1 O 155/24

**Landgericht Siegen**

**IM NAMEN DES VOLKES**

**Urteil**

In dem Rechtsstreit

des Herrn [redacted]

Klägers,

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

gegen

die Meta Platforms Ireland Ltd., vertr. d. Richard Kelley, Merrion Road, Dublin 4 D04 X2K5, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte White & Case, Bockenheimer Landstraße 20, 60323 Frankfurt,

hat die 1. Zivilkammer des Landgerichts Siegen
auf die mündliche Verhandlung vom 11.11.2025
durch die Vorsitzende Richterin am Landgericht [redacted] als Einzelrichterin

**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 der folgenden personenbezogenen Daten**

**der Klagepartei seit dem 1. Dezember 2021 mit Hilfe der „Meta Business Tools“ erfasst, an die Server der Beklagten weitergeleitet, dort gespeichert und anschließend verwendet wurden und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Facebook “ unter dem Benutzernamen [redacted] der Klagepartei verknüpft wurden,**

**a. auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der Klagepartei, ob direkt oder in gehashter Form übertragen, d.h.**

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

**sowie 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 von der Klagepartei auf der Webseite angeklickten Buttons sowie**
- **weitere von der Meta „Events“ genannte Daten, die die Interaktionen der Klagepartei auf der jeweiligen Webseite dokumentieren**

**c. in mobilen Dritt-Apps**

- **der Name der App sowie**
- **der Zeitpunkt des Besuchs**
- **die von der Klagepartei in der App angeklickten Buttons sowie**

**• die von der Meta „Events“ genannte Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren**

**außerdem für jedes erhobene Datum,**

**ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 1. Dezember 2021 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 1. Dezember 2021 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;**

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

**2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. dem Antrag zu 1. sämtliche gem. dem Antrag zu 1 a. seit dem 1. Dezember 2021 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. dem Antrag zu 1 b. sowie c. seit dem 1. Dezember 2021 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren oder wahlweise nach Wahl der Beklagten zu löschen.**

**3. Die Beklagte wird verurteilt, an die Klagepartei eine Entschädigung in Höhe von 5.000 EUR nebst Zinsen hieraus i. H. v. fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 1. März 2024 zu zahlen.**

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

**5. Die Kosten des Rechtsstreits trägt die Beklagte.**

**6. Das Urteil ist gegen Sicherheitsleistungen i. H. v. 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.**

## Tatbestand:

Die Parteien streiten über Ansprüche des Klägers im Zusammenhang mit der Verwendung von sog. Business Tools der Beklagten.

Die Beklagte betreibt u. a. das soziale Netzwerk „facebook“. Die Beklagte entwickelte verschiedene 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. Der Kläger nutzt ausschließlich privat das Netzwerk „facebook“ unter der E-Mail-Adresse [redacted] seit dem 1. Dezember 2021. Als Gegenleistung für die Nutzung des Netzwerks fordert die Beklagte kein Geld. Das soziale Netzwerk wird maßgeblich durch Online-Werbung finanziert. Dem Kläger wird bei Nutzung des Netzwerks Werbung angezeigt, die auf seinen Interessen basiert, welche die Algorithmen der Beklagten ausgewertet haben. Wahlweise können die Nutzer seit November 2023 ein Abonnement-Modell wählen, bei dem sie gegen Zahlung einer monatlichen Gebühr die Anzeige von Werbung abschalten können. Die Einrichtung eines Kontos im Netzwerk der Beklagten setzt voraus, dass der Nutzer den Nutzungsbedingungen der Beklagten (Anlage B2, Fassung vom 12. Januar 2024, Bl. 339ff. der Akte) zustimmt. Diese Nutzungsbedingungen enthalten unter anderem den Hinweis: „Meta kann auf jegliche Informationen, die es über dich erfasst, zugreifen, sie aufbewahren, verwenden und teilen, wenn es in gutem Glauben der Ansicht ist, dass dies gesetzlich vorgeschrieben oder zulässig ist.“ (Seite 4, Bl. 342 der Akte) und verweisen wegen weiterer Informationen zur Verwendung der Nutzerinformationen auf die 150-seitige Datenschutzrichtlinie der Beklagten (Anlage K1, Fassung vom 7. September 2023, Bl. 39ff. der Akte). Diese sieht unter anderem vor, dass der Kläger die von der Beklagten erhobenen Daten, einschließlich solcher, die sich aus der Nutzung anderer konzerneigener Dienste sowie aus sonstigen Internetaktivitäten des Nutzers außerhalb (Seite 9 der Datenschutzrichtlinie, Bl. 47 der Akte) der Netzwerke der Beklagten ergeben, der Beklagten zur Darbietung „personalisierter Erlebnisse“ sowie zu „anderen Zwecken“ zur Verfügung stellt (Seite 23 der Datenschutzrichtlinie, Bl. 61 der Akte). Als andere Zwecke für die Aufbewahrung von Nutzer-Informationen werden in der Datenschutzrichtlinie als Beispiele aufgeführt: „Als Reaktion auf eine rechtliche Anfrage“, „Um geltende Gesetze einzuhalten“, „Zu Zwecken von Schutz, Sicherheit und Integrität“, „Für Rechtsstreitigkeiten“ (Seite 81ff. der Datenschutzrichtlinie, Bl. 119ff. der Akte). In der Datenschutzrichtlinie der Beklagten wird weiter erläutert, dass die vom Nutzer bereitgestellten Informationen, einschließlich der über die Business Tools übersandten Informationen der Partner der Beklagten, übergreifend über alle Produkte der Beklagten und alle Geräte des Nutzers hinweg verwendet und automatisch von den Systemen der Beklagten verarbeitet werden (Seite 23 der Datenschutzrichtlinie, Bl. 61 der Akte). Eine Cookie-Richtlinie, auf die wiederum die Datenschutzrichtlinie verweist, enthält die Mitteilung, dass die Beklagte seitenbezogene Textinformationen (Cookies) auf dem Nutzergerät platziert und so Informationen erhalten kann, die dort gespeichert werden, wenn der Nutzer Anwendungen der Beklagten oder Internetseiten von anderen Unternehmen, die Business Tools der Beklagten nutzen, aufruft, und zwar ohne dass eine weitere Handlung des Nutzers erforderlich wäre. Die Beklagte teilt die „Informationen“ des Nutzers mit Partnern, die die „Analysedienste“ der Beklagten nutzen, „integrierten“ Partnern, Anbietern für Messlösungen, Anbietern für Marketinglösungen, verschiedensten „Dienstleistern“ und „externen Forschern“ (Seite 50ff. der Datenschutzrichtlinie, Bl. 88ff. der Akte). Der Kläger willigte gegenüber der Beklagten über die Einstellung „Informationen von Werbepartnern über deine Aktivitäten“ weder

in die Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung noch in die Nutzung optionaler Cookies ein (Protokoll vom 11. November 2025, Seite 2, Bl. 2491 der Akte). Die Integration der streitgegenständlichen Business Tools Apps und Webseiten von Drittunternehmen 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 Website- und App-Betreiber („Conversions API“ und „App Events API“), wodurch die Erfassung der Daten nicht mehr auf dem Rechner des Nutzers durchgeführt wird. Auch dies wird vom technisch versierten Nutzer nicht bemerkt und kann auch nicht mehr verhindert werden. 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, tfp-fertility.com (Samenbank), nie-wieder-alkohol.de, nvve.nl (Sterbehilfe) (siehe hierzu die Auflistung der Recherche der Klägervertreter in der Anlage K2, Bl. 189ff. der Akte). Die Business Tools verarbeiten dort persönliche und höchstpersönliche Daten der Nutzer zur Gesundheit, zur politischen Einstellung, zur Weltanschauung, zu Finanzen sowie zur Sexualität. 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 zum einen durch sogenanntes „Digital Fingerprinting“, durch welches ein Nutzer dauerhaft online zurückverfolgbar ist. Dazu werden die gesammelten Daten im Rahmen des „Advanced Matching“ der individuellen Meta-ID des Nutzers zugewiesen und zusammen mit den Standortdaten des Mobilgeräts verknüpft, verwendet und so vollständig individualisiert. Die Daten werden auch gesammelt, wenn der Nutzer nicht in seinen Account bei der Beklagten eingeloggt ist und ihre Cookies nicht zulässt. Zum anderen ist jeder einzelne Klick und jede Texteingabe auf solchen Dritt-Webseiten und -Apps durch die Beklagte nachverfolgbar. Diese erhält Informationen dazu, welche Seiten und Unterseiten wann besucht wurden, was dort angeklickt, gesucht oder gekauft wurde. Die angefallenen Daten sendet die Beklagte weltweit in Drittstaaten, insbesondere die USA, und gibt sie bei Bedarf an Dritte sowie an Behörden weiter. Da die Anbieter der wichtigsten Browser (Apple Safari, Mozilla Firefox, Google Chrome) seit 2019 die Cookie-Setzung von Drittanbietern stückweise unterbinden und auch die Ausführung von Skriptanwendungen zumindest im Inkognito-Modus schwieriger gemacht wird, führte die Beklagte 2021 die „Conversions API“ und die „App Events API“ ein. 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 – in diesem Fall 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 die Nutzer mit sämtlichen anderen aggregierten Daten. 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. Sodann werden sämtliche Daten an die Server der Beklagten geschickt. Erst dort wertet die Beklagte aus, ob sie die rechtliche Befugnis hat, die Daten weiter zu verarbeiten. 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 K11 Meta_Playbook, insbesondere S. 23, Bl. 731ff. der Akte). Da sie nicht in den Browser des Nutzers geladen werden muss, kann der Nutzer sie nicht abschalten. Die entsprechenden Systeme nutzt die Beklagte auch bei Nutzern, die die Schaltflachen „Optionale Cookies erlauben“ und „Informationen über Aktivitäten von Werbepartnern“ nicht aktiviert haben. Die verarbeiteten Informationen werden von den Business Tools ab dem Zeitpunkt ihrer Installation durch den jeweiligen Websitesbetreiber 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. Die Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien“ erlaubt es den Nutzern, eine Zusammenfassung der mit ihren Konten verknüpften Informationen über die Aktivitäten des Nutzers auf Apps und/oder Webseiten, die von Drittunternehmen mit der Beklagten geteilt wurden, zu kontrollieren und abzurufen („Von Drittunternehmen geteilte Informationen über Aktivitäten“). Zusätzlich zu der Möglichkeit für Nutzer, über die Einstellung „Deine Aktivitäten außerhalb von Meta-Technologien“ eine Zusammenfassung ihrer „Neueste Aktivitäten“ abzurufen, können die Nutzer die von Drittunternehmen geteilten Informationen über Aktivitäten von dem jeweiligen Facebook-Konto „trennen“ lassen und/oder die künftigen Verknüpfungen zwischen dem Facebook-Konto und den von Drittunternehmen geteilten Informationen über Aktivitäten ausschalten. Die Beklagte stellt ihren Nutzern dabei jedoch keine Möglichkeit zur Verfügung, die Löschung der Off-Site-Daten herbeizuführen. Über das Tool werden zudem nur solche Drittwebseiten oder -apps angezeigt, die besucht wurden, während der Nutzer auf dem gleichen Gerät im Netzwerk der Beklagten eingeloggt war. Die innerhalb des Tools zu findenden Informationen teilen außerdem nicht mit, an welche konkrete Empfänger die Daten weitergegeben wurden. Zudem sind die Informationen auf einen Zeitraum von wenigen Monaten begrenzt. Die irische Datenschutzbehörde DPC verhängte im Mai 2023 ein Bußgeld i. H. v. 1,2 Milliarden EUR gegen die Beklagte wegen der unerlaubten Übermittlung von Daten der europäischen Nutzer

der Beklagten in die USA. Mit Schreiben vom 1. Februar 2024 (Anlage K3, Bl. 201ff. der Akte) forderte der Kläger die Beklagte auf, bis zum 22. Februar 2024 anzuerkennen, dass der Nutzungsvertrag bzgl. der Nutzung des Netzwerks „facebook“ eine Datenverarbeitung personenbezogener Daten des Klägers, die dessen Aktivitäten außerhalb des Netzwerks „facebook “ oder weiterer Produkte der Beklagten betreffen, und die über den Aufruf dritter Webseiten und Apps entstehen, ohne wirksame Einwilligung des Klägers grundsätzlich nicht zulasse. Weiterhin wurde die Beklagte zur Abgabe einer strafbewehrten Verpflichtungserklärung aufgefordert. Darin sollte sich die Beklagte verpflichten, die personenbezogenen Daten des Klägers nur noch auf ausdrückliche Weisung des Klägers zu verarbeiten. Weiterhin sollte sich die Beklagte verpflichten, die personenbezogenen Daten zu löschen, sobald der Kläger sie hierzu auffordere. Darüber hinaus sollte die Beklagte anerkennen, dass sie auf Anfrage des Klägers Auskunft über die o. g. erhobenen personenbezogenen Daten erteile. Die Beklagte sollte ferner eine strafbewehrte Unterlassungserklärung abgeben, wonach sie es zu unterlassen habe, personenbezogene Daten des Klägers, die dessen Aktivitäten außerhalb des sozialen Netzwerks über den Aufruf dritter Webseiten und Apps betreffen, ohne nachweisbare wirksame Einwilligung des Klägers zu verarbeiten, solange im Einzelfall kein Rechtfertigungsgrund nach Art. 6 DSGVO vorliege. Schließlich sollte sich die Beklagte zur Zahlung eines Schmerzensgeldes i. H. v. 5.000 EUR verpflichten. Die Beklagte reagierte auf das Schreiben zunächst nicht. Erst im Rahmen des Klageverfahrens antwortete sie dem Kläger mit Schreiben vom 10. Dezember 2024 (Anlage B8, Bl. 458ff. der Akte).

Der Kläger behauptet, er habe Internetseiten besucht, auf denen die streitgegenständlichen Business Tools installiert seien. Durch die damit einhergehende Verarbeitung seiner personenbezogenen Daten habe er einen Kontrollverlust in Bezug auf diese Daten erlitten. Er fühle sich unwohl, überwacht und eingeschränkt. Er sei sich über das komplette Ausmaß der Spionage der Beklagten nicht bewusst gewesen und habe die Befürchtung, dass die Daten missbräuchlich verwendet werden. Er fühle sich – insbesondere, weil er keine Einwilligung diesbezüglich erteilt habe – in seiner Privatsphäre verletzt.

Der Kläger meint, er könne gegenüber der Beklagte umfassend Auskunft über die von ihr mittels der Business Tools erlangten personenbezogenen Daten verlangen. Nach erfolgter Auskunftserteilung habe er das Recht, die Löschung bzw. wahlweise Anonymisierung der Daten zu verlangen. Die Verarbeitung der über die Business Tools erlangten personenbezogenen Daten durch die Beklagte sei von Anfang an rechtswidrig und insbesondere nicht von einer Einwilligung gedeckt. Durch die Einbindung der Business Tools auf Webseiten Dritter werde die Beklagte nach der Rechtsprechung des EuGH „Verantwortlicher“ i. S. d. DSGVO für sämtliche Webseiten und Apps, auf denen ihr Code laufe. Der Kläger ist der Ansicht, der ihm zustehende Schadensersatzanspruch sei auf mindestens 1.500 EUR zu beziffern.

Der Kläger hat mit Schriftsatz vom 27. März 2025 die ursprünglichen Anträge aus der Klageschrift unter Ziff. 1 und 2 abgeändert. Innerhalb dieses Schriftsatzes hat der Kläger neben den prozessual gestellten Anträgen auf Auskunftserteilung ein

außergerichtliches Auskunftsverlangen geltend gemacht (S. 41ff. des Schriftsatzes, Bl. 564ff. der Akte).

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 der folgenden personenbezogenen Daten der Klagepartei seit dem 01.12.2021 mit Hilfe der „Meta Business Tools“ erfasst, an die Server der Beklagten weitergeleitet, dort gespeichert und anschließend verwendet wurden und im Zuge dessen mit dem Nutzeraccount des Netzwerks „Facebook “ unter dem Benutzernamen [redacted] der Klagepartei verknüpft wurden,

a. auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der Klagepartei, ob direkt oder in gehashter Form übertragen, d.h.

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

sowie 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 von der Klagepartei auf der Webseite angeklickten Buttons sowie

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

c. in mobilen Dritt-Apps

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

außerdem für jedes erhobene Datum,

ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 01.12.2021 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 01.12.2021 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

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

2. Die Beklagte wird verpflichtet, nach vollständiger Auskunftserteilung gem. des Antrags zu 1. sämtliche gem. des Antrags zu 1 a. seit dem 01.12.2021 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 01.12.2021 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 01.03.2024, 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 meint, die Datenerhebung auf Drittwebseiten und -Apps sei rechtmäßig. Sie erfolge gemäß der in der Datenschutzrichtlinie dargelegten und einschlägigen Rechtsgrundlagen. Im Gegensatz zu den Ausführungen des Klägers sei der Betreiber der Drittwebseite bzw. der App-Anbieter dafür verantwortlich, eine entsprechende Einwilligung beim Nutzer einzuholen. Die Drittunternehmen seien Hauptverantwortliche für die Installation und Nutzung der Business Tools sowie für die Bereitstellung von Informationen zur Nutzung der Business Tools für die Besucher der jeweiligen Webseite oder App; schließlich obliege ihnen die Verantwortung zur Schaffung einer rechtlichen Grundlage für die Sammlung und Übermittlung von Daten an die Beklagte mittels der streitgegenständlichen Business Tools. Gemäß Abs. 3d der Business Tool Geschäftsbedingungen seien Drittunternehmen dafür verantwortlich, die nach der ePrivacy-Richtlinie erforderliche Zustimmung für die Speicherung und den Zugriff auf Cookies oder andere Informationen auf dem Gerät eines Endbenutzers einzuholen. Die Beklagte ist der Ansicht, mit dem außergerichtlichen Schreiben vom 10. Dezember 2024 (Anlage B8, Bl. 458ff. der Akte) habe sie das Auskunftsverlangen des Klägers bereits hinreichend beantwortet. Dem Kläger stünden zudem mehrere Tools zur Verfügung, mittels derer die angefragten Auskünfte jederzeit abgerufen werden könnten. Die übrigen angefragten Informationen seien in der beklagteneigenen Datenschutzrichtlinie enthalten. Der Anspruch auf Anonymisierung der Nutzerdaten finde keine Grundlage in der DSGVO. Schließlich habe der Kläger stets die Möglichkeit, über die bereitgestellten Nutzertools die von Drittunternehmen geteilten Informationen über Aktivitäten von seinem facebook-Konto zu trennen, auch könne er jederzeit seinen Account im Netzwerk der Beklagten vollständig löschen. Auch sonst sei die Datenverarbeitung mittels der Business Tools rechtmäßig und im Einklang mit der DSGVO. Nach der Auffassung der Beklagten wende sich die Klägerseite in der Hauptsache lediglich gegen die Datenverarbeitung zu Zwecken der Bereitstellung von personalisierter Werbung. Insoweit setze die Beklagte stets auf eine wirksame Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO. Eine Datenverarbeitung zu Werbezwecken finde hier jedoch nicht statt, da der Kläger eine entsprechende Einwilligung gerade nicht erteilt hat. Der Kläger habe die Möglichkeit, sich dafür zu entscheiden, das werbefreie Abonnement abzuschließen. Dann bekomme er überhaupt keine Werbung mehr angezeigt. Die im Übrigen vorgenommene Datenverarbeitung sei insbesondere aus Sicherheits- und Integritätszwecken gerechtfertigt. Dies erkläre auch die Datenschutzrichtlinie der Beklagten. Des Weiteren werde innerhalb der Klage nicht hinreichend konkretisiert, welche spezifischen Verarbeitungszwecke der Kläger angreifen wolle. Eine Darlegung der konkret besuchten und mit einem Business Tool ausgestatteten Webseiten und Apps fehle, sodass die Beklagte ihr prozessuales Verhalten hierauf nicht einstellen könne. Tools wie die streitgegenständlichen Business Tools seien natürlicher und allgegenwärtiger Bestandteil des Internets.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze und die zu den Akten gereichten Unterlagen Bezug genommen.

**Entscheidungsgründe:**

Die zulässige Klage hat auch in der Sache Erfolg.

I.
Die Klage ist vollumfänglich zulässig.

1.
Das Landgericht Siegen ist international, sachlich und örtlich zuständig. Die internationale und örtliche Zuständigkeit ergibt sich für die Verbraucherklage des Klägers aus Art. 6 Abs. 1, Art. 18 Abs. 1 Var. 2 EuGVVO (Brüssel Ia-VO) und Art. 79 Abs. 2 DSGVO.

2.
Soweit die Anträge aus der Klageschrift mit Schriftsatz vom 27. März 2025 teilweise geändert wurden, ist dies zulässig. Bei der Änderung der ursprünglichen Klageanträge unter den Ziffern 1 und 2 handelt es sich um einen Fall des § 264 Nr. 1 ZPO und damit nicht um eine echte Klageänderung, da die Anträge lediglich präzisiert wurden und eine Veränderung des ursprünglichen Streitgegenstands nicht stattfand.

3.
Insbesondere ist auch der Klageantrag zu 2, mit welchem eine Löschung bzw. Anonymisierung der im Klageantrag zu 1 benannten Daten verlangt wird, zulässig. Nach den vorliegenden Umständen ist die Besorgnis gerechtfertigt, dass die Beklagte sich der rechtzeitigen Leistung entziehen werde, § 259 ZPO. Voraussetzung für die Zulässigkeit des Antrags ist insoweit die begründete Erwartung des Gläubigers, dass sich der Schuldner der rechtzeitigen Leistung entziehen werde, was in der Regel begründet ist, wenn der Schuldner den Anspruch ernsthaft bestreitet. Die Beklagte hat zunächst das Schreiben der Prozessbevollmächtigten des Klägers vom 1. Februar 2024 (Anlage K3, Bl. 201ff. der Akte), mit dem bereits unter Fristsetzung Auskunfterteilung und anschließende Löschung bzw. Anonymisierung der Daten gefordert wurden, ignoriert. Nach Klageerhebung hat die Beklagte sich dann mit Schreiben vom 10. Dezember 2024 (Anlage B8, Bl. 458ff. der Akte) an den Kläger gewandt, dort dargelegt, wie sie sein Auskunftsbegehren verstehe, und darauf gestützt mitgeteilt, dass es unter Zugrundelegung dieses Verständnisses keine Daten gebe, über die Auskunft erteilt werden könne. Das mitgeteilte Verständnis der Beklagten von dem klägerischen Auskunftsbegehren, das dieses ohne nachvollziehbaren Grund auf die Datenverarbeitung zur Bereitstellung personalisierter Werbung verkürzt, ist angesichts der Ausführungen der Prozessbevollmächtigten des Klägers sowohl in dem vorprozessualen Schreiben vom 1. Februar 2024 als auch in der Klageschrift nicht verständlich. Vielmehr zeigt sich dadurch, dass die Beklagte weder gewillt ist, die begehrte Auskunft zu erteilen, noch dazu bereit, im Anschluss hieran die entsprechenden Daten zu löschen bzw. zu anonymisieren. Das Schreiben endet mit

dem Absatz: „Vor diesem Hintergrund gehen wir davon aus, dass keine weiteren Maßnahmen durch Meta erforderlich sind. Alle Recht sind ausdrücklich vorbehalten."

II.
Die Klage ist begründet.

1.
Dem Kläger stehen Auskunftsansprüche gegen die Beklagte gem. Art. 15 Abs. 1 lit. a, c, g und h DGSVO im tenorierten Umfang zu.

a)
Bei sämtlichen Datums-Angaben, die vom Klageantrag unter Ziff. 1 umfasst sind, handelt es sich um vom sachlichen Anwendungsbereich der Vorschrift erfasste personenbezogene Daten.

Unter „personenbezogenen Daten" sind gemäß der Legaldefinition in Art. 4 Nr. 1 DSGVO alle Informationen zu fassen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Dabei wird als identifizierbar eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Dazu gehören die E-Mail des Klägers, dessen Telefonnummer, sein Vor- und Nachname, sein Geburtsdatum, sein Geschlecht und der Ort, an dem er sich befindet. Ebenso handelt es sich bei der IP-Adresse des genutzten Clients um ein personenbezogenes Datum. Auch bei der internen Klick-ID der Meta Ltd und der internen Browser-ID der Meta Ltd. handelt es sich um personenbezogene Daten. Mit diesen Daten können die Aufrufe der Drittwebseite und die Aktionen darauf eindeutig einem bestimmten facebook-Konto zugeordnet werden, in diesem Fall dem Konto des Klägers. Auch die Lead-ID, die Abonnement-ID, die anon_id sowie die externe ID anderer Werbetreibender sind personenbezogene Daten, denn als „ID" stellen sie Identitätsdokumente bzw. Kennungen des Klägers dar bezüglich seiner Aktionen/Kontakte im Internet als potenzieller Kunde („Lead"), als Abonnent und hinsichtlich Installationen […] sowie die Kennung des Klägers bei anderen Werbetreibenden. Bei den Daten zum User-Agent des Clients, welche ausweislich des unstreitig gebliebenen klägerischen Vortrags die für das Digital Fingerprinting nutzbaren Daten darstellen, handelt es sich ebenfalls um personenbezogene Daten des Klägers.

Die URLs der Webseiten samt ihrer Unterseiten, der Zeitpunkt des Besuchs, der „Referrer" (d.h. die Webseite, über die der Nutzer zur aktuellen Webseite gekommen ist), die auf der Webseite angeklickten Buttons sowie die weiteren, von der Beklagten „Events" genannten Daten, die die Interaktion des Klägers auf der jeweiligen Webseite dokumentieren, sind ebenfalls personenbezogene Daten, da sie jeweils in

Verbindung mit weiteren Informationen dem Kläger zugeordnet werden können und dadurch Informationen zu Webseitenbesuchen über ihn beinhalten. Dies gilt entsprechend für den Namen der App, sowie den Zeitpunkt des Besuchs, den vom Kläger in der App angeklickten Buttons, sowie den von der Beklagten „Events“ genannten Daten, die die Interaktionen des Klägers in der jeweiligen App dokumentieren.

Der Kläger hat auch ein Interesse am Erhalt sämtlicher dieser Daten. Denn gerade erst aufgrund des Zusammenspiels der einzelnen technischen Daten ergibt sich ein Gesamtbild im Sinne eines Digital Fingerprintings. Auch wenn einzelne Daten bei getrennter Betrachtung aufgrund ihrer Abstraktheit auf den ersten Blick wertlos sein mögen, eröffnet die Addition aller erhobenen Daten die Möglichkeit, das Ausmaß des Digital Fingerprintings zu überprüfen. Aus diesem Grund darf es dem Kläger nicht verwehrt sein, Auskunft über die erhobenen Einzeldaten zu beanspruchen (vgl. LG Leipzig, Urteil vom 15. August 2025, Az. 5 O 1939/24, GRUR-RS 2025, 21426).

b)
Die Beklagte ist Verantwortliche im Sinne der DSGVO.

„Verantwortlicher“ i. S. d. DSGVO ist gem. Art. 4 Nr. 7 DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hierfür genügt es nach der Rechtsprechung des EuGH auch, dass die fragliche Person aus Eigeninteresse Einfluss auf die Mittel und Zwecke der Datenverarbeitung nimmt (BeckOK DatenschutzR/Spoerr, 53. Ed. 01.08.2025, DS-GVO Art. 26 Rn. 18 m. w. N.). Der erforderliche Beitrag zur Datenverarbeitung kann dabei nach der Rechtsprechung des EuGH bereits in der Ermöglichung der Erhebung der Daten und der Einflussnahme auf die Kategorien der Daten, welche erhoben werden sollen, liegen. Das trifft auf die Beklagte zu, die die von ihr entwickelten Business-Tools zur Verfügung stellt, die hier zugrunde gelegte Datenerhebung selbst konfiguriert hat und die ihr von den Drittanbietern übermittelten Daten auch nach eigenem Vortrag selbst und zum eigenen wirtschaftlichen Vorteil nutzt. Die Beklagte kann dem auch nicht überzeugend entgegenhalten, dass die Daten letztlich von den Drittwebseitenbetreibern erhoben und dann an sie weitergeleitet werden. Denn sie ist jedenfalls - ggf. neben den Drittwebseitenbetreibern – mitverantwortlich (vgl. EuGH, Urteil vom 29. Juli 2019, Az. C-40/17, MMR 2019, 579).

c)
Die Beklagte verarbeitet personenbezogene Daten i. S. v. Art. 4 Nr. 1 und 2 DSGVO in der im Tatbestand genannten Form: Die Beklagte erhebt personenbezogene Daten der Nutzer, sobald diese Webseiten oder Apps mit den Business Tools aufrufen bzw. wenn sie auf diese Webseiten Interaktionen durchführen. Sodann verknüpft die Beklagte die gewonnenen Daten mit dem Nutzerkonto des Klägers. Schließlich werden die Daten für die o. g. Zwecke verwendet.

Gem. § 138 Abs. 3 und 4 ZPO ist der vollständige klägerische Vortrag zum Vorgehen der Beklagten in Bezug auf die Datenerhebung und -verarbeitung, insbesondere zur Funktionsweise der Business Tools, der Übertragung der personenbezogenen Daten und der Erstellung von Nutzerprofilen, als unstreitig zugrunde zu legen. Die Beklagte ist dem klägerischen Vortrag in nicht erheblicher Weise entgegengetreten. Die Beklagte, die über die Daten des Klägers verfügt und damit dessen Vortrag substantiiert bestreiten müsste, beschränkt sich in ihrem Vortrag darauf, dass sie mangels Einwilligung des Klägers keine Datenverarbeitung zum Zweck der Bereitstellung personalisierter Werbung vornehme. Darüber hinaus gesteht die Beklagte zu, dass sie die Daten, welche ihr über die Business Tools übermittelt werden, für andere Zwecke wie beispielsweise „Sicherheits- und Integritätszwecke“ nutzt (siehe u. a. Schriftsatz vom 30. Oktober 2025, Rn. 47, Bl. 2418 der Akte).

Der Kläger hat auch ausreichend dargelegt, dass die Beklagte seine Daten in den streitgegenständlichen Business Tools verarbeitet. Der Kläger muss im Rahmen der Festlegung des streitgegenständlichen Sachverhalts nicht den konkreten Zweck der Datenverarbeitung, die er angreifen will, benennen. Die DSGVO nimmt lediglich auf der Seite der Rechtfertigung, insbesondere in Art. 6 und 9 DSGVO, eine Differenzierung nach dem Zweck der Datenverarbeitung vor. Demnach ist es allein die Aufgabe der Beklagten, im Rahmen der Darlegung eines Rechtfertigungsgrunds den von ihr verfolgten Zweck näher zu spezifizieren.

d)
Der Auskunftsanspruch wurde bislang weder außergerichtlich noch gerichtlich durch die Beklagte im Sinne von § 362 Abs. 1 BGB erfüllt.

aa)
Ein Auskunftsanspruch ist dann als erfüllt im Sinne von § 362 Abs. 1 BGB anzusehen, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 3. September 2020, Az. III ZR 136/18, NJW 2021, 765). Die Annahme eines derartigen Erklärungsinhalts setzt allerdings voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (BGH, Urteil vom 15. Juni 2021, Az. VI ZR 576/19, NJW 2021, 2726 m. w. N.).

bb)
Nach Auslegung des Erklärungswillens der Beklagten anhand objektiver Kriterien (vgl. §§ 133,157 BGB) bezweckte die Beklagte mit ihrem Schreiben vom 10. Dezember 2024 und auch mit den Schriftsätzen im Prozess keine Erfüllung

sämtlicher Auskunftsverlangen des Klägers, sondern waren in der tatsächlich erteilten Auskunft erkennbar bestimmte Auskunftsfragen ausgespart.

Aus allen Schreiben der Beklagten, insbesondere aber auch aus dem Schreiben vom 10. Dezember 2024 an den Kläger (Anlage B8, Bl. 458ff. der Akte), geht hervor, dass die Beklagte den vom Kläger geltend gemachten Auskunftsanspruch auf solche personenbezogenen Daten beschränkt ansehen möchte, die sie zur Bereitstellung personalisierter Werbung verarbeitet hat (vgl. Bl. 460 der Akte).

Eine solche Beschränkung ist dem Auskunftsbegehren des Klägers aber an keiner Stelle zu entnehmen. Hierauf hat der Kläger die Beklagte auch ausdrücklich, so zum Beispiel im Schriftsatz vom 27. März 2025, hingewiesen: „Außerdem ist die Nutzung der betreffenden Daten zur Bereitstellung personalisierter Werbung (im Beklagtennetzwerk) gerade nicht Kern des hiesigen Vorwurfs." (Seite 36 des Schriftsatzes vom 27. März 2025, Bl. 558 der Akte). Hiervon zeigte sich die Beklagte aber unbeeindruckt und beharrte auch in ihrem Folgeschriftsatz vom 23. April 2025 darauf, dass der Kläger nur Auskunft über die Verarbeitung von Daten von Drittwebseiten und -apps zur Bereitstellung personalisierter Werbung begehre (Seite 69 des Schriftsatzes vom 23. April 2025, Bl. 963 der Akte). Eine solche Auslegung ist jedoch, gerade auch in Anbetracht des ausdrücklichen klägerischen Entgegentretens, nicht nachvollziehbar und kann auch von der Beklagten nicht ernstgemeint gewesen sein. Vielmehr zeigt sich dadurch, dass die Beklagte – entgegen ihrem scheinbaren Entgegenkommen – das Auskunftsbegehren des Klägers gerade nicht beantworten wollte und will.

cc)
Die Beklagte erfüllt den Auskunftsanspruch des Klägers auch nicht dadurch, dass sie ihn auf ihr Service-Tool unter der Einstellung „Deine Aktivitäten außerhalb der Meta-Technologien" verweist. Der Verweis ist bereits grundsätzlich nicht geeignet, die Auskunftsfragen des Klägers zu beantworten, da auch diese Auskünfte allein nach dem Verständnis der Beklagten in Bezug auf die Verwendung personenbezogener Daten zu Werbezwecken erfolgen. Im Übrigen tritt die Beklagte der aus diesem Grund gem. § 138 Abs. 3 ZPO als zugestanden anzusehenden Behauptung des Klägers nicht entgegen, wonach über dieses Tool nur solche Drittwebseiten angezeigt werden, die besucht wurden, während der Nutzer auf dem gleichen Gerät im Netzwerk der Beklagten eingeloggt war. Dies gilt auch für Behauptung, die innerhalb des Tools zu findenden Informationen teilten nicht mit, an welche Dritten sie weitergegeben wurde. Zudem seien die Informationen auf einen Zeitraum von wenigen Monaten begrenzt. Darüber hinaus erklärt die Beklagte selbst, dass nicht sämtliche Daten über die von ihr zur Verfügung gestellten Tools beauskunftet werden: „Wir erhalten mehr Einzelheiten und Aktivitäten, als du unter „Aktivitäten außerhalb von Meta-Technologien" siehst. Aus technischen Gründen und aus Gründen der Zuverlässigkeit zeigen wir nicht alle Aktivitäten, über die wir informiert wurden. Das betrifft unter anderem Informationen, die wir erhalten haben, während du nicht bei Facebook angemeldet warst, oder Situationen, in denen wir nicht überprüfen können, ob du auf einem bestimmten Gerät zuvor Facebook verwendet hast. Ebenso wenig zeigen wir Einzelheiten an, wie etwa den Artikel, den du zu

deinem Einkaufswagen hinzugefügt hast.“ (Hilfeseite https://www.facebook.com/help/2207256696182627/, Bl. 461 der Akte), wobei die Beklagte diesen Textteil der Hilfeseite in ihrem Schreiben vom 10. Dezember 2024 gerade nicht mehr abdruckt (vgl. Bl. 463 der Akte).

dd)
Für eine Unmöglichkeit oder Unverhältnismäßigkeit der Erfüllung des Auskunftsanspruchs ist nichts ersichtlich und wurde von der Beklagten auch nichts vorgetragen.

2.
Der Antrag des Klägers, die Beklagte zur zukünftigen Löschung bzw. nach Wahl der Beklagten zur Anonymisierung sämtlicher im streitgegenständlichen Zeitraum erhobenen Daten zu verpflichten, ist begründet. Gem. Art. 17 Abs. 1 lit. d DSGVO i. V. m. § 259 ZPO kann die betroffene Person vom Verantwortlichen der Datenverarbeitung die Löschung der Daten verlangen, wenn die personenbezogenen Daten nicht rechtmäßig verarbeitet wurden.

a)
Die im Antrag Ziff. 1 aufgeführten personenbezogenen Daten des Klägers wurden durch die Beklagte durch die Verwendung der Business Tools unrechtmäßig verarbeitet. Dies geschah ohne Einwilligung oder sonstige Rechtfertigung.

aa)
Insbesondere der Nutzungsvertrag zwischen den Parteien gestattet die Verarbeitung der personenbezogenen Daten seit dem 25. Mai 2018 nicht. Die dem Urteil zugrunde zulegenden Datenverarbeitungsvorgänge sind nicht von einer Einwilligung des Klägers abgedeckt. Die Beklagte kann sich insbesondere nicht auf eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO berufen, da der Kläger eine entsprechende Einwilligung in den Profileinstellungen seines Accounts schon nach dem eigenen Vortrag der Beklagten nicht erteilt hat (vgl. insbesondere Protokoll vom 11. November 2025, Seite 2, Bl. 2491 der Akte).

bb)
Sonstige Rechtfertigungsgründe nach Art. 6 und 9 DSGVO hat die Beklagte nicht hinreichend vorgetragen.

Die Beklagte darf anders als in ihren AGB aufgeführt „App-, Browser- und Geräteinformationen“ und „Informationen von Partnern, Anbietern und Dritten“ nicht dauerhaft und uneingeschränkt ohne eine gesonderte Einwilligung zur „Erfüllung eines Vertrages“, zur „Erfüllung einer rechtlichen Verpflichtung“, zum Schutz „wesentlicher Interessen“, zur „Wahrung öffentlicher Interessen“ oder für die „berechtigten Interessen“ der Beklagten verarbeiten. Nach Art. 5 DSGVO trägt der Verantwortliche die Beweislast dafür, dass die Daten u. a. für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

(1)
Eine Rechtfertigung im Sinne von Art. 6 Abs. 1 UnterAbs. 1 Buchst. b DSGVO setzt voraus, dass die Verarbeitung objektiv unerlässlich wäre, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für diese Nutzer bestimmten Vertragsleistung ist, so dass der Hauptgegenstand des Vertrags ohne diese Verarbeitung nicht erfüllt werden könnte (vgl. (EuGH, Urteil vom 4. Juli 2023, Az. C-252/21, NJW 2023, 2997).

Die Beklagte trägt diesbezüglich nichts Konkretes vor, sodass der Rechtfertigungsgrund nicht in Betracht kommt.

(2)
Eine Rechtfertigung im Sinne von Art. 6 Abs. 1 UnterAbs. 1 Buchst. c DSGVO setzt voraus, dass die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche gemäß einer Vorschrift des Unionsrechts oder des Rechts des betreffenden Mitgliedstaats unterliegt, tatsächlich erforderlich ist, diese Rechtsgrundlage ein im öffentlichen Interesse liegendes Ziel verfolgt und in einem angemessenen Verhältnis zu dem verfolgten legitimen Ziel steht und diese Verarbeitung in den Grenzen des absolut Notwendigen erfolgt (vgl. EuGH a. a. O.).

Auch insoweit fehlt es an konkretem Vortrag der Beklagten.

(3)
Eine Rechtfertigung im Sinne von Art. 6 Abs. 1 UnterAbs. 1 Buchst. d und e DSGVO setzt voraus, dass die Verarbeitung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (lit. d), oder für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (lit. e) (vgl. EuGH a. a. O.).

In ihren Schriftsätzen beruft sich die Beklagte allein auf eine Datenverarbeitung zum Zwecke der Sicherheit und Integrität ihrer Systeme, d.h. auf Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DSGVO: „Vorliegend gestattet das Facebook-Konto der Klageseite die Nutzung von Meta Cookies auf Drittwebseiten und -Apps mit der Einstellung „Meta Cookies auf anderen Apps und Webseiten“ nicht. Entsprechend nutzt Meta Daten der Klageseite von Cookies und ähnlichen. Technologien für begrenzte Zwecke, wie Sicherheits- und Integritätszwecke.“ (Schriftsatz vom 23. April 2025, S. 47f., Bl. 940f. der Akte). Über diese pauschale Bemerkung hinaus trägt die Beklagte allerdings nicht weiter substantiiert vor. Der Vortrag der Beklagten reicht damit nicht aus, um den strengen Anforderungen des EuGH zu Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DSGVO gerecht zu werden. Die Beklagte erklärt nicht, wie personenbezogene Daten der Nutzer eingesetzt werden können, um den genannten Zwecken gerecht zu werden. Zudem wird nicht klar, in welchem Umfang und auf welche Art und Weise personenbezogene Daten erhoben werden. Eine Überprüfung der Angemessenheit der Datenverarbeitung ist damit nicht möglich.

(4)

Eine Rechtfertigung im Sinne von Art. 6 Abs. 1 UnterAbs. 1 Buchst. f DSGVO setzt voraus, dass der Betreiber eines sozialen Online-Netzwerks den Nutzern, von denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, dass die Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses absolut notwendig ist und dass sich aus einer Abwägung der einander gegenüberstehenden Interessen unter Würdigung aller relevanten Umstände ergibt, dass die Interessen oder Grundrechte und Grundfreiheiten dieser Nutzer gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (vgl. EuGH a. a. O.).

Dazu hat die Beklagte erklärt, dass sie sich auf diesen Rechtfertigungsgrund nicht stützt (Seite 45 der Klageerwiderung, Bl. 298 der Akte).

b)
Das Vorgehen der Beklagten verstößt darüber hinaus aus den gleichen Gründen gegen Art. 5 Abs. 2 DSGVO. Nach dem in dieser Vorschrift verankerten Grundsatz der Rechenschaftspflicht muss der Verantwortliche nachweisen können, dass die personenbezogenen Daten unter Einhaltung der in Art. 5 Abs. 1 DSGVO genannten Grundsätze erhoben und verarbeitet werden (EuGH, Urteil vom 4. Oktober 2024, Az. C-44621, NJW 2025, 207). In Artikel 5 Abs. 1 DSGVO ist unter anderem der Grundsatz der Datenminimierung (lit. c) verankert, der bestimmt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen (vgl. EuGH NJW 2023, 2997).

c)
Soweit es der Kläger für die Daten unter Antrag Ziff. 1 lit. b und c der Beklagten freistellt, ob diese eine Löschung oder Anonymisierung der Daten vornimmt, kann dahinstehen, ob sich dogmatisch ein selbstständiger Anspruch auf Anonymisierung von Daten überhaupt aus der DSGVO herleiten lässt (zum Streitstand Spindler/Schuster/Kaesling, Recht der elektronischen Medien, 5. Auflage 2026, Art. 17 DS-GVO Rn. 10 m. w. N.).

Der von Art. 17 DSGVO verwendete Begriff der Löschung ist rechtlicher Art und legt selbst nicht fest, auf welche Art und Weise die Löschung vollzogen wird. Löschung meint im technischen Kontext die Unbrauchbarmachung der personenbezogenen Daten oder die technische Löschung von elektronischen Daten. Eine Löschung im technischen Sinn meint einen Vorgang, nach dessen Ende auf die Daten bzw. deren Inhalt nicht mehr mit den üblichen Verfahren zugegriffen werden kann. Entscheidend ist dabei, dass die Daten nicht mehr verarbeitet und zu diesem Zweck auch nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können. Die theoretische Möglichkeit einer Wiederherstellung mit Spezialprogrammen hat hierbei keinen Einfluss auf die Löschung im Sinne der Norm (Paal/Pauly, DS-GVO BDSG, 3. Auflage 2021, Art. 17 DSGVO Rn. 30 m. w. N.).

Der Antrag des Klägers ist dahingehend auszulegen, dass die Unbrauchbarmachung der personenbezogenen Daten verlangt wird durch Löschung im Sinne des

allgemeinen Sprachgebrauchs oder durch Anonymisierung. In diesem Sinne vertritt auch der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) die Ansicht, dass die Anonymisierung von Daten mit deren Löschung gleichgesetzt werden kann, da sowohl bei einer Löschung als auch bei einer Anonymisierung keine Daten mehr vorliegen, die in den Anwendungsbereich der relevanten DSGVO-Vorschriften fallen. Entscheidend für die Gleichsetzung ist, dass der Personenbezug wirksam beseitigt wird (BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 29. Juni 2020, Seite 8, abgerufen unter https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Konsultationsverfahren/1_Anonymisierung/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 26. November 2025). Dies muss hier nach Auffassung des Gerichts unabhängig davon gelten, ob die Daten rechtmäßig oder rechtswidrig erhoben wurden, denn der Kläger lässt der Beklagten im Hinblick auf die Daten nach Buchst. b und c gerade die Wahl, in welcher konkreten Form sie die erlangten Daten löscht.

d)
Die Beklagte hat den Anspruch des Klägers auf Löschung bzw. Anonymisierung noch nicht erfüllt, insbesondere nicht durch die Zurverfügungstellung ihres Self-Service-Tools.

Zwar ist der Beklagten die Verwendung von automatisierten Verfahrensweisen zur Löschung bzw. Anonymisierung der Nutzerdaten grundsätzlich zuzubilligen (vgl. PaalPauly, Art. 17 DSGVO Rn. 29). Die Beklagte hat aber nicht hinreichend dazu vorgetragen, dass die von ihr zur Verfügung gestellten Tools eine vollständige Löschung sämtlicher unter Antrag Ziff. 1 genannten Daten ermöglichen. Auch über die Auswahl der Optionen „Frühere Aktivitäten Löschen“ bzw. „Künftige Aktivitäten trennen“ in seinen Datenschutzeinstellungen kann der Kläger lediglich erreichen, dass die Off-Site-Daten von seinem Account getrennt werden, nicht hingegen gelöscht. Die Trennung bedeutet eine Pseudonymisierung der Daten, die aber umkehrbar ist. Dies reicht gerade nicht für eine Löschung (vgl. LG Stuttgart, Urteil vom 5. Februar 2025, Az. 27 O 190/23, GRUR-RS 2025, 920).

e)
Der Kläger muss sich auch nicht auf die Löschung seines Nutzerprofils verweisen lassen. Aufgrund der überragenden marktübergreifenden Stellung der Beklagten im Bereich der Social-Media-Plattformen handelt es sich für die Teilhabe am gesellschaftlichen Leben bei den Netzwerken der Beklagten mittlerweile um für den durchschnittlichen Bürger essenzielle Dienstleistungen (vgl. Erwägungsgründe Nr. 1, 3 zur VO 2022/2065), die faktisch nicht durch ein alternatives Netzwerk ersetzt werden können (vgl. Mohr, EuZW 2019, 265). Dem Kläger ist es deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss ihm die Möglichkeit eröffnet bleiben, die Netzwerke der Beklagte zu nutzen, ohne dass die streitgegenständliche Datenverarbeitung über die Business Tools stattfindet.

3.
Der Kläger hat einen Anspruch auf Ersatz des immateriellen Schadens in Höhe von 5.000 EUR gem. Art. 82 DSGVO nebst Zinsen hieraus im tenorierten Umfang. Ob im Weiteren auch ein Anspruch gem. § 823 Abs. 1 BGB i. V. m. Art. 1, 2 GG besteht, kann dahinstehen, da dieser jedenfalls keinen höheren Schadensersatzanspruch begründen würde.

Nach der Rechtsprechung des EuGH besteht ein Schadensersatzanspruch im Sinne des Art. 82 Abs. 1 DSGVO, wenn ein Verstoß gegen die Datenschutz-Grundverordnung zu einem materiellen oder immateriellen Schaden führt (EuGH, Urteil vom 4. Oktober 2024, Az. C-507/23; BGH, Urteil vom 18. November 2024, Az. VI ZR 10/24, jeweils m. w. N.).

a)
Die Beklagte hat gegen Vorgaben der DSGVO verstoßen, indem sie personenbezogene Daten des Klägers ohne Rechtsgrundlage verarbeitet hat (s. o.).

b)
Der Kläger hat einen immateriellen Schaden erlitten.

aa)
Der Begriff des "immateriellen Schadens" ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren. Dabei soll nach ErwG 146 Satz 3 DSGVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Ein Schaden i. S. d. Art. 82 DSGVO kann jede materielle oder immaterielle Einbuße sein. Der bloße Verstoß gegen die DSGVO reicht zwar selbst noch nicht für die Begründung eines Schadensersatzanspruchs aus, es gibt jedoch umgekehrt auch keine Erheblichkeitsschwelle, deren Überschreitung es festzustellen gilt (EuGH, Urteil vom 4. Mai 2023, Az. C-300/21, GRUR-RS 2023, 8972).

Als Schaden ist nach der Rechtsprechung des EuGH bereits der nur kurzzeitige Verlust von Kontrolle über personenbezogene Daten oder die Befürchtung der missbräuchlichen Verwendung der eigenen Daten anerkannt (BGH, Urt. v. 18. November 2024, Az. VI ZR 10/24, GRUR-RS 2024, 31967 mit Verweis auf die Rechtsprechung des EuGH). Steht der Kontrollverlust fest, bedarf es darüber hinaus erst einmal nicht der Darlegung besonderer Ängste oder Befürchtungen der betroffenen Person, da diese Umstände lediglich zur Feststellung einer weiteren Schadensvertiefung herangezogen werden können (BGH a. a. O.).

bb)
Nach diesen Maßstäben liegt es auf der Hand, dass der Kläger einen solchen Kontrollverlust erlitten hat. Die Beklagte hat personenbezogene Daten des Klägers über die streitgegenständlichen Meta Business Tools ohne seine Einwilligung erhoben und bei sich gespeichert. Nach Einlassung der Beklagtenseite kann der Nutzer des sozialen Netzwerkes gerade nicht über die Ablehnung der

Nutzungsbedingungen oder Einstellungen seiner Privatsphäre eine Datenerhebung und Datenverarbeitung der Beklagten ausschließen. Selbst eine Ablehnung der Cookies der Drittwebseite führt insbesondere nicht zu einem Ausschluss der Datenerhebung der Beklagten, wie sie selbst einräumt. Es spielt insoweit keine Rolle, dass „nur“ http-Daten des Nutzers erhoben werden. Nach Überzeugung des Gerichts ist aus dem Umstand, dass eine Datenverarbeitung durch die Beklagte bereits mit Aufruf der Drittwebseite, auf der sich ein Business Tool der Beklagten befindet, stattfindet und nicht von Seiten des Nutzers ausgeschlossen werden kann, eine unzulässige Datenverarbeitung gegeben. Die Beklagte nimmt eine Datenverarbeitung ungeachtet einer Zustimmung vor. Dabei spielt es auch keine Rolle, dass es sich (auch) nur um „automatisch“ generierte Daten, wie http-Daten, handelt.

Nach dem der Klage zugrundeliegenden Tatbestand wurde das nahezu gesamte Online-Verhalten des Klägers 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 -betrug, 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 Oberzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhangende Sicherungsmaßregeln 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.“ Hierin liegen in jedem Fall ein erheblicher Kontrollverlust sowie das Risiko einer weiteren missbräuchlichen Verwendung der

Daten. Da die Verarbeitung personenbezogener Daten im hiesigen Fall besonders umfangreich ist – sie betrifft potenziell unbegrenzte Datenmengen und hat nahezu die vollständige Überwachung des Online-Verhaltens des Nutzers zur Folge – ist es nach der Feststellung des EuGH bereits abstrakt möglich, dass beim Nutzer das Gefühl einer kontinuierlichen Überwachung verursacht wird (EuGH, Urteil vom 4. Juli 2023, Az. C-252/21, GRUR 2023, 1131).

Zur Überzeugung des Gerichts ist der Kläger von der streitgegenständlichen Datenverarbeitung mittels der sog. Business Tools auch individuell betroffen. Substantiierter Vortrag zu einzelnen besuchten Webseiten war insoweit entbehrlich, da das Maß der Substantiierungspflicht von der jeweiligen Zumutbarkeit im Einzelfall abhängig ist. Die Pflicht zur Substantiierung findet ihre Grenzen in dem subjektiven Wissen der Partei und der Zumutbarkeit weiterer Ausführungen (vgl. etwa Mertins, Substantiierung im Zivilprozess, NJ 2009, 441). Hier war es dem Kläger grundsätzlich nicht zumutbar ist, näher zu den im streitgegenständlichen Zeitraum im Einzelnen aufgesuchten und mit Business Tools der Beklagten versehenen Homepages vorzutragen. Es reicht vielmehr grundsätzlich aus, dass der Kläger vorträgt, dass jeder Facebook-Nutzer mit erheblicher Wahrscheinlichkeit von Überwachungsmaßnahmen durch die eingesetzten Business- Tools betroffen war. Zum einen kann schon naturgemäß niemand mit vertretbarem Aufwand rekonstruieren, welche Homepages zu welchem Zeitpunkt er oder sie in der Vergangenheit besucht hat und auch ist niemand verpflichtet entsprechende Verlaufsprotokolle in seinen Rechnern vorzuhalten. Zum anderen wäre dem Kläger aber auch selbst dann, wenn dieses Wissen vorhanden wäre, kein substantiierterer Vortrag möglich, da die Klägerseite keinen auch nur ansatzweise vollständigen Überblick darüber hat, auf welchen Homepages zu welchem Zeitpunkt welche Business Tools der Beklagten enthalten waren. Faktisch wäre der Kläger dann entsprechend gezwungen, sein gesamtes Internetnutzungsverhalten offen zu legen, was gerichtlicherseits zu verlangen ersichtlich im eklatanten Widerspruch zum Normzweck der DSGVO stünde.

c)
Der Schaden ist kausal auf das Verhalten der Beklagten zurückzuführen, da diese den Kontrollverlust insbesondere durch den Einsatz der Business Tools verursacht hat.

d)
Art und Umfang des Schadensersatzanspruchs richten sich nach den nationalen Vorschriften in §§ 249ff. BGB und § 287 ZPO i. V. m. den europarechtlichen Vorgaben des haftungsbegründenden Tatbestands in Art. 82 DSGVO.

aa)
Die DSGVO enthält keine Bestimmung zu den Kriterien, nach denen die Höhe des Schadensersatzes zu bemessen wäre. Die Bemessung richtet sich vielmehr entsprechend dem Grundsatz der Verfahrensautonomie nach den innerstaatlichen Vorschriften über den Umfang der finanziellen Entschädigung. In Deutschland ist somit insbesondere die Verfahrensvorschrift des § 287 ZPO anzuwenden. Allerdings

unterliegt die Ermittlung des Schadens unionsrechtlichen Einschränkungen. Die Modalitäten der Schadensermittlung dürfen bei einem unter das Unionsrecht fallenden Sachverhalt nicht ungünstiger sein als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz). Auch dürfen sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz). In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs, wie sie in Erwägungsgrund 146 Satz 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld als "vollständig und wirksam" anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO dagegen nicht erfüllen. Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen hat. Im Ergebnis soll die Höhe der Entschädigung zwar nicht hinter dem vollständigen Ausgleich des Schadens zurückbleiben, sie darf aber auch nicht in einer Höhe bemessen werden, die über den vollständigen Ersatz des Schadens hinausginge. Ist der Schaden gering, ist daher auch ein Schadensersatz in nur geringer Höhe zuzusprechen. Dies gilt auch unter Berücksichtigung des Umstandes, dass der durch eine Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung (EuGH, Urteil vom 20. Juni 2024, Az. C-182/22, C-189/22, NJW 2024, 2599). Schließlich ist zu berücksichtigen, dass der Schadensersatzanspruch nach Art. 82 DSGVO neben den Sanktionen des Art. 83 DSGVO ebenfalls geeignet sein muss, die Einhaltung der Vorschriften der DSGVO sicherzustellen (EuGH, Urteil vom 11. April 2024, Az. C-741/21, NJW 2024, 1561).

bb)
Gemäß § 287 ZPO entscheidet das Gericht nach Würdigung aller Umstände nach freier Überzeugung, wobei hier die o. g. europarechtlichen Vorgaben zu beachten sind.

(1)
Ist nach den Feststellungen des Gerichts allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten – wie hier – gegeben, weil weitere Schäden nicht nachgewiesen sind, sind bei der Schätzung des Schadens insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten (vgl. Art. 9 Abs. 1 DSGVO) und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Weiter hat er die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle etwa durch Entfernung einer Veröffentlichung aus dem Internet (inkl. Archiven) oder Änderung des personenbezogenen Datums (z.B. Rufnummernwechsel; neue Kreditkartennummer) in den Blick zu nehmen.

Anknüpfungspunkt für die Bemessung eines immateriellen Schadensersatzanspruchs muss hier zudem vordergründig der auf der Klägerseite eingetretene Verlust der Daten sein. Dieser ist hinsichtlich des unterschiedlichen grundrechtlich garantierten Schutzniveaus der betroffenen Daten zu differenzieren. Dies gilt insbesondere, wenn besondere Kategorien personenbezogener Daten i. S. v. Art. 9 DSGVO betroffen sind. Zudem sind vor allem der Umfang der gesammelten Daten und die Dauer des Verstoßes bzw. der Verletzungshandlung zu berücksichtigen. Hierbei handelt es sich um Kategorien zur Feststellung der Schadenstiefe bzw. -intensität, die nicht gleichzusetzen sind mit dem Grad der Schwere des Verstoßes, den der EuGH für nicht berücksichtigungsfähig erklärt (OLG Dresden, Urteil vom 10. Dezember 2024, Az. 4 U 808/24, ZD 2025, 221).

(2)
Im Hinblick auf das Ausmaß und den Umfang der betroffenen Daten wird auf die obigen Ausführungen verwiesen, auch soweit es um die Grundrechtssensibilität der betroffenen Daten geht. Es kommt hinzu, dass der Kläger wegen des Schweigens der Beklagten zur streitgegenständlichen Datenverarbeitung im Ungewissen bleibt, ob er die Kontrolle der Daten durch Löschung o. ä. wiedererlangen könnte und ob und in welchem Umfang die Daten bereits an Dritte weitergegeben wurden und eine Datensicherung auch aus diesem Grund ausgeschlossen ist.

Es kommt hinzu, dass die allgemeine und unterschiedslose Sammlung von Daten eklatant gegen den Grundsatz der Datenminimierung verstößt und die unbegrenzte Speicherung personenbezogener Daten zu Zwecken der zielgerichteten Werbung auch bei Vorliegen einer entsprechenden Einwilligung des Klägers unverhältnismäßig wäre (vgl. EuGH, Urteil vom 4. Oktober 2024, Az. C-446/21, NJW 2025, 207).

Für den Wert der Daten für die Beklagte hat das Gericht auf die Feststellungen des BKartA (Beschluss vom 2. Mai 2022, Az. B 6-27/21, BeckRS 2022, 47486) zurückgegriffen. Demnach verfügt die Beklagte im Bereich der sozialen Medien über eines der führenden Werbeangebote. Im Jahr 2020 erzielte die Beklagte 86 Mrd. USD an Werbeeinnahmen, im Jahr 2021 bereits 115 Mrd. USD. Der Gesamtumsatz betrug im Jahr 2021 118 Mrd. USD, sodass der Anteil der Werbeeinnahmen einen Anteil i. H. v. 97 % ausmachte. Die Werbung wird hierbei überwiegend personalisiert geschaltet und basiert auf einem individuellen Zuschnitt für den jeweiligen Nutzer. Es soll dem Nutzer die Werbung angezeigt werden, die die ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte. Will ein Nutzer keine personalisierte Werbung angezeigt bekommen, hat er die Möglichkeit eine solche Option gegen Zahlung eines monatlichen Beitrags auszuwählen. Ausgehend hiervon hat sich das Gericht davon überzeugt, dass der Wert von Daten für das Geschäftsmodell der Beklagten unerlässlich ist und dass die von der Beklagten gesammelten Daten einen erheblichen Wert für diese haben – auch wenn sie die Daten nach dem insoweit zulässigen Bestreiten nicht für Werbezwecke nutzt. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm.

Es erschiene im Übrigen nicht zeitgemäß, einzelne Daten als belanglos einzustufen, da es dem vorliegenden Datenschutzverstoß gerade immanent ist, dass die für sich genommen abstrakten Daten erst in der Gesamtschau, d. h. nach Verbindung zu einem Persönlichkeitsprofil, ihr vollständiges Nutzungspotenzial entfalten (vgl. näher Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, Art. 82 DSGVO Rn. 18b).

(3)
Obwohl der BGH in seiner Rechtsprechung (BGH, Urteil vom 18. November 2024, Az. VI ZR 10/24, GRUR-RS 2024, 31967) ausführt, dass die entwickelten besonderen Befürchtungen und Ängste der betroffenen Person als Grundlage für das Gericht dienen, wie groß der eingetretene Schaden ist, bedurfte es im hiesigen Fall keiner Anhörung des Klägers, da sich der Kläger jedenfalls auf die sich aus der o. g. Reichweite des Schadens ergebende Mindestbeeinträchtigung für den Durchschnittsbetroffenen i. S. d. DSGVO im konkreten Fall berufen kann. Mit dem EuGH (zuletzt Urteil vom 4. Oktober 2024, Az. C-446/21, NJW 2025, 207) hat die potenziell unbegrenzte Datenverarbeitung der Beklagten zur Folge, dass bei den Betroffenen ein Gefühl der kontinuierlichen Überwachung des Privatlebens eintreten kann. Ausgehend von einem Durchschnittsbetroffenen i. S. d. DSGVO, der sich den o. g. Verletzungshandlungen ausgesetzt sieht, ist es dem Gericht möglich, den hieraus erwachsenden Grad der individuellen Betroffenheit zu schätzen.

(a)
Nach der Rechtsprechung des BGH ist es dem Tatgericht nach der nationalen Norm des § 286 ZPO grundsätzlich erlaubt, allein aufgrund des Vortrags der Parteien und ohne Beweiserhebung festzustellen, was für wahr und was für nicht wahr zu erachten ist (BGH, Beschluss vom 27. September 2017, Az. XII ZR 48/17, NJW-RR 2018, 249). Obwohl diese Rechtsprechung konkret auf die Überzeugungsbildung des Tatgerichts anhand einer informatorischen Anhörung abzielt, ist sie darüber hinaus auch so zu verstehen, dass das Gericht frei darin ist, seine Überzeugung nach § 286 ZPO jenseits der Strengbeweismittel zu bilden. Dies gilt insbesondere im Falle der Schadensschätzung nach § 287 ZPO, bei der die Freiheit der richterlichen Überzeugungsbildung zusätzlich geweitet ist. Insofern war es dem Gericht freigestellt, auf eine informatorische Anhörung des Klägers – so wie sie die meisten anderen Gerichte bislang vorgenommen haben – zu verzichten. Bei einer Anhörung des Klägers wäre nach Überzeugung des Gerichts gerade kein weiterer Erkenntnisgewinn zu erwarten gewesen, der über die Mitteilung des im Allgemeinen eher diffusen Gefühls des Datenverlusts und der Verunsicherung hinausgeht. Grund hierfür ist, dass es gerade das Problem des Klägers und auch des Gerichts ist, festzustellen, was konkret die Beklagte mit den Daten vorhat bzw. was sie bereits jetzt unternimmt. Da dies bis zuletzt nicht bekannt geworden ist, kann sich die Erwartung oder Befürchtung des Klägers nicht auf ein bestimmtes Verhalten konkretisieren. Dies kann und darf ihm nicht zum Nachteil gereichen.

(b)
Wie der EuGH in seiner Rechtsprechung jenseits des Datenschutzrechts, beispielsweise im Markenrecht, betont, ist auch unionsrechtlich für eine

Dienstleistung, die sich an ein allgemeines Publikum richtet, Prüfungsmaßstab für die Gerichte ein normal informierter, angemessen aufmerksamer und verständiger Durchschnittsverbraucher (siehe nur EuGH, Urteil vom 29. April 2004, Az. C-456/01 P und C-457/01 P, GRUR Int 2004, 631; Urteil vom 8. Oktober 2020, Az. C-456/19, GRUR 2020, 1195). Diese Grundsätze lassen sich auch auf den hiesigen Fall übertragen, da die Dienstleistungen bzw. das Produkt der Beklagten dem allgemeinen Verkehr gegenüber eröffnet sind. Damit lässt sich neben der spezifischen Betroffenheit einer einzelnen Person auch die des Durchschnittsbetroffenen i. S. d. DSGVO feststellen. Soweit – wie im vorliegenden Fall – die vorgetragene spezifische Betroffenheit nicht über das Maß der allgemeinen Betroffenheit hinausgeht und sich damit keine Schadensvertiefung aus dem klägerischen Vortrag ableiten lässt, kann sich das Gericht allein auf die allgemeine Beeinträchtigung des Durchschnittsbetroffenen i. S. d. DSGVO beziehen. Die Kammer konnte daher ohne auf das jeweilige subjektive Empfinden des konkreten Klägers abstellen zu müssen, eine durchschnittliche, aufgeklärte und verständige betroffene Person zu Grunde legen, und deren Betroffenheit als Maßstab für einen Mindestschaden zu nehmen.

(4)
Die Mindestbeeinträchtigung ist ohne das Hinzutreten weiterer Umstände bereits besonders schwerwiegend und hebt sich maßgeblich von den sog. Scraping-Fällen ab, in denen ein Mindestschaden i. H. v. 100 EUR für den bloßen Kotrollverlust für angemessen erachtet wird (siehe nur OLG Dresden a.a.O. m.w.N.). Anders als in den Scraping-Fällen ist die Quantität und Qualität der streitgegenständlichen Daten um ein Vielfaches größer, sodass der Mindestschaden weitaus höher einzustufen ist. Die Datenverarbeitung durch die Beklagte stellt nach der Rechtsprechung des EuGH per se einen schweren Eingriff in die durch Art. 7 und 8 der Charta der Grundrechte der Europäischen Union gewährleisteten Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten dar (EuGH, Urteil vom 4. Oktober 2024, Az. C-446/21, NJW 2025, 207), der nicht gerechtfertigt ist.

Die Verletzung dieser Grundrechte wird auch durch den Durchschnittsbetroffenen i. S. d. DSGVO als erhebliche Beeinträchtigung im o. g. Sinne wahrgenommen. Der aufgeklärte und verständige Durchschnittsbetroffenen i. S. d. DSGVO wird sich der Bedeutung und Tragweite der über ihn gesammelten Daten bewusst, denn er kennt die Relevanz von personenbezogenen Daten innerhalb einer digitalisierten Gesellschaft und Wirtschaft. Der Kontrollverlust über nahezu sämtliche Daten seiner Online-Nutzungsaktivitäten bedeutet für ihn eine dauerhafte und nicht ohne Weiteres zu beseitigende negative Beeinflussung, die sich nach außen hin in unterschiedlichen Sorgen und Ängsten manifestiert. In jedem Falle setzt sich der Nutzer gezwungenermaßen mit dem Verlust der personenbezogenen Daten auseinander und wird hierdurch in Bezug auf sein weiteres Verhalten bei der Nutzung des Internets dauerhaft beeinflusst.

Das Gericht erachtet anhand der obigen Ausführungen in der Gesamtschau einen Betrag i. H. v. 5.000 EUR für einen angemessenen Schadensersatz. Zum Vergleich hat das OLG Dresden in einer Entscheidung wegen Ausspähung durch Einschaltung

eines Detektivbüros einen Schadensersatzanspruch i. H. v 5.000 EUR für angemessen erachtet (OLG Dresden, Urteil vom 30. November 2021, Az. 4 U 1158/21, NZG 2022, 335). Die Reichweite der im hiesigen Verfahren betroffenen Daten geht über das Maß in dem Verfahren vor dem OLG Dresden hinaus, da nach dem als zugestanden anzusehenden klägerischen Vortrag dessen gesamtes im digitalen Bereich stattfindendes Privatleben dauerhaft und nicht nur auf einzelne Aspekte begrenzt aufgezeichnet wurde und immer noch wird. Seit dem Inkrafttreten der DSGVO handelt es sich bei dem als zugestanden anzusehenden Vorgehen der Beklagten um einen solch weitgehenden Verstoß, der den Rahmen der bisher bekannten Fälle bei weitem überschreitet, sodass der Mindestbetrag ohne Darlegung einer besonderen individuellen Betroffenheit mit dem des OLG Dresden in dem o. g. Verfahren gleichgesetzt werden kann.

Das Gericht ist sich bei dieser Entscheidung der Tatsache bewusst, dass das Zusprechen eines Betrags i. H. v. 5.000 EUR ohne das Erfordernis der spezifischen Darlegung einer über das gerichtlich festgestellte Maß der Mindestbeeinträchtigung hinausgehenden Intensität praktisch bedeutet, dass eine Vielzahl von Nutzern der Beklagten ohne größeren Aufwand Klage erheben kann. Dem stehen jedoch keine durchgreifenden Bedenken gegenüber, denn diese Form der privaten Rechtsdurchsetzung ist nach dem Willen des europäischen Gesetzgebers und der Rechtsprechung des EuGH nach den obigen Ausführungen gerade bezweckt und dient in Form des sog. Private Enforcement dazu, die Einhaltung der Vorschriften der DSGVO und damit deren Effektivität zu gewährleisten. Die Tendenz des europäischen Gesetzgebers zur Ermöglichung eines Private Enforcement ist dabei in jüngerer Zeit nicht zu verkennen, bspw. im Rahmen des Digital Markets Act. Art. 82 DSGVO ist in diesem Sinne „nur“ eine weitere Facette der Entwicklung hin zu mehr Private Enforcement (so auch Paal/Kritzer, NJW 2022, 2433).

(5)
Nicht anspruchsmindernd im Sinne eines widersprüchlichen Verhaltens wirkt sich aus, dass der Kläger die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Aufgrund der überragenden marktübergreifenden Stellung der Beklagten auf Social-Media-Plattformen (s.o.) ist es dem Nutzer, auch wenn er Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, deshalb nicht zuzumuten, dass er sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass der Kläger ihre Netzwerke DSGVO-konform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt der Kläger zum Ausdruck, dass ihm die Datenschutzverstöße der Beklagten nicht egal sind, sondern er eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es dem Kläger hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, sein Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden (vgl. Paal, ZfDR 2023, 325).

Demnach scheidet auch ein Mitverschulden des Geschädigten i. S. v. § 254 BGB aus.

e)
Der Kläger hat des Weiteren Anspruch auf Verzugszinsen aus der Schadensersatzforderung gem. §§ 286 Abs. 1, 288 Abs. 1 BGB. Durch die vorgerichtliche Zahlungsaufforderung vom 1. Februar 2024 (Anlage K 3, Bl. 201ff. der Akte) mit Fristsetzung bis zum 22. Februar 2024 befand sich die Beklagte in Verzug, sodass Zinsen wie beantragt, § 308 Abs. 1 ZPO, ab dem 1. März 2024 zuzusprechen waren.

4.
Der Kläger kann von der Beklagten Freistellung von den vorgerichtlichen Rechtsanwaltskosten i. H. v. 367,23 EUR verlangen, Art. 82 Abs. 1 DSGVO, §§ 249 Abs. 1, 257 Satz 1 BGB.

Außergerichtlich wurde u. a. ein Schmerzensgeldanspruch i. H. v. 5.000 EUR geltend gemacht. Der Klageantrag wurde später lediglich mit einem Betrag i. H. v. mindestens 1.500 EUR beziffert. Soweit das Gericht dennoch auf einen Schmerzensgeldbetrag i. H. v. 5.000 EUR erkennt, erfasst der Schadensersatzanspruch nach Art. 82 DSGVO als weitere materielle Schadensposition auch die Kosten, die durch die außergerichtliche Beauftragung eines Rechtsanwalts angefallen sind (BGH, Urteil vom 18. November 2024, Az. VI ZR 10/24, GRUR 2024, 1910). Die außergerichtliche Vertretung durch einen Rechtsanwalt war im damaligen Zeitpunkt erforderlich und zweckmäßig. Insbesondere war zur damaligen Zeit nicht absehbar, dass die Beklagte jegliche vorgerichtliche Einigung ablehnte. Im Übrigen handelt es sich um einen äußerst komplexen Sachverhalt, dessen außergerichtliche Geltendmachung dem Kläger allein nicht zuzumuten war. Damit waren die außergerichtlichen Kosten in jedem Fall auf Grundlage eines Streitwerts i. H. v. mindestens 5.000 EUR gerechtfertigt. Der geltend gemachte Betrag i. H. v. 367,23 EUR war demgemäß nach § 308 Abs. 1 ZPO begrenzt auf diese Höhe zuzusprechen.

III.
Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus § 709 Satz 1 ZPO.

IV.
Der Streitwert wird nach §§ 63 Abs. 2, 39 Abs. 1, 40, 43 Abs. 1, 48 Abs. 2 Satz 1, 48 Abs. 1 Satz 1 GKG i. V. m. §§ 3 ff. ZPO auf 8.000 EUR festgesetzt. Dabei wurden für den Auskunftsanspruch Ziff. 1 2.000 EUR, für den Klageantrag Ziff. 2 1.000 EUR und für den Klageantrag Ziff. 3 5.000 EUR zugrunde gelegt.