



Landgericht Ellwangen (Jagst)

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:

Rechtsanwälte **BRR Verbraucherschutz Rechtsanwaltsgesellschaft mbH**, Viktoria-Luise-Platz 7, 10777 Berlin, Gz.: DTS-000058-24

gegen

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

- Beklagte -

Prozessbevollmächtigte:

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

hat das Landgericht Ellwangen (Jagst) - 2. Zivilkammer - durch die Richterin _____ als Einzelrichterin aufgrund der mündlichen Verhandlung vom 09.04.2025 für Recht erkannt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 09.08.2023 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Instagram" unter dem Benutzernamen _____ der Klagepartei verknüpft hat, dies insbesondere, aber

nicht ausschließlich durch die „Meta Business Tools“,

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

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

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

die URLs der Webseiten samt ihrer Unterseiten

- der Zeitpunkt des Besuchs

- der Referrer (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),
- die auf der Webseite angeklickten Buttons sowie
- weitere von der Meta „Events“ genannte Daten, die die Interaktionen auf der jeweiligen Webseite dokumentieren

c. in mobilen Dritt-Apps

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

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 09.08.2023 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat, unter Benennung dieser Dritten,

ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte seit dem 09.08.2023 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

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

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 09.08.2023 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 09.08.2023 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.

3. Die Beklagte wird verurteilt, an die Klagepartei 10.000,00 €, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz aus 1.500,00 € seit dem 31.01.2024, aus weiteren 8.500,00 € seit dem 23.08.2024 zu zahlen.
4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 Euro freizustellen.
5. Die Beklagte hat die Kosten des Rechtsstreits zu tragen.
6. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

Tatbestand

Der Kläger verlangt von der Beklagten Auskunft, Löschung der gespeicherten Daten sowie Geldentschädigung aufgrund behaupteter illegaler Datenverarbeitung der Beklagten.

Der Kläger nutzt ausschließlich privat das Netzwerk Instagram unter dem Benutzernamen [REDACTED] seit dem 09.08.2023. Er willigte nicht über die Einstellung „Informationen von Werbepartnern über deine Aktivitäten“ zur Datenverarbeitung zur Bereitstellung personalisierter Werbung ein. Betreiberin des Netzwerks, Vertragspartnerin und Verantwortliche im Sinne des Art. 4 DSGVO ist die Beklagte. Als Gegenleistung für die Nutzung des Netzwerks fordert diese kein Geld. Der Kläger wird bei Nutzung des Netzwerks Werbung angezeigt, die auf seinen Interessen basiert, welche die Algorithmen der Beklagten aus den Tätigkeiten des Klägers auf Facebook sowie den sozialen Kontakten, die er pflegt, extrahieren können. Wahlweise können die Nutzer seit Dezember 2023 ein Abo-Modell wählen, bei dem sie gegen Zahlung einer monatlichen Gebühr die Anzeige von Werbung abschalten können. Die Beklagte räumt sich nach dem unbestrittenen Klägervortrag gemäß ihrer „Datenschutzrichtlinie“ (Fassung vom 07.09.2023, Anlage K 1) das Recht ein, das Verhalten ihrer Nutzer nicht nur bei der Nutzung von deren Produkten zu analysieren, sondern annähernd im gesamten Internet und auf einer Vielzahl von mobilen Apps. Hierfür entwi-

ckelte sie verschiedene sogenannte „Meta Business Tools“, die Webseitenbetreibern und App-Entwicklern Werbeeinnahmen verschaffen können und aus diesem Grund von diesen auf ihren Webseiten und in ihren Apps eingebunden werden (vgl. Anlage B 3). Dies geschieht durch Einfügen eines einfachen Skripts im Code der Webseiten und Apps („Meta Pixel“ für Webseiten und „App Events über Facebook-SDK“ für Apps), das vom technisch durchschnittlich versierten Nutzer nicht bemerkt wird, und seit 2021 wahlweise durch Einbindung eines Skripts auf den Servern der Webseiten- und App-Betreiber („Conversions API“ und „App Events API“), wodurch die Erfassung der Daten nicht mehr auf dem Rechner des Nutzers durchgeführt und auch vom technisch versierten Nutzer nicht mehr bemerkt und auch nicht mehr verhindert werden kann. Auf zahlreichen reichweitenstarken Webseiten und Apps in Deutschland laufen „Meta Pixel“ oder „App Events über Facebook-SDK“ im Hintergrund, unter anderem bei zahlreichen großen Nachrichtenseiten und -Apps (z.B. spiegel.de, bild.de, welt.de, faz.net, stern.de), großen Reiseseiten und -Apps (z.B. tripadvisor.de, hrs.de, holidaycheck.de, kayak.de, momondo.de), Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, aerzte.de, helios-gesundheit.de, jameda.de), Dating- und Erotikseiten (parship.de, amorelie.de, orion.de, lovescout24.de), sowie Seiten mit Inhalten aus der innersten Intimsphäre (krebshilfe.de, ttfp-fertility.com (Samenbank), nie-wieder-alkohol.de, nvve.nl (Sterbehilfe; vgl. insgesamt Auflistung der Recherche der Klägervertreter in Anlagen K 2, K 13-16). Sie verarbeiten dort persönliche und höchstpersönliche Daten zur Gesundheit, zur politischen Einstellung, zur Weltanschauung, zu Finanzen sowie zur Sexualität. Nach dem unbestrittenen Klägervortrag lässt sich nicht nachvollziehen, welche Seiten und Apps die „Conversions API“ und die „App Events API“ nutzen, um die streitgegenständlichen Daten der Klagepartei auf den Servern der Webseiten- und App-Betreiber abzugreifen. Nutzer haben keine Möglichkeit, dies technisch zu überprüfen. Jeder Nutzer ist zu jeder Zeit individuell erkennbar, sobald er sich im Internet bewegt oder eine App benutzt, auch wenn er nicht bei den Netzwerken der Beklagten eingeloggt ist oder deren Apps installiert hat. Diese Erkennung erfolgt durch sogenanntes „Digital Fingerprinting“, durch welches ein Nutzer über Jahre und Jahrzehnte online nachverfolgbar ist. Zum anderen ist jeder einzelne Klick und jede Texteingabe auf solchen Dritt-Webseiten und -Apps durch die Beklagte nachverfolgbar. Diese weiß, welche Seiten- und Unterseiten wann besucht wurden, was dort angeklickt, gesucht oder gekauft wurde (vgl. Beispiele der Seiten niewiederalkohol.de, shop-apotheke.com, medikamente-per-klick.de, jameda.de, amorelie.de, Bl. 10-12 d.A.). Die angefallenen Daten sendet die Beklagte weltweit in Drittstaaten, insbesondere die USA, und gibt sie bei Bedarf an Dritte sowie an Behörden weiter.

Das „Digital Fingerprinting“ führt die Beklagte anhand der im Antrag zu 1 aufgeführten personenbezogenen Daten des Nutzers durch. All diese Daten werden im Rahmen des „Advanced Matching“ der individuellen Meta-ID zugewiesen und zusammen mit den Standortdaten des Mobilgeräts verknüpft und verwendet und so vollständig individualisiert. Aufgrund des Fingerprintings funktioniert die Zuordnung eines technischen Geräts zum Nutzer mit einer Genauigkeit von über 99 % auch dann, wenn der Nutzer seinen Account bei der Beklagten nicht nutzt bzw. nicht eingeloggt ist und ihre Cookies nicht zulässt. Entsprechend werden sämtliche Daten auch gesammelt, wenn Nutzer nicht bei ihren Netzwerken eingeloggt sind. Da die Anbieter der wichtigsten Browser (Apple Safari, Mozilla Firefox, Google Chrome) seit 2019 die Cookiesetzung von Drittanbietern stückweise unterbinden und auch die Ausführung von Skriptanwendungen zumindest im Inkognito-Modus schwieriger gemacht wird, hat die Beklagte 2021 die „Conversions API“ und die „App Events API“ eingeführt. Deren einziger Zweck besteht nach dem unbestrittenen Klagevortrag darin, unter Mitwirkung der Webseitenbetreiber und App-Anbieter alle Schutzversuche der Nutzer und der Browserhersteller zu umgehen und die - nun auch für den technisch versierten Nutzer nicht bemerkbare - Datenerhebung weiterhin zu ermöglichen; dies auch, wenn der Nutzer den Inkognito-Modus benutzt und Cookies von Drittseiten nicht zulässt und sogar dann, wenn er ein VPN (virtuelles privates Netzwerk) nutzt. Nutzer, die sich im Laufe ihres Lebens einmal auf den Netzwerken der Beklagten eingeloggt haben, kann sie zuordnen und verknüpft diese mit sämtlichen anderen aggregierten Daten. Dies wird möglich, indem sich die Conversions API serverseitig an den Server des Webseitenbetreibers anbinden lässt und von dort die für Fingerprinting notwendigen Daten sowie „analoge“ persönliche Daten wie den Namen oder die Anschrift des Nutzers in gehashter Form geben lässt, ohne dass der Nutzer dies nachvollziehen oder gar verhindern kann. Bildlich gesprochen sind Hashwerte die „Fingerabdrücke von Dateien“. Die Business Tools der Beklagten zeichnen dabei unterschiedslos die Daten aller Nutzer auf, weil in den Business Tools keine Entscheidungsmöglichkeit eingebaut ist, welche Daten verarbeitet werden und welche nicht. Sie prüfen nicht, wer vor dem Computer sitzt, sondern schicken sämtliche Daten an die Server der Beklagten. Erst dort wertet die Beklagte aus, ob sie die rechtliche Befugnis hat, die - bereits verarbeiteten - Daten zu verarbeiten. Als „Digitalen Fingerabdruck“ bezeichnet man eine Verknüpfung einer solchen Menge an im Browser (sog. „Browser-Fingerprint“) oder vom Nutzergerät (sog. „Device-Fingerprint“) abrufbaren Daten, dass es möglich wird, den jeweiligen Nutzer allein anhand dieser zu identifizieren. Eine solche Zuordnung ist nach den Feststellungen des Bundeskartellamts in über 99,24 % aller Fälle möglich (vgl. BKartA Beschluss v. 06.02.2019, Az. B6-22/16, Rn. 580, Liste der Identifizierungsparameter bei Meta Pixel, Anlage K 9 Bl. 244 - 255). Über diese persönlichen Daten kann die Beklagte dann den bereits als einzigartig identifi-

zierten Browser mit absoluter Sicherheit mit dem tatsächlichen Menschen vor dem Rechner verbinden (advanced matching). Selbst wenn keinerlei Cookies gesetzt sind, übertragen die Business Tools alle in Antrag zu 1 genannten personenbezogenen Daten, derer sie habhaft werden können, an die Beklagte. Die Beklagte kann alle Techniken - d. h. Third Party Cookies, First Party Cookies zum Aggregieren von Daten über einen langen Zeitraum ohne sofortige Zuordnung zum Nutzer, aber zum von diesem verwendeten Browser, First Party Cookies im Zusammenspiel mit der Klick-ID zur Zuordnung der aggregierten Daten zum Nutzer, Digital Fingerprinting zum Aggregieren von Daten über einen langen Zeitraum ohne sofortige Zuordnung zum Nutzer über Daten aus dem „HTTP-Header“ und IP-Adresse sowie Digital Fingerprinting bei Vorliegen von Nutzerdaten (siehe Anlage K 10, Bl. 256 - 275 d.A.) - zur Zuordnung der aggregierten Daten zum Nutzer miteinander kombinieren und somit beispielsweise die über den First Party Cookie über einen langen Zeitraum aggregierte Daten über Aktivitäten auf Drittseiten durch die einmalige Identifikation durch Digital Fingerprinting einem eindeutigen Nutzer zuordnen. Als „Events“ bezeichnet die Beklagte Nutzeraktionen, die sie aufzeichnen kann. Dies kann zum Beispiel das Aufrufen einer Seite („PageView“), das Absenden eines Suchbefehls („Search“), das Ausfüllen eines Formulars („Lead“), das in den Warenkorb Legen eines Artikels („AddToCart“) oder der Kauf eines Artikels („Purchase“) sein. Die Business Tools der Beklagten durchsuchen die Webseiten und Apps, auf denen sie aktiviert sind, selbständig nach entsprechenden Events und ändern deren Code so um, dass die Nutzung der entsprechenden Schaltflächen oder die Tastatureingaben bei jeder Nutzung an die Beklagte gesendet werden. Die Beklagte kann hierdurch „mitlesen“, was ein Nutzer auf einer Webseite oder App macht.

Um einen möglichst umfangreichen Datensatz zu erhalten, ermutigt die Beklagte Webseitenbetreiber dazu, ihr möglichst viele Informationen der Webseitenbesucher zu übermitteln. Die Webseitenbetreiber haben ebenfalls ein großes Interesse daran, der Beklagten alle verfügbaren Informationen über die jeweiligen Nutzer zu übersenden, denn je mehr Daten der Beklagten zur Verfügung stehen, desto besser gelingt die Kundenakquise. So wird es von der Beklagten offensiv beworben (Anlage K 11, Bl. 277 - 308 d.A.). Die Conversions API erfüllt die gleiche Funktion wie Meta Pixel und stellt nach Auffassung des Klägers die Reaktion der Beklagten auf die DSGVO und die zunehmende Sensibilität der Nutzer dar. Die Beklagte bewirbt die Conversions API aktiv damit, dass sie von Webseitenbetreibern eingesetzt werden soll, um Daten von denjenigen Nutzern zu erheben und an die Beklagte zu senden, welche einer Nutzung ihrer Daten nicht zustimmen (Anlage K 11, insb. S. 23, Bl. 277 - 308 d.A.). Da sie nicht in den Browser des Nutzers geladen werden muss, kann der Nutzer sie nicht abschalten. Weder ein „Inkognito-Modus“, noch eine AntiS-

py-Software noch VPN helfen hier weiter (Anlagenkonvolut K 12, Bl. 309 - 325 d.A.). Die entsprechenden Systeme nutzt sie auch bei Nutzern, die die Schaltflächen „Optionale Cookies erlauben“ und „Informationen über Aktivitäten von Werbepartnern“ nicht aktiviert haben (vgl. Beispiel einer Nutzung von spiegel.de, Replik S. 25 bis 33, Bl. 199 ff.).

Die verarbeiteten Informationen werden von den Business Tools ab dem Zeitpunkt ihrer Installation durch den jeweiligen Webseitenbetreiber unmittelbar an die Server der Beklagten weitergeleitet. Es folgen serverseitig weitere Verarbeitungsvorgänge, wie die Speicherung, der Abgleich mit den bei der Beklagten hinterlegten Datensätzen zur eindeutigen Zuordnung, ggf. eine Veränderung durch Pseudonymisierung und die weitere Verwendung. Ob die erfassten und weitergeleiteten Informationen nun im Rahmen eines Abgleichs einem Nutzer zugeordnet werden können, der mit dieser Art der Verarbeitung einverstanden war, stellt die Beklagte erst jetzt fest und entscheidet sich sodann ggf. für eine Pseudonymisierung der Daten und eine weitere Verwendung für „eingeschränkte Zwecke“. Aus den AGB der Beklagten ergibt sich, dass die Beklagte das hierfür erstellte Persönlichkeitsprofil auch zu nicht werberelevanten Zwecken nutzt. Hinsichtlich der weiteren technischen Einzelheiten der Datensammlung und -verarbeitung der Beklagten, zum Beispiel „Third Party Cookies“, insbesondere den „User Login Cookie“ der Beklagten, „First Party Cookies“, insbesondere „_fbp“ und „_fbc“ der Beklagten, die durch die Business Tools generierte interne Browser-IDs und interne Klick-IDs beinhalten, „Klick-ID“ sowie den digitalen Fingerabdruck über „automatisiertes Advanced Matching“ und „manuelles Advanced Matching“, wird auf die Ausführungen in der Replik vom 23.12.2024, Seiten 12 bis 36 Bezug genommen (Bl. 183 ff. d.A.).

Mit Anwaltsschreiben vom 02.01.2025 (Anlage K 3) machte der Kläger ohne Erfolg die Ansprüche gegen die Beklagte geltend.

Der Kläger trägt vor,

die Beklagte spioniere das Privatleben sämtlicher Nutzer aus die bei einem ihrer Netzwerke wie „Instagram“ angemeldet seien. Deren digitale Bewegungen, die diese auf Webseiten oder mobilen Apps, d.h. im gesamten Internet, unternehmen, würden rechtswidrig aufgezeichnet. Dies betreffe Daten aus der Privat- wie auch aus der Intimsphäre der Nutzer. Die technischen Methoden seien dabei dergestalt, dass inzwischen nicht mehr nur ohne, sondern auch gegen den ausdrücklichen Willen der Nutzer die Daten aufgezeichnet würden. Die Tätigkeit der Beklagten sei nicht nur illegal, sondern auch strafbar gem. § 42 Abs. 2 BDSG. In welchem Umfang die Informationen, die sie über ihre Kunden sammele, verwendet würden, sei nicht bekannt. Er könne immateriellen

Schadensersatz von mindestens 1.500,00 € verlangen für das von der Beklagten verursachte Gefühl der alltäglichen, permanenten Unsicherheit, nicht zu wissen, welcher Klick und welche Texteingabe im Internet heimlich von der Beklagten mitgelesen und weiterverarbeitet worden sei und weiterhin werde.

Durch die Einbindung der Business Tools auf Webseiten Dritter werde die Beklagte nach der Rechtsprechung des EuGHs „Verantwortlicher“ i.S.d. Art. 26 DSGVO (Rechtssache C 40/17) für sämtliche Webseiten und Apps, auf denen ihr Code laufe. Rechtlich gesehen sei sie demnach Mitbetreiberin unzähliger Webseiten und Apps. Er nutze viele Webseiten und Apps, auf denen die „Meta Business Tools“ vorzufinden seien, regelmäßig. Die Business Tools der Beklagten seien auf 30 % bis 40 % aller Webseiten weltweit und einer großen Zahl beliebter Apps aktiv bzw. allein der erkennbare Meta Pixel werde auf 30 % bis 40 % aller Internetseiten und der ganz überwiegenden Mehrzahl der meistbesuchten 100 Webseiten Deutschlands ausgeführt (vgl. Anlagen K 2 Bl. 151 - 162 d.A., K 14 - K 16 Bl. 383 - 409, Anlagenkonvolut K 13 Bl. 326 - 382). Conversions API könne nicht entdeckt werden, so dass deren Verbreitung nicht eingeschätzt werden könne. Da nur der Meta Pixel der Beklagten ausfindig gemacht werden könne, die anderen Meta Business Tools hingegen nicht, dürfe der Umfang der streitgegenständlichen Datenverarbeitung sogar weit größer sein. Bei regelmäßiger Internetnutzung könne er der Aufzeichnung durch die Business Tools daher faktisch nicht entgehen. Dass der Kläger hiervon nicht betroffen sein könnte, liege außerhalb jeder Wahrscheinlichkeit. Auf dieser und den übrigen Webseiten hätten die Business Tools die Aufgabe, den einzelnen Besucher zu identifizieren und dessen Klicks und Texteingaben zu erfassen, um sie an die Beklagte zu senden. Sie liefen im Hintergrund, ohne sich dem Besucher bemerkbar zu machen. Der Besucher sei beim Aufruf sämtlicher von ihm aufgerufenen Webseiten und Apps im Unklaren, ob die Beklagte nun gerade mitlese oder nicht. Da die Beklagte unbemerkt im Hintergrund spioniere, habe sie die alleinige Kenntnis darüber, was konkret ausgespioniert worden sei. Auch wenn der Kläger nun die Existenz und die grundsätzliche Funktionsweise der Spionagetätigkeit der Beklagten bewusst sei, könne er nicht wissen, was konkret wann auf welchen Webseiten und Apps mitgelesen worden sei und weiterhin mitgelesen werde, wie das „Profiling“ der Beklagten funktioniere und mit welchen Dritten Daten des Klägers geteilt würden.

Es sei völlig unklar, was die Beklagte mit der riesigen Datensammlung mache. Sie behaupte vor allem, sie benötige diese, um „passende Werbung“ auszuspielen. Kenntnis der Vorlieben ihrer

Nutzer habe sie jedoch schon durch Auswertung der Tätigkeiten ihrer Nutzer in ihren Netzwerken. Warum das „Anzeigen noch genauerer personenbezogener Werbung“ eine durchgehende Durchleuchtung des Privatlebens rechtfertigen solle, bleibe ihr - für die Nutzer angsteinflößendes - Geheimnis. Bezüglich der Weitergabe der Daten an Dritte nehme sie sich in ihren äußerst schwammig formulierten AGB weitgehende Rechte heraus. Sie teile die „Informationen“ der Klagepartei mit Werbetreibenden und „Audience Network-Publishern“, mit Partnern, die die „Analysedienste“ der Beklagten nutzen, „integrierten“ Partnern, Anbietern für Messlösungen, Anbietern für Marketinglösungen, allen möglichen „Dienstleistern“ und „externen Forschern“. Die Beklagte überwache den Internetverkehr der Klagepartei seit 09.08.2023 unter grober und vorsätzlicher Missachtung des europäischen Datenschutzrechts, indem sie deren persönlichen und höchstpersönlichen Daten massenweise rechtswidrig erhebe, zu einem Profil zusammenfüge (vgl. Studien in Anlagenkonvolut K 5, Bl. 190 - 216 d.A.), in unsichere Drittstaaten übertrage, dort unbefristet speichere und sich das Recht herausnehme, diese in unbekanntem Maße auszuwerten und an Dritte weiterzugeben, ohne den betroffenen Nutzer hiervon zu informieren. Der genaue Umfang der bisher ausspionierten Daten sei für den Nutzer nicht nachvollziehbar. Wann sie auf welchen Seiten und in welchen Apps welche personenbezogenen Daten ausspioniert habe, lasse sich für den Nutzer nachträglich nicht überprüfen oder nachverfolgen. Der Kläger habe die Kontrolle über die Daten und „Spuren“, die er bei der täglichen Nutzung des Internets hinterlasse und die tiefe Einblicke in seine Persönlichkeit ermöglichen, vollständig verloren.

Rechtfertigungsgründe nach Art. 6 Abs. 1 lit. a bis f DSGVO seien nicht erfüllt, insbesondere liege keine Einwilligung nach lit. a vor, auf die sich die Beklagte nach verlorenen Rechtsstreitigkeiten nur noch berufe. Eine solche sei auch nicht gegenüber Webseiten- und App-Betreibern erteilt worden. Als Datenverantwortliche könne sie die Einholung von Einwilligungen nicht an solche Dritte delegieren. Die Sammlung von Daten aus verschiedenen Quellen zur Bildung eines umfassenden Persönlichkeitsprofils sei von einer Einwilligung gegenüber dem Webseitenbetreiber ohnehin nicht gedeckt. Eine explizite Einwilligung im Namen der Beklagten, dass Daten seitenübergreifend durch diese zu einem gigantischen Persönlichkeitsprofil zusammengestellt und unbegrenzt gespeichert werden dürfen, hole auch keine Webseite ein. Die Auskunft werde von der Beklagten nur rudimentär erteilt. Seit 2019 könnten Nutzer lediglich der Anzeige personalisierter Werbung, die auf den ausgewerteten Daten beruhe, widersprechen. Eine Möglichkeit, der rechtswidrigen Sammlung und Speicherung der Daten durch die Beklagte zu widersprechen oder diese auch nur einzuschränken, bestehe nicht. Die Beklagte lösche die Daten auch nicht nachträglich. Selbst wenn ein Nutzer ein Abonnement abschließe, erhalte er zwar keine personalisierte Wer-

bung mehr, die Datenerhebung werde dennoch weiter betrieben (vgl. Anlage K 21 Bl. 417 - 419 d.A.). Die Schaltfläche „Informationen zu Aktivitäten von Werbepartnern“ ermögliche lediglich, auszuwählen, ob aufgrund der ausspionierten Daten „relevantere Werbung“ angezeigt werde. Ob solche Daten für Werbeanzeigen verwendet würden oder nicht, habe jedoch nichts damit zu tun, ob die Datenspionage selbst statfinde oder nicht. Der Kläger habe keine Einwilligung erteilt. Er wolle nicht, dass die Beklagte über ihre Meta Business Tools seine personenbezogenen Daten erfasse und weiterverarbeite. Sollte er jemals eine Einwilligung hierzu erteilt haben - gleichgültig in welcher Form -, widerrufe er diese. Unsubstantiiert sei die Behauptung der Beklagten, dass dritte Webseitenanbieter eine wirksame Einwilligung einholen würden. Eine solche sei nie wirksam eingeholt worden.

Dem Kläger stehe ein Anspruch auf Löschung und Anonymisierung zu gem. 17 Abs. 1 DSGVO. Ferner stehe ihm gegen die Beklagte ein Anspruch auf Geldentschädigung nach §§ 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG und §§ 280 Abs. 1, 241 Abs. 2 BGB und hilfsweise aus Art. 82 Abs. 1 DSGVO aufgrund Verstoßes gegen Art. 6 Abs. 1 und Art. 5 Abs. 1 lit. a) DSGVO für die jahrelange, vorsätzlich durchgeführte Protokollierung des digitalen Lebens der Klagepartei in fünfstelliger Höhe zu, der hier geltend gemachte Anspruch i.H.v. 1.500,00 € stelle den absoluten Mindestanspruch dar, welcher unabhängig vom Umfang und der Sensibilität der konkret gesammelten Daten des Klägers bestehe. Der Schaden sei anders als im „Datenleck“ nicht der „Schmerz“ in seiner auf einzelne Daten bezogenen Ausprägung. Dementsprechend sei die Forderung auf Ausgleich des immateriellen Schadensersatzes keine Forderung von „Schmerzensgeld“, vielmehr sei Ausgleich zu leisten für die tiefgreifende, objektive Verletzung des allgemeinen Persönlichkeitsrechts in seiner Ausprägung der informationellen Selbstbestimmung durch die „Spionagetätigkeit“ der Beklagten an sich. Dementsprechend sei die konkrete psychische Beeinträchtigung der Klagepartei nicht relevant für die Bemessung der Höhe des Schadensersatzes, jedenfalls nicht für den geforderten Mindestbetrag i.H.v. 1.500,00 €. Dementsprechend sei die konkrete psychische Beeinträchtigung des Klägers nicht relevant für die Bemessung der Höhe des Schadensersatzes,

Der Kläger beschäftige sich privat durchschnittlich etwa 42 Stunden pro Monat mit sensiblen Themen im Internet (vgl. Anlage K 13). Hinsichtlich des Umfangs der erhobenen Daten treffe die Beklagte die (jedenfalls sekundäre) Darlegungs- und Beweislast sowie eine Beweislastumkehr nach Auskunftsverweigerung. Einer weitergehenden Darstellung welche Webseiten er besuche, bedürfe es daher auch nicht. Das außergerichtliche Schreiben der Beklagten vom 25.11.2024 sei

unzureichend und beantworte die konkret gestellten Fragen nicht (Anlage B 8 Bl. 148 - 171 d.A.). Die Beklagte sei selbst alleinige Verantwortliche für die Verarbeitung der Daten durch die eigenen „Meta Business Tools“.

Der Kläger beantragt zuletzt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 09.08.2023 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Instagram" unter dem Benutzernamen [REDACTED] der Klagepartei verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business Tools“,

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

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

- anon_id

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

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

c. in mobilen Dritt-Apps

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

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 09.08.2023 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat, unter Benennung dieser Dritten,

ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte seit dem 09.08.2023 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

inwieweit die Daten der Klagepartei für eine automatisierten Entscheidungsfindung einschließlich Profiling verwendet wurden und werden. Die Beklagte hat hierfür aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebte Auswir-

kung einer solchen Verarbeitung für die betroffene Person zu erteilen.

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 09.08.2023 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 09.08.2023 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.

3. Die Beklagte wird verurteilt, an die Klagepartei eine angemessene Entschädigung in Geld, deren Höhe in das Ermessen des Gerichts gestellt wird, die aber mindestens 1.500,00 Euro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 31.01.2024, zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 367,23 Euro freizustellen.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte wendet ein,

nicht die Beklagte, sondern die Drittunternehmen seien verantwortlich für Installation und Nutzung der Business Tools, für die Offenlegung von Informationen für Besucher der Webseiten oder Apps und die Erhebung und Übermittlung personenbezogener Daten über die Business Tools an die Beklagte. Sie stütze sich im Rahmen der Datenverarbeitung zur Bereitstellung personalisierter Werbung allein auf eine Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO. Sie nehme eine Datenverarbeitung zur Bereitstellung personalisierter Werbung lediglich dann vor, wenn die Klageseite ausdrücklich über die Einstellungen auf Facebook in diese Datenverarbeitung einwillinge. Der Kläger lege weder substantiiert dar noch biete er Beweis dafür an, dass sensible Daten der Klageseite tatsächlich über die streitgegenständlichen Business Tools an Meta übermittelt worden seien. Er habe zudem schon nicht vorgetragen, welche Privatsphäreinstellungen er bei Besuch von Webseiten von Drittanbietern vornehme. Auch lege der Kläger keine Beweise dafür vor, dass die Datenverarbeitung zur Bereitstellung personalisierter Werbung besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO („BKD“) umfasse oder offenlege. Es werde bestritten, dass die Business Tools der Überwachung der Privatleben der Nutzer dienten. Drittunternehmen, die Business Tools nutzten, seien an die Nutzungsbedingungen (Anlage B 5 Bl. 36 - 42 d.A.) gebunden, die das Teilen von sensiblen Daten untersagten (Anlage B 6 Bl. 13 - 14 d.A.). Wenn ein Nutzer das werbefreie Abonnement abgeschlossen habe, nehme sie keine

Datenverarbeitung zur Bereitstellung personalisierter Werbung vor, weil die Klageseite dann keine Werbung sehe. Nutzer, die sich entscheiden würden, Meta-Produkte weiterhin mit Werbung zu nutzen, seien über diverse Einstellungen in der Lage, Kontrolle über die Datenverarbeitung zur Bereitstellung personalisierter Werbung auszuüben. Erlaube ein Nutzer nicht, dass die Beklagte optionale Meta Cookies auf anderen Apps und Webseiten nutze, werde sie Daten, die über die Cookies und ähnliche Technologien erhoben würden, nur für eingeschränkte Zwecke, wie Sicherheits- und Integritätszwecke nutzen, einschließlich zum Zwecke der Überwachung von versuchten Angriffen auf die Systeme von Meta, wie z.B. durch die forcierte Überlastung der Webseite der Beklagten. Es sei notwendig, die über die Business Tools übermittelten Daten zu verarbeiten, um die Funktionalität und Sicherheit des Internets zu verbessern. Da die Klageseite nicht eingewilligt habe, verarbeite Meta keine Daten der Klageseite im Rahmen der Datenverarbeitung zur Bereitstellung personalisierter Werbung. Stimme ein Nutzer der Verwendung optionaler Meta Cookies auf Drittwebseiten nicht zu, werde sie Informationen dieses Nutzers, die über Cookies und ähnliche Technologien erhoben wurden, nur für begrenzte Zwecke, wie Sicherheits- und Integritätszwecke, nutzen. Zu diesen Sicherheits- und Integritätszwecken gehörten der Schutz und die Schadensverhütung (z. B. die Sicherheit von Kindern und die Bekämpfung potenzieller krimineller Aktivitäten (einschließlich gefährlicher Organisationen) und von Hassrede) sowie die Bekämpfung bestimmter bekannter Sicherheitsbedrohungen, wie z. B. die Bedrohungen der Cybersicherheit (z. B. durch Hackerangriffe, Cyberspionage). In diesen Fällen verarbeite Meta die von jedem Drittunternehmen über die streitgegenständlichen Business Tools erhaltenen Nutzerdaten, um das Risiko zu minimieren, dass böswillige Akteure eine Schwachstelle in einer einzelnen Website oder App ausnutzen, um beispielsweise einen Spam-, Scraping- oder anderen Cyberangriff durch diese Produkte auszuführen.

Der Nutzer könne Informationen über seine Aktivitäten auf Apps und Webseiten, die von Drittunternehmen mit der Beklagten geteilt worden seien, kontrollieren und abrufen. Jeder Nutzer könne auf seine Informationen zugreifen einschließlich von Informationen über Aktivitäten außerhalb von Facebook, die die Beklagte von Drittunternehmen erhalte. Die Datenübermittlung in die USA erfolge entsprechend des Datenschutzrahmens EU-USA und des dazugehörigen Angemessenheitsbeschlusses der Europäischen Kommission. Der Kläger lege nicht substantiiert dar, dass er tatsächlich Webseiten und Apps Dritter besucht habe, die eines der streitgegenständlichen Business Tools verwenden, ihre personenbezogenen Daten tatsächlich über die streitgegenständlichen Business Tools an Meta übermittelt worden seien und die Beklagte die Daten der Klageseite ohne eine gültige Rechtsgrundlage gemäß der DSGVO verarbeite. Soweit der Kläger sich gegen

andere Verarbeitungszwecke in Verbindung zu den Daten wenden wolle, die der Beklagten über die streitgegenständlichen Business Tools übermittelt wurden, konkretisiere er nicht, welche Verarbeitungszwecke er anfechten wolle. Die Ausführung im Performance Leitfaden, „die Conversions API ist nötig, um die Events von Nutzer*innen zu aggregieren, die sich gegen die Nutzung ihrer Daten entschieden haben“ sei irrelevant, da sie keinen Bezug zur Datenverarbeitung für personalisierte Werbung habe. Obwohl die Klageseite genau wisse, dass sie Daten, die über die streitgegenständlichen Business Tools übermittelt wurden, für andere Zwecke als die Verarbeitung von Daten von Drittwebseiten und -apps zur Bereitstellung personalisierter Werbung verarbeite, versäume jene es zu spezifizieren, gegen welche zusätzlichen Verarbeitungszwecke sich die Klageseite wenden wolle, und jedwede neuen Argumente darzulegen um zu substantiieren, weshalb ihre Datenverarbeitung für den jeweiligen Zweck angeblich gemäß Art. 6 DSGVO unzulässig wäre. Soweit die Klageseite andere Verarbeitungszwecke außerhalb der Verarbeitung von Daten von Drittwebseiten und -apps zur Bereitstellung personalisierter Werbung angreife, die in Bezug zu den Daten der Klageseite stehen, die Meta (angeblich) über die streitgegenständlichen Business Tools erhalten habe, spezifiziere die Klageseite keine Verarbeitungszwecke, sodass die Beklagte keine Darlegungslast treffe, bezüglich irgendwelcher anderen Datenverarbeitungen oder deren Rechtsgrundlagen auszuführen. Zur von Klägerseite dargestellten Funktionsweise der Business Tools, die für die Datenverarbeitung zur Bereitstellung personalisierter Werbung irrelevant seien, erfolge keine Erwiderung.

Der Kläger führe nicht aus, welche Webseiten und Apps Dritter er besucht oder verwendet haben soll, inwieweit er von der angeblichen Verarbeitung von Daten von Drittwebseiten und -apps zur Bereitstellung personalisierter Werbung betroffen gewesen sei - entsprechenden pauschalen Vortrag bestreite die Beklagte mit Nichtwissen - oder welchen Schaden er erlitten habe. Soweit Daten als Teil einer http-Anfrage an die Beklagte übermittelt würden, sei dies nicht verhinderbar, sondern der Funktionsweise des Internets geschuldet. Wenn Drittunternehmen weitere Daten, wie Kunden- und Eventdaten übermittelten, müssten sie zuvor eine Einwilligung einholen. Zwar sei sie mit den Drittunternehmen gemeinsam verantwortlich, nach den Datenverarbeitungsbedingungen habe sie jedoch den Drittunternehmen übertragen, die Einwilligung einzuholen (Anlagen B 10 Bl. 463 - 465 d.A., B 5 Bl. 36 - 42 d.A.). Nachdem ein Dritter Daten mittels der streitgegenständlichen Business Tools an sie übermittelt habe, stütze sie sich für die anschließende Verarbeitung der übermittelten Daten für verschiedene Zwecke als Datenverarbeiter auf eine valide Rechtsgrundlage, wie in der Datenschutzerklärung (Anlage B 10) beschrieben.

Ein Schadensersatzanspruch aus § 82 DSGVO scheide mangels Verstoß gegen die DSGVO aus. Zudem habe die Klageseite keinen tatsächlich erlittenen Schaden in Folge der Datenverarbeitung zur Bereitstellung personalisierter Werbung dargelegt oder nachgewiesen (Bl. 392 d.A.). Allein ein Verstoß gegen die DSGVO führe nicht unmittelbar zu einem Schaden. Sie bestreite, dass der Kläger eine angebliche Beeinträchtigung erlitten habe.

Hinsichtlich des weiteren Parteivortrags wird auf die Schriftsätze der Parteien nebst Anlagen in der Akte und die Niederschriften der mündlichen Verhandlung vom 09.04.2025 Bezug genommen.

Das Gericht hat zur Sache am 09.04.2025 mündlich verhandelt und die Parteien angehört. Hinsichtlich der Einzelheiten wird auf das Protokoll der mündlichen Verhandlung vom 09.04.2025 Bezug genommen.

Entscheidungsgründe

Die Klage ist zulässig und begründet.

I.

1. Die internationale Zuständigkeit des angerufenen Gerichts folgt aus Art. 82 Abs. 6 i.V.m. Art. 79 Abs. 2 Satz 2 DSGVO. Der Kläger als betroffene Person i.S.d. Norm hat seinen gewöhnlichen Aufenthalt im Bezirk des Landgerichts Ellwangen.

2. Die Datenschutz-Grundverordnung ist räumlich (Art. 3 Abs. 1 DSGVO) und, da die bei der Beklagten gespeicherten Informationen des Klägers personenbezogene Daten des Klägers enthalten, auch sachlich (Art. 2 Abs. 1 DSGVO) anwendbar. Hinsichtlich der zeitlichen Anwendbarkeit hat die streitgegenständliche Datenerhebung, -speicherung und -verarbeitung ab dem 09.08.2023 und somit auch nach dem 25.05.2018 und damit dem Zeitpunkt stattgefunden, seit dem die Datenschutz-Grundverordnung gilt (Art. 99 Abs. 2 DSGVO).

3. Die übrigen Sachurteilsvoraussetzungen liegen vor.

II.

Die Klagepartei hat gegen die Beklagte Anspruch auf die begehrte Auskunft (unter 2.) sowie Zahlung eines immateriellen Schadensersatzes im tenorierten Umfang (unter 3. und 4.). Weiterhin kann der Kläger die Löschung und Anonymisierung bereits gespeicherter personenbezogener Daten (unter 5.) sowie im zuerkannten Umfang Freistellung von vorgerichtlichen Rechtsanwaltsgebühren (unter 6.) verlangen. Bei allen Ansprüchen ist dabei inhaltlich vom nicht erheblich bestrittenen Vortrag der Klagepartei zu den technischen Abläufen auszugehen (unter 1.).

1. Insgesamt ist hinsichtlich des streitgegenständlichen Lebenssachverhalts der gesamte Klägervortrag zum Ablauf der Datenerhebung und -verarbeitung als unstreitig zugrunde zu legen, dies gilt insbesondere auch für die technischen Erläuterungen zu Art und Funktionsweise der Meta Business Tools, aber auch der Verarbeitung der erhaltenen und gespeicherten Daten zur Erstellung von Persönlichkeitsprofilen.

a) Das Bestreiten der Beklagten ist insoweit unbeachtlich. Die Beklagte bezieht sich in ihrem Vortrag auf eine Datenverarbeitung zur Bereitstellung personalisierter Werbung, die sie mangels Einwilligung des Klägers nicht durchführe. Dies ist nach dem eindeutigen Klagevortrag jedoch nicht der von dem Kläger definierte Streitgegenstand. Klageanträge wie Sachverhaltsvortrag richten sich offenkundig gegen die gesamte Datenerhebung durch die Meta Business Tools und die gesamte Datenverarbeitung bei der Beklagten angefangen von Empfangen und Speichern der Daten bis zur Erstellung von Persönlichkeitsprofilen und Weitergabe dieser Daten an Dritte, z.B. Geschäftspartner. Dabei trägt sie auch nachvollziehbar vor, dass auch ohne die unstreitig fehlende Zustimmung zur Datenverarbeitung zur Bereitstellung personalisierter Werbung diese Datenverarbeitung der Beklagten erfolgt. Insbesondere verweist sie auf das Business Tool Conversions API, das die Beklagte gegenüber Geschäftspartnern explizit damit bewirbt, dass mit diesem die gleiche Datenerhebung und -verarbeitung wie bei Meta Pixel erfolgt bei Kunden, die der personalisierten Werbung nicht zustimmen (Anlage K 11, insb. S. 23).

Dem tritt die Beklagte nicht erheblich entgegen. Einzelnes Bestreiten von aus dem Klagevortrag zitierten einzelnen Sätzen oder Passagen bezieht sich regelmäßig nur auf Formulierungen oder unterstellte Absichten wie Ziele des Ausspionierens oder Ähnliches. Vortrag zum tatsächlichen Inhalt der Datenerhebung und -verarbeitung bestreitet sie nicht. Damit ist der Klagevortrag als zugestanden anzusehen nach § 138 Abs. 3 ZPO.

Die Beklagte gesteht die streitgegenständliche Datenverarbeitung sogar ausdrücklich zu. So führt

sie aus, dass obwohl die Klageseite genau wisse, dass sie Daten, die über die streitgegenständlichen Business Tools übermittelt wurden, für andere Zwecke als die Verarbeitung von Daten von Drittwebseiten und -apps zur Bereitstellung personalisierter Werbung verarbeite, jene es versäume zu spezifizieren, gegen welche zusätzlichen Verarbeitungszwecke sich die Klageseite wenden will, und jedwede neuen Argumente darzulegen um zu substantiieren, weshalb ihre Datenverarbeitung für den jeweiligen Zweck angeblich gem. Art. 6 DSGVO unzulässig wäre. Damit stellt sie die streitgegenständliche Datenverarbeitung unstreitig und versucht allein ein Vortragsdefizit der Klägerseite zu behaupten, was jedoch nicht durchgreift.

Selbst wenn die Beklagte ihren pauschalen Einwendungen ein solches Bestreiten beimessen wollte, wäre dieses nicht erheblich, da es keinerlei substantiiertes Gegenvorbringen in den Tatsachen oder technischen Abläufen enthält. Ein Bestreiten mit Nichtwissen wäre zudem unzulässig nach § 138 Abs. 4 ZPO, da der Klagevortrag ihre eigenen technischen Programmierungen ihrer eigenen Business Tools betrifft, die sie wesentlich genauer und detaillierter kennt als der Kläger, jedoch nicht beschreibt.

b) Zudem träfe sie aufgrund ihres strukturellen Wissensvorsprungs als Urheberin und Verwenderin der Business Tools und Verantwortliche der Datenerhebung und Datenverarbeitung jedenfalls eine sekundäre Darlegungs- und Beweislast, wenn sie der Auffassung wäre, der von Klägerseite unter Bezugnahme auf wissenschaftliche und journalistische Recherchen gestützte Sachvortrag sei insgesamt oder in Einzelheiten unzutreffend. Dies behauptet sie jedoch nicht einmal. Ausdrücklich bestritten wird durchgehend, dass die Daten eines Nutzers, die über die Conversions-API von Drittunternehmen bezüglich der Aktivitäten der Klageseite auf den Websites/Apps von Drittunternehmen an Meta gesendet werden, verarbeitet werden, um diesem Nutzer auf Instagram personalisierte Werbung anzuzeigen, selbst wenn der Nutzer nicht über die Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ eingewilligt hat (Bl. 489 d.A.). Dies ist aber nicht Gegenstand des klägerischen Vortrags. Auch wäre es der Beklagtenseite ein Leichtes zu behaupten, dass sie bei Nutzern wie dem Kläger keinerlei Daten gesammelt und verarbeitet hat, wenn es denn so wäre. Auch dies behauptet sie nicht.

c) Nicht durchzugreifen vermag der Einwand der Beklagten, dass sie sich inhaltlich nicht zum technischen Sachvortrag der Klägerseite verhalten müsse, da der Kläger keine Verarbeitungszwecke bezeichnet habe, die die Beklagte unrechtmäßig verfolge, da sie sich andernfalls nicht verteidigen könne. Die vom Verantwortlichen im Sinne des § 4 Nr. 7 DSGVO verfolgten Zwecke

sind für den Nutzer als subjektive Merkmale grundsätzlich nicht oder schwer erkennbar. Zudem unterscheidet die DSGVO nicht nach Verarbeitungszwecken, insbesondere nicht bei den Rechtfertigungsgründen nach Art. 6 Abs. 1 DSGVO. Im Übrigen ist nicht erkennbar, weshalb erst aufgedeckte und vorgehaltene Verarbeitungszwecke eine Rechtsverteidigung zulassen könnten. Sollten keine Daten erhoben, diese nicht gespeichert, keine Persönlichkeitsprofile angelegt, solche oder andere persönliche Daten nicht Dritten weitergegeben werden, könnte all dies leicht behauptet werden, träfe es denn zu. Wären die Funktionsweisen der Meta Business Tools unzutreffend wiedergegeben, ließe sich das als Hersteller und Verwender dieser Tools ebenfalls korrigieren und vortragen. Weshalb eine Verteidigung nicht möglich sei, ist daher nicht nachvollziehbar.

d) Die Beklagte hat sich hingegen ausdrücklich dafür entschieden, zur von Klägerseite dargestellten Funktionsweise der Business Tools keine Erwiderung vorzutragen, da diese für die Datenverarbeitung zur Bereitstellung personalisierter Werbung irrelevant sei. Sie ist der Auffassung, sie trage keine Darlegungslast ohne Spezifikation anderer Verarbeitungszwecke, so dass sie nicht zu anderen Datenverarbeitungen oder deren Rechtsgrundlagen ausführen werde.

Mit dieser Rechtsauffassung beantwortet die Beklagte nicht die Fragen des Gerichts in der mündlichen Verhandlung, welche Daten sie erhebe, was sie mit diesen mache, wenn sie diese über die Business Tools von Drittunternehmen erhalte, ob und in welcher Art sie verarbeitet werden für eigene Zwecke, z.B. ob sie Profile wie von dem Kläger vorgetragen über die Nutzer erstelle, ob sie Angaben zum Business Tool Conversions API machen könne, für das sie damit werbe, dass hiermit Daten – wie von der Klägerseite vorgetragen – auch Daten erhoben und verarbeitet werden bei Nutzern, die keine Einwilligung in personalisierte Werbung abgeben haben zu Zwecken außerhalb der Anzeige personalisierter Werbung, usw. Die Parteivertreterin war nicht dazu bereit, diese Fragen in der mündlichen Verhandlung eingehender zu beantworten. Trotz Anordnung des persönlichen Erscheinens eines informierten Vertreters ist für die Beklagte außer dem Prozessbevollmächtigten keiner erschienen. Erheblicher Sachvortrag erfolgte daher in den mündlichen Verhandlungen hierzu nicht. Insoweit ist der detaillierte, nachvollziehbare und schlüssige Vortrag der Klägerseite zur Datenerhebung und Datenverarbeitung der Beklagten als zugestanden anzusehen und der rechtlichen Bewertung zugrunde zu legen nach § 138 Abs. 3, 4 ZPO.

e) Dem steht auch nicht der Einwand der Beklagten entgegen, dass der Kläger nicht darlege, welche Webseiten sie genau im streitgegenständlichen Zeitraum besucht habe oder weiter nutze, denn nur dann könne die Beklagte prüfen, ob diese Webseiten ihre Business Tools verwendeten. Der Kläger mit Anlagen K 2, K 13 bis K 16 umfangreich vorgetragen, dass 30 % bis 40 % der

Webseiten weltweit und die ganz überwiegende Mehrzahl der meistbesuchten 100 Webseiten in Deutschland mit diesen Tools arbeiten. Zutreffend weist der Kläger darauf hin, dass bei seinem üblichen Internetnutzungsverhalten von der Datenerhebung der Beklagten betroffen ist. Es ist allgemein bekannt, dass es unzählige Webseiten im Internet gibt. Wenn 30 % bis 40 % der Webseiten die Business Tools nutzen, sind damit nahezu alle üblichen und bekannten Seiten umfasst, denn vor allem die Masse der Privatpersonen wird zu den restlichen Prozenten gehören, die diese Tools nicht auf ihren privaten Homepages einbauen, bereits weil sie kein Interesse daran haben dürften, gezielt durch Persönlichkeitsprofile für eigene Produkte werben zu können. Zudem sind die Business Tools auf der ganz überwiegenden Mehrzahl der meistbesuchten 100 Webseiten in Deutschland nach dem nicht erheblich bestrittenen Klägervortrag enthalten. Erneut ist das Bestreiten der Beklagten punktuell beschränkt, dieses Mal dahingehend, dass die Klageseite keinerlei zuverlässige Methode zur Bestimmung oder Herkunft dieser Prozentsätze angegeben oder ihre Methode erklärt habe und einzelne der von der Klägerseite angeführten Internetseiten nicht betroffen seien, wobei die konkreten Seiten von der Beklagten nicht benannt werden. Dieses Bestreiten ist unerheblich, da es nicht die Tatsache selbst angreift. Ein Bestreiten mit Nichtwissen wäre unzulässig, da die Beklagte den Umfang des Einsatzes ihres Business Tools auf Webseiten von Geschäftspartnern kennt. Von diesen erhält sie gerade die streitgegenständlichen Daten. Die Darstellung einer Ermittlungsmethode ist unerheblich. Ein Blick auf die vorgelegten Listen betroffener Webseiten in Anlagen K 2, K 13 bis K 16 belegt zudem, dass nahezu sämtliche übliche Webseiten größerer Unternehmen, Verlage oder Dienstleister betroffen sind. Es wäre umgekehrt ein äußerst ungewöhnliches Verhalten, wenn Nutzer zur Vermeidung der streitgegenständlichen Datenverarbeitung der Beklagten all jene dort aufgeführten Webseiten meiden würden oder könnten. Im Übrigen könnten Nutzer nur solche Seiten meiden, bei denen eine Datenverarbeitung über Meta Pixel bekannt ist. Eine Datenverarbeitung über Conversions API hingegen ist weder erkennbar noch vermeidbar.

f) Zudem benötigt die Beklagte diese Angaben nicht für ihre Verteidigung. Sie bedarf lediglich eines Blickes in ihre Datenbank um zu sehen, ob sie einen Datensatz des Klägers gespeichert und welchen Umfang dieser hat, insbesondere ob ein oder mehrere Persönlichkeitsprofile von ihm erstellt wurden. Zudem kann sie erkennen, welche Daten von welchem ihrer Geschäftspartner hinsichtlich des Klägers an sie übermittelt wurden. Sie behauptet jedoch nicht, keine Daten von dem Kläger gespeichert zu haben, und bestreitet auch keine Profilerstellung. Damit ist der Einwand der Beklagten unerheblich, dass der Kläger nicht dargetan habe, über welche Nutzung welcher Seite über viele Jahre hinweg Daten von Webseitenbetreibern an die Beklagte übermittelt worden sein könnten.

2. Der mit Klageantrag Ziff 1 geltend gemachte Auskunftsanspruch folgt aus Art. 15 DSGVO.

a) Die Klagepartei ist betroffene Person i.S.d. Art. 4 Nr. 1 DSGVO. Denn bei ihr handelt es sich um eine identifizierbare natürliche Person. Die im Streit stehenden Daten beziehen sich personenbezogen auf den Kläger als Person.

b) Die Beklagte ist Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO, da durch die Einbindung der ihrerseits entwickelten Meta Business Tools auf dritten Webseiten und in Apps von ihr oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entschieden wird.

Dahinstehen kann der Einwand der Beklagten, dass sie bei der Erhebung der Daten allenfalls gemeinsam Verantwortliche mit den Webseitenanbietern nach Art. 26 DSGVO wäre, an die sie die Verantwortung für die Erfüllung der Datenschutzpflichten delegieren will (vgl. zur gemeinsamen Verantwortlichkeit EuGH NJW 2019, 2755 m.w.N.). Die Klagepartei weist insoweit zutreffend darauf hin, dass eine solche Vereinbarung zur gemeinsamen Verantwortlichkeit nach Art. 26 Abs. 1 DSGVO im Innen-, nicht jedoch im Außenverhältnis zum Nutzer relevant ist. Vielmehr bedarf es für jeden der Verantwortlichen einer Rechtsgrundlage im Sinne des Art. 5 Abs. 1 lit. a DSGVO, welche die Verarbeitung personenbezogener Daten legitimiert. Keiner der Verantwortlichen kann sich darauf zurückziehen, für das Anspruchsbegehren des Betroffenen nicht zuständig zu sein. Art. 26 Abs. 3 DSGVO entspricht vielmehr einer gesamtschuldnerischen Haftung wie in § 421 BGB (Kühling/Buchner/Hartung, DSGVO BDSG, 4. Aufl. 2024, Art. 26 Rn. 1 m.w.N.; Paal/Pauly, DSGVO BDSG, 3. Aufl. 2021, Art. 26 Rn. 36, 36a m.w.N.). Jedenfalls ist sie allein Verantwortliche für das Empfangen der von den Webseitenanbietern erhobenen Daten, deren Speichern auf eigenen Servern sowie deren Verwendung durch Profilerstellung der Nutzer und Weitergabe dieser Analysen an Geschäftspartner.

c) Der Auskunftsanspruch der Klagepartei wurde nicht bereits mit außergerichtlichem Schreiben vom 25.11.2024 (Anlage B8) der Beklagten erfüllt.

Mit Schreiben vom 25.11.2024 teilte die Beklagte mit, sie verarbeite vor dem Hintergrund, dass die Klagepartei nicht über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ eingewilligt habe, keine personenbezogenen Daten der Klagepartei im Rahmen der streitgegenständlichen Datenverarbeitung, weshalb sie auch keine Informationen hierzu bereitstellen könne. Mit „streitgegenständlicher Datenverarbeitung“ meint sie jedoch nach ihren eigenen Angaben die Verarbeitung der personenbezogenen Daten, die durch Meta Business Tools erhalten werden, um der Klagepartei personalisierte Werbung auf Facebook oder Instagram anzuzeigen (vgl. Anla-

ge B8, dort S. 1 f.). Die beklagteseits erteilte Auskunft ist daher unvollständig, denn das Auskunftsverlangen der Klagepartei ist nicht (lediglich) auf eine Datenverarbeitung zur Bereitstellung personalisierter Werbung gerichtet, sondern geht darüber hinaus. Dem Kläger geht es bei seinem Auskunftsbegehren nämlich um den gesamten Datenverarbeitungsvorgang bezüglich der Erhebung und Verarbeitung seiner personenbezogenen Daten, der insbesondere, aber nicht ausschließlich über die Meta Business Tools erfolgt sowie das Empfangen jener über Drittwebseiten und -Apps. Hierzu enthält das Schreiben der Beklagten keine Angaben.

3. Dem Kläger steht aus Art. 82 DSGVO die Zahlung immateriellen Schadensersatzes nebst Zinsen zu. Die Datenverarbeitung der Beklagten verstößt gegen das Transparenzgebot, das Gebot der Zweckbindung und der Datenminimierung nach Art. 5 Abs. 1 lit. a bis c DSGVO.

a) Die Beklagte ist Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO (s.o.).

b) Ein Verstoß gegen die Datenschutz-Grundverordnung ist gegeben, insbesondere liegt auch eine Verletzung von Art. 5 Abs. 1 lit. b und c DSGVO vor.

aa) Nach Art. 4 Nr. 2 DSGVO umfasst der Begriff Verarbeitung von Daten jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie 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. Unstreitig liegt jedenfalls eine Speicherung sämtlicher Daten vor, die die Business Tools auf Drittseiten erheben und an die Beklagte senden. Damit ist eine Datenverarbeitung im Sinne der DSGVO gegeben. Nach dem nach § 138 Abs. 3, 4 ZPO unstreitigen Tatsachenvortrag verwendet die Beklagte diese Daten zudem zur Profilerstellung über die Klagepartei.

bb) Nach Art. 6 Abs. 1 UAbs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens einer der Rechtfertigungsgründe nach lit. a bis f erfüllt ist.

(1) Rechtfertigungsgründe nach Art. 6 Abs. 1 UAbs. 1 lit. b bis f DSGVO liegen nicht vor. Insbesondere erfolgt keine Verarbeitung für die Erfüllung eines Vertrags nach lit. b oder zur Wahrung berechtigter Interessen nach lit. f (vgl. auch EuGH NJW 2023, 2297).

(2) Vielmehr rechtfertigt die Beklagten ihre Datenverarbeitung allein mit einer Einwilligung der Partei nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO und Art. 9 Abs. 2 lit. a DSGVO zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke. Diese

Einwilligung behauptet sie dabei grundsätzlich allein für eine Datenverarbeitung zur Bereitstellung personalisierter Werbung. Unstreitig hat die Klagepartei selbst eine solche im vorliegenden Fall nicht erteilt. Eine darüberhinausgehende Einwilligung trägt die Beklagte nicht vor.

(3) Die Beklagte benennt in diesem Zusammenhang allein den Verarbeitungszweck der Sicherheit und Integrität des Systems. Diese Angabe bleibt pauschal und vage. Es ist nicht erkennbar, weshalb dafür sämtliche personenbezogenen Daten des Nutzers bis hin zur Profilbildung über Nutzerinteressen bei Einkäufen, Nachrichtenkonsum und Freizeitgestaltung relevant sein könnten. Zudem ist auch insoweit kein einwilligungsfreier Raum gegeben, eine Einwilligung des Klägers hierzu behauptet die Beklagten nicht einmal, eine solche liegt auch nicht vor.

(4) In die Datenerhebung und -verarbeitung über die Meta Business Tools hat die Klagepartei auch nach dem Beklagtenvortrag nicht eingewilligt.

(5) Damit ist der gesamte Datenverarbeitungsvorgang vom Erheben personenbezogener Daten über die Business Tools, Empfangen jener von Geschäftspartnern, Speichern auf eigenen Servern und Verarbeiten zur Profilbildung und Weiterverwendung u.a. durch Weitergabe an Dritte nicht von einer Einwilligung gedeckt. Infolgedessen ist die Datenverarbeitung der Beklagten unrechtmäßig nach Art. 4 Nr. 2, 6 Abs. 1 UAbs. 1 DSGVO.

Dahinstehen kann, dass eine etwaig behauptete Einwilligung nicht hinreichend transparent, das heißt in verständlicher und leicht zugänglicher Form, sowie in einer klaren und einfachen Sprache erfolgt sein könnte und eine etwaige Einwilligungserklärung auf dieser Grundlage nicht in informierter Weise und unmissverständlich sowie freiwillig abgegeben sein könnte (vgl. BGH NJW 2025, 298).

c) Zudem liegt jedenfalls ein Verstoß der Beklagten gegen den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO vor, nachdem personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Dazu müssen sich die Ausnahmen und Einschränkungen dieses Grundsatzes des Schutzes solcher Daten auf das absolut Notwendige beschränken (BGH NJW 2025, 298 Rz. 87 m.w.N., u.a. EuGH EuZW 2022, 527 Rz. 73 und EuGH BeckRS 2019, 31011 Rz. 46). Bei Verstößen gegen die Vorschriften der Art. 5 bis 11 DSGVO, mithin des zweiten Kapitels der Datenschutz-Grundverordnung, welche Grundsätze für die Verarbeitung von Daten aufstellen, liegt zugleich eine unrechtmäßige Datenverarbeitung vor (BGH NJW 2025, 298 m.w.N., insb. EuGH ZD 2023, 606 - Bundesrepublik Deutschland (Elektronisches Gerichtsfach)).

d) Ferner liegt ein Verstoß gegen den Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO vor.

e) Die Pflichtverletzung der Beklagten ist auch ursächlich für den Schaden der Klagepartei.

Ein Kontrollverlust stellt bereits einen Schaden dar, der allein bereits zu einem Anspruch führt, wenngleich der Höhe nach im Bereich von 100,00 € (BGH NJW 2025, 298). Mit dem Landgericht Landau (Versäumnisurteil vom 26.02.2024, Az.: 2 O 239/23) dürfte insoweit nach der einschlägigen Verfahrensvorschrift des § 287 ZPO (BGH NJW 2025, 298) ein Schadensersatz in Höhe von 1.500,00 € begründet sein in Anbetracht des Umfangs und der Intensität der unrechtmäßigen Datenverarbeitung. Insoweit können psychische Beeinträchtigungen des Nutzers und weitere Schäden berücksichtigt werden (vgl. BGH NJW 2025, 298; zur Schadensberechnung im Einzelnen vgl. OLG Stuttgart GRUR-RS 2023, 32883 m.w.N.).

4. Dem Kläger steht ein weitergehender Anspruch gem. § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG zu. Mit dem Anspruch unter Ziff. 3 wird dem Klagebegehren des Klägers nicht genüge getan, denn die berücksichtigungsfähigen Elemente im Rahmen des Art. 82 DSGVO sind auf die Ausgleichsfunktion begrenzt. In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadensersatzanspruchs, wie sie in Erwägungsgrund 146 Satz 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO dagegen nicht erfüllen (BGH NJW 2025, 298 mit Hinweis auf EuGH GRUR-RS 2024, 13978; EuGH NJW 2025, 141; EuGH NJW 2024, 2599; EuGH NJW 2024, 1561; EuGH NJW 2024, 2009). Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen und ob er vorsätzlich gehandelt hat (BGH NJW 2025, 298 mit Hinweis auf EuGH NJW 2024, 1561; EuGH NJW 2024, 2599).

Diese Aspekte sind jedoch beim primär von dem Kläger geltend gemachten Anspruch auf Geldentschädigung aufgrund der Verletzung ihres Grundrechts auf informationelle Selbstbestimmung nach § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG zu berücksichtigen, welchen er in einer ins Ermessen des Gerichts gestellten Höhe begehrt, wobei er bereits einen fünfstelligen Betrag, mindestens aber 1.500,00 € als angemessen erachtet.

a) Art. 82 DSGVO schließt diesen Anspruch aus nationalem Recht nicht aus. Grundsätzlich haben zwar die von der DSGVO zur Verfügung gestellten Rechtsbehelfe abschließenden Charakter, wie sich insbesondere aus den Erwägungsgründen 9 und 10 der Verordnung ergibt. Dies gilt jedoch in Anbetracht des Erwägungsgrundes 146 Satz 4 nicht für Art. 82 DSGVO. Dementsprechend können konkurrierende Ansprüche aus §§ 823 ff. BGB ebenso wie aus quasivertraglichen oder vertraglichen Sonderverbindungen (§§ 280 Abs. 1, 241 Abs. 2, 311 Abs. 2 BGB) bestehen (Sydow/Marsch/Kreße, DSGVO BDSG, 3. Aufl. 2022, Art. 82 DSGVO Rn. 27; Gola/Heckmann/Gola/Piltz, BDSG, 3. Aufl. 2022, Art. 82 DSGVO Rn. 38; Kühling/Buchner/Bergt, DSGVO BDSG, 4. Aufl. 2024, Art. 82 DSGVO Rn. 68 m.w.N.; Paal/Pauly/Frenzel, DSGVO BDSG, 3. Aufl. 2021, Art. 82 DSGVO Rn. 20; BSG BeckRS 2023, 5209; BFH BeckRS 2022, 17323 m.w.N.; OLG Hamm ZD 2024, 104 Rz. 66; zu § 7 BDSG a.F. BAG NJW 2015, 2749; BeckOK Datenschutzrecht/Quaas, 50. Edition Stand 01.08.2024, Art. 82 Rn. 8; Ehmann/Selmayr/Nemitz, DSGVO, 3. Aufl. 2024, Art. 82 Rn. 8; EuGH NJW 2023, 1930 Rz. 41). Soweit eine Persönlichkeitsrechtsverletzung vorliegt, gewährt § 823 Abs. 1 BGB einen Schadensersatzanspruch (Borges/Keil/Borges, Rechtshandbuch Big Data, 1. Aufl. 2024, § 7 Rn. 264; Paal/Pauly/Frenzel, DSGVO BDSG, 3. Aufl. 2021, Art. 82 DSGVO Rn. 20; BeckOGK/Hermann, BGB, Stand 01.11.2024, § 823 Rn. 1285, 1288 m.w.N.). Die allgemeinen Schadenersatzansprüche des deutschen Rechts auf Grundlage von § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG bleiben daher weiterhin anwendbar (Simitis/Hornung/Spiecker gen. Döhmman/Boehm, Datenschutzrecht, 2. Aufl. 2025, Art. 82 DSGVO Rn. 36; Gola/Heckmann/Gola/Piltz, BDSG, 3. Aufl. 2022, Art. 82 DSGVO Rn. 38).

b) Die Voraussetzungen des Anspruchs auf Geldentschädigung nach § 823 Abs. 1 BGB i.V.m. Art. 1 Abs. 1, 2 Abs. 1 GG sind vorliegend erfüllt. Insbesondere ist das Recht des Klägers auf informationelle Selbstbestimmung betroffen und liegt eine schwere Persönlichkeitsrechtsverletzung vor. Gegenstand dieses Antrags ist Geldentschädigung wegen einer Verletzung des allgemeinen Persönlichkeitsrechts. Hierbei handelt es sich um ein besonderes Rechtsinstitut, das auf den Schutzauftrag aus Art. 1 und Art. 2 Abs. 1 GG zurückgeht (BGHZ 240, 45 = NJW 2024, 2836 mit Hinweis auf BGHZ 160, 298, 302; BGHZ 165, 203; BGH ZfSch 2022, 259).

aa) Durch die Verletzungshandlung ist das Rechtsgut des Persönlichkeitsrechts in seiner Gestalt des Rechts auf informationelle Selbstbestimmung des Klägers betroffen. Art. 2 Abs. 1 GG gewährleistet in Verbindung mit Art. 1 Abs. 1 GG das allgemeine Persönlichkeitsrecht. Das daraus hergeleitete Schutzgut ist das Recht auf informationelle Selbstbestimmung, das über den Schutz der Privatsphäre des Einzelnen hinausgeht und ihm die Befugnis gibt, grundsätzlich selbst über

die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es umfasst die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, ob ein Kommunikationsinhalt einzig dem Gesprächspartner, einem bestimmten Personenkreis oder der Öffentlichkeit zugänglich sein soll (BGH NJW 2014, 2276; BGH NJW 2013, 3029). Davon erfasst werden alle Daten, die für Dritte erkennbar einer bestimmten Person zugeordnet sind, etwa das eigene Bild, das gesprochene und geschriebene Wort oder sonstige Einzelheiten des privaten Lebensbereichs (BGH NJW 2013, 3029).

Der Kläger ist in seinem Recht auf informationelle Selbstbestimmung betroffen. Der Schutz der persönlichen Daten der Nutzer des Internets ist dabei ein wichtiger Teil des Persönlichkeitsrechts. Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit. Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist. Die zunehmende Verbreitung vernetzter informationstechnischer Systeme begründet für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen (BVerfGE 120, 274 = NJW 2008, 822 Rz. 170 ff.).

Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme wie etwa Personalcomputer ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (BVerfGE 120, 274 = NJW 2008, 822 Rz. 170, Rz. 178 mit Hinweis auf BVerfGE 65, 1, auch zu den aus solchen Folgerungen entstehenden Persönlichkeitsgefährdungen).

Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfGE 120, 274 = NJW 2008, 822 Rz. 170 ff. mit Hinweisen auf BVerfGE 65, 1; BVerfGE 84, 192). Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann. Der Schutzzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben (BVerfGE 120, 274 = NJW 2008, 822 Rz. 181, 198; BVerfG NJW 2007, 2464).

Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure (vgl. BVerfG JZ 2007, 576 = BeckRS 2008, 36962) zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können (BVerfGE 120, 274 = NJW 2008, 822 Rz. 199 mit Hinweis auf BVerfG NJW 2007, 2464; BVerfGE 65, 1; BVerfGE 113, 29; BVerfGE 115, 320). Jedoch trägt das Recht auf informationelle Selbstbestimmung den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potenziell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen,

vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus. Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten (BVerfGE 120, 274 = NJW 2008, 822 Rz. 200 f.).

bb) Eine Verletzungshandlung der Beklagten liegt vor durch ihre unrechtmäßige Datenverarbeitung. Eine schuldhafte Verletzung des allgemeinen Persönlichkeitsrechts begründet einen Anspruch auf eine Geldentschädigung, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann. Ob eine so schwerwiegende Verletzung des Persönlichkeitsrechts vorliegt, dass die Zahlung einer Geldentschädigung erforderlich ist, kann nur aufgrund der gesamten Umstände des Einzelfalls beurteilt werden. Hierbei sind insbesondere die Bedeutung und Tragweite des Eingriffs, also das Ausmaß der Verbreitung der Veröffentlichung, die Nachhaltigkeit und Fortdauer der Interessen- oder Rufschädigung des Verletzten, ferner Anlass und Beweggrund des Handelnden sowie der Grad seines Verschuldens zu berücksichtigen (vgl. BGH VersR 2022, 830; BGHZ 183, 227 = NJW 2010, 763; BGHZ 199, 237 = NJW 2014, 2029 Rn. 38; BGH NJW 2015, 2500). Außerdem ist der besonderen Funktion der Geldentschädigung bei Persönlichkeitsrechtsverletzungen Rechnung zu tragen, die sowohl in einer Genugtuung des Verletzten für den erlittenen Eingriff besteht als auch ihre sachliche Berechtigung in dem Gedanken findet, dass das Persönlichkeitsrecht gegenüber erheblichen Beeinträchtigungen anderenfalls ohne ausreichenden Schutz bliebe. Zudem soll die Geldentschädigung der Prävention dienen (BGH NJW 2022, 1751 mit Hinweis auf BGHZ 199, 237 = NJW 2014, 2029 Rn. 38 m.w.N.). Bei der gebotenen Gesamtwürdigung ist auch ein erwirkter Unterlassungstitel zu berücksichtigen; der Titel und die mit ihm verbundenen Vollstreckungsmöglichkeiten können den Geldentschädigungsanspruch beeinflussen und im Zweifel sogar ausschließen (BGH NJW 2022, 1751 mit Hinweis auf BGHZ 206, 347; BGH NJW-RR 2016, 1136, jeweils m.w.N.).

Die Zuerkennung einer Geldentschädigung dient dem Ausgleich einer schwerwiegenden Beein-

trächtigung des Persönlichkeitsrechts, die nicht in anderer Weise befriedigend aufgefangen werden kann, nicht hingegen dem Ausgleich von Beeinträchtigungen anderer absolut geschützter Rechtsgüter. Die Wesensverschiedenheit der Ansprüche zeigt sich unter anderem darin, dass der Schmerzensgeldanspruch vererblich ist, der Anspruch auf Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts hingegen grundsätzlich nicht (so BGHZ 240, 45 = NJW 2024, 2836 mit Hinweis auf BGHZ 232, 68 Rn. 10). Die Zubilligung einer Geldentschädigung unter den genannten Voraussetzungen findet ihre sachliche Berechtigung in dem Gedanken, dass das Persönlichkeitsrecht gegenüber schwerwiegenden Beeinträchtigungen anderenfalls ohne ausreichenden Schutz bliebe mit der Folge, dass der Rechtsschutz der Persönlichkeit verkümmern würde (vgl. BGHZ 95, 212, 215; BGHZ 206, 347 Rn. 38, jeweils m.w.N.).

Das Recht auf informationelle Selbstbestimmung gewährt Schutz vor Gefährdungen und Verletzungen der Persönlichkeit, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben. Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht gewährleistet damit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BGH NJW 2024, 2836 m.w.N.).

cc) Unter Anwendung dieser Grundsätze ist ein Anspruch auf Geldentschädigung gegeben. Der Kläger begehrt vor allem wirksamen Rechtsschutz gegenüber der Beklagten dahingehend zu erhalten, zukünftig nicht mehr der permanenten Gefährdung ausgesetzt zu sein, dass die Beklagte ohne sein Wissen und Wollen und ohne Rechtfertigungsgrund tagtäglich seine das Surfverhalten protokollierenden personenbezogenen Daten verarbeitet, und dies nicht im Einzelfall, sondern durch ein System der umfassenden, unbestimmten und ausufernden Datenverarbeitung. Insoweit fehle es bisher an einem wirksamen Rechtsschutz, die Beklagte betreibe

Geschäftsmodell öffentlich und für alle sichtbar, obwohl seit dem 04.07.2023 höchstrichterlich festgestellt sei (EuGH, Urteil vom 04.07.2023, C-252/21), dass die von ihr ins Feld geführten Rechtfertigungsgründe nicht greifen und sie keinerlei alternative valide Rechtfertigungsgründe ins Feld führen könne. Zur Erzielung eines effektiven Rechtsschutzes sei eine höhere Geldentschädigung erforderlich.

Das Recht auf informationelle Selbstbestimmung ist im vorliegenden Fall durch die konkrete extensive Datenverarbeitung der Beklagten verletzt. Die Datenverarbeitung der Beklagten verstößt

gegen das Transparenzgebot, das Gebot der Zweckbindung und der Datenminimierung nach Art. 5 Abs. 1 lit. a bis c DSGVO. Jedenfalls hat die Beklagte nicht dargelegt und erst recht nicht nachgewiesen gemäß Art. 5 Abs. 2 DSGVO, dass sie diese Pflichten eingehalten hat. Insoweit hat die Klägerseite nachvollziehbar dargelegt, dass die systemische Verletzung des Anspruchs des Einzelnen, „Herr/Herrin der Daten“ zu sein, durch eine umfassende, unbestimmte und ausufernde Datenverarbeitung durch die Beklagte, die umfassende Rückschlüsse auf deren Persönlichkeit zulassen, einen besonders intensiven Eingriff in die informationelle Selbstbestimmung darstellt und ganz besonders schadensrelevant ist.

Die Beklagte wertet das Online-, Surf- und Kaufverhalten des Nutzers aus, und zwar in einer Weise, die bei Einwilligung Persönlichkeitsprofile und Interessenanalysen des Nutzers erstellt, so dass personenbezogene Werbung angeboten werden kann. Mit ihren Businessstools werden sehr umfangreich gängige Internetseiten ausgestattet und dort erhobene Daten an sie übertragen. Die Profilbildung bietet der Beklagten nach dem als unstreitig zugrunde zu legenden Vortrag des Klägers auch Informationen zu persönlichen und hochpersönlichen Daten, wie gesundheitlichen, politischen, religiösen und sexuellen Interessen des Nutzers. Mangels Transparenz, welche Internetseiten Business Tools der Beklagten nutzen, kann der Kläger eine Unsicherheit bei seiner gesamten Internetnutzung darlegen. Über das Tool Conversions API ist technisch nicht erkennbar, welche weitere Webseiten über solche mit Meta Pixel hinaus diese Datenerhebung und -verarbeitung ebenfalls unternehmen, dies auch bei Ablehnung der Datenverarbeitung für personalisierte Werbung. Jedenfalls diese nach Art. 15 DSGVO von dem Kläger verlangten Informationen hat die Beklagte bisher nicht beantwortet. Es besteht momentan keine Möglichkeit für den Kläger, eine ausreichende Sicherheit zu erreichen, dass die streitgegenständliche Datenverarbeitung zukünftig eingestellt wird, auch dann nicht, wenn ein entsprechender Unterlassungstitel rechtskräftig wird. Die Beklagte löscht bereits erhobene Daten auch nicht, unklar ist dem Kläger, was bei einer allein angebotenen Trennung erfolgt. Umfang der erfassten Daten und Verwendungszwecke werden nicht konkret benannt. Die allein zugestandene Datenverarbeitung zu Sicherheits- und Integritätszwecken des Systems bleibt vage und pauschal. Als Beweggrund gibt die Klägerseite unwidersprochen lediglich die ökonomischen Interessen der Beklagten an. Insoweit gründet ihr „milliardenschweres Geschäftsmodell“ auf einer „illegalen Datenverarbeitung“. Die Beklagte handelt insoweit auch mit Wissen und Wollen, mithin vorsätzlich.

Es ist weder vorgetragen und auch nicht anderweitig erkennbar, dass die Beklagte ihre allein angegebenen Sicherheits- und Integritätsinteressen nicht bereits aufgrund der Datenauswertung erreichen könnte, in die ihre Nutzer bei der Nutzung ihrer eigenen social media Dienste wie vorlie-

gend Facebook zustimmen. Die Auswertung des gesamten Surfverhaltens ihrer Nutzer jenseits ihrer Plattformen erscheint insoweit nicht erforderlich für jegliche von ihr angeführten Verarbeitungszwecke.

Vor diesem Hintergrund ist der Aspekt, dass der Nutzer selbst einer solchen Datenverarbeitung bei der Nutzung von Facebook zugestimmt hat und daher weiß, dass die Beklagte überhaupt Daten erhebt und dort erhobene Daten verarbeitet, nicht geeignet, den schweren Eingriff der Beklagten in das Recht auf informationelle Selbstbestimmung zu entkräften.

dd) Die Pflichtverletzung der Beklagten ist auch ursächlich für die Verletzung des Rechts auf informationelle Selbstbestimmung und den Schaden des Klägers. Die Beklagte handelte auch mit Wissen und Wollen, mithin vorsätzlich. Mit diesem Geschäftsmodell erwirtschaftet sie ihren ganz erheblichen Umsatz und Gewinn.

c) Die Beeinträchtigung kann auch nicht anderweitig als durch Zahlung einer Geldentschädigung ausgeglichen werden. Zwar bieten die Unterlassungsansprüche einen gewissen Schutz vor künftiger Datenerfassung und -verarbeitung. Jedoch weist der Kläger nachvollziehbar darauf hin, dass sie die Nichteinhaltung dieser Unterlassungspflichten nicht erkennen könnte, wenn die Beklagte die Datenerhebung über Conversions API fortsetzen würde, wofür jene wirbt. Auch bisherige Entscheidungen des EuGHs und Bußgelder in Milliardenhöhe europäischer Behörden hätten die Beklagte nicht veranlasst, weniger Daten zu erheben. Zudem habe sie einen wirtschaftlichen Anreiz, die Datenpraxis fortzuführen, wenngleich eher mit dem derzeit nicht aufdeckbaren Conversions API, den sie für diese Zwecke gerade bewirbt (Anlage K 11, insb. S. 23), da ihr gesamtes Geschäftsmodell vor allem auf dieser Datenerhebung, -verarbeitung, -auswertung und -weitergabe an Dritte beruhe. Zudem ist von bereits in der Vergangenheit umfangreicher Persönlichkeitsprofilbildung auszugehen. Hier soll der Löschungsanspruch einen Ausgleich verschaffen. Doch auch insoweit ist für den Kläger nicht überprüfbar, ob dem tatsächlich in vollem Umfang nachgekommen werden wird. An einer solch konkreten und detaillierten Auskunft der Beklagten nach Art. 15 DSGVO fehlt es jeweils gerade, und auch deren Vollständigkeit ist für den Nutzer nicht prüfbar. Die bereits erfolgte Pflichtverletzung wird in ihrem Gewicht auch bei einer unterstellten vollständigen Löschung sämtlicher streitgegenständlicher Daten ebenfalls nicht ausgeglichen.

d) Zu den Folgen der Datenverarbeitung hat der Kläger in seiner Anhörungen angegeben, dass er das Gefühl habe, dass Informationen etwa zu seiner Gesundheit, seinem Sozialverhalten oder vielleicht sogar zu seiner Sexualität gesammelt werden und ihn das Gefühl eines Kontrollverlusts

auf emotionaler Ebene treffe.

e) Es handelt sich vorliegend um einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung. Das nahezu gesamte Online-Verhalten des Klägers wird dokumentiert und in Persönlichkeitsprofilen ausgewertet. Damit ist auch der unantastbare Kernbereich der privaten Lebensgestaltung des Klägers tangiert. Gerade auch dieses sogenannte Profiling stellt einen sehr intensiven Eingriff dar. Nach Erwägungsgrund 60, 63 der DSGVO ist die betroffene Person insbesondere darauf hinzuweisen, dass Profiling stattfindet und welche Folgen das hat. Nach Erwägungsgrund 75 stellt insbesondere die Verarbeitung persönlicher Daten zum Zwecke der Erstellung persönlicher Profile ein besonderes Risiko für einen Schaden dar. Dieser führt aus: Die Risiken für die Rechte und Freiheiten natürlicher Personen - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Zudem ist beim Schaden neben der Intensität gemäß Erwägungsgrund 75 insbesondere auch zu berücksichtigen, dass auch hoch sensible Daten, auch aus der Intimsphäre, und eine extrem große Menge personenbezogener Daten erhoben werden. So hat auch der EuGH bereits hinsichtlich

der streitgegenständlichen Datenverarbeitung der Beklagten über ihre Business Tools festgestellt, dass diese Verarbeitung besonders umfassend ist, da sie potenziell unbegrenzte Daten betrifft und erhebliche Auswirkungen auf den Nutzer hat, dessen Online-Aktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta Platforms Ireland aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird (EuGH NJW 2023, 2997, C-252/21 Meta Platforms Inc. u.a./BKartA).

Zudem handelt die Beklagte vorsätzlich mit Gewinnerzielungsabsicht, da rein aus ökonomischen Gesichtspunkten. Mit den erhobenen Daten erwirtschaftet sie ihren Umsatz und Gewinn. Für sie streitende weitere Grundrechtspositionen führt die Beklagte nicht an, solche sind auch nicht anderweitig erkennbar.

f) Die Höhe der Geldentschädigung ist zu schätzen nach § 287 ZPO (BGH NJW 2025, 298 m.w.N.; OLG Stuttgart GRUR-RS 2023, 32883 m.w.N. und grundsätzlichen Ausführungen zu Ausgleichs-, Genugtuungs- und Präventionsfunktion, auf die verwiesen wird). Auf die Vermögenslage des Beeinträchtigten kommt es zur Bemessung der Entschädigung nicht entscheidend an, aber eventuell auf die wirtschaftliche Leistungsfähigkeit des Rechtsverletzers. Für Medien muss der aufzubringende Entschädigungsbetrag einen echten Hemmungseffekt bedeuten, weniger orientiert an Prominenz oder Nichtprominenz des Betroffenen als ausgerichtet auf Art, Ausmaß und Intensität der jeweiligen Persönlichkeitsverletzung (Geigel/Pardey, Haftpflichtprozess, 29. Aufl. 2024, Kapitel 23 Rn. 130 m.w.N.). 10.000,00 € und 15.000,00 € werden in der gerichtlichen Praxis häufig zugunsten Betroffener je entschädigungswürdigem Rechtsverstoß - unter Gesamtbetrachtung - in Betracht gezogen (vgl. Geigel/Pardey, Haftpflichtprozess, 29. Aufl. 2024, Kapitel 23 Rn. 131, 135 m.w.N. und Einzelfällen, z.B. 15.000,00 € bei unzulässiger Weitergabe eines Attests, unstatthafte Bildveröffentlichungen mit 20.000,00 € und 30.000,00 €, vgl. OLG München BeckRS 2014, 16144; OLG Köln BeckRS 2018, 39601; LG Frankfurt BeckRS 2019, 15418). Wenn man beim Ersatz immaterieller Schäden an Leib und Seele von Genugtuung spricht, so ist dabei weniger auf die subjektive Befriedigung des Verletzten, sondern vornehmlich darauf abzuheben, dass sich der gesetzlich umfassend angelegte Rechtsgüterschutz auch im immateriellen Bereich objektiv zu bewähren hat. So gesehen geht es schadensersatzrechtlich nicht maßgeblich darum, dass der Verletzte persönlich gegenüber dem Verletzer Genugtuung empfindet. Das wäre nicht nur zu interpersonal gesehen, sondern das passt immer dann nicht, wenn der Verletzte bewusstlos ist oder dessen Persönlichkeit so gelähmt oder zerstört ist, dass er nichts mehr zu empfinden vermag. Die Genugtuungsfunktion darf aber nicht in den schlimmsten Schadensfällen versagen. Ein anderes Ergebnis würde der verfassungsrechtlichen Wertentscheidung in Art. 1 GG wider-

sprechen. Die Geldentschädigung findet ihre sachliche Berechtigung auch in dem Gedanken, dass das Persönlichkeitsrecht gegenüber erheblichen Beeinträchtigungen anderenfalls ohne ausreichenden Schutz bliebe (OLG Hamburg BeckRS 2017, 109789; Geigel/Pardey, Haftpflichtprozess, 29. Aufl. 2024, Kapitel 23 Rn. 131).

In die Abwägung zur Schätzung der Höhe der Geldentschädigung nach § 287 ZPO sind alle genannten Aspekte des Einzelfalls einzubeziehen. Zur Vermeidung von Wiederholungen wird insoweit auf die Darlegungen unter e) sowie b) und c) Bezug genommen. Dabei wird auch berücksichtigt, dass der Kläger aufgrund der Datenschutzrichtlinie der Beklagten bekannt war bzw. gewesen sein konnte, dass entsprechende Daten gesammelt und gegebenenfalls weitergegeben wurden (vgl. LG Landau, Versäumnisurteil vom 26.02.2024, Az.: 2 O 239/23). In Anbetracht der Schwere des Eingriffs - in Intensität und Umfang - in das Grundrecht auf informationelle Selbstbestimmung, des Verschuldensgrads, der technischen Umgehungsmöglichkeiten der Beklagten bei Unterlassungs- und Löschungsansprüchen sowie dem Präventivgedanken erscheint ein Betrag der Geldentschädigung in Höhe von 10.000,00 € nach Auffassung des Gerichts unter Abwägung sämtlicher erwähnter Umstände des Einzelfalls angemessen, aber auch ausreichend. Gerade in Abgrenzung zu Art. 82 DSGVO ist der Präventivgedanke des Geldentschädigungsanspruchs zu berücksichtigen, der einen echten bzw. effektiven Hemmungseffekt bewirken soll. Nur bei spürbaren Folgen wird die Beklagte bewegt werden können, ihr Geschäftsmodell umzustellen und den Datenschutz ihrer Nutzer zu achten. Dieser Geldentschädigungsbetrag umfasst auch den Betrag, der nach Art. 82 DSGVO als immaterieller Schadensersatz zu erstatten wäre (vgl. OLG Köln GRUR-RS 2020, 38050 Rn. 41).

g) Der Anspruch auf Zahlung der geltend gemachten Verzugszinsen folgt aus §§ 286 Abs. 1, 288 Abs. 1 BGB. Mit Anwaltsschreiben vom 02.01.2024 hat der Kläger Zahlung des Schmerzensgeldes in Höhe von 5.000,00 € verlangt mit Fristsetzung bis 23.01.2024 (Anlage K 3). Zwar reicht für § 286 Abs. 2 Nr. 1 BGB die einseitige Festlegung einer Leistungszeit durch den Gläubiger grundsätzlich nicht (BGH NJW 2008, 50). In der einseitigen Bestimmung eines Zahlungsziels durch den Gläubiger liegt jedoch eine Mahnung nach § 286 Abs. 1 BGB, wenn - wie im vorliegenden Schreiben - der Gläubiger den Schuldner auffordert, die Rechnung bis zu einem bestimmten Zeitpunkt zu begleichen, und damit die für eine Mahnung erforderliche eindeutige Leistungsaufforderung zum Ausdruck bringt (vgl. BGH NJW 2006, 3271; Ernst in: Münchener Kommentar, BGB, 9. Aufl. 2022, § 286 Rn. 65, 73; Staudinger/Feldmann, BGB, Neub. 2019, § 286 Rn. 71 m.w.N.). Somit ist der Zinsanspruch aus einem Betrag von 1.500,00 € berechtigt gemäß Klageantrag zu 3 ab dem 24.01.2024 gemäß § 308 Abs. 1 ZPO. Da der Zinsanspruch erst für den Zeitraum ab dem

31.01.2024 beantragt wurde, war auch nur insoweit zuzusprechen. Der darüber hinausgehende Zinsanspruch ergibt sich aus §§ 291, 288 Abs. 1 BGB. Die Klage wurde der Beklagten am 22.08.2024 zugestellt, so dass die Beklagte dem Kläger seit dem 23.08.2024 hinsichtlich des Betrages, der dem Kläger über den vorgerichtlich geltend gemachten Betrag hinausgehend zugesprochen wurde, d.h. hinsichtlich weiteren 8.500,00 €, Prozesszinsen schuldet.

5. Der dem Klageantrag zu Ziff. 2 zugrundeliegende Anspruch folgt, soweit die künftige Löschung begehrt wird, aus Art. 17 Abs. 1 lit. d DSGVO i.V.m. § 259 ZPO. Denn die personenbezogenen Daten wurden unrechtmäßig erlangt (s.o.), sodass - bei entsprechender Aufforderung - ein Anspruch auf unverzügliche Löschung besteht.

Soweit die vollständige Anonymisierung verlangt wird, folgt dies aus Art. 18 Abs. 1 lit. b DSGVO. Da die Daten unrechtmäßig erlangt wurden (s.o.) und diesbezüglich gerade keine Löschung verlangt wird, kann die Einschränkung der Verarbeitung verlangt werden.

Die Anonymisierung der Daten ist zwar nicht unmittelbar in Art. 4 Nr. 2 DSGVO als Bestandteil des „Verarbeitens“ genannt. Aus dem Gesamtkontext und dem Verständnis heraus ist dies jedoch als „Veränderung“ der Daten zu verstehen, was wiederum Bestandteil der Verarbeitung ist, sodass die Klagepartei diese Maßnahme als Einschränkung der Verarbeitung verlangen kann (so insgesamt zutreffend LG Landau, Versäumnisurteil vom 26.02.2024, Az.: 2 O 239/23).

6. Der Kläger hat ferner einen Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten. Die außergerichtlichen Rechtsanwaltskosten sind als eigenständige Schadensposition im Rahmen des Anspruchs nach § 823 BGB, § 280 BGB ersatzfähig und in Höhe einer 1,3-Geschäftsgebühr aus dem Gegenstandswert von 15.000,00 € zuzüglich Post- und Telekommunikationspauschale und Mehrwertsteuer begründet, §§ 13, 14 RVG, Nr. 2300, 7002, 7008 VV RVG, mithin in Höhe von insgesamt 1.148,80 €. Die Zuziehung eines Rechtsanwalts war im vorliegenden Fall erforderlich. Der Kläger verlangt mit dem Antrag 4 die Freistellung von 367,23 €, weshalb die Beklagte nur insoweit zu verurteilen war (§ 308 Abs. 1 ZPO).

III.

Die Kostenentscheidung folgt aus § 91 Abs. 1 ZPO. Der Ausspruch über die vorläufige Vollstreckbarkeit folgt aus § 709 ZPO. Die Streitwertfestsetzung hat ihre Rechtsgrundlage in den §§ 39 Abs.1, 43 Abs.1, 48 Abs.1 Satz 1 i.V.m. § 3 ZPO. Insoweit ist für die Klageanträge 1 und 2 ein

Streitwert von 5.000,00 € als angemessen zu erachten. Für Klageantrag Ziffer 3 bemisst sich der Gebührenstreitwert danach, welcher Betrag unter Zugrundelegung des klägerischen Tatsachenvortrags gerechtfertigt erscheint (vgl. BGH GRUR 2012, 959 m.w.N.; OLG Naumburg NJOZ 2014, 52; KG VersR 2011, 1073; OLG Saarbrücken BeckRS 2010, 450; Schneider/Volpert/Fölsch, Gesamtes Kostenrecht, 3. Aufl. 2021, § 3 Rn. 197 m.w.N.; Anders/Gehle/Gehle, ZPO, 83. Aufl. 2025, Anh. zu § 3 Rn. 99, 115 m.w.N.). Nach den obigen Ausführungen zur Begründetheit des Klageantrags Ziffer 3, auf die zur Vermeidung von Wiederholungen verwiesen wird, beläuft sich dieser Betrag auf 10.000,00 €. Auf die Mindestangabe des Klägers kommt es insoweit nicht an.

Rechtsbehelfsbelehrung:

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

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

Landgericht Ellwangen (Jagst)
Marktplatz 7
73479 Ellwangen (Jagst)

einzulegen.

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

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

Rechtsbehelfe können auch als elektronisches Dokument eingelegt werden. Eine Einlegung per E-Mail ist nicht zulässig. Wie Sie bei Gericht elektronisch einreichen können, wird auf www.ejustice-bw.de beschrieben.

Schriftlich einzureichende Anträge und Erklärungen, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.