

Titel:

Erforderlichkeit der Substantiierung der individuellen Betroffenheit durch Meta-Business-Tools

Normenketten:

DSGVO Art. 15, Art. 17, Art. 24, Art. 82

BGB § 362

Leitsätze:

1. Ein Auskunftsanspruch nach Art. 15 DSGVO ist erfüllt, wenn der Verantwortliche erkennbar zum Ausdruck bringt, die begehrte Auskunft abschließend und vollständig erteilen zu wollen. Hierfür genügt es, wenn er die bereits mitgeteilten Informationen durch den Hinweis ergänzt, dass die betroffene Person über ein bereitgestelltes elektronisches Auskunftssystem selbst eine Übersicht ihrer verarbeiteten personenbezogenen Daten abrufen kann. Die Nutzung eines solchen Selbstbedienungstools stellt eine unionsrechtlich anerkannte Form der Auskunftserteilung dar. (Rn. 36 – 38) (redaktioneller Leitsatz)

2. Für eine auf Löschung personenbezogener Daten gerichtete Klage fehlt das Rechtsschutzbedürfnis, wenn die betroffene Person die begehrte Löschung ihres Nutzerkontos ohne Mitwirkung des Verantwortlichen jederzeit selbst über ein bereitgestelltes Self-Service-Verfahren veranlassen kann und weder rechtliche noch technische Hindernisse für die Eigenvornahme dargelegt werden. Wer die weitere Nutzung seines Accounts ausdrücklich fortsetzen will, kann zudem weder die vollständige Löschung noch die umfassende Anonymisierung sämtlicher Kontodaten verlangen, ohne konkret zwischen für den Accountbetrieb erforderlichen und entbehrlichen Datenbeständen zu unterscheiden. (Rn. 40 – 47) (redaktioneller Leitsatz)

3. Ein auf die Nutzung von Meta-Business-Tools gestützter Schadensersatzanspruch setzt substantiierten Vortrag dazu voraus, dass die betroffene Person tatsächlich solche Drittwebseiten oder Dritt-Apps genutzt hat, auf denen die betreffenden Tools zum maßgeblichen Zeitpunkt eingesetzt wurden. Allgemeine Ausführungen zur Datenerhebung durch Meta, die Vorlage von Listen potentiell betroffener Webseiten oder pauschale Schilderungen eigener Internetnutzungsgewohnheiten genügen nicht, um eine konkrete Verarbeitung personenbezogener Daten im Einzelfall darzutun. Die sekundäre Darlegungslast des Verantwortlichen entsteht erst dann, wenn die betroffene Person die von ihr genutzten Webseiten oder Anwendungen hinreichend konkret bezeichnet hat. (Rn. 57 – 62) (redaktioneller Leitsatz)

4. Auch unter Berücksichtigung der unionsrechtlichen Rechtsprechung, wonach bereits ein Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden i.S.d. Art. 82 DSGVO darstellen kann, bleibt die betroffene Person für das Vorliegen eines solchen Schadens darlegungs- und beweisbelastet. Erforderlich ist ein auf den konkreten Einzelfall bezogener Vortrag dazu, welche personenbezogenen Daten betroffen sind und worin sich der geltend gemachte Kontrollverlust oder die behauptete Beeinträchtigung manifestiert. Standardisierte, von der individuellen Betroffenheit losgelöste Darstellungen sowie die bloße Ablehnung einer Datenverarbeitung reichen hierfür nicht aus. (Rn. 66 – 73) (redaktioneller Leitsatz)

Schlagworte:

Auskunftsanspruch, Kontrollverlust, Erfüllung, Selbstbedienungstool, Rechtsschutzbedürfnis, Lösungsanspruch, Meta-Business-Tools, individuelle Betroffenheit

Rechtsmittelinstanzen:

OLG Bamberg, Beschluss vom 02.10.2025 – 10 U 43/25

BGH, Beschluss vom 26.02.2026 – I ZB 93/25

Tenor

1. Die Klage wird abgewiesen.
2. Die Klägerin hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Die Klägerin kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

4. Der Streitwert wird auf 7.000,- Euro festgesetzt.

Tatbestand

1

Die Klagepartei macht Auskunfts-, Verpflichtungs- und Entschädigungsansprüche wegen der Verletzung der Datenschutz-Grundverordnung (DSGVO) seitens der Beklagten geltend.

2

Die Klagepartei wendet sich insbesondere gegen die Verwendung der „Meta Business Tools“, insbesondere „Meta Pixel“, „App Events über F. SDK“ (bzw. „F. SDK“), „Conversions API“ und „App Events API“.

3

Die Klagepartei nutzt ausschließlich privat das Netzwerk ... unter dem Benutzernamen „...“ seit dem 31.12.2015. Betreiberin des Netzwerks und Verantwortliche im Sinne des Art. 4 DSGVO ist die Beklagte, bis zum 27.10.2021 als „...“ firmierend.

4

Die Klagepartei bekommt bei Nutzung des Netzwerks Werbung angezeigt, die auf ihren Interessen basiert, welche die Algorithmen der Beklagten u.a. aus den Tätigkeiten der Klagepartei in I. sowie den sozialen Kontakten, die sie in I. pflegt, extrahieren können.

5

Die Beklagte hat verschiedene sogenannte „Meta Business Tools“ entwickelt, die andere Webseitenbetreibern und App-Entwickler auf ihren Webseiten und in ihren Apps einbinden können, um ihrerseits Werbeeinnahmen zu generieren. Dies geschieht durch Einfügen eines einfachen Skripts im Code der Webseiten und Apps („Meta Pixel“ für Webseiten und „App Events über F.-SDK“ für Apps). Mittels dieser Tools werden Daten von I.-Nutzern auf Drittwebseiten und -Apps erhoben, wobei ein Teil dieser Daten (sog. technische Standarddaten) stets an die Beklagte übermittelt werden.

6

In ihrem I.-Account hat die Klagepartei unter der Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ die Auswahl getroffen, in die Datenverarbeitung durch die Beklagte zum Zwecke des Anzeigens von Werbung einzuwilligen.

7

Die Klagepartei behauptet, die Beklagte überwache den Internetverkehr der Klagepartei seit 25.05.2018 unter grober und vorsätzlicher Missachtung des europäischen Datenschutzrechts, indem sie deren persönlichen und höchstpersönlichen Daten massenweise rechtswidrig erhebe, 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. Die Beklagte überwache die durch die Business Tools erhaltenen personenbezogenen Daten dabei in einer Weise ähnlich der Staatssicherheit in der ehemaligen DDR.

8

Der genaue Umfang der bisher ausspionierten Daten sei dabei schwer nachzuweisen. Wann die Beklagte auf welchen Seiten und in welchen Apps was ausspioniert habe, lasse sich für den Nutzer nachträglich nicht überprüfen oder nachverfolgen. Die Klagepartei habe die Kontrolle über die Daten und „Spuren“, die sie bei der täglichen Nutzung des Internets hinterlasse, vollständig verloren. Eine Möglichkeit zur tatsächlichen Überprüfung, wie die Daten verwendet wurden, an wen sie weitergegeben wurden und was insbesondere der Mutterkonzern der Beklagten in den USA mit den Daten mache, sei der Kontrolle durch die deutsche Gerichtsbarkeit, erst recht dem Nutzer selbst längst vollständig entzogen.

9

Die Beklagte führe anhand der im Klageantrag zu 1) aufgeführten personenbezogenen Daten des Nutzers ein „Digital Fingerprinting“ durch. All diese Daten würden 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 beziehungsweise nicht eingeloggt sei und Cookies der Beklagten nicht zulasse. Entsprechend würden sämtliche Daten auch gesammelt, wenn Nutzer nicht bei den Netzwerken der Beklagten eingeloggt seien. Nutzer, die sich im Laufe ihres Lebens einmal auf den Netzwerken der Beklagten eingeloggt hätten, könne die Beklagte zuordnen und verknüpfe diese mit den anderen aggregierten Daten.

10

Da die Anbieter der wichtigsten Browser (Apple Safari, Mozilla Firefox, mit deutlicher Verspätung Google Chrome) seit 2019 die Cookiesetzung von Drittanbietern stückweise unterbänden und auch die Ausführung von Skriptanwendungen zumindest im Inkognito-Modus schwieriger gemacht hätten, habe die Beklagte 2021 die „Conversion API“ und die „App Events API“ eingeführt. Deren einziger Zweck bestehe 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 – Spionage weiterhin zu ermöglichen. Dies auch, wenn der Nutzer den Inkognito-Modus benutze und Cookies von Drittseiten nicht zulasse und sogar dann, wenn er ein VPN nutze. Dies werde möglich, indem sich die Conversion API serverseitig an den Server des Webseitenbetreibers anbinden lasse und von dort die für Fingerprinting notwendige Daten sowie „analoge“ persönliche Daten wie den Namen oder die Anschrift des Nutzers in gehashter Form geben lasse, ohne dass der Nutzer dies nachvollziehen oder gar verhindern könne. Diese Datenverarbeitung durch die Beklagte sei offensichtlich illegal. Die massenweise Datenerhebung über den gesamten Internetverkehr der Nutzer der Beklagten sei durch keine der in Art. 6 und 9 DSGVO normierten Rechtsgrundlagen gedeckt.

11

Eine wirksame Einwilligung – ob gegenüber der Beklagten selbst oder gegenüber Dritten – zur Weitergabe, dauerhaften Speicherung und Verarbeitung ihrer persönlichen und höchstpersönlichen Daten durch die Beklagte habe die Klagepartei niemals abgegeben. Die Klagepartei habe auf Dritt-Webseiten und in Dritt-Apps keine wirksame Einwilligung zur Verarbeitung der dort angefallenen Daten erteilt. Eine „Auslagerung“ dieser Verantwortung an die Webseitenbetreiber, welche die entsprechenden Einwilligungen einholen sollen, sei nicht möglich. Denn die Beklagte sei selbst alleinige „Verantwortliche“ für die Verarbeitung der Daten durch die eigenen „Meta Business Tools“ im Sinne des Art. 28 DSGVO.

12

Der Verstoß der Beklagten gegen die DSGVO stehe auch unabhängig vom individuellen Fehlverhalten gegenüber der Klagepartei fest. Durch die „Meta Business Tools“ sei die Integrität der informationstechnischen Systeme „Browser“ bzw. „Mobiltelefon“ auf den Geräten Nutzer und insbesondere der Klagepartei rechtswidrig angetastet worden. Zudem seien Webserver der Webseiten- und App-Betreiber ohne Wissen der Klagepartei so manipuliert worden, dass die Aktionen der Klagepartei auf den entsprechenden Seiten und Apps ausgelesen werden konnten. Hierdurch sei die entscheidende technische Hürde für eine vollständige Ausspähung und Überwachung des Privatlebens der Klagepartei genommen worden. Hierin liege die tiefgreifende, den Menschenwürdekern berührende Beeinträchtigung der informationellen Selbstbestimmung.

13

Die Klagepartei habe das Gefühl, im Privatleben vollständig von der Beklagten überwacht zu werden und fühle sich ihr ausgeliefert, da sie große Teile ihrer sozialen Kontakte über Social Media pflege. Zudem habe sie große Sorge, dass für die Beklagte mit Hilfe von künstlicher Intelligenz eine Analyse ihrer Interessen, Reizthemen, Hoffnungen und Sorgen möglich werde, die genutzt werden könne, um sie zu manipulieren. Darüber hinaus ärgere sie sich darüber, dass sie in einem demokratischen Rechtsstaat durch private Unternehmen aus Drittstaaten auf Schritt und Tritt ausspioniert werden könne und aufgrund der Übermittlung der Daten der Beklagten in die USA die Kontrolle über diese Daten niemals wieder zurückzuerlangen sei.

14

Die Klagepartei meint, die Verarbeitung ihrer personenbezogenen Daten gemäß Antrag 1 sei seit dem 25.05.2018 rechtswidrig gewesen.

15

Der Verpflichtungsanspruch gemäß Klageantrag zu 2) basiere auf Art. 9,6 DSGVO und zudem als vertragliche Nebenpflicht auf § 242 BGB sowie auf Art. 15 DSGVO, der Löschungsanspruch auf Art. 17 DSGVO, § 259 ZPO.

16

Der immaterielle Schadensersatzanspruch ergebe sich vorrangig aus Art. 82 DSGVO und § 823 BGB und sei in einer Höhe von mindestens 5000,-Euro angemessen. Es liege durch die vollständige Überwachung seitens der Beklagten seit dem 25.05.2018 ein schwerwiegender Eingriff des Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts vor. Die Klagepartei fühle sich der Beklagten aufgrund von deren Marktmacht ausgeliefert.

17

Die Freistellung von vorgerichtlichen Anwaltskosten sei aus Verzugsgesichtspunkten gerechtfertigt. Verzugsbegründend sei bereits die Installation der Überwachungsinstrumente der Beklagten in Form der „Meta Business Tools“ gewesen.

18

Die Klagepartei beantragt zuletzt,

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DSGVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 25.05.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks „...“ 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
- 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 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 25.05.2018 zu welchem Zeitpunkt an Dritte (Werbepartner, sonstige Partner, im Konzern verbundene Unternehmen oder sonstige Dritte) weitergegeben hat, unter Benennung dieser Dritten,

ob, und wenn ja welche konkreten Daten der Klagepartei die Beklagte seit dem 25.05.2018 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 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu löschen sowie sämtliche gem. des Antrags zu 1 b. sowie c. seit dem 25.05.2018 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 5.000,00 Euro beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 11.01.2024, zu zahlen.

4. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 627,13 Euro freizustellen.

19

Die Beklagte beantragt,

die Klage abzuweisen.

20

Die Beklagte ist der Auffassung, dass die Klage auf unzutreffenden Behauptungen und haltlosen Vorwürfen basiere.

21

Die Beklagte generiere Umsatz, indem sie Werbetreibenden die Möglichkeit biete, gegen Entgelt Anzeigen für ein Publikum auf i. zu präsentieren. Als Teil der Meta Produkte biete die Beklagte Funktionen wie die streitgegenständlichen Business Tools an, deren vorrangiger Zweck es sei, Drittunternehmen bei der Integration von Meta Produkten zu unterstützen sowie die Effektivität ihrer Werbeanzeigen zu messen und auf Meta Produkten Personen zu erreichen, die ihre Produkte oder Dienstleistungen nutzen oder an diesen interessiert sein könnten. Um die Drittunternehmen bei der Umsetzung dieser Ziele zu unterstützen, könnten sich die Drittunternehmen, welche die streitgegenständlichen Business Tools auf ihrer Webseite oder in ihrer App integriert hätten, dazu entscheiden, Kundendaten mit der Beklagten zu teilen. Kundendaten beinhalteten „event data“, das heißt Daten zur Aktivität auf der Webseite oder der App des Drittunternehmens, abhängig davon, welches der streitgegenständlichen Business Tools das

Drittunternehmen integriert habe. Ferner seien die Informationen enthalten, die Drittunternehmen entschieden hätten mit der Beklagten zu teilen, um bessere und interaktivere Inhalte und Werbeanzeigen zu erstellen und ein Publikum für Werbekampagnen aufzubauen.

22

Die Beklagte sei nicht der Inhaber oder Betreiber der Webseiten und/oder Apps Dritter und könne folglich auch nicht deren Webdienste „manipulieren“. Es sei daher nicht nachvollziehbar, auf welcher Grundlage die Klagepartei die Schlussfolgerung ziehe beziehungsweise unterstelle, die Beklagte solle die „Webserver“ von Drittunternehmen „manipuliert“ haben. Entscheidend sei, dass — wie aus den Business Tool Nutzungsbedingungen eindeutig hervorgehe — die Drittunternehmen maßgebliche Pflichten gegenüber den Besuchern ihrer Webseite und/oder App hätten. Insofern seien sie die maßgeblich Verantwortlichen für die Installation und Nutzung der streitgegenständlichen Business Tools, die Offenlegung von Informationen gegenüber den Besuchern ihrer Webseite oder Apps in Bezug auf die Nutzung der Meta Business Tools und die Erhebung und Übermittlung der Daten an die Beklagte durch Tools wie die streitgegenständlichen Business Tools. Dies entspreche zudem der praktischen Realität, wonach die Drittunternehmen diejenige Partei seien, die eine rechtzeitige Bereitstellung von Informationen gegenüber Besuchern ihrer eigenen Webseite oder App gewährleisten könnten. Die Beklagte hingegen sei weder Inhaber noch Verwalter oder Betreiber der Drittwebseiten und habe folglich auch keine Möglichkeit, den Besuchern Informationen über die Datenverarbeitungsaktivitäten dieser Webseiten zur Verfügung zu stellen.

23

Darüber hinaus lege die Klagepartei nicht konkret dar, dass die streitgegenständlichen Webseiten und/oder Apps, die in der Klageschrift oder der Anlage K2 gelistet werden, angeblich die vorstehend genannten Pflichten verletzt haben sollen. Die Business Tool-Nutzungsbedingungen würden den Drittunternehmen zudem ausdrücklich das Teilen von sensiblen Daten untersagen.

24

Die durch die Beklagte vorgenommene Datenverarbeitung sei aufgrund wirksamer Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO gerechtfertigt. Die Beklagte verwende für bestimmte Verarbeitungsvorgänge keine über Cookies und ähnliche Technologien erhobenen Daten des Nutzers, wenn ein Nutzer den Einsatz der optionalen „Cookies auf anderen Apps und Webseiten“ nicht erlaube. Selbst wenn ein Nutzer die Verwendung der optionalen „Cookies auf anderen Apps und Webseiten“ erlaube, müsse der Nutzer dennoch ausdrücklich über die Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ in die streitgegenständliche Datenverarbeitung nach Art. 6 Abs. 1 lit. a DSGVO einwilligen. Wenn ein Nutzer seine Einwilligung nicht über die Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ erteile, nehme die Beklagte keine streitgegenständliche Datenverarbeitung zum Zwecke personalisierter Werbung vor. Vorliegend habe die Klagepartei über die Einstellung „Informationen von Werbepartnern zu deinen Aktivitäten“ ausdrücklich und zustimmend in die Datenverarbeitung eingewilligt, weshalb die Datenverarbeitung zur Bereitstellung personalisierter Werbung zulässig sei.

25

Die Klagepartei habe nicht substantiiert vorgetragen, dass sie tatsächlich Webseiten oder Apps Dritter genutzt habe, die eines der streitgegenständlichen Business Tools verwendet habe, dass dabei tatsächlich persönliche Informationen der Klagepartei mittels der streitgegenständlichen Business Tools an die Beklagte übermittelt worden seien und dass die Beklagte die Daten der Klagepartei ohne eine valide Rechtsgrundlage im Rahmen der DSGVO verarbeitet habe. Die Klagepartei habe bewusst ihre Darlegungs- und Beweislast missachtet, indem sie keine Tatsachen oder Beweise bezüglich der angeblich eingetretenen Schäden durch die angeblich erfolgte streitgegenständliche Datenverarbeitung mitteile.

26

Die Auskunftspflichtung habe die Beklagte mit außergerichtlichem Schreiben vom 18.12.2024 (Anlage B 8a) erfüllt.

27

Hinsichtlich des Antrags auf Entschädigung habe die Klagepartei nicht dargelegt, dass sie infolge der streitgegenständlichen Datenverarbeitung einen tatsächlichen Schaden erlitten habe. Die angeblichen Ängste und Befürchtungen der Klageseite seien lediglich subjektive Empfindungen in Bezug auf potenzielle Ereignisse, deren Eintritt unwahrscheinlich sei. Zudem habe die Klagepartei ein grundlegend falsches

Verständnis von der streitgegenständlichen Datenverarbeitung. Ein Strafschadenersatz sei dem deutschen Rechtssystem fremd und auch nicht durch Unionsrecht vorgesehen.

28

Hinsichtlich des Antrags auf Entschädigung habe die Klagepartei nicht dargelegt, dass sie infolge der streitgegenständlichen Datenverarbeitung einen tatsächlichen Schaden erlitten habe. Die angeblichen Ängste und Befürchtungen der Klageseite seien lediglich subjektive Empfindungen in Bezug auf potenzielle Ereignisse, deren Eintritt unwahrscheinlich sei. Zudem habe die Klagepartei ein grundlegend falsches Verständnis von der streitgegenständlichen Datenverarbeitung. Ein Strafschadenersatz sei dem deutschen Rechtssystem fremd und auch nicht durch Unionsrecht vorgesehen.

29

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen, das Protokoll der mündlichen Verhandlung vom 21.01.2025 und vom 15.04.2025 und den sonstigen Akteninhalt Bezug genommen.

Entscheidungsgründe

30

Die Klage ist teilweise bereits unzulässig und im Übrigen unbegründet.

A.

31

Das Landgericht Bamberg ist zuständig.

32

Die internationale Zuständigkeit folgt aus Art. 82 Abs. 6, 79 Abs. 2 DSGVO sowie infolge rügeloser Einlassung aus Art. 26 Abs. 1 EuGVVO. Die sachliche Zuständigkeit ergibt sich aus § 1 ZPO in Verbindung mit den §§ 71 Abs. 1, 23 GVG, weil der Streitwert 5.000,00 Euro übersteigt und eine streitwertunabhängige Zuständigkeit des Amtsgerichts nach § 23 Nr. 2 GVG nicht vorliegt, sowie infolge rügeloser Einlassung aus § 39 ZPO. Die örtliche Zuständigkeit des Landgerichts Bamberg folgt aus § 44 Abs. 1 S. 2 BDSG.

B.

Klageantrag zu 1)

33

Der mit der Klage unter dem Antrag zu 1) geltend gemachte Auskunftsanspruch ist unbegründet.

34

Er wurde durch die Beklagte spätestens während des Rechtsstreites mit dem Schreiben vom 18.12.2024 (Anlage B8a), also noch vor dem insoweit maßgeblichen Zeitpunkt des Schlusses der mündlichen Verhandlung, erfüllt.

35

Die Beklagte hat durch dieses Schreiben der Klagepartei Auskunft erteilt. Außerdem hat sie in diesem Schreiben erläutert, wie die Klagepartei eine Übersicht der von der Beklagten verarbeiteten personenbezogenen Daten herunterladen kann.

36

Grundsätzlich gilt, dass ein Auskunftsanspruch erfüllt ist, 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 daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. So kann auch eine Erklärung, die den Besitz von Gegenständen verneint, eine Auskunft bilden, wenn der Wille des Erklärenden dahin geht, durch sie zum Ausdruck zu bringen, dass Gegenstände nicht vorhanden oder Handlungen nicht erfolgt sind, die der Aufklärungspflicht unterliegen oder wenigstens unterliegen könnten, d. h., wenn die verneinende Erklärung zur Beantwortung einer dem Erklärenden gestellten oder von ihm erwarteten Frage geschieht (BGH, Urteil vom 03.09.2020, III ZR 136/18, Rnr. 43 m.w.N.). Hier ergibt sich aus dem Inhalt des Schreibens der Beklagten eindeutig, dass

diese damit die in dem vorliegenden Rechtsstreit geltend gemachten Auskunftsansprüche der Klagepartei vollumfänglich erfüllen wollte.

37

In diesem Zusammenhang ist es auch ausreichend, wenn die Beklagte darin anstelle einer noch weitergehenden Auskunft erläutert hat, wie die Klagepartei eine Übersicht der von der Beklagten verarbeiteten personenbezogenen Daten herunterladen kann.

38

Eine Auskunftserteilung über ein elektronisches Auskunftssystem ist ausweislich Erwägungsgrund 63 DSGVO eine zulässige Art und Weise der Erteilung der Auskunft nach Art. 15 DSGVO. So heißt es in EG 63 DSGVO: „Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, das der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde.“ Damit hat der europäische Gesetzgeber die Möglichkeit eines Selbstbedienungstools gerade vorgesehen (LG Stuttgart, Urteil vom 24. Oktober 2024, 12 O 170/23 m.w.N.).

C.

Klageantrag zu 2)

39

Der Antrag zu 2) ist bereits unzulässig.

40

Ein Rechtsschutzbedürfnis für den Antrag auf Löschung der Daten ist nicht gegeben.

41

Die Klagepartei kann – als einfachere Möglichkeit – ihr Konto bei der Beklagten ohne weiteres selbst löschen. Die Klagepartei hat die Möglichkeit, ihr ... -Konto jederzeit zu löschen, indem sie das Self Service Tool der Beklagten nutzt, um die dauerhafte Löschung ihres Kontos zu initiieren. Die Klagepartei macht weder geltend, dass die Beklagte insoweit irgendwelche rechtlichen Einwände erhoben und das Recht der Klagepartei zur jederzeitigen Löschung ihrer Kontodaten bestritten habe, noch dass aus technischer Sicht in irgendeiner Weise eine Mitwirkung der Beklagten bei der Löschung der Daten erforderlich sei. Vorliegend möchte die Klagepartei jedoch nach eigenem Sachvortrag die Plattformen der Beklagten weiterhin nutzen, um insbesondere Kontakt zu Freunden und Bekannten zu pflegen sowie Informationen zum Nachrichtengeschehen in Erfahrung zu bringen. Bei innerer Abwägung der vorgetragenen Vorbehalte gegen das Geschäftsmodell der Beklagten einerseits und den Vorzügen desselben andererseits, hält die Klagepartei an der Nutzung des Angebots der Beklagten fest, wobei sie eine Änderung der Datenschutzeinstellungen bislang nicht für erforderlich erachtete. Die Klagepartei hat auch bislang darauf verzichtet, das Bezahlmodell ohne Tracking zu verwenden oder ihr Konto zu löschen und ein neues Konto anzulegen, um Altdaten aus ihrem Profil zu entfernen.

42

Sofern die Klagepartei wahlweise eine Anonymisierung der Daten fordert, gibt es keine Anspruchsgrundlage für eine solche „geleitete“ Verarbeitung.

43

Art. 17 DSGVO begründet nur ein Recht auf Löschung von Daten, sowie implizit eine Verpflichtung, diese Daten auch künftig nicht wieder zu speichern. Sonstige Rechte und Pflichten im Hinblick auf die Verarbeitung der Daten, etwa ein Verbot, diese an Dritte weiterzugeben, lassen sich aus der Vorschrift jedoch nicht ableiten.

44

Ein Anspruch gemäß Art. 18 Abs. 1 b) DSGVO kommt ebenfalls nicht in Betracht. Die Klagepartei hat schon nicht dargetan, dass die Verarbeitung der Daten unrechtmäßig ist (s.u.). Darüber hinaus behauptet nicht einmal die Klagepartei selbst, dass jedwede Verarbeitung ihrer Daten durch die Beklagte rechtswidrig sei.

45

Ansprüche aus nationalem Recht gemäß § 1004,823 BGB kommt ebenfalls nicht in Betracht. Die Anwendung nationalen deutschen Rechts ist im Hinblick auf den Anwendungsvorrang des unionsweit

abschließend vereinheitlichten Datenschutzrechts ausgeschlossen (BGH, Urteil vom 12. 10 2021, VI ZR 488/19; OLG Stuttgart Urteil vom 22.11.2023 4 U 20/23 Rnr 260ff).

46

Schließlich hat die Klagepartei auch nicht dargetan, dass sich aus dem zwischen den Parteien bestehenden Nutzungsvertrag irgendwelche Ansprüche auf die beantragte Einschränkung der Datenverarbeitung ergeben könnten.

47

Schließlich kommt hinzu, dass eine Löschung oder Anonymisierung sämtlicher Daten nicht in Betracht kommt, solange die Klagepartei weiterhin ihren bestehenden Account bei der Beklagten nutzen will. Die Klagepartei müsste deshalb in ihrem Antrag konkret differenzieren, welche Daten die Beklagte löschen oder anonymisieren muss, und welche sie für den weiteren Betrieb des Accounts unverändert weiter nutzen darf.

D.

Klageantrag zu 3)

48

Die Klagepartei hat keinen Anspruch auf Zahlung eines Schadensersatzes aus Art. 82 Abs. 1 DSGVO oder einer anderen denkbaren Anspruchsgrundlage.

49

Ein Verstoß gegen die DSGVO-Verordnung kann bereits nicht festgestellt werden. Die Verarbeitung der Daten erfolgte im Ergebnis rechtmäßig, sodass es nicht darauf ankommt, ob die Klagepartei einen (immateriellen) Schaden erlitten hat.

50

I. Soweit die Klagepartei letztlich beanstandet, dass die Beklagte den Betreibern von Drittseiten bzw. -Apps die Meta Business-Tools zur Verfügung stellt, hält das Gericht die Beklagte nicht für eine Verantwortliche im Sinne der Art. 4, 26 DSGVO. Dabei verkennt das Gericht nicht, dass die Zurverfügungstellung (ggf. auch) mit dem Ziel erfolgt, durch den tatsächlichen Einsatz der Tools seitens der Drittanbieter Daten zugeleitet zu erhalten.

51

Im Sinne des Art. 4 Nr. 7 DSGVO ist „Verantwortlicher“ eine natürliche oder juristische Person [...], die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

52

Der Begriff des Verantwortlichen dient dazu, die Verantwortlichkeit für die Einhaltung des Datenschutzes zuzuweisen und den Schutz der Rechte der betroffenen Personen sicherzustellen (vgl. Kühling/Buchner, DS-GVO BDSG, 4. Auflage 2024, Art. 4 Nr. 7 DSGVO, Rn. 6 mwN.).

53

Die Zurverfügungstellung der Tools ist bereits kein Datenverarbeitungsvorgang, von dem die Nutzer der Seiten der Drittanbieter unmittelbar betroffen wären. Die bloße Zurverfügungstellung der Tools ist gar kein Datenverarbeitungsvorgang. Betroffen sind die Nutzer durch den Einsatz der Tools, der indes von den Drittanbietern gesteuert wird. Diesen ist es auch überantwortet, sich mit dem jeweiligen Nutzer über den Einsatz der Tools resp. die Zulässigkeit einer Verarbeitung von dessen Daten überhaupt zu vereinbaren. Die Beklagte gibt den Drittanbietern lediglich ein technisches Instrument an die Hand, welches bei einer (zugelassenen) Datenverarbeitung genutzt werden kann.

54

Dies verdeutlicht die Beklagte ihren Nutzern auch, indem sie in ihrer Datenschutzrichtlinie (Anlage K1, dort S. 44) erläutert:

„Integrierte Partner behandeln die Informationen, die du mit ihnen teilst, gemäß ihren eigenen Nutzungsbedingungen und Richtlinien und nicht gemäß denen von Meta. Du kannst ihre Datenschutzrichtlinie auf/in ihrer jeweiligen Website bzw. App nachlesen. Darin erfährst du, wie sie deine Informationen erhalten und verarbeiten.“

55

II. Das Gericht geht allerdings davon aus, dass eine Verarbeitung der mittels Meta Business-Tools auf Drittwebsites oder Apps erhobenen und an Meta weitergeleiteten Daten im Sinne des Art. 4 Nr. 2 DSGVO durch die Beklagte erfolgt.

56

Entgegen dem Vortrag der Beklagten findet eine Verarbeitung der Daten nicht ausschließlich auf den Drittseiten/Apps und damit im Verantwortungsbereich der Drittanbieter statt. Die Beklagte hat diesbezüglich selbst vorgetragen, dass eine Überprüfung der übermittelten Datenbestände auf das Vorliegen einer Einwilligung erst nach Übermittlung und Speicherung dieser Daten auf den Servern der Beklagten erfolgt. Bereits in diesem Empfangen, Speichern sowie Abgleichen der Daten liegt eine Verarbeitung personenbezogener Daten, für welche die Beklagte die alleinige Verantwortung im Sinne des Art. 24 DSGVO trägt. Durch den Abgleich mit den zur Verfügung stehenden Daten sorgt die Beklagte für eine Identifizierbarkeit, indem sie den empfangenen Datenbestand einem I.-Nutzer zuordnet. Dieser Vorgang erfolgt nach dem Verständnis des Gerichts vorgelagert und damit vor jeder Prüfung einer entsprechenden Einwilligung des Nutzers.

57

Der geltend gemachte Anspruch scheitert bereits daran, dass die Klagepartei die Verarbeitung ihrer Daten durch die Beklagte nicht ausreichend substantiiert dargelegt hat. Voraussetzung sowohl für einen Anspruch auf Zahlung eines immateriellen Schadensersatzes nach Art. 82 DSGVO als auch für eine Entschädigung in Geld nach § 823 Abs. 1 BGB in Verbindung mit Art. 2 Abs. 1, Art. 1 Abs. 1 GG ist, dass die Beklagte überhaupt Daten der Klägerin auf Dritt-Webseiten oder Dritt-Apps verarbeitet. Denn fehlt es bereits an der streitgegenständlichen Datenverarbeitung durch die Beklagte, kann auch ein Verstoß gegen die Vorschriften der DSGVO oder eine Verletzung des Persönlichkeitsrechts der Klägerin nicht vorliegen.

58

Die Klagepartei hat indes nicht darzulegen vermocht, welche dieser drittbetriebenen Webseiten oder Apps sie besucht bzw. benutzt hat und dass dort zum relevanten Zeitpunkt Business-Tools zum Einsatz kamen.

59

Der sehr allgemein gefasste Vortrag der Klagepartei, der wenig Bezug zu ihrer persönlichen Situation aufweist, reicht nicht aus, um eine Verarbeitung ihrer Daten auf Dritt-Webseiten oder Dritt-Apps durch die Beklagte annehmen zu können. Es ist ein konkreter, auf die jeweilige Klagepartei zugeschnittener Vortrag zu fordern. Nicht ausreichend ist daher, lediglich allgemein vorzutragen, dass die Beklagte auf Dritt-Webseiten und Dritt-Apps Daten ihrer Nutzer erhebt und verarbeitet. Denn dieser Vortrag lässt zur Frage der individuellen Betroffenheit der Klagepartei noch keine konkreten Rückschlüsse zu. Daran ändert auch der Umstand nichts, dass die Klagepartei eine Liste mit einer Vielzahl von „großen“ Webseiten vorlegt und hierzu behauptet, diese nutzten die Meta-Business-Tools. Denn auch hieraus lässt sich nicht entnehmen, inwiefern die Klagepartei davon betroffen wäre. Zu keinem anderen Ergebnis führt sodann der einzig vorhandene individuelle Vortrag der Klagepartei zu ihren Internet-Nutzungsgewohnheiten (Seite 37 bis 42 des klägerischen Schriftsatzes vom 09.12.2024, Bl. 190 ff. d.A.). Dieser Vortrag ist zwar individuell auf die Klägerin bezogen, erschöpft sich inhaltlich aber in pauschalen Behauptungen, ohne auch nur eine einzige Webseite oder App konkret zu benennen. Dass die Klägerin nach ihrem Vortrag „regelmäßig einige der in Anlage K14 aufgeführten Webseiten“ bestimmter Kategorien besucht, stellt keinen ausreichend substantiierten Vortrag dar. Weder das Gericht noch die Beklagte können anhand dieses Vortrags eine konkrete Nutzung von bestimmten Webseiten, auf denen Meta-Business-Tools verwendet werden, feststellen.

60

Auf eine sekundäre Darlegungslast der Beklagten kann sich die Klägerin in diesem Zusammenhang nicht berufen. Eine sekundäre Darlegungslast der eigentlich nicht darlegungsbelasteten Partei wird angenommen, wenn die primär darlegungsbelastete Partei keine nähere Kenntnis von den maßgeblichen Umständen und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Prozessgegner alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. In diesem Fall trifft den Prozessgegner eine sekundäre Darlegungslast, im Rahmen derer es ihm auch obliegt, zumutbare Nachforschungen zu unternehmen. Genügt er seiner sekundären Darlegungslast

nicht, gilt die Behauptung des Anspruchstellers nach § 138 Abs. 3 ZPO als zugestanden.“ (vgl. BGH, Urteil vom 20.07.2021 — Az.: VI ZR 152/20, in: NJW-RR 2021, 1464, Rn. 16, m.w.N.).

61

Diese Voraussetzungen liegen hier nicht vor. Zwar mag der Klagepartei unbekannt sein, auf welchen Webseiten die Business-Tools der Beklagten genutzt werden. Jedenfalls ist ihr aber aus eigener Wahrnehmung bekannt, welche Webseiten sie selbst genutzt hat. Dies teilt sie indes nicht mit, was zu ihren Lasten geht. Die Klagepartei hätte hier konkret dazu vortragen müssen, welche Webseiten sie nutzt. Sodann wäre es gegebenenfalls Aufgabe der Beklagten gewesen, im Rahmen ihrer sekundären Darlegungslast aufzuzeigen, dass sie auf diesen konkret benannten Webseiten über ihre Business-Tools keine Daten der Klägerin erhebt.

62

Die Klagepartei hat insbesondere auch nicht dargetan, dass die Beklagte im konkreten Einzelfall der Klagepartei entgegen Art. 9 Abs. 1 DSGVO besonders sensible Daten der Klagepartei verarbeitet hat. Auch insoweit hat die Klagepartei nicht konkret und auf den Einzelfall bezogen dargelegt, dass sie irgendwelche Internetseiten aufgesucht hat, aus denen sich besonders sensible Daten im Sinne des Art. 9 Abs. 1 DSGVO ergeben würden.

63

III. Des weiteren – ungeachtet der Frage der Rechtmäßigkeit der Datenerhebung infolge Einwilligung der Klagepartei gemäß Art 6 Abs. 1 S. 1 lit. a) DSGVO – scheitert ein immaterieller Schadensersatzanspruch nach § 82 DSGVO zudem daran, dass das Gericht keinen Schaden, der durch etwaige Verstöße gegen die DSGVO verursacht worden wäre, festzustellen vermag.

64

1. Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

65

Für den hier geltend gemachten immateriellen Schadensersatz gelten dabei die im Rahmen von § 253 BGB entwickelten Grundsätze; die Ermittlung obliegt dem Gericht nach § 287 ZPO (BeckOK-DatenschutzR/Quaas, 43. Ed. 1.2.2023, DS-GVO Art. 82 Rn. 31). Es können für die Bemessung die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden, beispielsweise die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die betroffenen Kategorien personenbezogener Daten.

66

Die Darlegungslast für den Eintritt eines konkreten immateriellen Schadens liegt beim Betroffenen und kann bei behaupteten persönlichen/psychologischen Beeinträchtigungen nur durch die Darlegung konkretindividueller und nicht in einer Vielzahl von Fällen gleichartiger, dem Beweis zugänglicher Indizien erfüllt werden.

67

Der Begriff des „immateriellen Schadens“ ist in Ermangelung eines Verweises in Art. 82 I DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (stRspr, EuGH GRUR-RS 2024, 13978 Rn. 31 = DB 2024, 1676 – PS GbR; EuGH GRUR-RS 2024, 530 Rn. 64 = CR 2024, 160 – MediaMarktSaturn; EuGH GRUR 2023, 980 Rn. 30 u. 44. = VersR 2023, 920 – Österreichische Post). Dabei soll nach Erwgr. 146 S. 3 DSGVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich (stRspr, vgl. EuGH GRUR-RS 2024, 13978 Rn. 25 = DB 2024, 1676 – PS GbR; EuGH GRUR 2024, 784 Rn. 34 = NJW 2024, 1561 – juris; EuGH GRUR 2023, 980 Rn. 42 = VersR 2023, 920 – Österreichische Post).

68

Der Gerichtshof hat in seiner jüngeren Rechtsprechung unter Bezugnahme auf Erwgr. 85 DSGVO (vgl. ferner Erwgr. 75 DSGVO) klargestellt, dass schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (EuGH ECLI:EU:C:2024:827 = GRUR-RS 2024, 26255 Rn. 145, 156 iVm Rn. 137 = GRUR 2024, 1928 Ls. – Agentsia po vprisvaniyata; EuGH GRUR-RS 2024, 13978 Rn. 33 = DB 2024, 1676 – PS GbR; EuGH GRUR 2024, 784 Rn. 42 = NJW 2024, 1561 – juris; vgl. zuvor bereits EuGH GRUR-RS 2024, 530 Rn. 66 = CR 2024, 160 – MediaMarktSaturn; EuGH GRUR 2024, 150 Rn. 17-23 = NZA 2024, 56 – Gemeinde Ummendorf, sowie EuGH NJW 2024, 1091 = GRUR-RS 2023, 35786 Rn. 82 – Natsionalna agentsia za prihodite).

69

Freilich muss auch insoweit die betroffene Person den Nachweis erbringen, dass sie einen solchen – d.h. in einem bloßen Kontrollverlust als solchem bestehenden – Schaden erlitten hat (vgl. EuGH GRUR-RS 2024, 13978 Rn. 33 = DB 2024, 1676 – PS GbR; EuGH GRUR 2024, 784 Rn. 36 u. 42 = NJW 2024, 1561 – juris). Ist dieser Nachweis erbracht, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern.

70

Aber auch dann, wenn ein Kontrollverlust nicht nachgewiesen werden kann, reicht die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, aus, um einen Schadensersatzanspruch zu begründen (vgl. EuGH GRUR-RS 2024, 530 Rn. 67 = CR 2024, 160 Rn. 67 – MediaMarktSaturn; EuGH NJW 2024, 1091 = GRUR-RS 2023, 35786 Rn. 85 – Natsionalna agentsia za prihodite). Die Befürchtung samt ihrer negativen Folgen muss dabei ordnungsgemäß nachgewiesen sein (vgl. EuGH GRUR-RS 2024, 13978 Rn. 36 = DB 2024, 1676 – PS GbR; EuGH NJW 2024, 1091 = GRUR-RS 2023, 35786 Rn. 75-86 – Natsionalna agentsia za prihodite). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (vgl. EuGH GRUR-RS 2024, 13978 Rn. 35 = DB 2024, 1676 – PS GbR; EuGH GRUR-RS 2024, 530 Rn. 68 = CR 2024, 160 – MediaMarktSaturn).

71

2. Die Klagepartei hat nicht dargetan, dass ihr ein solcher Schaden entstanden ist.

72

Ein immaterieller Schaden in Form einer Beeinträchtigung des persönlichen Wohlbefindens ist nicht dargetan. Schriftsätzlich beschränkt sich der Klagevortrag hierzu auf die immergleichen standardisierten Formulierungen. Auch im Rahmen ihrer persönlichen Anhörung hat die Klagepartei lediglich geäußert, mit der Datenverarbeitung- und Nutzung auf I. nicht einverstanden zu sein, wobei besonders auffällt, dass die Klagepartei das Netzwerk I. auch nach Klageerhebung und bis zuletzt unter unveränderten Datenschutzeinstellungen verwendet. Eine nachvollziehbare Beeinträchtigung des persönlichen Wohlbefindens der Klagepartei ist nicht ersichtlich.

73

Auch ein immaterieller Schaden in Form eines Kontrollverlustes über persönliche Daten (vgl. hierzu zuletzt BGH Urteil vom 18.11.2024 – VI ZR 10/24, NJW 2005, 298 ff.) ist nicht dargetan. Auch dies würde voraussetzen, dass die Klagepartei konkret vorträgt, über welche persönlichen Daten sie durch ein Verhalten der Beklagten die Kontrolle verloren habe. Auch hier ist der völlig allgemeine und nicht auf den konkreten Einzelfall der Klagepartei bezogene Sachvortrag nicht ausreichend. Dies gilt insbesondere auch unter dem Aspekt, dass die Bemessung eines immateriellen Schadensersatzes nicht möglich ist, solange nicht feststeht, welche konkreten Daten von dem Kontrollverlust betroffen sind und inwieweit daher die Klagepartei hierdurch beeinträchtigt wird.

74

IV. Ein Schadensersatzanspruch gemäß § 823 Abs. 1 BGB i.V.m. dem Grundrecht auf informationelle Selbstbestimmung kommt aus denselben Gründen ebenfalls nicht in Betracht. Ein Schaden der Klagepartei ist bereits nicht dargetan.

E.

Klageantrag zu 4)

75

Mangels Zuerkennung des Hauptantrages steht der Klagepartei auch kein Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten zu.

F.

Nebenentscheidungen

76

Die Kostenentscheidung beruht auf § 91 Abs. 1 ZPO.

77

Der Ausspruch über die vorläufige Vollstreckbarkeit richtet sich nach §§ 708 Nr. 11, 711 ZPO. Die Festsetzung des Streitwertes richtet sich nach folgenden Überlegungen:

Antrag zu 1) 500, – Euro (§ 3 ZPO)

Antrag zu 2) 1.500, – Euro (§ 3 ZPO)

Antrag zu 3) 5.000, – Euro (§ 3 ZPO)

Antrag zu 4) 0, – Euro (§ 4 ZPO, § 43 Abs. 1 GKG)

GESAMT: 7.000, – Euro