



Oberlandesgericht Dresden

Zivilsenat

Aktenzeichen: **12 U 1554/25**
Landgericht Dresden, 3 O 165/25

IM NAMEN DES VOLKES

URTEIL

In dem Rechtsstreit

- Kläger und Berufungskläger -

Prozessbevollmächtigte:

BK Verbraucherschutz Rechtsanwalts-gesellschaft mbH, Viktoria-Luise-Platz 7,
10777 Berlin, Gz.: BKD-017111-24

gegen

Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Irland

vertreten durch Direktoren Yvonne Cunnane, David Harris, Genevieve Hughes, Majella
Mungovan und Anne O'Leary

- Beklagte und Berufungsbeklagte -

Prozessbevollmächtigte:

wegen Datenverarbeitung

hat der 12. Zivilsenat des Oberlandesgerichts Dresden durch

Vorsitzenden Richter am Oberlandesgericht

Richter am Oberlandesgericht

Richter am Oberlandesgericht

aufgrund der mündlichen Verhandlung vom 03.06.2026 am 08.07.2026

für Recht erkannt:

- I. Auf die Berufung des Klägers wird das Urteil des Landgerichts Dresden vom 26.11.2025, 3 O 165/25, unter Zurückweisung der weitergehenden Berufung teilweise abgeändert und insgesamt wie folgt neu gefasst:
 1. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festgesetzten Ordnungsgeldes bis zu 250.000,00 € ersatzweise an deren gesetzlichen Vertreter zu vollstreckende Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers mithilfe der Meta-Business-Tools zu erfassen, an die Firma der Beklagten weiterzuleiten, dort zu speichern und anschließend zu verwenden.
 2. Die Beklagte wird verurteilt, an den Kläger 1.500,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 25.02.2025 zu zahlen.
 3. Im Übrigen wird die Klage abgewiesen.
- II. Von den Kosten des Rechtsstreits in beiden Instanzen haben der Kläger zwei Drittel und die Beklagte ein Drittel zu tragen.
- III. Dieses Urteil ist vorläufig vollstreckbar, hinsichtlich des Unterlassungsanspruchs gegen Sicherheitsleistung in Höhe von 1.000,00 €. Wegen des sonstigen vollstreckungsfähigen Inhalts des Urteils kann jede Partei die Vollstreckung der Sicherheitsleistungen in Höhe von 115 % des jeweils vollstreckbaren Betrages abwenden, wenn der Gläubiger vor der Vollstreckung Sicherheit in Höhe von 115 % des jeweils zu vollstreckenden Betrages leistet.

Beschluss:

Der Streitwert wird unter teilweiser Abänderung der Streitwertfestsetzung für beide Instanzen auf 5.500 EUR festgesetzt.

A.

Der Kläger macht im Zusammenhang mit seiner Nutzung des Sozialen Netzwerkes „Instagram“ Unterlassungs- und Schadensersatzansprüche wegen einer unzulässigen Verarbeitung personenbezogener Daten unter anderem durch Nutzung sogenannter „Business-Tools“ durch die Beklagte geltend.

Die Beklagte ist Betreiberin des Sozialen Netzwerkes „Facebook“ und „Instagram“. Seit 2014 hat der Kläger mit dem Benutzernamen [REDACTED] das Soziale Netzwerk „Instagram“ genutzt.

Die Nutzung der Plattform ist für Privatpersonen - abgesehen von der frei wählbaren Möglichkeit eines Abo-Modells, das der Kläger nicht gewählt hat - kostenfrei.

Mit der Registrierung bei der von der Beklagten betriebenen Sozialen Netzwerke stimmen Nutzer diesbezüglich Nutzungsbedingungen der Beklagten zu. Dort wird ausdrücklich auf Regelungen verwiesen, wie die Beklagte Informationen verwendet, um Werbeanzeigen, kommerzielle und werbliche Inhalte zu zeigen, für deren Bewerbung Unternehmen und Organisationen an die Beklagte Zahlungen leisten. Des Weiteren wird in das Nutzungsverhältnis eine „Datenschutzrichtlinie“ sowie eine „Cookie-Richtlinie“ einbezogen.

Die Beklagte verarbeitet die personenbezogenen Daten ihrer Nutzer, die bei Benutzung ihrer Netzwerke erfasst werden (sogenannte „On-Plattform“-Daten), insbesondere Informationen, die der Nutzer bei der Registrierung und Erstellung eines Profils bereitstellt wie beispielsweise Namen und E-Mail-Adresse sowie Informationen über Aktivitäten des Nutzers auf der jeweiligen Plattform, wie zum Beispiel vom Nutzer erstellte Beiträge, gesendete und empfangene Nachrichten, eingesehene Inhalte sowie sonstige Interaktionen. Darüber hinaus werden App-, Browser- und Geräteinformationen, genutzte Software sowie weitere Identifikatoren des Gerätes zur Unterscheidung von Geräten anderer Nutzer, Signale von dem Gerät, Informationen zur Netzwerkverbindung des Geräts einschließlich IT-Adresse und standortbezogene Informationen erfasst, überdies Informationen über Kontakte des Nutzers und deren Nutzungsverhalten innerhalb der Netzwerke der Beklagten sowie schließlich auch Informationen über den Nutzer soweit sie auf der Aktivität anderer Nutzer basieren (vgl. Anlage „Datenschutzrichtlinie“ K3, Seiten 6 ff.). Darüber hinaus bietet die Beklagte 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 bestimmte Daten mit der Beklagten jedenfalls nach Maßgabe von Nutzungsbedingungen teilen. Zu diesen Tools gehören die Applikationen „Meta-Pixel“, „Conversions-API“, „Facebook-SDK für App-Events“, „Offline-Conversions“ und „App Events API“ mit den 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 ein dem jeweiligen registrierten Nutzer Facebook oder Instagram zuzuordnen.

Die von der Beklagten und den Drittanbietern zur Verfügung gestellten Tools werden - für den Nutzer nicht oder nicht ohne Weiteres erkennbar - in zahlreichen reichweitenstarken Internetseiten eingebettet, hierzu zählen etwa Nachrichtenseiten, Webseiten von Reiseanbietern,

Shopping-Portale, Webseiten zu Finanzthemen, Webseiten und Apps zur Information zu Gesundheitsfragen anbieten, Dating- und Erotikseiten sowie Seiten zu anderen Themen. Über die vorgenannten Business-Tools können an die Beklagte sogenannte „Off-Plattformen“ - Daten, die sie über die zuvor dargestellten „On-Plattformen“ - Daten hinaus verarbeiten kann, übermittelt werden. Zu den Informationen, welche die Beklagte über Meta Business Tools von Drittanbietern erhalten kann, gehören sogenannte Kontaktinformationen, mit denen Einzelpersonen identifiziert werden können, z. B. Namen, E-Mail-Adressen, Telefonnummern in „gehashter“ (verschlüsselter) Form und außerdem sogenannte „Event-Daten“ mit Informationen über Nutzeraktionen auf Dritt-Webseiten, wie z. B. das Aufrufen einer Seite, die Installation von Apps oder auch der Kauf von Produkten (vgl. Anlage B4 „Nutzungsbedingungen für Meta-Business-Tools“). Die vorgenannten Nutzungs- und Datenverarbeitungsbedingungen regeln gemeinsam mit weiteren Regelungswerken wie etwa den „unzulässigen Informationen“ (Anlage B5), welche Informationen Drittanbieter mit der Beklagten teilen dürfen.

Im Rahmen der zugehörigen Nutzungsbedingungen verpflichtet die Beklagte Dritte, 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 und verlangt deshalb von dem Dritten 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.

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

Einzelne Einstellungen sollen dem privaten Nutzer dabei zur Kontrolle der Nutzung der Daten von Dritt-Webseiten und -Apps durch die Beklagte die Möglichkeit geben, sogenannte optionale Cookies in anderen Apps und auf anderen Webseiten zu teilen, bzw. das Setzen solcher Cookies nicht zu erlauben sowie über die Einstellung „Informationen von Werbepartnern zu Aktivitäten verwenden, um Werbung anzuzeigen“ zu entscheiden. So soll die voreingestellte Verwendung optionaler Cookies deaktiviert und - unabhängig davon - die Erlaubnis erteilt wer-

den, Informationen von Werbepartnern für 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 Dritt-Webseiten und -Apps erhobenen Daten nicht, um den Nutzer relevante Werbung anzuzeigen.

Der Kläger hat in den Einstellungen eine Erlaubnis zur Verwendung von Information zur Anzeige personalisierter Werbung nicht erteilt. Er hat in den Einstellungen eine optionale Einwilligung zum Setzen der Cookies erteilt.

Die Datenschutzrichtlinie der Beklagten und die Angaben auf ihrer Webseite bei den Einstellungen geben an, dass die mittels Business Tools übermittelten Daten von der Beklagten dann, wenn die vorgenannten Einwilligungen nicht erteilt werden, nicht zum Zweck der Bereitstellung personalisierter Werbung für diesen Nutzer. Die Daten können aber nach den eigenen Angaben der Beklagten in eingeschränktem Umfang zu anderen Zwecken verarbeitet, gespeichert und genutzt werden, etwa zum Schutz der Sicherheit und Integrität ihrer Server sowie auch zur Messung der Effizienz von Werbekampagnen. Der Nutzer kann durch die Deaktivierung der vorgenannten Einstellungen nicht verhindern, dass die Beklagte über Dritte generierte Daten erhält.

Nutzer haben ferner die Möglichkeit, sich in den Einstellungen Informationen über ihre Aktivitäten, die Drittunternehmen mit der Beklagten geteilt haben, in eingeschränktem Umfang anzeigen zu lassen. Darüber hinaus besteht auch die Möglichkeit, die von Drittunternehmen geteilten Daten von ihrem Nutzerkonto zu trennen und - bezogen auf konkrete Drittunternehmen - eine Verknüpfung von Informationen mit ihrem Nutzerkonto für die Zukunft auszuschließen, wobei die Daten unstreitig infolge der Trennung nicht gelöscht werden. Die vorgenannte Einstellung verhindert auch nicht, dass die Beklagte weiterhin Daten von Drittunternehmen enthält; es wird lediglich keine Verknüpfung mit dem Nutzerkonto vorgenommen. Die Beklagte ist ferner dem Vortrag des Klägers, dass es ihr technisch möglich sei, die Trennung nachträglich wieder aufzuheben, nicht entgegengetreten.

Der Kläger hat in erster Instanz seine Anträge auf Unterlassung und immaterielle Entschädigung sowie Erstattung vorgerichtlicher Anwaltskosten damit begründet, dass nach Übertragung von Daten an die Beklagte mittels Business Tools, die entweder auf dem Rechner des Nutzers oder den Servern von Webseiten und App-Betreibern laufen, ein Abgleich erfolge, durch den die Beklagte ermittle, wessen personenbezogene Daten sie durch Business Tools gesammelt, an ihre Server übertragen lassen und bereits verarbeitet habe. Die Daten des Klä-

gers verarbeite die Beklagte automatisch ohne jede Unterscheidung ebenso 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, gespeichert und auch in anderer Weise verarbeitet werden. Die Beklagte gebe ihm keine Möglichkeit, diese Nutzung, Speicherung und Verarbeitung zu beenden, die stets statfinde und nicht berücksichtige, ob der Kläger hierin eingewilligt habe oder ob er seinen Account weiter betreibe oder lösche. Der Vortrag der Beklagten, der sich letztlich auf allgemeine Behauptungen zu Verträgen mit unbenannten Dritten verweise, in denen diese sich verpflichteten, wirksame Einwilligungen mit den Nutzern einzuholen, sei unsubstantiiert und nicht einlassungsfähig. Rechtfertigungsgründe für die Datensammlung und Speicherung bestünden nicht; spätestens bei der Verarbeitung auf ihren eigenen Servern sei die Beklagte auch nicht mehr „gemeinsam verantwortlich“ im Sinne des Art. 26 DSGVO und könne sich auf eine gegenüber diesen etwa erteilte Einwilligung nicht mehr berufen. Die Auskunftsansprüche des Klägers seien nicht erfüllt, weder mit dem Schreiben vom 11.08.2025 (Anlage B7) noch durch die Schriftsätze der Beklagten im Rechtsstreit.

Die Beklagte hat in Abrede gestellt, dass von Dritt-Webseiten oder Dritt-Apps stammende personenbezogene Daten des Klägers in rechtswidriger Weise für personalisierte Werbung von ihr verarbeitet würden. Die Klage sei unsubstantiiert. Es fehle an einer konkreten Darlegung einer Datenverarbeitung durch die Beklagte. Art und Umfang der Verarbeitung von Off-Plattformen-Daten hingen von der jeweiligen technischen Implementierung in den Meta Business Tools für die Drittunternehmen sowie von den Entscheidungen und Einstellungen der Nutzer auf den Seiten der Drittunternehmen ab.

Wegen des weiteren Vorbringens der Parteien wird auf die erstinstanzlichen Schriftsätze Bezug genommen, mit dem das Landgericht die Klage abgewiesen hat. Zur Begründung hat das Landgericht ausgeführt, dass die zulässige Klage unbegründet sei. Die Beklagte habe eine Datenverarbeitung bestritten. Eine Betroffenheit des Klägers lasse sich allein aus der Darlegung des Geschäftsmodells der Beklagten nicht ableiten. Der Kläger habe Kenntnis davon, hinsichtlich welcher Webseiten und Apps es zur aus seiner Sicht unzulässigen Datenverarbeitung gekommen sei, während die Beklagte keine Kenntnis darüber habe, welche Webseiten der Kläger nutze. Es habe dem Kläger obliegen, vorzutragen, wann er welche Webseiten genutzt habe und dass dabei personenbezogene Daten des Klägers verwendet worden sind; erst dies hätte eine sekundäre Darlegungslast der Beklagten ausgelöst. Auch in seiner persönlichen Anhörung durch das Landgericht habe der Kläger den behaupteten datenschutzrechtlichen Verstoß weder zeitlich noch inhaltlich eingrenzen können. Auch wenn er angegeben ha-

be, auch auf sensiblen Webseiten zur Gesundheit und sexuellen Orientierung gewesen zu sein, beinhalte dies noch keine Behauptung und keinen Beleg dafür, dass es dabei zum Einsatz der Business Tools gekommen ist. Es sei unstrittig, dass die Beklagte die Verarbeitung von Daten über die Business Tools von einer Einwilligung des Nutzers abhängig mache. Die Behauptung, die Beklagte spioniere das Privatleben derjenigen Nutzer, die bei Facebook oder Instagram angemeldet seien, durch ein sogenanntes „Finger-Printing“ aus, entbehre jeder konkretisierten Grundlage. Zudem fehle es an einer Rechtsgrundlage für einen Unterlassungsanspruch. Hinsichtlich der weiteren Einzelheiten und insoweit, wie das Landgericht wegen fehlender Konkretisierung der besuchten Webseiten und wegen des Fehlens eines Schadens auch die Zahlungsklage abgewiesen hat, wird auf die Entscheidungsgründe der angefochtenen Entscheidung Bezug genommen.

Hiergegen wendet sich der Kläger mit seiner Berufung, mit der er die erstinstanzlich gestellten Anträge vollständig weiterverfolgt.

Das Landgericht habe verkannt, dass sich die Klage nicht gegen einzelne, konkrete Datenverarbeitungen richte, sondern gegen die generelle Anwendung der Software Business Tools auf den Kläger und die von ihm nicht abstellbaren Voreinstellungen hinsichtlich der Verarbeitung seiner personenbezogenen Daten durch diese Software, da dies die beständige Gefahr der Nachverfolgung und Protokollierung seines digitalen Privatlebens mit sich bringe. Der Antrag auf Unterlassen der Datenverarbeitung stütze sich primär auf §§ 1004 Abs. 1 S. 2 BGB analog, 823 Abs. 1 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG und sei begründet; die Nennung einzelner vom Kläger aufgesuchter Webseiten sei nicht notwendig und auch nicht möglich. Der auf Zahlung immateriellen Schadensersatzes gerichtete Antrag sei nach Art. 82 DSGVO begründet. 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. Diese gingen mit einem vollständigen Kontrollverlust des Klägers über seine Daten einher; er könne nicht mehr wissen, was die Beklagte über ihn weiß, müsse jedoch damit rechnen, dass dieses Wissen sehr weitgehend sei. Die Beklagte verweigere die Auskunft hierzu. Die Beklagte bestreite 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, sondern sie bestreite lediglich die systematische Verarbeitung von Daten des Klägers zur Bereitstellung von personalisierter Werbung an diesen zu nutzen. Dies führe zu erheblicher Unsicherheit des Klägers. Deswe-

gen 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 beantragt,

das erstinstanzliche Urteil des Landgerichts Dresden vom 26.11.2025 abzuändern, neu zu fassen und

1. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers mit Hilfe der Meta Business Tools zu erfassen, an die Server der Beklagten weiterzuleiten, die Daten dort zu speichern und anschließend zu verwenden,
2. die Beklagte zu verurteilen, an ihn eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt werde, die aber mindestens 5.000,00 Euro betrage, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem 10.07.2024, zu zahlen, und
3. die Beklagte zu verurteilen, ihn von vorgerichtlichen Rechtsanwaltskosten i. H. v. 887,03 Euro freizustellen.

Die Beklagte beantragt,

die Berufung zurückzuweisen.

Sie verteidigt das angefochtene Urteil und hält die Klageanträge überwiegend für zu unbestimmt und damit unzulässig. Eine Datenverarbeitung zur Bereitstellung personalisierter Werbung erfolge nur, wenn ein Nutzer eine Einwilligung erteilt habe. Anderenfalls könne eine solche Datenverarbeitung nicht erfolgen. Wenn Werbepartner Aktivitäten eines Nutzers außerhalb der Plattform der Beklagten übermittelten, erfolge ein Abgleich zur Feststellung, ob der Nutzer in ihren sozialen Netzwerken registriert sei und welche Einstellungen er vorgenommen 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 Webseite 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 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, 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 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. 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 obliegen, kon-

kret 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; eine sekundäre Darlegungslast treffe die Beklagte nicht.

Von Dritten erhobene Daten würden 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 spielen, 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 behandle.

Hinsichtlich des weiteren Sach- und Streitstandes wird auf die wechselseitigen Schriftsätze nebst Anlagen und das Protokoll der mündlichen Verhandlung Bezug genommen.

B.

Die Berufung des Klägers ist zulässig und teilweise begründet. Der Kläger hat einen durchsetzbaren Anspruch auf die begehrte Unterlassung. Zudem steht ihm ein Anspruch auf Zahlung von 1.500,00 EUR zu. Darüber hinaus hat seine Klage keinen Erfolg.

I.

Die Berufung ist zulässig. Sie wurde form- und fristgerecht eingelegt und in gleicher Weise mit einer Begründung versehen. Die internationale Zuständigkeit deutscher Gerichte hat das Landgericht zutreffend gemäß Art. 79 Abs. 2 Satz 2 DSGVO angenommen. Der sachliche, räumliche und zeitliche Anwendungsbereich der am 25.05.2018 in Kraft getretenen DSGVO ist eröffnet. Daneben folgt die internationale Zuständigkeit auch aus Art. 18 Abs. 1 EuGVVO.

II.

Die Klage ist hinsichtlich des Unterlassungsanspruchs (nachfolgend Nummer 1) im vollen Umfang begründet. Schadenersatz steht dem Kläger aber nur in Höhe von 1.500,00 EUR zu (nachfolgend Nummer 2). Ersatz vorgerichtlicher Anwaltskosten kann der Kläger nicht verlangen (nachfolgend Nummer 3).

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

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 nachstehend aufgezeigt – 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 al-

ler auf dem europäischen Markt zugelassener Anwendungen – und somit auch Social-Media-Plattformen – gewährleisten soll. Würde man den Kläger auf das Löschen seines 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 unstreitig nicht.

Der Antrag ist zudem begründet, weil der Kläger einen Anspruch auf die Unterlassung hat. 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 (nachfolgend Nummer 1.1) sowie aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 2 GG (nachfolgend Nummer 1.2), jeweils i.V.m. § 1004 Abs. 1 S. 2 BGB (analog).

- 1.1. Die Voraussetzungen für einen Unterlassungsanspruch aus § 823 Abs. 2 BGB i.V.m. Art. 5 Abs. 1 lit. a und lit. c, Art. 6 Abs. 1 DSGVO Artikel 5 Abs. 1 lit. a und lit. c, Art. 6 Abs. 1 DSGVO sind Schutzgesetze i. S. v. § 823 Abs. 2 BGB liegen vor. Der Kläger ist von der Datenerhebung und -verarbeitung mittels Business Tools, die die Beklagte verantwortet, mit seinen personenbezogenen Daten betroffen (nachfolgend Nummer 1.1.1). Diese Datenverarbeitung ist rechtswidrig (nachfolgend Nummer 1.1.2). Die Beklagte ist als Störerin passivlegitimiert (nachfolgend Nummer 1.1.3). Die Gefahr weiterer Beeinträchtigungen i.S.d. § 1004 Abs. 1 S. 2 BGB ist gegeben (nach-

folgend Nummer 1.1.4). Einer Berücksichtigung etwaiger künftiger Rechtfertigungsgründe bedarf es nicht (nachfolgend Nummer 1.1.5).

- 1.1.1. 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. In Auslegung des Klagebegehrens sind vorliegend sämtliche Datenverarbeitungsvorgänge streitgegenständlich, welche über die von der Beklagten bereitgestellten Business Tools veranlasst worden sind und personenbezogene Informationen des Klägers betreffen, nicht hingegen nur – wie die Beklagte trotz eindeutigen und vielfach wiederholtem Vortrag des Klägers unzutreffend darstellt – die anschließende Verwendung dieser Daten zu Werbezwecken. Dies ergibt sich schon aus dem Wortlaut der Sachanträge des Klägers und aus dessen Vortrag in erster und zweiter Instanz.

Bei dem vom Kläger in seinem Auskunftsverlangen in der Klageschrift aufgeführten Daten handelt es sich um „personenbezogene Daten“ im Sinne der Legaldefinition in Art. 4 Nr. 1 DSGVO (vgl. oben). 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. 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. (vgl. EuGH, Urteil vom 20.12.2017, Az.: C-434/16, Rn. 34 f., juris; BGH, Urteil vom 18.12.2025, Az.: I ZR 115/25, m.w.N., Rn. 22 ff., juris). Die über Meta Business Tools übermittelten Daten, zu denen etwa Namen, E-Mail-Adressen, Telefonnummern, Geburtsdatum, IP-Adresse oder Geräteinformationen zählen, sind zur Identifizierung des Nutzers unstreitig geeignet. 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, Az.: 9 O 2615/23, Rn. 106, juris mit Verweis auf den Beschluss des Bundeskartellamts vom 06.02.2019, Az.: B6-22/16, Rn. 575 ff.; abrufbar unter <https://www.bundeskartell->

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).

Die Voraussetzungen einer Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO liegen ebenfalls vor. Hierzu zählen das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten. In tatsächlicher Hinsicht ist unstreitig, dass die in Webseiten und Apps von Drittunternehmen eingebundenen Business-Tools der Beklagten die Daten der Besucher und Nutzer verarbeiten.

Der Kläger ist nach seinem Vortrag von dieser Verarbeitung personenbezogener Daten durch die Business Tools der Beklagten betroffen. Unstreitig verfügt er über einen Account bei dem von der Beklagten betriebenen sozialen Netzwerk „Instagram“. Er hat sowohl schriftsätzlich als auch ergänzend im Rahmen seiner informatorischen Anhörung vorgetragen, dass er das Internet mit verschiedener Webseiten bzw. Themen nutzt. 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 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:

- 1.1.1.1. 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 mindestens einen Account bei dem von der Beklagten betriebenen sozialen Netzwerk „Instagram“.

Der Kläger hat in seiner persönlichen Anhörung vor dem Landgericht angegeben, dass er online auch sensible Websites etwa zur Gesundheit oder sexuellen Orientierung nutze.

Es ist dem Kläger grundsätzlich nicht zumutbar, detaillierter zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten Webseiten vorzutragen. Zum einen lässt sich für den Privatanutzer 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.

Zudem hat der Kläger schriftsätzlich 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 Beklagte 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 „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. Ihr Bestreiten beschränkt sich nur auf das Ziel der Verarbeitung, indem sie geltend macht, dass dies nicht zum Zwecke der Erstellung personalisierter Werbung für den Kläger erfolge.

Der Kläger hat in den Anlagen K 4 und K 5 eine dreistellige Anzahl bekannter und vielgenutzter Internetseiten aufgelistet, auf denen seine Rechtsanwälte beispielsweise den Dienst „Meta Pixel“ hätten nachweisen können; insgesamt seien die Business Tools der Beklagten auf etwa 30 Prozent aller Webseiten weltweit und einer großen Zahl beliebter Apps aktiv. Dem ist die Beklagte lediglich insoweit entgegengetreten, dass sie bei einzelnen 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 unstrittig. 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 ausnahmslos sein Einverständnis mit der Verarbeitung seiner personenbezogenen Daten verweigert hätte. Weder das eine noch das andere ist feststellbar. Vielmehr hat die Beklagte nicht konkret in Abrede gestellt, dass - wenngleich möglicherweise entgegen der Nutzungsbedingungen - eine nicht ordnungsgemäße Installation von Business Tools durch Drittanbieter dazu führen kann, dass Kontaktinformationen oder Eventdaten der Nutzer auch ohne Einwilligung des Nutzers an die Beklagten übertragen werden.

- 1.1.1.2. Der Beklagten ist substantiierter Gegenvortrag möglich und zumutbar, weil die behaupteten Tatsachen in ihrem Wahrnehmungsbereich liegen. Entscheidend ist, dass die Beklagte nicht in Abrede stellt, anhand ihres eigenen Systems und der Abfrage der Nutzerkonten ohne weiteres überprüfen und darlegen zu können, ob und gegebenenfalls welche Daten ihr von welchen Drittseiten oder -Apps übermittelt wurden. Der Kläger kann hingegen nicht mit zumutbarem Aufwand ermitteln 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 mit der Anlage B 7 und ihrem Vortrag im Rechtsstreit 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. Die Beklagte hat ebenso wenig vorgebracht, auf welchen Webseiten und Apps ihre Business Tools zum Einsatz kommen. Die Hinweise der Beklagten in den Auskunftsschreiben auf ihr Selbstbedienungstool „Deine Aktivitäten außerhalb der Meta Technologien“ genügen 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 Hamm a.a.O. Rn. 82 ff.; LG Lübeck, Urteil vom 27.11.2025, 15 O 15/24, Rn 92, juris). Die Parteien tragen außerdem übereinstimmend vor, es seien (nur) „Zusammenfassungen“ über das Tool abrufbar (vgl. für die Beklagte Seite 45 des Schriftsatzes vom 24.10.2025). Soweit der Kläger schließlich behauptet, dass das Tool nur über Aktivitäten informiere, die stattgefunden haben, als er auf demselben Gerät zugleich in einem Netzwerk der Beklagten eingeloggt war, hat die Beklagte

dies nicht bestritten. Eine substantiierte Offenlegung der tatsächlich verarbeiteten Daten erfolgt 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.

- 1.1.1.3. 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 werden jedoch nicht geschildert. Die Beklagte übernimmt insoweit auch keine Verantwortlichkeit für das Verhalten der Drittwebseitenanbieter. Unstreitig ist zwischen den Parteien mithin, 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 nicht nur, dass auch ohne vorherige Zustimmung der Webseitenbesucher oder App-Nutzer Daten an die Beklagte übermittelt 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 20, 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 der Parteivortrag der Beklagten bestätigt 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 nur 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, Seite 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“ Informationen 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 1).

- 1.1.1.4. 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 20) belegt (vgl. OLG Dresden, Urteil vom 03.02.2026, 4 U 292/25, Rn. 164, juris).

Ohne Erfolg beruft sich die Beklagte überdies darauf, sie habe freiwillig Maßnahmen wie eine Kategorisierung der Datenquellen, eine automatisierte Filterung sowie erweiterte Datenbeschränkungen (z.B. „Core Set-up“) implementiert, die dazu dienen sollen, den Erhalt und die Nutzung potentiell sensibler Daten zu verhindern. Dass diese Maßnahmen vor der Übertragung sensibler Daten an die Beklagte bei einer automatisierten Datenverarbeitung mittels Business-Tools ausreichend Schutz bieten, erscheint bereits deshalb zweifelhaft, weil die Beklagte an anderer Stelle vorträgt, nur die Drittunternehmen hätten die Möglichkeit, 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, was die Beklagte selbst nicht kontrolliere.

- 1.1.1.5. 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, Urteil 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 Drittunternehmen 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 4, Nutzungsbedingungen unter Nummer 5 a. ii.). Aus denselben Gründen kann sich die Beklagte auch nicht darauf berufen, entsprechend ihrer Nutzungsbedingungen unter Nummer 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 4, Nutzungsbedingungen unter Ziff. 5. a. i). Nimmt eine Stelle – wie hier die Beklagte – aus Eigeninteresse auf die Verarbeitung Einfluss und wirkt auf die-

se 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 Drittunternehmen ihre Business Tools anbietet, mit deren Hilfe sie unstreitig möglichst viele Daten der Drittseitenutzer für ihre eigenen Zwecke 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).

1.1.2. 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 als der 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.

1.1.2.1. 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 Datenver-

arbeitungsvorgänge allerdings nicht hinreichend 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 und noch verarbeitet. Insofern bleiben Überlegungen zu einer möglichen Rechtfertigung spekulativ.

1.1.2.2. Unabhängig davon greifen die von der Beklagten benannten Erlaubnistatbestände auch aus anderen Gründen nicht. 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.

1.1.2.2.1. Die Beklagte stützt sich auf eine Einwilligung ihrer Nutzer nur, um eine Personalisierung von Werbung zu rechtfertigen. Eine derartige Einwilligung erhält 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.

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 nicht hierauf stützt – 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.

- 1.1.2.2.2. 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.

- 1.1.2.2.3. 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 Verantwortli-

chen 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 eigenständige 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 könn-

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

- 1.1.2.2.4. 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, 56. Ed., DS-GVO Art. 6 Rn. 56, beck-online).
- 1.1.2.2.5. 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 festzu-

stellen.

- 1.1.2.2.6. 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 streitgegenständlichen Business Tools übermittelt wurden, um die Sicherheit und Integrität ihrer Server und Systeme vor böswilligen 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. An nachprüfbaren Kriterien für die Daten-Speicherung fehlt es demnach.

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 sol-

chen 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.

- 1.1.2.2.7. 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.

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.

1.1.2.2.8. 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.

1.1.3. 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; Datenabgleich und -speicherung führt sie selbst durch. Insofern ist ihr Verhalten für jede der angegriffenen Formen der Datenverarbeitung ursächlich (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, Rn. 153, beck-online; 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.).

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 die unmittelbare Ursache der Beeinträchtigung des Klägers in einem 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 Business Tools eine ausreichende Rechtsgrundlage vorliegt.

- 1.1.4. 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.).
- 1.1.5. Die Einschränkung der Unterlassungsverpflichtung mit Blick auf eine möglicherweise noch in der Zukunft erteilte Einwilligung oder einen sich in der Zukunft ergebenden

den 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, sollte der Kläger gleichwohl trotz nach Schluss der mündlichen Verhandlung erteilter Einwilligung das Urteil vollstrecken, kann dies die Beklagte ggf. durch eine Vollstreckungsabwehrklage nach § 767 Abs. 2 ZPO abwehren, 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 Unterlassungsanspruchs 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 Dresden, Urteil vom 12.03.2026, 17 U 625/25, a.a.O. Rn. 157).

- 1.2. 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 oben stehenden Ausführungen verwiesen.
2. Der Antrag zu Nummer 2 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.

- 2.1. 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).

- 2.1.1. 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 Nummer 1 Bezug genommen.
- 2.1.2. Dem Kläger ist ein immaterieller Schaden entstanden.
- 2.1.2.1. Der Begriff des immateriellen Schadens ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (EuGH, Urteil vom 04.09.2025, C-655/23; BGH, Urteil vom 12.05.2026, VI ZR 375/24, Rn. 37). 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

len Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern (BGH, a.a.O., Rn. 42).

- 2.1.2.2. 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 Behörden 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 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).

- 2.1.3. 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 sozialen 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.
- 2.1.4. 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.
- 2.1.5. 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. Da-

nach 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).

Unter Berücksichtigung der Angaben des Klägers dazu, dass er auch Internetseiten nutze, die Fragen der Gesundheit oder sexuellen Orientierung betreffen, er sich aber ausspioniert fühle, zeigt auf, 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.

Das durch die von dem Kläger in seiner Anhörung vor dem Landgericht trotz seiner 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 immateriell-

len 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 Be-

obachtung 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.

- 2.1.6. 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 hinreichend individualisierbaren Anhaltspunkte vorgetragen.
- 2.2. 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), 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).

- 2.3. Dem Kläger stehen gemäß den §§ 291, 288 Abs. 1 S. 2, 187 Abs. 1 (analog) BGB Rechtshängigkeitszinsen ab dem Tag nach der Zustellung (24.02.2025) zu. Ein weitergehender Zinsanspruch mit Blick auf die unter Fristsetzung erfolgte außergerichtliche Aufforderung des Klägers vom 02.07.2024 zur Zahlung einer Entschädigung in Höhe von 5.000,00 Euro (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).
3. 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 aufgrund der vorhandenen Erfahrungen seines Rechtsanwaltes 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 nicht nachgelassene Schriftsatz des Klägers vom 07.07.2026 bietet keinen Anlass zur Wiedereröffnung der mündlichen Verhandlung.

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 hinsichtlich der Verurteilung der Beklagten zu Ziffer I des Tenors beschränkt auf die Verpflichtungen, es zu unterlassen, personenbezogene Daten des Klägers mithilfe der Meta Business Tools zu erfassen und an die Firma der Beklagten weiterzuleiten gemäß § 543 Abs. 2 Nr. 2 ZPO zur Sicherung einer einheitlichen Rechtsprechung die Revision zu. Wie sich aus den Ausführungen unter Ziffer II der Gründe ergibt, werden zu diesen Verurteilungen streitentscheidende Rechtsfragen von den Oberlandesgerichten nicht einheitlich beurteilt.

Der Senat setzt den Streitwert im Wege des Beschlusses unter geringfügiger Abänderung der erstinstanzlichen Streitwertfestsetzung für beide Instanzen auf 5.500,00 EUR fest (Anträge zu 2: 500,00 EUR, Antrag zu 1: 5.000,00 EUR).