlich oder schikanös (dazu (3)).

(1) Die Beklagte ist Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die Daten, welche sie mittels Business Tools von Drittwebseiten und -Apps erlangt und weiterarbeitet.

Gemäß Art. 4 Nr. 7 DSGVO ist Verantwortlicher diejenige 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. Eine gemeinsame Verantwortung besteht nach Art. 26 Abs. 1 Satz 1 DSGVO, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verwendung festlegen. Das Ziel dieser Bestimmungen liegt darin, durch eine weite Definition des Begriffs des Verantwortlichen einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten (EuGH, Ur-

teil vom 13.05.2014, C-131/12, Rn. 34, Urteil vom 05.06.2018, C-210/16, Rn. 28, jeweils juris). Der Europäische Gerichtshof hat für die insoweit dem Art. 4 Nr. 7 DSGVO entsprechende Vorschrift des Art. 2 Buchst. d der mit Ablauf des 24.05.2018 außer Kraft getretenen und durch die DSGVO abgelösten Datenschutzrichtlinie (Richtlinie 95/46/EG) entschieden, dass eine natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, als für die Verarbeitung Verantwortlicher angesehen werden kann (EuGH, Urteil vom 29.07.2019, C-40/17, Rn. 68, Urteil vom 10.07.2018, C-25/17, Rn. 68, jeweils juris).

Indem die Beklagte Drittunternehmern ihre Business Tools anbietet, mit deren Hilfe sie unstreitig Daten der Drittseitennutzer für ihre eigenen Zwecke erhalten möchte, wird sie für die Datenerhebung durch die Business Tools unter Anlegung des vorgenannten Maßstabs zur Mitverantwortlichen im Sinne des Art. 26 DSGVO (vgl. EuGH, Urteil vom 29.07.2019, C-40/17, Rn. 67 ff., juris; OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 169 ff., juris; OLG München, Urteil vom 18.12.2025, 14 U 2300/25 e, Rn. 270, juris; vgl. auch OGH Wien, Urteil vom 26.11.2025, 6 Ob 189/24y, Rn. 84 ff., beck-online).

Diese Verantwortlichkeit kann sie weder durch vertragliche Vereinbarungen mit den Drittanbietern auf diese abwälzen, noch kann sie sich durch etwaige Belehrungen Dritter im Hinblick auf deren datenschutzrechtlichen Pflichten von der eigenen Verantwortlichkeit freizeichnen, schon weil sie selbst gegenüber ihren Kunden der Business Tools die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO feststellt (Anlage B 5, Nutzungsbedingungen unter Ziff. 5 a. ii.). Aus denselben Gründen kann sich die Beklagte auch nicht darauf berufen, entsprechend ihrer Nutzungsbedingungen unter Ziff. 5 hinsichtlich bestimmter Verarbeitungszwecke (Abgleich-, Messung- und Analysedienste) lediglich als Auftragsverarbeiter im Sinne von Art. 4 Nr. 9 DSGVO der Drittunternehmer tätig zu werden (vgl. Anlage B 5, Nutzungsbedingungen unter Ziff. 5. a. i). Nimmt eine Stelle – wie hier die Beklagte – aus Eigeninteresse auf die Verarbeitung Einfluss und wirkt auf diese Weise neben einem anderen Beteiligten an der Entscheidung über Zweck und Mittel der Verarbeitung mit, führt dies regelmäßig zu einer (gemeinsamen) Verantwortlichkeit (EuGH, Urteil vom. 29.07.2019, a.a.O., Rn. 80; OLG Dresden a.a.O. Rn. 170).

Die Verantwortlichkeit der Beklagten betrifft bereits die durch Meta Business Tools erfassten Daten, bevor sie an die Server der Beklagten weitergeleitet und dort gespeichert und anschließend verwendet wurden. Indem die Beklagte Drittunternehmern ihre Business Tools anbietet, mit deren Hilfe sie unstreitig möglichst viele Daten der Drittseitennutzer für ihre eigenen Zwe-

cke erhalten möchte, wird sie auch für die Datenerhebung auf Drittseiten zur Mitverantwortlichen im Sinne des Art. 26 DSGVO (OLG Dresden a.a.O. Rn. 169; OLG Stuttgart, Urteil vom 29.04.2026, 4 U 353/24, Rn. 143, juris; OLG Hamm a.a.O. Rn. 81; OGH Wien a.a.O. Rn. 89).

(2) Bei den vom Kläger in seinem Auskunftsantrag aufgezählten Daten handelt es sich um „personenbezogene Daten“ im Sinne der Legaldefinition in Art. 4 Nr. 1 DSGVO. Der Begriff der personenbezogenen Daten ist weit zu verstehen und umfasst alle Arten von Informationen sowohl objektiver als auch subjektiver Natur unter der Voraussetzung, dass es sich um Informationen über die in Rede stehende Person handelt. Die letztgenannte Voraussetzung ist erfüllt, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten natürlichen Person verknüpft ist, sodass sie aufgrund dessen direkt oder indirekt identifiziert oder identifizierbar ist (EuGH, Urteil vom 20.12.2017, C-434/16, Rn. 34 f., juris; BGH, Urteil vom 18.12.2025, I ZR 115/25, Rn. 22 ff., juris). Die übermittelten Daten sind zur Identifizierung des Nutzers geeignet, was die Beklagte ausdrücklich nicht bestreitet. Die Identifizierung des Nutzers auf Webseiten und Apps Dritter erfolgt durch verschiedene Techniken. Dafür werden "Third Party Cookies", "First Party Cookies", die "Klick-ID" sowie "automatisiertes Advanced Matching" und "manuelles Advanced Matching" verwendet (vgl. LG Braunschweig, Urteil vom 04.06.2025, 9 O 2615/23, Rn. 106, juris, mit Verweis auf BKartA, Beschluss vom 06.02.2019, B6-22/16, Rn. 575 ff.).

Die Beklagte kann sich hinsichtlich des Merkmals der Personenbezogenheit nicht mit Erfolg darauf berufen, die Privatsphäre der Nutzer sei gewahrt, da sie personenbezogene Daten aggregiere, also einzelne Datenpunkte zu Gruppen zusammenfasse, sodass Erkenntnisse aus den gesammelten Informationen mehrerer Personen und nicht aus denen einer einzelnen Person gewonnen würden. Dagegen steht, dass es schon wegen der Vielzahl der durch Offsite-Aktivitäten bzw. „Third-Party Activity Data“ gewonnenen Datenpunkte und Informationen zumindest nicht ausgeschlossen erscheint, dass einzelne Nutzer und/oder ihm zugeordnete Events identifizierbar bleiben. Welche Daten die Beklagte konkret aggregiert und nutzt – und dies für welche Zwecke –, wird in ihrer Datenschutzrichtlinie nur beispielhaft und damit unzureichend erläutert (vgl. Anlage K 3, S. 48).

Art. 15 Abs. 1 DSGVO verleiht ein verfahrensmäßiges Recht, Informationen über die Verarbeitung personenbezogener Daten zu verlangen (EuGH, Urteil vom 22.06.2023, C-579/21, Rn. 35, juris). Nach Art. 15 Abs. 1 DSGVO kann Auskunft insbesondere über die Kategorien personenbezogener Daten, die verarbeitet werden (lit. b), sowie die Empfänger oder Kategorien von Empfängern (lit. c) verlangt werden. Konkret bedingt das in Art. 15 Abs. 1 Hs. 2 lit. c DSGVO

vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen (EuGH, Urteil vom 12.01.2023, C-154/21, Rn. 51, juris; OLG Hamm, Urteil vom 15.08.2023, I-7 U 19/23, Rn. 244 ff., juris). Schließlich besteht ein Auskunftsanspruch über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und - zumindest in den dort genannten Fällen - auf aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (lit. h).

Art. 15 Abs. 1 DSGVO umfasst eine Auskunftspflicht bezüglich der Datenspeicherung in Drittstaaten. Insbesondere beschränkt Art. 15 Abs. 2 DSGVO nicht die Auskunftspflicht nach Art. 15 Abs. 1 DSGVO. Dem steht bereits entgegen, dass in Art. 15 Abs. 1 Hs. 2 lit. c DSGVO ausdrücklich die Informationspflicht über Empfänger in Drittländer genannt wird. Zudem widerspräche ein solches Verständnis dem Sinn des Art. 15 DSGVO, welcher dem Betroffenen einen Einblick in das Ob und Wie der Verarbeitung seiner personenbezogenen Daten ermöglichen soll, um ihm so eine informierte und umfassende Überprüfung der Rechtmäßigkeit der Verarbeitung zu ermöglichen. Hierzu gehört auch die Frage, welche seiner personenbezogenen Daten in einen Drittstaat übermittelt werden (OLG Jena, Urteil vom 02.03.2026, 3 U 31/25, Rn. 155, juris; OLG Stuttgart a.a.O. Rn. 188 f.).

(3) Zu Unrecht nimmt die Beklagte an, aus dem Umstand einer gleichlautenden Antragsstellung in Tausenden von Parallelverfahren folge ein rechtsmissbräuchliches, die Beklagte schikanierendes Verhalten (S. 156 dA). Dabei verkennt sie, dass das Auskunftsrecht nicht an ein irgendwie geartetes rechtliches Interesse geknüpft ist, sondern sich allein aus dem Umstand ergibt, dass der Verantwortliche personenbezogene Daten über die betroffene Person verarbeitet. Die in einer Vielzahl von Fällen gleichlautende Geltendmachung ist Ausfluss der Natur des Auskunftsrechts selbst, nicht aber einer auf Rechtsmissbrauch zielenden Behandlung der Beklagten. Dies folgt auch aus Art. 12 Abs. 5 DSGVO, der das Weigerungsrecht des Verantwortlichen bei exzessiven Anträgen an die Antragstellung einer betroffenen Person koppelt und damit die gleichlautende Antragstellung einer Vielzahl unterschiedlicher Personen gerade nicht erfasst (OLG Jena a.a.O. Rn. 143).

bb) Ohne Erfolg wendet die Beklagte ein, sie habe den Auskunftsanspruch erfüllt.

Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO ist im Sinne des § 362 Abs. 1 BGB erfüllt, wenn der Verantwortliche – gegebenenfalls auch konkludent – erklärt, dass die dem Antragsteller erteilte Auskunft dem geschuldeten Gesamtumfang entspricht, d.h. vollständig ist (BGH, Urteil vom 15.06.2021, VI ZR 576/19, juris, Rn. 18 ff.). Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (BGH a.a.O. Rn. 32). Die Erfüllungswirkung kann allerdings auch dann nicht eintreten, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (BGH a.a.O. Rn 20).

Daraus ergibt sich für die begehrten Auskünfte das Folgende:

(1) Der Anspruch auf Benennung verarbeiteter und mit dem Nutzeraccount verknüpfter Daten ist nicht erfüllt.

Aus dem Schreiben der Beklagten vom 25.04.2025 (Anlage B 8) lassen sich keine individuellen Informationen zu personenbezogenen Daten des Klägers entnehmen.

Der Hinweis der Beklagten im Auskunftsschreiben auf ihr Selbstbedienungstool „Deine Aktivitäten außerhalb der Meta-Technologien“ genügt ebenfalls nicht. Zwar kann der Auskunftsanspruch grundsätzlich auch durch Bereitstellung eines Fernzugriffes zu einem sicheren System erfolgen (Erwägungsgrund Nr. 63 zur DSGVO). Das schließt auch den Verweis auf eine Website ein, über die die jeweiligen Informationen abgerufen werden können. Erforderlich ist aber, dass dort die Auskunft in dem erforderlichen individuellen Umfang für den Kläger zugänglich ist. Zwar hat die Beklagte deutlich gemacht, dass sie ihre Auskunft über das Tool für vollständig und abschließend hält. Ihr Vortrag dazu, wie sie ihre Auskunftspflicht erfüllt haben will, erschöpft sich aber weitgehend in allgemeinen Verfahrensbeschreibungen und reicht angesichts des substantiierten Vortrags des Klägers, warum das Tool der Beklagten zum lückenlosen Erhalt der begehrten Auskünfte untauglich sei, nicht aus (ebenso OLG Stuttgart a.a.O.

Rn. 194; OLG Dresden, Urteil vom 14.04.2026, 4 U 981/25, n.v., S. 14; OLG Hamm a.a.O. Rn. 82 ff.; LG Lübeck, Urteil vom 27.11.2025, 15 O 15/24, Rn 92, juris). So enthält die Kategorie „Erfahre mehr über Aktivitäten außerhalb von Meta-Technologien“ in den von der Beklagten bereitgestellten Informationen (Anlage B 7, S. 45 ff.) nur allgemeine Informationen über den Erhalt sowie die Verwendung von Offsite-Daten. Ansehen kann sich der Nutzer danach nur die „neuesten Aktivitäten“ (Anlage B 7, S. 18). Dabei sind auch diese nicht vollständig; so heißt es in Abb. 54 (Anlage B 7, S. 47): „Hier siehst du eine Übersicht deiner Aktivitäten, zu denen Unternehmen und Organisationen Informationen an uns übermittelt haben“ und weiter „Möglicherweise werden hier nicht alle deine Aktivitäten angezeigt“. Auch in ihrem Auskunftsschreiben führt die Beklagte aus (Anlage B 8, S. 5): „Einige Informationen, die du gelöscht hast, werden eventuell aus Sicherheitsgründen vorübergehend gespeichert. Sie erscheinen aber nicht, wenn du auf deine Informationen zugreifst oder sie herunterlädst“. Die Parteien tragen außerdem übereinstimmend vor, es seien (nur) „Zusammenfassungen“ über das Tool abrufbar (vgl. für die Beklagte S. 406 ff., 442 dA LG). Soweit der Kläger schließlich behauptet, dass das Tool nur über Aktivitäten informiere, die stattgefunden haben, als Nutzer auf demselben Gerät in einem Netzwerk der Beklagten eingeloggt war, hat die Beklagte dies auf Nachfrage des Senats im Termin nicht bestritten.

Angesichts dieser Umstände hätte es der Beklagten oblegen, darzulegen und zu beweisen, dass über das Auskunfts-Tool (doch) sämtliche vom Auskunftsanspruch des Klägers umfassten Daten unschwer abgerufen und heruntergeladen werden können. Das hat sie nicht getan.

(2) Zu der vom Kläger gemäß Art. 15 Abs.1 lit. c DSGVO verlangten Auskunft über die Empfänger oder Kategorien von Empfängern von Daten hat die Beklagte in einer Anlage zu ihrem Schreiben vom 25.04.2025 (Anlage B 8, S. 12) zwei „individuelle Empfänger“ benannt.

Damit ist der Anspruch nicht erfüllt, weil die Auskunft mehrere Einschränkungen enthält: Sie steht unter dem Vorbehalt „zur Verfügung stehender Informationen“. Zudem soll die Auskunft Daten „als Nutzer von Instagram“ betreffen, was offen lässt, ob auch über Meta Business Tools erlangte Daten eingeschlossen sind. Schließlich ist von „individuellen Empfängern“ die Rede, sodass unklar bleibt, ob es - unbenannte - „kollektive Empfänger“ gibt.

(3) Zur Frage der Auslandsspeicherung hat die Beklagte keine Angaben gemacht.

(4) Der Anspruch des Klägers nach Art. 15 Abs.1 lit. h DSGVO auf Auskunft darüber, inwieweit seine Daten für eine automatisierte Entscheidungsfindung einschließlich Profiling im

Sinne von Art. 22 DSGVO verwendet wurden, ist nicht durch eine Negativauskunft im Schreiben der Beklagten vom 25.04.2025 (Anlage B 8, S. 11) erfüllt. Die Beklagte hat dort nur mitgeteilt, sie habe keine Verarbeitung i.S.d. Art. 22 DSGVO „festgestellt“; das schließt nicht aus, dass es eine solche Verarbeitung gab, sie aber nicht mehr „feststellbar“ ist (OLG Jena a.a.O. Rn. 157). Zudem betrifft die Feststellung nur die Vergangenheit; Art. 15 Abs. 1 lit. h DSGVO und das Auskunftsbegehren des Klägers beschränken sich indes nicht darauf (vgl. OLG Jena a.a.O). Dazu im Termin befragt, hat der Beklagtenvertreter mitgeteilt, dass er über die in dem Auskunftsschreiben gegebenen Auskünfte hinaus keine Auskunft erteilen könne.

2. Der Antrag zu Ziffer 3, mit dem der Kläger von der Beklagten verlangt, es zu unterlassen, mit Hilfe der Meta Business Tools die im Antrag zu 1 aufgeführten personenbezogenen Daten des Klägers zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden, ist begründet.

a) Maßgeblich ist die vom Kläger im Termin gestellte Antragsfassung. In der Benennung einzelner personenbezogener Daten liegt eine Antragsbeschränkung im Sinne des § 264 Nr. 2 ZPO. Im Übrigen ist die Einwilligung der Beklagten in die darin liegende Änderung der Klage anzunehmen, weil sie sich in der mündlichen Verhandlung auf den geänderten Antrag eingelassen hat (§§ 263, 267 ZPO). Jedenfalls ist die Klageänderung sachdienlich.

b) Der Unterlassungsantrag ist zulässig, insbesondere ist er hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Der Antrag lässt sich unter Heranziehung des Klagevorbringens sinngemäß dahingehend auslegen, dass der Kläger sich dagegen wendet, dass seine personenbezogenen Daten über die auf Drittwebseiten bzw. -Apps implementierten Meta Business Tools an die Beklagte gelangen und dort von ihr für eigene Zwecke genutzt werden. Er begehrt eine Unterlassung jeglicher Verarbeitung seiner durch Business Tools erhobenen Daten durch die Beklagte. Insoweit gibt es keine Auslegungsschwierigkeiten im Vollstreckungsverfahren, da der Kläger die Verarbeitung aller Daten, die über Meta Business Tools an die Beklagte gelangen, in Gänze unterlassen wissen will. Für die Zulässigkeit des Unterlassungsantrags ist es ausreichend, dass er greifbare Anhaltspunkte dafür aufzeigt, dass er von der streitigen Datenverarbeitung erfasst wurde und wird. Das ist vorliegend – wie die nachstehenden Ausführungen zur Begründetheit zeigen – der Fall.

Für den Antrag besteht auch ein Rechtsschutzbedürfnis. Zwar kann der Kläger sein Konto bei

der Beklagten ohne weiteres selbst löschen, indem er die Löschung seines Kontos initiiert. Allerdings ist das Rechtsschutzziel – die Untersagung einer unrechtmäßigen Verarbeitung ihrer Daten – mit dem dann erreichten Ergebnis nicht identisch. Dieses Rechtsschutzziel ist auch besonders schützenswert, weil die DSGVO allen europäischen Bürgern ein einheitliches und hohes Datenschutzniveau bezüglich aller auf dem europäischen Markt zugelassener Anwendungen – und somit auch Social-Media-Plattformen – gewährleisten soll. Würde man dem Kläger auf das Löschen ihres Nutzerprofils verweisen, so würde zugleich diese Regelungsabsicht ad absurdum geführt (vgl. OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 144, juris). Dem Rechtsschutzbedürfnis des Klägers steht auch nicht entgegen, dass die Beklagte ihm die Möglichkeit bietet, über die Schaltfläche „Deine Aktivitäten außerhalb der Meta-Technologien“ auf der Plattform selbst die Verarbeitung einzuschränken. Zwar führt die Einstellung „Bestimmte Aktivitäten trennen“ dazu, dass Aktivitäten von Apps und Websites, die der Nutzer auswählen muss, nicht mehr in seinen Konten gespeichert werden. Die Einstellung „Frühere Aktivitäten löschen“ führt dazu, dass die von Drittunternehmen geteilten Informationen über Aktivitäten vom Konto des Nutzers getrennt werden und die Einstellung „Verknüpfung mit künftigen Aktivitäten aufheben“ führt dazu, dass Informationen, die Unternehmen und Organisationen zu Interaktionen mit dem Nutzer an die Beklagte übermitteln, zukünftig nicht mehr verknüpft werden. Den Transfer personenbezogener Daten des Klägers von Drittunternehmen an die Beklagte mittels Meta Business Tools unterbindet dies aber nicht.

c) Der Antrag ist begründet, der Kläger hat einen Anspruch auf die Unterlassung.

Zwar ergibt sich der Unterlassungsanspruch nicht unmittelbar aus der DSGVO. Den Mitgliedsstaaten der Europäischen Union bleibt es aber durch die harmonisierten Regelungen der DSGVO unbenommen, in ihren jeweiligen Rechtsordnungen einen entsprechenden Anspruch auf Unterlassung von Datenschutzverstößen vorzusehen (EuGH, Urteil vom 04.09.2025, C-655/23, Rn. 52, juris), sodass ein Rückgriff auf nationale Vorschriften möglich ist.

Der Unterlassungsanspruch folgt nach deutschem Recht aus § 823 Abs. 2 BGB i.V.m. Art. 5 Abs. 1 lit. a und lit. c, Art. 6 Abs. 1 DSGVO (dazu aa)) sowie aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 2 GG (dazu bb)), jeweils i.V.m. § 1004 Abs. 1 S. 2 BGB (analog).

aa) Artikel 5 Abs. 1 lit. a und lit. c, Art. 6 Abs. 1 DSGVO sind Schutzgesetze i. S. v. § 823 Abs. 2 BGB (OLG Dresden, Urteil vom 12.03.2026, 17 U 625/25, n.v., S. 35 ff.). Die Voraussetzungen eines auf die Verletzung dieser Vorschriften gestützten Unterlassungsanspruchs liegen hier vor. Der Kläger ist von der Datenerhebung und -verarbeitung mittels Busi-

ness Tools, die die Beklagte verantwortet, mit seinen personenbezogenen Daten betroffen (dazu (1)). Diese Datenverarbeitung ist rechtswidrig (dazu (2)). Die Beklagte ist als Störerin passivlegitimiert (dazu (3)). Die Gefahr weiterer Beeinträchtigungen i.S.d. § 1004 Abs. 1 S. 2 BGB ist gegeben (dazu (4)). Einer Berücksichtigung etwaiger künftiger Rechtfertigungsgründe bedarf es nicht (dazu (5)).

(1) Der Kläger ist von der Datenerhebung und -verarbeitung mittels Meta Business Tools betroffen; die Beklagte verarbeitet als Verantwortliche die personenbezogenen Daten des Klägers, die sie mittels dieser Tools erhalten hat.

Bei dem vom Kläger in seinem Auskunftsantrag aufgeführten Daten, auf die er mit seinem Unterlassungsantrag Bezug nimmt, handelt es sich um „personenbezogene Daten“ im Sinne der Legaldefinition in Art. 4 Nr. 1 DSGVO (vgl. oben 1.c)aa)(2)).

In tatsächlicher Hinsicht ist auch unstreitig, dass die in Webseiten und Apps von Drittunternehmen eingebundenen Business Tools der Beklagten Daten der Website-Besucher und App-Nutzer i.S.v. Art. 4 Nr. 2 DSGVO verarbeiten.

(a) Der Kläger ist nach seinem Vortrag von dieser Verarbeitung personenbezogener Daten durch die Business Tools der Beklagten betroffen. Insoweit genügt das pauschale Bestreiten der Beklagten nicht, denn sie könnte und müsste sich zum Klagevortrag gemäß § 138 Abs. 2 ZPO substantiiert einlassen.

Nach der Rechtsprechung des Bundesgerichtshofs kann eine sekundäre Darlegungslast den Prozessgegner der primär darlegungsbelasteten Partei treffen, wenn diese keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Gegner alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. Genügt der Anspruchsgegner seiner sekundären Darlegungslast nicht, gilt die Behauptung des Anspruchstellers nach § 138 Abs. 3 ZPO als zugestanden (BGH, Urteil vom 17.11.2022, VII ZR 623/21, Rn. 20, juris, m.w.N.).

Nach diesem Maßstab besteht hier eine sekundäre Darlegungslast der Beklagten, weil der Kläger in einem für seinen Vortrag zentralen Punkt, nämlich der Frage, auf welchen (Dritt-)Webseiten und Apps Meta Business Tools zur Anwendung kommen und welche Daten des Klägers in der Folge von der Beklagten erhoben (bzw. von Dritten erhoben und an die Beklagte übermittelt) werden, außerhalb des darzulegenden Geschehensablaufs des Klägers

steht, während die Beklagte alle relevanten Tatsachen kennt:

(aa) Der Vortrag des Klägers enthält hinreichend greifbare Anhaltspunkte dafür, dass ihn betreffende personenbezogene Daten über Business Tools an die Beklagte gelangt sind und von ihr verarbeitet wurden und werden.

Unstreitig verfügt der Kläger über einen Account bei dem von der Beklagten betriebenen sozialen Netzwerk „Instagram“. Er hat beim Landgericht vorgetragen, dass er mehrere Stunden in der Woche über einen Browser im Internet surft, mindestens eine Stunde täglich in Apps verbringt und dabei zu finanziellen, gesundheitlichen und politischen Themen recherchiert (S. 274, 447 ff. dA LG). Nach den Erkenntnissen seiner Prozessbevollmächtigten seien in solchen Seiten Meta Business Tools integriert. Erst seit der Aufklärung durch seinen Prozessbevollmächtigten habe er das Bewusstsein dafür, dass Informationen über seine Aktionen außerhalb des Netzwerks der Beklagten, nämlich sein Verhalten auf Drittwebseiten und -Apps von der Beklagten aufgezeichnet würden. Seither sei er (noch) vorsichtiger geworden, was die Nutzung des Internets angehe. Cookie-Banner lehne er, soweit möglich, ab. Im Termin beim Senat hat der Kläger diesen Vortrag bestätigt.

Der Kläger hat damit summarische Angaben zu Art und Intensität seiner Internet-Nutzung gemacht. Dabei ist es ihm grundsätzlich nicht zumutbar, detailliert zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten Webseiten vorzutragen. Zum einen lässt sich für den Privatnutzer kaum mit vertretbarem Aufwand rekonstruieren, welche Homepages er zu welchem Zeitpunkt in der Vergangenheit besucht hat; eine Verpflichtung zum Vorhalten entsprechender Verlaufsprotokolle besteht nicht. Zum anderen wäre es dem Kläger selbst dann, wenn er über ein solches Verlaufsprotokoll verfügen sollte, nicht zumutbar, sein gesamtes Internetnutzungsverhalten über Jahre im Rahmen eines Zivilrechtsstreits offen zu legen. Dies stünde offensichtlich in einem Widerspruch zum Normzweck der DSGVO (vgl. OLG Dresden a.a.O. Rn. 142).

Zudem hat der Kläger hinreichend detailliert zu einzelnen Business Tools der Beklagten und deren Funktionsweise vorgetragen. Der Dienst „Meta Pixel“ beispielsweise werde in Form eines Programmcodes im Hintergrund des Browsers (regelmäßig vom Nutzer unbemerkt) ausgeführt, führe Identifizierungstechniken sowie die Protokollierung der Events durch und sende Daten an die Beklagte. Besuche ein Nutzer eine Dritt-Webseite, in die „Meta-Pixel“ eingebunden sei, so werde dieser vom Server der Beklagten geladen, setze im Browser des Nutzers Third Party Cookies und First Party Cookies, erhebe Daten des Nutzers, die er an die Beklag-

te übermittle. Die User-ID werde aus dem Third Party Cookie ausgelesen und diese zusammen mit weiteren für das Digital Fingerprinting nutzbaren, als User Agent bezeichneten Daten sowie der IP-Adresse direkt an die Beklagte übermittelt. „Facebook SDK“ funktioniere ähnlich, werde aber nicht in Webseiten, sondern in mobile Apps eingebunden. „Conversions API“ erfülle die gleiche Funktion auf Drittwebseiten wie der „Meta Pixel“, werde aber nicht im Browser des Nutzers geladen, sondern sende die Daten, welche der Server des Webseitenbetreibers vom Nutzer empfängt, direkt an die Beklagte, sodass sogenannte Cookie-Blocker auf dem Gerät des Nutzers umgangen würden. „App Events API“ sei für mobile Apps das Äquivalent zur „Conversions API“ bei Webseiten. Die beschriebene Funktionsweise der Tools bestreitet die Beklagte nicht.

Der Kläger hat in den Anlagen K 4 und K 5 eine dreistellige Anzahl bekannter und vielgenutzter Internetseiten aufgelistet, auf denen er beispielsweise den Dienst „Meta Pixel“ habe nachweisen können; insgesamt seien die Business Tools der Beklagten auf etwa 30 bis 40 Prozent aller Webseiten weltweit und einer großen Zahl beliebter Apps aktiv. Dem ist die Beklagte lediglich insoweit entgegengetreten, dass sie bei sieben der aufgelisteten Webseiten „zum Zeitpunkt der Überprüfung“ (im Jahr 2025) keine Verwendung von Business Tools habe feststellen können. Der Kläger kann aber – anders als die Beklagte – nicht wissen, auf welchen Webseiten und Apps wann welche Business Tools zum Einsatz gekommen sind. Dass die von der Beklagten angebotenen Tools weit verbreitet sind und auf einer erheblichen Anzahl namhafter und reichweitenstarker Webseiten in Deutschland zum Einsatz kommen, ist unstreitig. Für einen regelmäßigen Nutzer des Internets, der online einkauft, Reisen bucht und sich über Nachrichten, Wetter, Politik oder/und Gesundheitsfragen informiert, erscheint es praktisch nicht möglich, nur Webseiten aufzusuchen, die Business Tools nicht verwenden.

Auch unterstellt, dass es Drittunternehmen technisch möglich ist, ihre Websites und Apps so auszugestalten, dass eine Datenerhebung und Informationsübermittlung an die Beklagte über das eingebettete Business Tool nur bei Einverständnis des Endnutzers mit der Verarbeitung seiner personenbezogenen Daten erfolgt, folgt daraus nicht mit einer dem Vorliegen greifbarer Anhaltspunkte entgegenstehenden Gewissheit, dass tatsächlich keine Erfassung und Übertragung der personenbezogenen Daten des Klägers erfolgt wäre. Dies würde voraussetzen, dass jedes Drittunternehmen eine solche Einwilligungslogik implementiert und der Kläger auf sämtlichen Websites und Apps mit integriertem Business Tool seit dem 12.10.2018 ausnahmslos sein Einverständnis mit der Verarbeitung seiner personenbezogenen Daten verweigert hätte. Weder das eine noch das andere ist feststellbar. Vielmehr hat der Beklagtenvertreter im Termin beim Senat bestätigt, dass eine nicht ordnungsgemäße Installation von Busi-

ness Tools „dazu führen kann, dass Kontaktinformationen oder Eventdaten der Nutzer auch ohne Einwilligung des Nutzers an die Beklagten übertragen werden“.

Der Kläger hat außerdem anhand eines Einzelbeispiels (spiegel.de) aufgezeigt, dass der Dienst „Meta Pixel“ bisweilen sofort geladen wird, noch bevor der Webseitenbesucher eine Auswahl (Zustimmung oder Ablehnung) im dortigen Cookie-Banner getroffen hat. Insofern sind greifbare Anhaltspunkte dafür dargelegt worden, dass auf Drittwebseiten eingebundene Meta Business Tools (jedenfalls in Einzelfällen) nicht regelkonform implementiert sind und auch ohne Zustimmung Daten der Webseitenbesucher oder App-Nutzer an die Beklagte übermitteln.

Insofern ist im Ergebnis schlüssig und plausibel dargelegt, dass den Kläger betreffende Daten mittels Meta Business Tools an die Beklagte gelangt sind.

(bb) Der Beklagten ist substantiierter Gegenvortrag möglich und zumutbar, weil die behaupteten Tatsachen in ihrem Wahrnehmungsbereich gelegen haben. Entscheidend ist, dass die Beklagte anhand ihres eigenen Systems und der Abfrage der Nutzerkonten ohne weiteres überprüfen und darlegen kann, ob und gegebenenfalls welche Daten ihr von welchen Drittseiten oder -Apps übermittelt wurden. Der Kläger kann hingegen nicht wissen, welche Internetseiten und Apps wann mit welchen Business Tools der Beklagten ausgestattet waren und welche Daten übertragen wurden.

Datenschutzsachverhalte sind regelmäßig durch eine solche strukturelle Informationsasymmetrie geprägt. Die betroffene Person hat weder Einblick in die technischen Abläufe der Datenverarbeitung noch Zugriff auf interne Systeme, Server-Logs oder Datenverknüpfungen. Der maßgebliche Geschehensablauf liegt typischerweise vollständig in der Sphäre der verantwortlichen Stelle, hier also der Beklagten. Diese Wertung findet ihre gesetzliche Stütze in Art. 5 Abs. 2 DSGVO, wonach der verarbeitenden Stelle eine Rechenschaftspflicht obliegt und damit korrespondierend dem Betroffenen ein Auskunftsrecht zusteht, Art. 15 DSGVO. Das Auskunftsrecht verdeutlicht zudem, dass der Unionsgesetzgeber die Kenntnis der konkreten Verarbeitungsvorgänge grundsätzlich der verantwortlichen Stelle zuweist und davon ausgeht, dass die betroffene Person ohne Mitwirkung des Verantwortlichen nicht in der Lage ist, Art, Umfang und Zweck der Datenverarbeitung zu überblicken. Das Auskunftsrecht dient der Herstellung von Transparenz und Kontrolle der natürlichen Person, deren Daten verarbeitet werden, nicht jedoch dazu, der betroffenen Person im Zivilprozess die primäre Darlegungslast für außerhalb ihres Wahrnehmungsbereichs liegende Vorgänge aufzuerlegen.

Überdies hat der Kläger von seinem Auskunftsrecht Gebrauch gemacht. Eine vollständige, nachvollziehbare und systematische Darstellung der von ihr erhobenen, übermittelten, gespeicherten, verwendeten und den Kläger betreffenden Daten, hat die Beklagte dem Kläger nicht erteilt und auch nicht dargelegt, dass das von ihr zur Verfügung gestellte Selbsthilfe-Tool eine vollständige Darstellung auch bezogen auf die über Business Tools erlangten Daten des Klägers enthält (vgl. 1.). Die Beklagte hat ebenso wenig vorgetragen, auf welchen Webseiten und Apps ihre Business Tools zum Einsatz kommen. Eine substantiierte Offenlegung der tatsächlich verarbeiteten Daten erfolgte damit nicht. Die nähere Aufklärung des in der Sphäre der Beklagten liegenden Geschehens durch substantiiertes Bestreiten obliegt der Beklagten. Damit genügt der klägerische Vortrag für die Annahme der behaupteten Datenverarbeitung, während das pauschale und nicht substantiierte Bestreiten der Beklagten ungenügend ist. Dies hat zur Folge, dass der Vortrag des Klägers gemäß § 138 Abs. 3 ZPO als zugestanden gilt.

(cc) Darüber hinaus ergeben sich auch aus dem eigenen Vortrag der Beklagten und den von ihr selbst vorlegten Anlagen greifbare Anhaltspunkte dafür, dass sie personenbezogene Daten des Klägers verarbeitet, welche mittels Business Tools an sie gelangen.

Unter Zugrundelegung des Beklagtenvortrags werden bei Besuch von Webseiten oder Apps, die Meta Business Tools verwenden, (nur) dann keine Daten an die Beklagte übermittelt, wenn und soweit die Business-Tools-Verwender ihre Cookie-Einstellungen bzw. -Banner entsprechend den Nutzungsbedingungen der Beklagten und auch im übrigen datenschutzkonform konfiguriert haben und der Nutzer diese abgelehnt hat. Die Beklagte hat allerdings selbst eingeräumt, dass sie das Vorliegen dieser Voraussetzungen nicht überprüft oder anderweitig verlässlich sicherstellt. Sie verweist lediglich darauf, dass sie die Kunden, welche Business Tools einbinden, auf die Einhaltung der Vorgaben ihrer Nutzungsbedingungen und der Gesetze hinweise bzw. verpflichte und Hilfestellungen zur korrekten Implementierung ihrer Tools gebe. Effektive Absicherungsmechanismen in Gestalt von systematischen Kontrollen und daraus resultierenden Sanktionen fehlen aber. Die Beklagte übernimmt insoweit auch keine Verantwortlichkeit für das Verhalten der Drittwebseitenanbieter. Unstreitig ist zwischen den Parteien insoweit, dass dann, wenn es auf Drittwebseiten oder -Apps zu einer nicht ordnungsgemäß funktionierenden Installation von Business Tools kommt, dies dazu führen kann, dass Kontaktinformationen oder Eventdaten der Nutzer auch ohne Einwilligung des Nutzers an die Beklagte übertragen werden. Zur Überzeugung des Senats folgt aus dieser technischen Möglichkeit in Anbetracht des von dem Kläger geschilderten konkreten Internetnutzungsverhaltens, der sehr großen Zahl von Webseiten, die Meta Business Tools nutzen, und dem vom Kläger dargelegten Beispiel (spiegel.de; vgl. (aa)) nicht nur, dass auch ohne vorherige Zustimmung

der Webseitenbesucher oder App-Nutzer Daten an die Beklagte übermitteln werden, sondern dass hiervon auch der Kläger betroffen ist.

Die Beklagte hat überdies konzediert, an sie gelangte personenbezogene Daten (zumindest) für einen Abgleich in ihren Systemen zu nutzen, um festzustellen, ob es sich um Daten eines bei ihr registrierten Nutzer handelt. Bereits der Abgleich zur Prüfung, ob es sich um einen bei ihr registrierten Nutzer handelt, stellt eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Der Abgleich betrifft zudem Kontaktinformationen und Event-Daten (vgl. Anlage K 14, Parameter für Kund*innen-Informationen). Nach den Angaben der Beklagten ist davon auszugehen, dass sie diese Daten auf ihrer Plattform jedenfalls vorübergehend speichert und mit den sogenannten Onsite-Daten des Klägers zusammenführt, bevor diese in einem weiteren Schritt durch Zuweisung von Ad-IDs, Hash-Werten und Cookie-IDs pseudonymisiert werden.

Auch die in den Nutzungsvertrag mit dem Kläger einbezogenen Plattform-Nutzungsbedingungen (Anlage B 5) und Erläuterungen zu der Einstellung „Deine Aktivitäten außerhalb von Meta-Technologien“ Einstellung („Offsite Aktivitäten“ bzw. „Third-Party Activity Data“) bestätigen eine fortlaufende Verarbeitung der über Business Tools erhaltenen Daten. Selbst bei einem Nutzer, der – wie der Kläger – über die Plattform-Einstellungen die Übermittlung von Daten zum Zwecke personalisierter Werbung nicht erlaubt, folgt nach dem Beklagtenvorbringen hieraus nicht, dass die Beklagte über ihre Business Tools keine personenbezogenen Daten dieses Nutzers mehr erhält. Denn sie bestätigt, dass sie die Informationen in eingeschränktem Umfang für „Sicherheit und Integrität“ oder auch für andere Zwecke und nicht für die Anzeige von für den Nutzer relevanter Werbung verwendet. So lassen die Nutzungsbedingungen etwa auch eine Verarbeitung zu „weiteren eigenen Zwecken wie Messungen und Verbesserung unserer Werbesysteme“ zu. In ihrer an die Nutzer gerichteten Datenschutzrichtlinie (Anlage K 3, S. 62) teilt die Beklagte außerdem mit, die Datenverarbeitung auf verschiedene Rechtsgrundlagen zu stützen, so etwa auf „berechtigte Interessen“, wozu u.a. die Bereitstellung eines innovativen, personalisierten, sicheren und profitablen Dienstes für unsere Nutzer und Partner und die Reaktion auf rechtliche Anfragen zählen sollen. Auch zur Messung der Effizienz von Werbekampagnen können die Daten verarbeitet werden (Anlage K 6, S. 23: „Die Conversions API ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben“). Dass für diesen Nutzer lediglich keine Datenverarbeitung zum Zwecke der Bereitstellung personalisierter Werbung erfolgt, genügt zur Verneinung einer Datenverarbeitung (insgesamt) nicht.

Darüber hinaus kann die Beklagte nach ihrem Vorbringen aber auch weiterhin „aggregierte“ In-

formationen zu Aktivitäten in diesen Apps und auf diesen Websites erhalten. Zudem wird in den Plattform-Nutzungsbedingungen ausdrücklich darauf hingewiesen, dass die Beklagte im Fall einer Kontentrennung, und zwar bezogen auf zukünftige und vergangene Aktivitäten, auch weiterhin Informationen zu den Aktivitäten von Apps und Websites erhalte, die sie für Messungen sowie zur Verbesserung ihrer Werbesysteme verwenden könne (vgl. Anlage B 2, S. 23, Infobox: „Das solltest du wissen“).

(dd) Schließlich ist auch das „Hashen“ (Verschlüsseln) der von Drittanbietern an die Beklagte übermittelten Daten nicht geeignet, ihre Behauptung zu stützen, sie verarbeite bei fehlender Einwilligung der Nutzer keine personenbezogenen Daten, die ihr mittels Business Tools übermittelt werden. Da die Beklagte ihren Geschäftspartnern die hierfür zu verwendende Technologie verbindlich vorschreibt und diese auch selbst verwendet, begründet dies in den meisten Fällen die Möglichkeit einer Zuordnung. Dass sie die erfolgte Verschlüsselung rückgängig machen kann, wird durch die Nutzungsbedingungen für die Business Tools sowie den detaillierten Regelungen in den „Parametern für Kund*innen-Informationen“ (Anlage K 14) belegt (vgl. OLG Dresden a.a.O. Rn. 164).

(b) Die Beklagte ist Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die Daten, welche sie mittels Business Tools von Drittwebseiten und -Apps erlangt und weiterarbeitet (vgl. 1.b)aa)(1)).

(2) Die Datenverarbeitung seitens der Beklagten von mittels Business Tools erlangten personenbezogenen Daten des Klägers ist nicht nach Art. 6 DSGVO gerechtfertigt und daher rechtswidrig. Die Beklagte trägt als Verantwortliche gemäß Art. 5 Abs. 2 und Art. 7 Abs. 1 DSGVO die Darlegungs- und Beweislast dafür, dass die Daten für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Außerdem obliegt es ihr nach Art. 13 Abs. 1 UAbs. 1 lit. c DSGVO dem Verantwortlichen, wenn personenbezogene Daten bei der betroffenen Person erhoben werden, diese Person über die Zwecke, für die diese Daten verarbeitet werden sollen, sowie über die Rechtsgrundlage für die Verarbeitung zu informieren (EuGH, Urteil vom 04.07.2023, C-252/21, Rn. 95, juris). Der ihr insoweit obliegenden Darlegungslast ist die Beklagte nicht nachgekommen. Auch für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO liegen keine rechtfertigenden Gründe vor. Die Datenverarbeitung verstößt darüber hinaus auch gegen den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

(a) Anders als die Beklagte meint, muss nicht der Kläger bestimmte Verarbeitungszwecke in Frage stellen, sondern die Beklagte hat zu erklären, zu welchem Zweck sie welche Daten erhoben hat und weshalb die Verarbeitung der Daten rechtmäßig sein soll. Die Beklagte hat zur Rechtfertigung bestimmter konkreter Datenverarbeitungsvorgänge allerdings nichts Konkretes vorgetragen. Eine Rechtfertigung nach Art. 6 DSGVO setzt voraus, dass die verarbeiteten Daten im ersten Schritt benannt werden und dass in einem zweiten Schritt jeder einzelne Datenverarbeitungsvorgang gerechtfertigt wird. Die Beklagte trägt schon nicht vor, welche Daten des Klägers sie überhaupt verarbeitet hat, sodass eine Subsumtion unter Art. 6 DSGVO oder Art. 9 DSGVO von vornherein ausscheidet. Die Beklagte wird damit ihrer Darlegungslast nicht gerecht; die als unstreitig zu behandelnde Verarbeitung von Daten des Klägers erfolgt schon deswegen rechtswidrig. Die von der Beklagten ins Feld geführten Erlaubnistatbestände können nicht überprüft werden, solange die Beklagte nicht offenlegt, welche Daten des Klägers sie verarbeitet (hat). Insofern bleiben Überlegungen zu einer möglichen Rechtfertigung spekulativ.

(b) Unabhängig davon greifen die von der Beklagten benannten Erlaubnistatbestände auch aus anderen Gründen nicht.

(aa) Es liegt keine rechtfertigende Einwilligung des Klägers gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO vor. Dafür müsste die Beklagte nachweisen, dass ihre Verarbeitung personenbezogener Daten des Klägers, die sie mittels Meta Business Tools erlangt hat, von einer auf konkrete Zwecke bezogenen, freiwilligen Einwilligung des Klägers gedeckt ist, die den Anforderungen des Art 7 DSGVO erfüllt. Das ist nicht der Fall.

(aaa) Die Beklagte stützt sich auf eine Einwilligung ihrer Nutzer nur, um eine Personalisierung von Werbung zu rechtfertigen. Eine derartige Einwilligung erholt sie mittels der Einstellung „Information von Werbepartnern zu deinen Aktivitäten“. Hier trägt die Beklagte aber selbst vor, dass der Kläger diese Einwilligung nicht erteilt hat (S. 84 dA LG).

(bbb) Das in den Einstellungen der Beklagten unter „Meta Cookies in anderen Apps und auf anderen Websites“ erteilte Einverständnis des Klägers mit „optionalen Cookies“ kann die Datenverarbeitung – ungeachtet dessen, dass sich die Beklagte zu deren Legitimierung ausdrücklich nicht hierauf stützt (S. 103 dA LG) – ebenfalls nicht rechtfertigen. Die Einwilligungserklärung ist jedenfalls unwirksam, weil für den Nutzer weder erkennbar ist, welche konkreten Daten welchen Arten der Datenverarbeitung unterworfen werden sollen, noch um welche Cookies der Beklagten es überhaupt gehen soll und wie diese jeweils funktionieren.

(ccc) Die Beklagte kann sich auch nicht auf eine etwaig erteilte Einwilligung des Klägers auf Drittwebseiten und -Apps berufen, da sich diese nur auf Datenverarbeitungszwecke des Webseiten- bzw. App-Betreibers bezieht, nicht aber auf diejenigen des Anbieters der Meta-Business-Tool-Technologien (vgl. EuGH, Urteil vom 29.07.2019, C-40/17, Rn. 102, juris). Es obliegt nicht den Drittunternehmen, eine Einwilligung des Nutzers für eine Verarbeitung von Daten für Zwecke der Beklagten einzuholen.

Davon abgesehen hat die Beklagte zu keiner einzigen Einwilligung des Klägers auf einer Drittwebseite vorgetragen, sodass der Senat auch nicht prüfen kann, ob eine solche etwa erteilte Einwilligung wirksam ist. Das ist von Relevanz, weil eine Einwilligung freiwillig erfolgt sein müsste, für den bestimmten Fall, in informierter Weise für definierte Zwecke und unmissverständlich durch Erklärung oder eine sonstige bestätigende Handlung. Selbst wenn der Verwender von Meta Business Tools nach den einschlägigen Nutzungsbedingungen für das Einholen der Einwilligung verantwortlich sein soll, darf die Beklagte die personenbezogenen Daten nur verarbeiten, wenn eine wirksame Einwilligung der betroffenen Person vorliegt, was sie zu überprüfen hat. Die Beklagte trägt nicht vor, das Vorliegen wirksamer Einwilligungen jeweils zu überprüfen. Unabhängig davon könnte eine unterstellt wirksam erteilte Einwilligung auf einer Drittseite nur die Erhebung und Weiterleitung von Daten an die Beklagte rechtfertigen, nicht aber die Speicherung und spätere Verwendung für eigene Zwecke seitens der Beklagten.

(bb) Es ist auch nicht ersichtlich, dass die Verarbeitung von mittels Business Tools erhaltenen personenbezogenen Daten bei der Beklagten erforderlich zur Erfüllung ihrer der Verträge mit ihren Nutzern wäre und insofern gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gerechtfertigt sein könnte.

Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH, Urteil vom 04.07.2023, C-252/21, Rn. 98, juris). Entscheidend ist dabei, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen. Zudem ist bei einem Vertrag, der mehrere Dienstleistungen oder mehrere ei-

genständige Elemente einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit des Rechtfertigungstatbestandes für jede dieser Dienstleistungen gesondert zu beurteilen (vgl. EuGH a.a.O. Rn. 100). Dass die Verwendung der Business Tools und die Verarbeitung der durch sie gewonnenen personenbezogenen Daten zur Nutzung der sozialen Plattform unerlässlich wäre, lässt sich anhand des Vortrags der Beklagten nicht feststellen. Es ist bereits zweifelhaft, ob die von der Beklagten angeführte Personalisierung von Funktionen, Inhalten und Vorschlägen zu Personen, Gruppen und Veranstaltungen auf ihrer Social-Media-Plattform notwendiger Bestandteil der Vertragsleistung der Beklagten ist. Eigentlicher Zweck des sozialen Netzwerks ist es nach dem Vortrag der Beklagten, den Nutzern die Möglichkeit zu geben, Verbindungen herzustellen, zu kommunizieren und Inhalte mit anderen Nutzern unabhängig von ihrem physischen Standort auf der ganzen Welt auszutauschen. Die Verarbeitung personenbezogener Daten ist stattdessen erforderlich für Erfüllung der Verträge gegenüber den (gewerblichen) Kunden der Beklagten, die ihre Business Tools zur Unterstützung ihrer Produktplatzierung oder der Messung der Effektivität ihrer Werbeanzeigen, nutzen. Dieser Vertrag ist aber von dem Nutzungsvertrag mit den (privaten) Accountinhabern des Netzwerks zu unterscheiden. Jedenfalls aber ist die streitgegenständliche Verarbeitung von mittels Business Tools gewonnenen Daten zur Erreichung dieses damit verfolgten Zweckes nicht objektiv unerlässlich, denn eine hinreichende Personalisierung ließe sich schon durch Onsite-Daten erreichen. Dass der Betrieb und die Nutzung der streitgegenständlichen Plattform auch ohne Einbindung der Business Tools möglich ist, wird nicht zuletzt durch die Einführung des werbefreien Bezahlmodells deutlich.

Die vage Angabe der Beklagten, die Verarbeitung von Business-Tool-Daten sei aus Sicherheits- und Integritätszwecken für die Vertragserfüllung geboten, genügt nicht, denn auch insofern fehlt es an nachvollziehbarem, hinreichend konkretem Sachvortrag der Beklagten. Der Hauptgegenstand des Vertrags liegt hier in der Nutzung der Social-Media-Plattform der Beklagten. Warum dies ohne zusätzliche und außerhalb des eigentlichen Vertragszwecks liegende, umfassende Verarbeitung von Offsite-Daten ihrer Geschäftspartner nicht erfüllt werden könnte, diese also objektiv unerlässlich für den mit dem Kläger bestehenden Nutzungsvertrag sein sollten, erklärt die Beklagte nicht. Es fehlt die Darlegung zu konkreten, den Kläger betreffenden Datenverarbeitungsvorgängen und deren jeweiliger Notwendigkeit zur Erreichung eines bestimmten Zwecks. Soweit die Beklagte vortragen lässt, aufgrund der Komplexität der Prozesse und der vielfältigen Faktoren, die bei der Untersuchung potenziell schwerwiegender oder böswilliger Aktivitäten eine Rolle spielen, seien Aufbewahrungsfristen für Daten, die in Sicherheits- und Integritätsuntersuchungen angewendet würden, schwer präzise zu definieren, im Allgemeinen betrage die Speicherdauer aber bis zu 90 Tage, wäre eine solche Vorgehens-

weise nicht pauschal unerlässlich, um den Nutzungsvertrag mit dem Kläger zu erfüllen.

(cc) Eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. c, d oder e DSGVO scheidet aus. Die Beklagte macht nicht geltend, dass die Verarbeitung der streitgegenständlichen, über ihre Business Tools erlangten Offsite-Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder gar zum Schutz lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich sei. Soweit die Beklagte insoweit die Aufklärung oder Verhinderung von Straftaten anführt und sich damit wohl (auch) auf öffentliche Interessen berufen möchte, ist nicht ersichtlich, dass ihr eine derartige Aufgabe übertragen worden wäre (vgl. Albers/Veit in BeckOK DatenschutzR, 55. Ed., DS-GVO Art. 6 Rn. 56, beck-online).

(dd) Eine Rechtfertigung der Verarbeitung von mittels Business Tools erhaltenen Offsite-Daten der Nutzer nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO scheidet ebenfalls aus. Nach dieser Vorschrift kann die Verarbeitung von personenbezogenen Daten zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gerechtfertigt sein. Voraussetzung dafür ist, dass von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen wird, die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein muss und die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder des Dritten nicht überwiegen (EuGH, Urteil vom 04.07.2023, C-252/21, Rn. 105, juris). Das ist hier auf der Grundlage des Beklagtenvortrags nicht festzustellen.

Die Beklagte hat, wie bereits oben ausgeführt, im vorliegenden Verfahren schon nicht hinreichend genau bezeichnet, welche konkreten Daten zu welchem konkreten Zweck erhoben und verarbeitet werden, sodass es dem Senat schon deswegen nicht möglich ist, eine Rechtfertigung im Sinne des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zu prüfen. Dies entspricht im Übrigen auch dem Befund des Bundeskartellamtes, wonach der Vortrag der Beklagten keine hinreichend klare Artikulation der berechtigten Interessen darstellt, die der Abwägungsprüfung mit den Interessen und Rechten der betroffenen Person zugänglich wäre (vgl. Beschluss des Bundeskartellamts vom 06.02.2019, a.a.O., Rn. 727 ff., 735 ff., 796 ff.).

Insbesondere die Ausführungen der Beklagten zu Sicherheits- und Integritätsinteressen sind so allgemein gehalten, dass sie keine Prüfung der Rechtfertigung ermöglichen. So macht sie etwa geltend, sie nutze – ohne diese näher zu spezifizieren – Daten, die über die streitgegen-

ständlichen Business Tools übermittelt wurden, um die Sicherheit und Integrität ihrer Server und Systeme vor bösartigen Angriffen zu schützen, bei denen die streitgegenständlichen Tools zur Verbreitung von Spam, Scraping oder anderen Cyberattacken missbraucht werden könnten. Mit Blick auf den Schutz vor Sicherheitsbedrohungen kann nicht etwa erkannt werden, dass die Schaffung zahlreicher Programmierschnittstellen auf Drittseiten und -Apps bei der Verwendung durch Business Tools einem entsprechenden Schutz, etwa vor „Scraping“ oder „Hacking“, dienlich wäre. Vielmehr dürfte durch die Bereitstellung der Business Tools und die damit verbundenen zahlreichen Datenschnittstellen die Gefahr wachsen, dass die insoweit eingepflegten Informationen unzulässig ausgelesen werden könnten; die Verknüpfung mit den Servern der Beklagten schafft erst Einfallstore für Hacker-Angriffe zu ihren Lasten. Demgemäß möchte die Beklagte einer Gefahr, die dadurch entsteht, dass die Datenerhebung mittels Business Tools zugleich ein Einfallstor für kriminelle Aktivitäten bzw. für eine Ausnutzung der Systeme sein kann, dadurch begegnen, dass sie diese Daten speichert und auswertet. Diese Begründung ist nicht geeignet, die Verarbeitung von individualisierten und/oder individualisierbaren Nutzerdaten auf ihrer Plattform zu rechtfertigen (ebenso OLG Dresden a.a.O. Rn. 177). Letztlich nimmt die Beklagte für sich in Anspruch, von Fall zu Fall selbst zu bestimmen, welche Daten sie als notwendig zur Untersuchung und Bekämpfung „böswilliger und krimineller Aktivitäten“ betrachtet und wie lange sie diese speichert. Konkrete Aufbewahrungsfristen für Daten kann die Beklagte nicht präzise festlegen (vgl. (b)). An nachprüfbaren Kriterien für die Daten-Speicherung fehlt es demnach. Davon abgesehen ist es offensichtlich nicht so, dass bei entsprechender Optionswahl des Nutzers dessen Offsite-Daten nur für Sicherheits- und Integritätszwecken genutzt würden. Denn die Beklagte teilt in ihren Informationen zum Thema „Einstellungen und Privatsphäre“ mit, dass es die Einstellung „Bestimmte Aktivitäten trennen“ Nutzern erlaubt, „die Verknüpfung ihrer zukünftigen Third-Party Activitiy Data mit ihrem Instagram-Konto zu trennen, wenn diese von einem bestimmten Drittunternehmen, das der Nutzer ausgewählt hat, empfangen werden“ (vgl. Anlage B 7, S. 51 mit Abb. 59). Die Beklagte teilt dort aber auch mit, dass sie gleichwohl weiterhin Informationen zu den Aktivitäten des Nutzers erhalte und diese „für Messungen sowie zur Verbesserung ihrer Werbesysteme“ verwendet werden (vgl. Anlage B 7, S. 52 mit Abb. 60).

Die von der Beklagten in Bezug genommene Aufklärung und Verhinderung von Straftaten ist, soweit dies nicht ihre eigenen wirtschaftlichen Interessen betrifft, nicht als berechtigtes Interesse im Sinne von Art. 6 Abs. 1 lit. f DSGVO berücksichtigungsfähig (vgl. EuGH, Urteil vom 04.07.2023, C-252/21, Rn. 113, 124, juris). Soweit sich die Beklagte überdies auf einen – ggf. berechtigten – Nutzerschutz beruft, ist nicht ersichtlich, ob und inwieweit die Beklagte diese Informationen tatsächlich zum Schutz ihrer Nutzer verwendet; ihre Ausführungen beschränken

sich hier auf Einzelbeispiele. Auch ist nicht erkennbar, inwiefern die behaupteten Interessen nicht mit weniger grundrechtsrelevanten Eingriffen als der Implementierung der Business Tools und der Verarbeitung dort erhobener Daten entsprochen werden könnte. Plausibel ist insoweit schlussendlich auch nicht der Umfang der Implementierung von Meta Business Tools; dass über jede einzelne darüber mit der Beklagten verbundenen Drittwebseite und -App eine Aufdeckung beispielsweise von Pädophilie oder kriminellen Netzwerken möglich ist, erscheint abwegig. Die von der Beklagten zur Rechtfertigung ihrer Datenverarbeitung bemühte anlasslose Massenüberwachung ist nicht durch das Interesse gerechtfertigt, einzelne Straftäter aufzuspüren; erst recht ist es nicht Aufgabe der Beklagten, Daten für eine flächendeckende Überwachung zu verarbeiten, weil ihr eine solche Aufgabe nicht übertragen worden ist.

Die nach Art. 6 Abs. 1 lit. f DSGVO vorzunehmende Interessenabwägung ergibt kein zugunsten der Beklagten überwiegendes Interesse an der Verarbeitung der Business-Tool-Daten. Dem berechtigten Interesse der Beklagten an einem profitablen Dienst kommt jedenfalls kein höheres Gewicht zu als dem Recht der Nutzer auf Datensicherheit und -minimierung sowie informationelle Selbstbestimmung. Der Europäische Gerichtshof hat insoweit bereits entschieden, dass auch bei Unentgeltlichkeit der Dienste eines sozialen Online-Netzwerks der Nutzer dieses Netzwerks vernünftigerweise nicht damit rechnen müsse, dass dessen Betreiber seine personenbezogenen Daten ohne seine Einwilligung zum Zweck personalisierter Werbung verarbeitet oder sogar noch umfänglicher nutzt. Daher sei davon auszugehen, dass die Interessen und Grundrechte eines solchen Nutzers bereits gegenüber dem Interesse dieses Betreibers an einer solchen Personalisierung der Werbung, mit der er seine Tätigkeit finanziert, überwiegen, sodass die von ihm zu solchen Zwecken vorgenommene Verarbeitung nicht unter Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO fallen könne (EuGH, Urteil vom 04.07.2023, C-252/21, Rn. 117, juris). Davon ausgehend kann erst recht die der Nutzung der Plattform der Beklagten vorgelagerte oder gar unabhängig von einer Plattformnutzung erfolgende Verarbeitung personenbezogener Daten nicht gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gerechtfertigt sein.

(c) Dies gilt erst recht, soweit die Beklagte auch „besondere Kategorien personenbezogener Daten“ im Sinne von Art. 9 Abs. 1 DSGVO (Gesundheits- oder Finanzdaten, Informationen von und über Kinder unter 13 sowie nicht zugelassene IDs, wie etwa Sozialversicherungs- oder Kreditkartennummern) verarbeitet, wovon der Senat überzeugt ist. Nach dem Vortrag des Klägers sind Gegenstand seiner Internetnutzung Recherchen zu medizinischen Themen und Finanzfragen, sodass sich auch insoweit eine persönliche Betroffenheit ergibt.

Die Datenverarbeitung über die Business Tools der Beklagten unterscheidet insofern nicht

zwischen einfachen und sensiblen Daten, extrahiert solche also nicht mit der notwendigen Verlässlichkeit. Zwar untersagt die Beklagte ihren Geschäftspartnern die Übermittlung solcher Daten, bei Verstößen hiergegen umfasst der Datenverarbeitungsvorgang allerdings auch solche Daten (vgl. OLG Dresden a.a.O. Rn. 167). Dass die von der Beklagten insoweit angeführten freiwilligen Maßnahmen vor der Übertragung sensibler Daten an die Beklagte bei einer automatisierten Datenverarbeitung mittels Business Tools einen hinreichend verlässlichen Schutz bieten, ist nicht erkennbar. Dies ergibt sich auch daraus, dass die Beklagte vorbringt, die streitgegenständliche Datenverarbeitung ermögliche es, schwerkriminelle Straftäter aufzuspüren und insoweit u.a. auf den Schutz Minderjähriger vor sexuellem Missbrauch hinweist. Sie räumt damit auch ein, anhand der Datenverarbeitung derart sensible Rückschlüsse ziehen zu können, dass sexuelle Neigungen betroffener Personen erkennbar würden, womit unzweifelhaft besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO verarbeitet werden. Art. 9 Abs. 1 DSGVO verbietet u.a. die Verarbeitung personenbezogener Daten, aus denen Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person hervorgehen.

Dafür, dass eine entsprechende Datenverarbeitung nach Art. 9 Abs. 2 DSGVO hier ausnahmsweise zulässig wäre, ist nichts ersichtlich.

(d) In der Gesamtschau ist demnach festzustellen, dass der Einsatz der Meta Business Tools in seiner derzeitigen Ausgestaltung, bei der personenbezogene Daten auf (Dritt-)Webseiten erhoben, an die Beklagte übermittelt und anschließend in deren Systemen weiterverarbeitet (gespeichert, verwendet, ausgewertet und an andere übermittelt) werden, auch gegen den in Art. 5 Abs. 1 lit. c DSGVO niedergelegten Grundsatz der Datenminimierung verstößt. Auf der Grundlage des Parteivortrags muss der Senat davon ausgehen, dass die Beklagte mit den Meta Business Tools ein System bereitstellt, welches personenbezogene Daten des Klägers, die durch Nutzung von (Dritt-)Webseiten und -Apps entstehen, in einem erheblichen Umfang und undifferenziert verarbeitet, statt die Verarbeitung auf ein für den jeweiligen konkret definierten Zweck notwendiges Maß zu beschränken. Die Beklagte erhält über ihre Business Tools weitreichende Offsite Daten ihrer Nutzer über deren Aktivitäten im Internet und verfolgt allgemein auch deren Navigationsverhalten. Es steht dem Grundsatz der Datenminimierung entgegen, wenn – wie hier – sämtliche personenbezogenen Daten, die ein verantwortlicher Betreiber einer Social-Media-Plattform von der betroffenen Person oder von Dritten erhält und die sowohl auf als auch außerhalb dieser Plattform erhoben wurden, zeitlich unbegrenzt und ohne Unterscheidung nach ihrer Art für eine Vielzahl nicht hinreichend konkretisierter Zwecke aggregiert, analysiert und verarbeitet werden.

(3) Die Beklagte ist als Störerin i.S.d. § 1004 BGB passivlegitimiert.

Störer ist, wer, auch ohne Täter oder Teilnehmer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Beeinträchtigung des Rechtsguts beiträgt oder dessen Verhalten eine Beeinträchtigung befürchten lässt, unabhängig von Art und Umfang seines Beitrags. Unmittelbarer Handlungsstörer ist, wer die Beeinträchtigung durch eine eigene Handlung mitverursacht. Hat die Beeinträchtigung ihre unmittelbare Ursache im Verhalten Dritter, ist zusätzlich die Verletzung von Handlungspflichten erforderlich, die sich, von speziellen gesetzlichen Verpflichtungen abgesehen, allgemein danach bestimmt, inwieweit der Verantwortliche zu der Verletzung beiträgt und ihm zumutbare Einwirkungsmöglichkeiten zur Verfügung stehen (vgl. Retzlaff in Grüneberg, BGB, 85. Aufl., Einf v § 823 Rn. 31, 35).

Die Beklagte ist unmittelbare Handlungsstörerin, weil sie die verfahrensgegenständlichen Business Tools entwickelt und den Drittunternehmen gerade zu dem Zweck zur Verfügung gestellt hat, damit Daten bei Website-Besuchern und App-Nutzern zu erheben und an ihre Server weiterzuleiten (OLG Koblenz, Urteil vom 30.04.2026, 1 U 415/25, n.v., S. 53; OLG Dresden, Urteil vom 12.03.2026, 17 U 625/25, S. 56; vgl. auch OLG Hamm a.a.O. Rn. 81; OLG München, Urteil vom 18.12.2025, 14 U 881/25 e, Rn. 144, juris; a.A. im Ergebnis OLG Stuttgart a.a.O Rn. 141 ff.). Der Kläger hat zudem im Termin - unbestritten - darauf verwiesen, dass die Beklagte sich mittels ihrer Business Tools „die Daten von fremden Servern selbst hole und nicht auf eine etwaige Weiterleitung warten müsse“; auch insofern ist von der unmittelbaren Verursachung der Beeinträchtigung des Klägers durch die Beklagte selbst auszugehen.

Soweit das OLG Stuttgart (a.a.O Rn. 141 ff.) unter Verweis auf das Urteil des EuGH vom 29.07.2019 (C-40/17, Rn. 102, juris) annimmt, die Einwilligung zum Erheben und Übermitteln der Daten müsse vor diesen Verarbeitungsschritten erklärt werden und sei daher von dem Dritten und nicht der Beklagten einzuholen, steht dies der Annahme, die Beklagte sei unmittelbare Störerin, nicht entgegen. Im Übrigen ist der Entscheidung des EuGH aber auch zu entnehmen, dass die dem Dritten gegenüber zu erklärende Einwilligung nur die Vorgänge der Verarbeitung personenbezogener Daten betrifft, für die er tatsächlich über die Zwecke und Mittel entscheidet. Wegen der Datenverarbeitung zu Zwecken der Beklagten sind die Drittunternehmen daher an der Einholung der Einwilligung gehindert *(*vgl. OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 173, juris*).*

Selbst dann aber, wenn aber die unmittelbare Ursache der Beeinträchtigung des Klägers in ei-

nem Verhalten der Drittunternehmen - durch eine Datenerhebung und -übermittlung ohne ausreichende Rechtsgrundlage - zu sehen wäre, würde jedenfalls aus Art. 24 Abs. 1 DSGVO eine Handlungspflicht der Beklagten resultieren, im Verhältnis zu den Dritten ein effektives Kontroll- und Sanktionsregime einzurichten, um sicherzustellen, dass bei der Datenverarbeitung durch die Business Tools eine ausreichende Rechtsgrundlage vorliegt.

(4) Die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr wird durch das festgestellte rechtsverletzende Verhalten der Beklagten indiziert. Dies gilt nicht nur für identische Verletzungshandlungen, sondern auch für andere Pflichtverletzungen, soweit die Verletzungshandlungen – wie hier – im Kern gleichartig sind (BGH, Urteil vom 29.07.2021, III ZR 192/20, Rn. 115 f., juris).

Dass der Kläger am 30.03.2026 sein Instagram-Konto selbst deaktiviert hat (S. 99 dA), steht der Wiederholungsgefahr schon deshalb nicht entgegen, weil die Deaktivierung nicht ausschließt, dass die Beklagte bei Dritten den Kläger betreffende Daten erhebt und verarbeitet. Zudem kann der Kläger sein Konto auch jederzeit wieder aktivieren (vgl. S. 160 dA).

(5) Die Einschränkung der Unterlassungsverpflichtung mit Blick auf eine möglicherweise noch in der Zukunft erteilte Einwilligung oder einen sich in der Zukunft ergebenden Rechtfertigungsgrund ist nicht geboten (anders OLG München, Urteil vom 18.12.2025, 14 U 881/25e, Rn. 191 ff, juris; OLG Naumburg, Urteil vom 05.02.2026, 9 U 124/24, Rn. 293 ff., juris). Der Kläger hat gegenüber der Beklagten keine Einwilligung in die streitgegenständliche Datenverarbeitung erteilt. Auch sonstige Rechtfertigungsgründe für ihre Datenverarbeitung sind von der Beklagten nicht in ausreichender Weise dargelegt. Wird zu einem späteren Zeitpunkt eine wirksame Einwilligung erteilt oder ergibt sich ein Rechtfertigungsgrund für eine Datenverarbeitung durch die Beklagte, ist dies ggf. durch eine Vollstreckungsabwehrklage nach § 767 Abs. 2 ZPO geltend zu machen, die auch gegen einen Unterlassungsanspruch gerichtet werden kann (OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 183, juris; Urteil vom 12.03.2026, 17 U 625/25, n.v., S. 57; OLG Koblenz a.a.O. S. 53). Die Ergänzung des Unterlassungsausspruchs um abstrakte Rechtfertigungsgründe wäre mit einer Entwertung des Erkenntnisverfahrens und des Titels verbunden, weil sich ein gerichtliches Gebot, wonach die Beklagte eine bestimmte Form der Datenverarbeitung zu unterlassen hat, „sofern ihr die Verarbeitung nicht erlaubt ist“, im Ergebnis auf die bloße Wiedergabe der abstrakten Rechtslage beschränken würde. Die eigentlich verfahrensgegenständliche Frage, nämlich ob die Verarbeitung personenbezogener Daten im konkreten Einzelfall unterbleiben muss, würde hingegen vollumfänglich in das hierfür nicht ausgelegte Vollstreckungsverfahren verlagert (OLG Dres-

den, Urteil vom 12.03.2026, 17 U 625/25, a.a.O.).

bb) Durch den mit dem Einsatz der Business Tools verbundenen und den Kläger betreffenden Verstoß gegen Art. 5 Abs. 1 lit. a, c und Art. 6 Abs. 1 DSGVO wird zugleich rechtswidrig in das allgemeine Persönlichkeitsrecht des Klägers eingegriffen (vgl. OLG Koblenz a.a.O S. 50 ff.; OLG Dresden, Urteil vom 12.03.2026, 17 U 625/25, S. 53 ff.). Aus diesem rechtswidrigen Eingriff in sein Persönlichkeitsrecht resultiert ein Unterlassungsanspruch des Klägers. Insoweit wird auf die Ausführungen unter aa) (3) bis (5) verwiesen.

3. Der Antrag zu Ziffer 2, mit dem der Kläger die Löschung der Daten im Sinne ihres Antrags zu Ziffer 1 verlangt, ist zulässig und auch begründet.

a) Der Antrag ist zulässig.

Er ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO, weil die zu löschenden Daten hinreichend genau bezeichnet werden.

Auch fehlt es dem Löschungsantrag nicht deshalb am Rechtsschutzbedürfnis, weil die Beklagte auf ihrer Plattform ein „Self-Service-Tool“ zur Verfügung stellt, welches die Optionen „Frühere Aktivitäten löschen“ bzw. „Künftige Aktivitäten trennen“ anbietet. Es ist nicht ersichtlich, dass der Kläger hierdurch die Offsite-Daten nicht nur von seinem Account trennen, sondern die von der Beklagten gespeicherten Daten insgesamt – im Sinne einer Unmöglichkeit der anschließenden Informationswahrnehmung (vgl. Kühling/Buchner/Herbst, DS-GVO/BDSG, 4. Aufl., Art. 17 DSGVO Rn. 37) – löschen kann; der Prozessbevollmächtigte der Beklagten hat dies in der mündlichen Verhandlung bestätigt. Nach dem eigenen Vorbringen der Beklagten (Anlage B 7, Abb. 26, 32) erhält sie außerdem trotz erfolgter Trennung weiterhin Informationen zu den Aktivitäten und verwendet diese für Messungen sowie zur Verbesserung ihrer Werbesysteme. Der Kläger kann auch nicht auf die Löschung seines Accounts verwiesen werden, denn dies liefe dem Zweck von Art. 17 DSGVO ersichtlich zuwider.

Die von der Beklagten bestrittene Voraussetzung gemäß § 259 ZPO der „Besorgnis nicht rechtzeitiger Leistung“ liegt schon deshalb vor, weil sie den Anspruch leugnet.

Nicht zu folgen vermag der Senat den Ausführungen des OLG Hamm (a.a.O. Rn. 64), wonach die Einschränkung, dass die Löschung erst nach Auskunftserteilung erfolgen soll, zur Unbestimmtheit führe und - im Sinne eines Verzichts auf diese Einschränkung - auszulegen sei

(wie der Senat im Ergebnis auch: OLG Stuttgart a.a.O.; OLG München, Urteil vom 18.12.2025, 14 U 2300/25e). Aus dem vom OLG Hamm in Bezug genommenen Urteil des Bundesgerichtshofs vom 05.03.2024 (VI ZR 330/21, Rn. 8, juris) folgt zwar, dass der Klageantrag so genau sein muss, dass das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abgewälzt wird und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwartet werden kann; andererseits hat der BGH (a.a.O.) festgestellt, dass nicht jede mögliche Unsicherheit bei der Zwangsvollstreckung zur Unbestimmtheit des Klageantrags führt. Es ist auch nicht anzunehmen, dass ein Vollstreckungsorgan nicht beurteilen kann, wann eine (vollständige) Auskunftserteilung gegeben ist. Wenn das Vollstreckungsorgan im Rahmen der Vollstreckung des Auskunftsanspruchs die Erteilung der Auskunft feststellen kann, ist ihm das erforderlichenfalls auch im Rahmen der Vollstreckung des Löschungsanspruchs möglich.

b) Der Antrag ist auch begründet.

Gemäß Art. 17 Abs. 1 lit. d DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden; der Verantwortliche ist dann hierzu verpflichtet.

Diese Voraussetzungen liegen hier vor. Wie sich aus den Ausführungen unter 2. ergibt, sind personenbezogene Daten des Klägers unrechtmäßig verarbeitet worden. Die Beklagte hat keine ausreichenden Rechtfertigungsgründe gemäß Art. 6 Abs. 1 DSGVO dargelegt. Sie hat darüber hinaus auch nicht nachvollziehbar vorgetragen, wie sie mit von Drittwebseiten übermittelten sensiblen Daten im Sinne von Art. 9 Abs. 1 DSGVO verfährt; die Verarbeitung dieser personenbezogenen Daten ist grundsätzlich untersagt. Ein Ausschlussgrund nach Art. 17 Abs. 3 DSGVO, welcher einem Anspruch nach Abs. 1 ausnahmsweise entgegenstehen könnte, besteht vorliegend nicht. Die Beklagte hat hierzu nichts vorgebracht und auch sonst ist hierfür nichts ersichtlich.

4. Der Antrag zu Ziffer 4, mit dem der Kläger eine angemessene Entschädigung in Geld für einen immateriellen Schaden begehrt, ist zulässig und teilweise begründet. Ihm steht wegen der Verarbeitung seiner mittels Business Tools verarbeiteten personenbezogenen Daten gegen die Beklagte ein immaterieller Schadenersatz in Höhe von 1.500,00 EUR zu.

a) Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen

diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter, wobei gemäß Art. 82 Abs. 3 DSGVO jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden haftet, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurde. Der Verantwortliche wird (nur) von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist (Art. 82 Abs. 3 DSGVO).

Nach ständiger Rechtsprechung des EuGH erfordert ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO einen Verstoß gegen Vorschriften der DSGVO, das Vorliegen eines materiellen oder immateriellen Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß. Die Darlegungs- und Beweislast für diese Voraussetzungen trifft grundsätzlich die Person, die auf der Grundlage von Art. 82 Ziff. 1 DSGVO den Ersatz eines (immateriellen) Schadens verlangt (vgl. EuGH, Urteil vom 04.10.2024, C-200/23, Rn. 140, juris; BGH, Urteil vom 18.11.2024, VI ZR 10/24, Rn. 21, juris).

aa) Die Beklagte hat als Verantwortliche personenbezogene Daten des Klägers ohne Rechtfertigungsgrund verarbeitet und damit gegen die Vorschriften der DSGVO verstoßen. Insoweit wird auf die Ausführungen unter 1. Bezug genommen.

bb) Dem Kläger ist ein immaterieller Schaden entstanden. Nach der Rechtsprechung des Bundesgerichtshofs (a.a.O. Rn. 30) und des Europäischen Gerichtshofs (Urteil vom 04.09.2025, C-655/23, Rn 60, juris) kann bereits ein Kontrollverlust über personenbezogene Daten als Schaden angesehen werden, sofern die betroffene Person nachweist, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert. Steht ein Kontrollverlust fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern.

Hier ist ein Kontrollverlust festzustellen, denn der Kläger hat keine Kenntnis darüber, auf welchen der von ihm besuchten Webseiten die von der Beklagten entwickelten Business Tools eingesetzt, welche Daten mit deren Hilfe dort über ihn erhoben und an die Beklagte weitergeleitet und in welchem Ausmaß diese Daten bei der Beklagten gespeichert, aggregiert und genutzt und möglicherweise auch an weitere Personen, Unternehmen, Organisationen oder Be-

hörden weitergeleitet werden. Die Tatsache, dass eine erhebliche Menge seiner personenbezogenen Daten, welche seinem Benutzerkonto zugeordnet sind oder die ihm – z.B. mittels eines Abgleichs von IP-Adressen und Geräte-Informationen – zugeordnet werden können, sich auf Servern der Beklagten in der ganzen Welt (vgl. Anlage K 3, Datenschutzrichtlinie, S. 72 f.) befinden, möglicherweise auch auf Servern von Dritten, oder Dritten zur Verfügung gestellt werden können, stellt einen Kontrollverlust dar. Als Dritte, mit denen Informationen geteilt werden (können), bezeichnet die Datenschutzrichtlinie der Beklagten u.a. Werbetreibende, Unternehmen, die Produkte vermarkten oder die mit Kundenservice oder Umfragen beauftragt werden, Anbieter von Mess- und Analysediensten, Forscher, Behörden sowie Strafverfolgungsbehörden (vgl. Anlage K 3, S. 49 f., 76 f).

Der Kläger kann nicht wissen, welche Informationen die Beklagte über sein Internet- und App-Nutzungsverhalten über das hinaus, was er selbst durch die Nutzung des sozialen Netzwerks preisgibt, bislang erhalten hat und bis zu welchem Grad sie genaue Kenntnisse über ihn und seine individuellen Lebensumstände hat. Da die Erhebung und Übermittlung personenbezogener Daten durch die Meta Business Tools bei Nutzung des Internets und von Apps im Hintergrund läuft und die Beklagte nicht mitteilt, welche Informationen über den Kläger sie über die bei Nutzung des sozialen Netzwerks anfallenden Informationen hinaus hat, fehlt dem Kläger jedwede Kenntnis und erst recht die Kontrolle darüber, bis zu welchem Grad die Beklagte ohne seinen Willen über ein ihn betreffendes Persönlichkeitsprofil oder jedenfalls die dafür nutzbaren Informationen verfügt. Dies stellt einen immateriellen Schaden im vorstehenden Sinne dar (vgl. OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 197, juris; OLG Jena a.a.O. Rn. 227).

cc) Dieser Schaden ist auch kausal zurückzuführen auf die mit dem Empfang und der Verarbeitung der mittels Business Tools erfassten personenbezogenen Daten einhergehenden Verstöße der Beklagten gegen Art. 6 DSGVO. Denn bei Einhaltung dieser Bestimmungen hätte die Beklagte entweder selbst eine den Kriterien des Art. 7 DSGVO genügende, d.h. vollständig informierte und freiwillige Einwilligung des Klägers in die Verarbeitung jener personenbezogenen Daten, die außerhalb der sozialen Netzwerke anfallen, einholen – und zwar nicht allein bezogen auf die Anzeige personalisierter Werbung, sondern in Gänze hinsichtlich aller in Betracht kommenden Zwecke – oder aber auf die Bereitstellung dieser Tools verzichten müssen. Die Beklagte hat nicht dargelegt und es ist auch sonst nichts dafür ersichtlich, dass der Kläger ihr eine solche globale Einwilligung in die Erfassung seines Internetverhaltens freiwillig erteilt hätte. Deswegen ist davon auszugehen, dass der Beklagten bei rechtmäßigem Verhalten keine personenbezogenen Daten des Klägers vorliegen würden, welche außerhalb der so-

zialen Netzwerke durch die Nutzung von anderen Apps und Webseiten anfallen, sondern lediglich solche, die diese selbst auf den sozialen Netzwerken preisgibt. Kausalität in diesem Sinne besteht auch, soweit es um die vorbenannten weiteren Verstöße gegen die Grundsätze des Art. 5 Abs. 1 DSGVO geht.

dd) Exkulpationsgründe im Sinne von Art. 82 Abs. 3 DSGVO sind dem Vorbringen der Beklagten nicht zu entnehmen. Sie macht geltend, dass sie rechtmäßig gehandelt habe, nicht aber, dass sie für die anspruchsbegründenden Umstände nicht verantwortlich sei.

ee) Der Höhe nach hält der Senat einen Betrag von 1.500,00 EUR zur Kompensation des entstandenen immateriellen Schadens für angemessen.

Dem immateriellen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO kommt nach der Rechtsprechung des Gerichtshofs allein eine Ausgleichsfunktion zu, während die Vorschrift keinen Strafzweck verfolgt sowie keine Abschreckungsfunktion gegenüber dem Schädiger und keine Genugtuungsfunktion für den Geschädigten erfüllen soll (EuGH, Urteil vom 04.05.2023, C-300/21, Rn. 58, juris). Der Grad des Verschuldens des Schädigers ist ebenfalls kein relevanter Bemessungsfaktor (EuGH a.a.O.). Zur Bemessung der Höhe des Schadenersatzes ist auf die Grundsätze zurückzugreifen, die der Bundesgerichtshof anlässlich eines sog. „Scraping“-Falls zur Schadensbemessung bei Datenschutzverstößen entwickelt hat. Danach sind die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten nach Art. 9 Abs. 1 DSGVO, der Verwendungszweck, die Art des Kontrollverlusts etwa mit Blick auf den Empfängerkreis, dessen Dauer sowie die Möglichkeit der Wiedererlangung der Kontrolle maßgebliche Faktoren (BGH, Urteil von 18.11.2024, VI ZR 10/24, Rn. 99, juris).

Unter Berücksichtigung des Vortrags des Klägers zu seinen Internetrecherchen hinsichtlich medizinischer, politischer und finanzieller Themen ist davon auszugehen, dass im vorliegenden Fall auch sensible personenbezogene Daten besonderer Kategorien des Klägers im Sinne von Art. 9 Abs. 1 DSGVO von der rechtswidrigen Datenverarbeitung der Beklagten betroffen sind; gegenteiliges hat die Beklagte nicht in substantiierter Weise behauptet. Die vorgenannte Vorschrift verbietet die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Ausnahmen im Hinblick auf diese „besonderen Kategorien personenbezogener

Daten“ gelten nur unter bestimmten, in Art. 9 Abs. 2 und 3 DSGVO eng definierten, Umständen.

Die Beklagte, die auch insoweit eine sekundäre Darlegungslast trifft, weil es sich um Umstände aus ihrem Wahrnehmungs- und Kenntnisbereich handelt, zu denen sie ohne Weiteres konkret vortragen könnte (§ 138 Abs. 2 ZPO), ist diesem Vortrag des Klägers nicht substantiiert entgegengetreten. Daher ist es als zugestanden gemäß § 138 Abs. 3 ZPO anzusehen, dass unter den von der Beklagten mittels Business Tools erhaltenen und verarbeiteten personenbezogene Daten des Klägers sich auch solche befinden, die als besonders sensible Daten im Sinne von Art. 9 Abs. 1 DSGVO zu bewerten sind.

Die Kläger hat glaubhaft auf Befragung des Senats bekundet, der Umfang der von der Beklagten gesammelten Daten sei ihm ursprünglich gar nicht klar gewesen. Er sei deshalb deutlich vorsichtiger geworden, was die Nutzung von Internetseiten anbelange. Das durch die von dem Kläger angeführte Vorsicht zum Ausdruck kommende Gefühl des Überwachtwerdens und das schriftsätzlich geschilderte permanente Gefühl der Unsicherheit, welcher Klick und welche Texteingabe im Internet heimlich von der Beklagten mitgelesen bzw. weiterverarbeitet wird, sind nachteilige Folgen, die über einen „bloßen“ Kontrollverlust und die hiermit verbundenen Unannehmlichkeiten hinausgehen und daher einen immateriellen Schaden begründet. Dies gilt insbesondere, als nach dem hier zugrunde zu legenden Vorbringen anzunehmen ist, dass auch bei verweigerter Einwilligung eines Nutzers über Business Tools erlangte Daten zu einem Profiling im Sinne des Art. 22 DSGVO verwendet werden (können). Nach der Rechtsprechung des Gerichtshofs stellt das Erstellen detaillierter Profile der Nutzer in Verbindung mit der zeitlich unbegrenzten Weiterverarbeitung einen schweren Eingriff in die Grundrechte der betroffenen Nutzer, insbesondere auf Achtung ihres Privatlebens und den Schutz personenbezogener Daten, dar (EuGH, Urteil vom 04.10.2024, C-446/21, Rn 63, juris). Dies gilt nach Auffassung des Senats auch in den Fällen, in denen – wie hier – nicht nachgewiesen ist, dass die über Meta Business Tools erlangten Daten für Zwecke der personalisierten Werbung verwendet werden. Insbesondere kann ein Nutzer nicht wissen, ob bei dem Besuch bestimmter Webseiten über eingebundene Business Tools auch Daten im Sinne von Art. 9 Abs. 1 DSGVO an die Beklagte gelangen, was dazu führen kann, dass Nutzer davon absehen, bestimmte Webseiten zu besuchen. Dies kommt auch in der vom Kläger angeführten notwendigen Vorsicht bei der Internetnutzung zum Ausdruck.

Anders als in den sog. „Scraping“-Fällen werden vorliegend zwar die über die Business Tools erlangten Daten nicht im Internet veröffentlicht, sondern lediglich bei der Beklagten verknüpft

und gespeichert. Im Unterschied zu den „Scraping“-Sachverhalten, bei denen es im Wesentlichen um die Verknüpfung von Telefonnummer und/oder E-Mail-Adresse mit einem Facebook-Nutzerkonto geht, erfasst die Verarbeitung der mittels Business Tools gewonnenen Daten aber eine unabsehbare Vielzahl personenbezogener Daten, darunter je nach Einzelfall auch etwa Gesundheitsdaten oder Daten zur sexuellen Orientierung, religiöser und politischer Einstellung. Zu berücksichtigen ist auch, dass der Kläger keine Möglichkeit hat, durch eigenes Handeln die Kontrolle über diese Daten zurückzuerlangen; weder durch die Änderung der Datenschutzeinstellungen noch durch die Löschung des Kontos kann er eine vollumfängliche Löschung der bei der Beklagten gespeicherten Daten erreichen.

Der Senat geht nach alledem davon aus, dass bereits dieser abstrakt bestehende Kontrollverlust in Verbindung mit dem nachvollziehbar hieraus abgeleiteten Unsicherheitsgefühl für einen immateriellen Schaden ausreicht, ohne dass der Kläger diesen noch weiter individualisieren müsste. Die sehr umfassende Verarbeitung von personenbezogenen Daten durch die Beklagte sowie das allgemeine Gefühl der Beobachtung im privaten Umfeld sind ohne weiteres geeignet, bei jedem davon betroffenen Nutzer negative Gefühle in Form von Sorge und Ärger auszulösen, weshalb diese Empfindungen bei der Bemessung des immateriellen Schadens berücksichtigt werden können, ohne dass es auf weiteren Vortrag ankommt, welche Daten genau erhoben worden sind (so wohl auch Nemitz in Ehmann/Selmayr, DS-GVO/BDSG, 3. Aufl., Art. 82 DSGVO Rn. 17; Bergt in Kühling/Buchner, DS-GVO, 4. Aufl., Art. 82 Rn. 18c). Das unbestimmte Gefühl einer Überwachung ihres Verhaltens nicht nur im Internet liegt nachvollziehbar darin begründet, dass der Kläger nicht weiß und auch nicht wissen kann, welche und wie viele 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. Für den durch den Kläger erlittenen Schaden erscheint ein immaterieller Schadensersatz in Höhe von 1.500,00 EUR ausreichend und angemessen (vgl. OLG Dresden a.a.O. Rn. 197). Dabei ist davon auszugehen, dass der Kläger einen einheitlichen Anspruch auf immateriellen Schadensersatz aus Art. 82 Ziff. 1 DSGVO geltend macht, der sich auf eine Vielzahl einzelner, nicht konkretisierter Datenschutzverstöße der Beklagten stützt, aber in einem einheitlichen Geschehen – dem fortlaufenden Einsatz der Meta Business Tools – wurzelt.

Eine höhere immaterielle Entschädigung käme nur in Betracht, wenn der Kläger im Einzelfall nachvollziehbar darlegt (und erforderlichenfalls auch beweist), infolge der streitgegenständlichen Datenverarbeitung eine psychische Beeinträchtigung oder sonstige konkrete immaterielle Schäden erlitten zu haben. Sind derartige psychische Beeinträchtigungen nachgewiesen, ist der Entschädigungsbetrag in einer Höhe festzusetzen, die über dem im Falle eines bloßen

Kontrollverlustes zuzusprechenden Betrages liegt (BGH a.a.O. Rn. 101). Zu einer solchen emotionalen Betroffenheit hat der Kläger jedoch keine individualisierbaren Anhaltspunkte vorgetragen.

b) Ob neben dem unionsrechtlichen Entschädigungsanspruch aus Art. 82 DSGVO auch ein Schadensersatzanspruch aus § 823 Abs. 1 BGB i.V.m. Art. 1, 2 GG wegen Verletzung des allgemeinen Persönlichkeitsrechts besteht, bedarf keiner Entscheidung (ablehnend: OLG München, a.a.O., Rn. 301 ff.). Zweifelhaft ist dies schon deshalb, weil eine Geldentschädigung wegen schuldhafter Verletzung des allgemeinen Persönlichkeitsrechts erfordert, dass die Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann (BGH, Urteil vom 12.03.2024, VI ZR 1370/20, Rn. 70, juris), was allerdings im Hinblick auf den Zuspruch eines angemessenen Betrages gemäß Art. 82 DSGVO angenommen werden könnte. Entschieden werden muss diese Frage hier aber nicht, denn auf alleiniger Basis des nationalen Rechts und der sich hierzu etablierten Schmerzensgeldpraxis bei Datenschutzverstößen könnte nach den hier maßgeblichen Umständen des konkreten Einzelfalls jedenfalls kein höherer Entschädigungsbetrag verlangt werden als jener, welcher auf der Grundlage des Art. 82 DSGVO angemessen ist. So mag zwar nach nationalem Recht neben dem Ausgleichs- auch das Genugtuungsinteresse und der Gedanke der Prävention für die Bemessung von Relevanz sein. Daraus ließe sich aber angesichts der dann auch notwendigen verhältnismäßigen Einpassung in die nationale Schmerzensgeldrechtsprechung zu anderen Rechtsgütern kein höherer Betrag begründen (so auch OLG Jena a.a.O. Rn. 244; OLG Naumburg a.a.O. Rn. 375).

c) Dem Kläger stehen gemäß den §§ 291, 288 Abs. 1 S. 2, 187 Abs. 1 (analog) BGB Rechtshängigkeitszinsen ab dem Tag nach der Zustellung (09.01.2025) zu. Ein weitergehender Zinsanspruch mit Blick auf die außergerichtliche Aufforderung des Klägers vom 02.07.2024 zur Zahlung einer Entschädigung in Höhe von 5.000,00 Euro bis zum 23.07.2024 (Anlage K 7) besteht nicht. Dadurch ist kein Verzug eingetreten, weil der geforderte Betrag deutlich übersetzt war und nicht ersichtlich ist, dass die Beklagte das Schreiben als Aufforderung zur Zahlung eines angemessenen Betrages verstehen musste und der Kläger zur Annahme einer geringeren Leistung bereit war (vgl. OLG Hamm a.a.O. Rn. 194; Grüneberg in Grüneberg, BGB, 85. Aufl., § 286 Rn 20).

5. Der Kläger hat keinen Anspruch auf Freistellung von außergerichtlichen Anwaltskosten gemäß §§ 280, 286 BGB, weil nicht ersichtlich ist, dass die Kosten erforderlich waren.

Bei der Beurteilung der Frage, ob und in welchem Umfang der dem Geschädigten zustehende

Schadensersatzanspruch gemäß § 249 Abs. 1 BGB auch die Erstattung von Rechtsanwaltskosten umfasst, ist zwischen dem Innenverhältnis des Geschädigten zu dem für ihn tätigen Rechtsanwalt und dem Außenverhältnis des Geschädigten zum Schädiger zu unterscheiden. Voraussetzung für einen Erstattungsanspruch ist grundsätzlich, dass der Geschädigte im Innenverhältnis zur Zahlung der in Rechnung gestellten Kosten verpflichtet ist und die konkrete anwaltliche Tätigkeit im Außenverhältnis aus der maßgeblichen Sicht des Geschädigten mit Rücksicht auf seine spezielle Situation zur Wahrnehmung seiner Rechte erforderlich und zweckmäßig war (BGH, Beschluss vom 23.06.2022, VII ZR 394/21, Rn. 19, juris).

Vorliegend war die außergerichtliche Tätigkeit nicht zweckmäßig, weil der Kläger mit einer auch nur teilweisen Erfüllung der Forderungen nicht rechnen konnte. Bei vernünftiger Betrachtung musste ihm und seinem Prozessbevollmächtigten bei Begründung des Mandatsverhältnisses klar sein, dass die Beklagte außergerichtlich nicht auf ihre Forderungen eingehen würde, die ihr auf den Business Tools basierendes Geschäftsmodell grundlegend in Frage stellt (vgl. OLG Dresden a.a.O. Rn. 202).

III.

Der Senat ändert die erstinstanzliche Streitwertfestsetzung entsprechend der im Termin erfolgten Festsetzung für die 2. Instanz ab und setzt den Wert auf 7.000,00 EUR fest (Anträge zu 1 und 3: je 500,00 EUR, Antrag zu 2: 1.000,00 EUR, Antrag zu 4: 5.000,00 EUR).

Die Kostenentscheidung entspricht § 92 ZPO und berücksichtigt, dass der Kläger mit seiner Zahlungsforderung in Höhe von 3.500,00 EUR - der Hälfte des vom Senat festgesetzten Streitwerts - keinen Erfolg hat.

Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 10, 709, 711 ZPO.

Der Senat lässt die Revision zu. Wie sich aus den Ausführungen unter II. ergibt, werden streitentscheidende Rechtsfragen von den Oberlandesgerichten nicht einheitlich beurteilt.

[redacted] [redacted] [redacted]