

Amtsgericht Neukölln

Az.: 14 C 262/25



Im Namen des Volkes

Urteil

In dem Rechtsstreit

[REDACTED]

- Klägerin -

Prozessbevollmächtigte:

Rechtsanwälte **BK Baumeister & Kollegen Verbraucherkanzlei**, Viktoria-Luise-Platz 7,
10777 Berlin, Gz.: DTS-012782-24

gegen

Meta Platforms Ireland Ltd., vertreten durch d. Geschäftsführer, Merrion Road, Dublin 4, D04
X2K5, Irland

- Beklagte -

Prozessbevollmächtigte:

[REDACTED]

hat das Amtsgericht Neukölln durch den Richter am Amtsgericht Dr. [REDACTED] aufgrund der mündlichen Verhandlung vom 09.10.2025 für Recht erkannt:

1. Die Beklagte wird verurteilt, der Klägerin Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGS-VO darüber zu erteilen, welche der folgenden personenbezogenen Daten der Klagepartei seit dem 25.05.2018 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 „Instagram“ unter dem Benutzernamen [REDACTED] der Klagepartei verknüpft wurden,

a. auf Dritt-Webseiten und -Apps entstehende personenbezogene Daten der Klagepar-

tei, ob direkt oder in gehashter Form übertragen, d.h.

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

sowie bezogen auf sämtliche so verarbeiteten personenbezogenen Daten der Klagepartei

b. auf Dritt-Webseiten

- die URLs der Webseiten samt ihrer Unterseiten
- der Zeitpunkt des Besuchs
- der Referrer (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),

- die auf der Webseite angeklickten Buttons sowie
- weitere von der Meta „Events“ genannte Daten, die die Interaktionen auf der jeweiligen Webseite dokumentieren
- c. in mobilen Dritt-Apps
- der Name der App sowie
- der Zeitpunkt des Besuchs
- die in der App angeklickten Buttons sowie
- die von der Meta „Events“ genannte Daten, die die Interaktionen in der jeweiligen App dokumentieren

außerdem für jedes erhobene Datum,

- ob, und wenn ja welche konkreten personenbezogenen Daten der Klagepartei die Beklagte seit dem 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 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 5.000 € nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 13.05.2025 zu zahlen.

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

5. Im Übrigen wird die Klage abgewiesen.
6. Die Kosten des Rechtsstreits trägt die Beklagte.
7. Das Urteil ist für die Klägerin gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand

Die Parteien streiten über Ansprüche auf Auskunft, Löschung und Schadensersatz wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) im Zusammenhang mit der Verarbeitung von „Off-Site“-Daten über „Meta Business Tools“.

Die Klägerin nutzt das Netzwerk „Instagram“ seit dem 01.03.2014 teils privat und teils geschäftlich unter dem Nutzernamen [REDACTED]. Die Beklagte ist Betreiberin des Netzwerks. Sie hat ihren Unternehmenssitz in Dublin, Irland. Um das Netzwerk der Beklagten nutzen zu können, müssen Nutzende den Nutzungsbedingungen der Beklagten zustimmen. Innerhalb der dieser verlinkt die Beklagte auf ihre Datenschutzrichtlinie. Die Nutzung des Netzwerks ist kostenlos. Das Geschäftsmodell der Beklagten basiert darauf, dass Werbetreibende gegen Entgelt Anzeigen auf Instagram schalten.

Bei Nutzung des Netzwerks wird der Klägerin Werbung angezeigt, die auf ihren Interessen basiert. Diese Interessen werden von den Algorithmen der Beklagten aus den Tätigkeiten der Klagepartei auf Instagram sowie den dort gepflegten sozialen Kontakten extrahiert.

Die Beklagte ist Entwicklerin der sogenannten „Meta Business Tools“, zu denen „Meta Pixel“, „App Events über Facebook-SDK“ und „Conversions API“ und „App Events API“ (Meta Business Tools) gehören. Die Meta Business Tools können von Drittunternehmen auf deren Webseiten, Servern oder Apps eingebunden werden, um die Effektivität ihrer Werbeanzeigen zu messen und die Reichweite ihrer Werbeanzeigen in den Netzwerken der Beklagten zu erhöhen. Drittunternehmen können die Meta Business Tools in ihre Webseite („Meta Pixel“), oder App („App Events über Facebook-SDK“) einbinden, indem sie das entsprechende Skript in den Code der Webseite oder App einfügen. Seit dem Jahr 2021 ist auch eine Einbindung durch die Implementierung des entsprechenden Skripts auf den Servern der Drittunternehmen für deren Webseiten („Conversion API“) oder Apps („App Events API“) möglich. Drittunternehmen, die Meta Business Tools auf ihren Webseiten oder Apps einbinden, sind an die Nutzungsbedingungen für Meta Business

Tools gebunden.

Die Meta Business Tools der Beklagten sind auf zahlreichen reichweitenstarken Webseiten installiert. Für den durchschnittlichen Internetnutzer ist nicht erkennbar, ob die jeweilige Website mit einem solchen Tool ausgestattet wurde. Drittunternehmen, die Meta Business Tools auf ihrer Webseite oder in ihrer App eingebunden haben, können Kundendaten mit der Beklagten teilen. Die von den Drittunternehmen erhobenen Daten enthalten neben Geräteinformationen und Standortdaten sog. „event data“, d.h. Daten über die Nutzeraktivität. Dazu zählen beispielsweise Informationen darüber, wann die Website oder App des Drittunternehmens besucht wurde, welche Texte in die entsprechenden Felder eingegeben oder welche Optionen angeklickt wurden, welche Produkte in den Warenkorb gelegt wurden usw. Die Erfassung dieser „Off-site Daten“ erfolgt auf den Servern von Drittunternehmen, die diese an die Server der Beklagten weiterleiten. Die Beklagte speichert die empfangenen Datensätze ihrerseits und nimmt mindestens einen Abgleich mit ihren eigenen Datensätzen vor, um festzustellen, ob die Datenschutzeinstellungen des Nutzers es erlauben die Datensätze zu verwenden, um dem Nutzer personalisierte Werbung anzuzeigen. Die Beklagte überträgt die erfassten Daten weltweit, insbesondere in die USA.

Die Beklagte verwendet die mit den Business Tools auf Drittwebseiten und -Apps erfassten Daten zur Anzeige personalisierter Werbung, wenn der Nutzer in der Nutzeroberfläche des Netzwerks der Einstellung *„Cookies in Apps und auf Websites von anderen Unternehmen, die Meta Technologie nutzen“* zustimmt und in die Verarbeitung von Daten von Drittwebseiten- und -apps zur Bereitstellung personalisierter Werbung durch die Einstellung *„Informationen von Werbepartnern zu deinen Aktivitäten“* zugestimmt hat. Stimmt der Nutzer nicht zu, verarbeitet die Beklagte die Daten zu Sicherheits- und Integritätszwecken. Die Klägerin hat „Meta Cookies in anderen Apps und auf anderen Websites“ zugestimmt. In die Einstellung *„Informationen von Werbepartnern zu deinen Aktivitäten“* hat sie jedoch nicht eingewilligt.

Die Beklagte bietet Nutzern des Netzwerks „Instagram“ ein „Self-Service“ Tool an, mit dem sich Nutzer eine Zusammenfassung der von der Beklagten verarbeiteten Daten automatisiert übermitteln lassen können.

Mit Schreiben vom 18.03.2024 hat die Klägerin die Beklagte zur Auskunftserteilung und gegebenenfalls zur Löschung und Zahlung von Schadenersatz aufgefordert.

Die Klägerin behauptet, die Beklagte verarbeite die mit den Meta Business Tools erhobenen Daten auch, wenn der Nutzer nicht ausdrücklich in den Einstellungen zu *„Informationen von Werbepartnern zu deinen Aktivitäten“* zugestimmt hat.

Die Klägerin behauptet, die Beklagte verarbeite ihre personenbezogenen Daten besonderer Kategorien gemäß Art. 9 Abs. 1 DSGVO.

Die Klägerin behauptet, sie empfinde die weitreichende Überwachung ihres Privatlebens durch die Beklagte als äußerst beunruhigend. Die Übermittlung ihrer Daten in unsichere Drittstaaten wie die USA stelle eine erhebliche Hürde dar, um die Kontrolle über diese Daten wiederzuerlangen.

Die Klägerin behauptet, sie verbringe durchschnittlich mehr als eine Stunde pro Tag über einen Browser im Internet und nutze täglich gewöhnlich für länger als eine Stunde mobile Apps. Sie besuche regelmäßig einige der im Anlagenkonvolut K 14 aufgeführten Webseiten, insbesondere Webseiten der Kategorien Nachrichten und Politik, Finanzen, Gesundheit, Liebe und Sexualität, Rechtsdienstleistungen, Unterhaltung, Freizeit und Reisen, Shopping und Sonstiges. Des Weiteren lehne sie bereits seit längerer Zeit soweit möglich alle Cookies ab.

Die Klägerin ist der Auffassung, die Beklagte habe ihren Auskunftsanspruch aus Art. 15 DSGVO nur unzureichend erfüllt.

Die Klägerin hat zunächst das Landgericht Berlin II angerufen. Der Rechtsstreit wurde auf Antrag der Klägerin an das Amtsgericht Neukölln verwiesen.

Mit Schriftsatz vom 24.06.2025 hat die Klägerin den Klageantrag abgeändert.

Die Klägerin beantragt,

wie erkannt, wobei sie zu 3. Zinsen ab dem 16.04.2024 begehrt.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, sie verarbeite über Business Tools erhaltene personenbezogene Daten nur dann dazu, dem jeweiligen Nutzer personalisierte Werbung im Netzwerk Instagram anzuzeigen, wenn der Nutzer ausdrücklich in diese Datenverarbeitung gemäß Art.6 Abs. 1 lit. a) DSGVO eingewilligt habe. Andernfalls erfolge die Datenverarbeitung lediglich für andere Zwecke.

Die Beklagte meint, die begehrten Auskünfte seien der Klägerin mit Schreiben vom 05.06.2025 und 20.08.2025 erteilt worden, indem sie auf ihr „Self-Service“ Tool verwies.

Die Beklagte meint, die Erhebung und Verarbeitung der Daten über die Meta Business Tools sei

rechtmäßig.

Wegen der weiteren Einzelheiten wird auf den Inhalt der gewechselten Schriftsätze sowie das Protokoll der mündlichen Verhandlung vom 9. Oktober 2025 verwiesen.

Entscheidungsgründe

Die zulässige Klage hat auch in der Sache Erfolg.

Das Amtsgericht Neukölln ist gemäß Art. 79 Abs. 2 Satz 2 DSGVO international zuständig. Die internationale Zuständigkeit der deutschen Gerichtsbarkeit ergibt sich aus Art. 79 Abs. 2 S. 2 (i.V.m. Art. 82 Abs. 6) DSGVO. Gem. Art. 79 Abs. 2 S. 1 DSGVO sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Daneben dürfte auch Art. 18 Abs. 1 EuGVVO die internationale Zuständigkeit begründen (so OLG Dresden, Urt. v. 10.12.2024, Az. 4 U 815/24, GRUR-RS 2024, 38639 Rn. 2).

Das Gericht verweist zur Herleitung der Verantwortlichkeit der Beklagten i.S.d. DSGVO in unmittelbarem Bezug auf die Plattform umfassend auf die Ausführungen des LG Lübeck (Urt. v. 10.1.2025 – 15 O 269/23, GRUR-RS 2025, 81 Rn. 25): „Die Beklagte ist Verantwortliche bzw. Auftragsverarbeitende im Sinne der DSGVO. Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die Beklagte hat vorliegend als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden, sodass sie insoweit als Verantwortliche im Sinne der DSGVO anzusehen ist (vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris; vgl. im Einzelnen auch unten); sie ist auch keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.“

Die Beklagte ist nach dem tatsächlichen Vortrag der Klägerseite ebenfalls Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO für die streitgegenständlichen Business Tools. Insoweit sei auf die zutreffenden Ausführungen des LG Stuttgart verwiesen (Urt. v. 24.10.2024, Az. 12 O 170/23, GRUR-RS 2024, 36702 Rn. 23): „Die Beklagte trägt selbst vor, dass Drittunternehmen Business Tools der Beklagten auf ihrer Website oder in ihrer App integrieren und sich dazu entscheiden können, Kun-

dendaten mit der Beklagten zu teilen, um bessere und interaktivere Inhalte und Werbeanzeigen zu erstellen und ein Publikum für Werbekampagnen aufzubauen. Es führt zu keinem anderen Ergebnis, dass die Drittunternehmen – auch – maßgebliche Pflichten gegenüber den Besuchern ihrer Website und/oder App haben und insofern die maßgeblich Verantwortlichen für die Installation und Nutzung der streitgegenständlichen Business Tools, die Offenlegung von Informationen gegenüber den Besuchern ihrer Website oder Apps in Bezug auf die Nutzung der Meta Business Tools und die Erhebung und Übermittlung der Daten die Beklagte durch Tools wie die streitgegenständlichen Business Tools sind. Hieraus ergeben sich allenfalls weitere datenschutzrechtliche Ansprüche der Nutzer der jeweiligen Seiten gegen die jeweiligen Betreiber. Maßgeblich ist jedoch, dass die erhobenen Daten letztlich nicht bei den Drittunternehmen zur dortigen Verarbeitung und Nutzung verbleiben, sondern vielmehr zweckgerichtet mit der Beklagten geteilt werden. Ob diese Daten dabei anonymisiert oder sonst verfremdet werden, kann dahinstehen. Im Ergebnis führt die Weitergabe zu einer Personalisierung des Nutzererlebnisses bei der Beklagten und damit zu einer erneuten Nutzung der Daten durch die Beklagte. Dieser Umstand ist der Beklagten auch bewusst, da sie ihre Nutzer um eine entsprechende Einwilligung bei der Einstellung „Informationen über Aktivitäten von Werbepartnern“ bittet und gegen Gebühr auch eine werbefreie Nutzung der Plattform F. als werbefreies Abonnement anbietet.“

Die örtliche Zuständigkeit ergibt sich jedenfalls aus § 44 Abs. 1 S. 2 BDSG, da die Klagepartei ihren gewöhnlichen Aufenthaltsort an ihrem Wohnsitz in Neukölln hat.

Auf das streitgegenständliche Vertragsverhältnis ist nach Art. 3 Abs. 1, 6 Abs. 2 der VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO; ABl. 2008 L 177, 6) das von den Parteien gewählte deutsche Recht anzuwenden (vgl. hierzu und im Weiteren LG Leipzig Endurteil v. 4.7.2025 – 5 O 2351/23).

Die Anwendbarkeit der DSGVO ergibt sich in räumlicher Hinsicht aus Art. 3 Abs. 1 DSGVO und sachlich aus Art. 2 Abs. 1 DSGVO. Nach Art. 99 Abs. 2 DSGVO ist die Verordnung seit dem 25.05.2018 unmittelbar in den Mitgliedsstaaten anwendbar. Die streitgegenständliche Datenverarbeitung fand jedenfalls in der Zeit danach statt.

1. Auskunft

Die Klägerin kann von der Beklagten gemäß Art. 15 Abs. 1 lit. a, c, g, h DSGVO Auskunft über die Verarbeitung ihrer personenbezogenen Daten verlangen. Die Klägerin nutzt das Netzwerk „Instagram“ der Beklagten seit dem 01.03.2014 bis heute, mithin auch nach dem Inkrafttreten

der DSGVO. Die Klageanträge beziehen sich ausschließlich auf Datenverarbeitungsvorgänge ab dem 25.05.2018. Die Beklagte ist bezüglich der streitgegenständlichen Verarbeitungsvorgänge (gemeinsam) Verantwortliche, gemäß Art. 4 Nr. 7, 26 Abs. 1 Satz 1 DSGVO. Streitgegenständlich sind Verarbeitungsvorgänge über personenbezogenen Daten der Klägerin, die seit dem 25.05.2018 mit Hilfe der „Meta Business Tools“ von Drittunternehmen an die Server der Beklagten weitergeleitet, gespeichert, verwendet wurden und im mit dem Nutzeraccount des Netzwerks „Instagram“ unter ihrem Benutzernamen verknüpft wurden. Die streitgegenständlichen Verarbeitungsvorgänge umfassen

1. die Übermittlung der „Off-site Daten“ durch Drittunternehmen an die Beklagte,
2. die Speicherung der übermittelten „Off-site Daten“ durch die Beklagte,
3. den Abgleich der übermittelten „Off-site Daten“ mit den Datensätzen der Beklagten, zur Feststellung, ob die Daten zu Zwecken der personalisierten Werbung verarbeitet werden dürfen,
4. die Verarbeitung der übermittelten „Off-site Daten“ zu Sicherheits- und Integritätszwecken,
5. sowie die Verarbeitung der übermittelten „Off-site Daten“ zum Zweck der Anzeige personalisierter Werbung.

Die Beklagte verfolgt mit der Bereitstellung der Meta Business Tools das Ziel, die von den Drittunternehmen erhaltenen Daten zur verbesserten Produktwerbung einzusetzen. Als Entwicklerin der Meta Business Tools entscheidet die Beklagte auch maßgeblich über Art und Umfang der erhobenen Daten.

Nach der Rechtsprechung des EuGH im Fall „Fashion ID“ sind sowohl der Webseitenbetreiber als auch der Plugin-Ersteller Verantwortliche im Sinne der DSGVO, wenn der Webseitenbetreiber auf seiner Website ein Social Plugin einbindet, das den Browser des Webseitenbesuchers veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter übermittelt. Die bewusste Einbindung des Plugins mit dem Ziel, verbesserte Produktwerbung anzubieten, stellt eine Bestimmung über Zweck und Mittel der Erhebung personenbezogener Daten und deren Weitergabe durch Übermittlung dar (vgl. EuGH, Urteil vom 29.07.2019 - C-40/17). Diese Rechtsprechung ist entsprechend auf das vorliegend streitgegenständliche Meta Business Tool der Beklagten zu übertragen.

Die Beklagte ist ihrer datenschutzrechtlichen Verantwortlichkeit auch nicht dadurch enthoben, dass sie im Rahmen der mit den Drittunternehmen vereinbarten „Nutzungsbedingungen für Me-

ta-Business-Tools“, diese verpflichtet, einen stabilen und hinreichend auffälligen Hinweis für Nutzer bezüglich des Erfassens, Teilen sowie der Verwendung der Business-Tool-Daten bereitzustellen, der näher beschriebene Mindestangaben zu enthalten hat.

Die Klägerin ist auch individuell von der Datenverarbeitung betroffen. Sie ist Nutzerin des Netzwerks „Instagram“. Eine genaue Kenntnis und Darstellung der Webseiten, die Meta Business Tools verwenden und durch die Klägerin seit dem 25.05.2018 aufgerufen wurden, kann von der Klägerin nicht erwartet werden. Durchschnittliche Internetnutzer können nicht erkennen, ob die jeweilige Webseite mit einem Meta Business Tool ausgestattet worden ist. Wenn Drittunternehmen das Meta Business Tool „Conversions API“ an, ist dies selbst für technisch versierte Internetnutzer nicht erkennbar.

Die Beklagte führt die streitgegenständlichen Datenverarbeitungen unstrittig durch.

Der Anspruch auf Auskunftserteilung ist nicht durch Erfüllung erloschen. Die Beklagte hat den Auskunftsanspruch der Klägerin nicht erfüllt. Soweit die Beklagte in ihren Schreiben vom 05.06.2025 und 20.08.2025 auf ihr „Self-Service“- Tool verweist, vermag dies den Auskunftsanspruch der Klägerin nicht zu erfüllen. Das Tool ermöglicht Nutzern lediglich den Abruf rudimentärer Informationen, deren Umfang hinter dem der begehrten Auskünfte zurückbleibt. So zeigt das Tool lediglich, auf welchen Seiten die Nutzer getrackt wurden, solange sie auf demselben Gerät bei einem Netzwerk der Beklagten eingeloggt waren. Welche Seiten der Nutzer sonst noch (d. h. zu anderen Zeiten) besucht hat, auf welche Unterseiten er unterwegs war und welche Buttons er angeklickt hat, an welche Dritten Informationen weitergegeben wurden und welchem Verarbeitungszweck die jeweilige Datenverarbeitung diente, zeigt das Tool hingegen nicht.

2. Löschung

Die Klägerin hat einen Anspruch auf Löschung der im Tenor genannten personenbezogenen Daten, Art. 17 Abs. 1 DSGVO.

Die Beklagte hat als Verantwortliche die personenbezogenen Daten der Klägerin unrechtmäßig verarbeitet, § 17 Abs. 1 lit. d DSGVO. Die Beklagte ist in Bezug auf die streitgegenständlichen Datenverarbeitungen Verantwortliche im Sinne von Art. 4 Nr. 7, 26 Abs. 1 Satz 1 DSGVO und die Klägerin ist auch individuell durch die Datenverarbeitung betroffen.

Die Beklagte führt die streitgegenständlichen Datenverarbeitungen unstreitig durch. Für diese Datenverarbeitungen steht der Beklagten jedoch keine Rechtsgrundlage zur Seite. Nach Art. 6 Abs. 1 DSGVO ist die Verarbeitung nur rechtmäßig, wenn mindestens einer der Rechtfertigungsgrün-

de von Art. 6 Abs. 1 lit. a - f DSGVO erfüllt ist.

Eine Einwilligung der Klägerin in die Datenverarbeitungen liegt nicht vor. Soweit sich die Beklagte auf eine etwaige Einwilligung der Klägerin im Sinne des Art. 6 Abs. 1 lit. a DSGVO bezüglich der Verarbeitung der übermittelten „Off-site Daten“ zum Zweck der Anzeige personalisierter Werbung beruft, vermag diese aufgrund des Zweckbindungsgrundsatzes des Art. 5 Abs. 1 lit. b DSGVO die vorgelagerten Datenverarbeitungen bereits nicht zu rechtfertigen. Insoweit die Verarbeitung von „Off-Site“ Daten der Klägerin zur Bereitstellung von personalisierter Werbung erfolgt, liegt ebenfalls keine Rechtsgrundlage vor. Die Klägerin hat nicht in die Einstellung über „Informationen von Werbepartnern zu deinen Aktivitäten“ eingewilligt.

Die Datenverarbeitungen ist auch nicht nach Art. 6 Abs. 1 lit. b DSGVO zur Erfüllung des Nutzungsvertrages zwischen den Parteien notwendig. Dies ist der Fall, wenn die Datenverarbeitung objektiv unerlässlich ist, um dem Nutzer die Dienste des Netzwerks Instagram zur Verfügung zu stellen. Die Beklagte stellt den Nutzern jedoch gerade frei der Verarbeitung von „Off-Site Daten“ zuzustimmen.

Es bestehen weder eine rechtliche Verpflichtung noch lebenswichtige oder öffentliche Interessen an den Datenverarbeitungen gemäß Art. 6 Abs. 1 lit. c – e DSGVO.

In seiner Entscheidung vom 4.7.2023 hat der EuGH (a.a.O. = NJW 2023, 2997) die Anforderungen an die Rechtfertigung einer Datenverarbeitung nach den o.g. Vorschriften präzisiert. Er führt aus:

„4. Art. 6 I UAbs. 1 Buchst. b der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als im Sinne dieser Vorschrift für die Erfüllung eines Vertrags, dessen Vertragsparteien die betroffenen Personen sind, erforderlich angesehen werden kann, wenn diese Verarbeitung objektiv unerlässlich ist, 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.

5. Art. 6 I UAbs. 1 Buchst. f der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbei-

tung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich im Sinne dieser Vorschrift angesehen werden kann, wenn der fragliche Betreiber den Nutzern, bei denen die Daten erhoben wurden, ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses absolut notwendig ist und wenn 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.

6. Art. 61 UAbs. 1 Buchst. c der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, nach dieser Vorschrift gerechtfertigt ist, wenn sie 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.

7. Art. 6 I UAbs. 1 Buchst. d und e der VO (EU) 2016/679 ist dahin auszulegen, dass die Verarbeitung personenbezogener Daten durch den Betreiber eines sozialen Online-Netzwerks, die darin besteht, dass Daten der Nutzer eines solchen Netzwerks, die aus anderen Diensten des Konzerns, zu dem dieser Betreiber gehört, stammen oder sich aus dem Aufruf dritter Websites oder Apps durch diese Nutzer ergeben, erhoben, mit dem jeweiligen Nutzerkonto des sozialen Netzwerks verknüpft und verwendet werden, grundsätzlich – vorbehaltlich einer Überprüfung durch das vorlegende Gericht – nicht als im Sinne von Buchst. d erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, oder als im Sinne von Buchst. e für die Wahrnehmung einer

Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, angesehen werden kann.“

Über den pauschalen Vortrag, eine Datenverarbeitung diene dem Zwecke der Sicherheit und Integrität ihrer Systeme, trägt die Beklagte nicht weiter substantiiert vor. Der Vortrag reicht nicht aus, um den strengen Anforderungen des EuGHs zu Art. 6 Abs. 1 UAbs. 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 (vgl. LG Leipzig, a.a.O.). Insofern wird bereits dem Erforderlichkeitskriterium des EuGHs nicht hinreichend Rechnung getragen. Zudem wird nicht klar, in welchem Umfang und auf welche Art und Weise personenbezogene Daten erhoben werden. Insofern kann das Gericht keine Überprüfung zur Angemessenheit der Datenverarbeitung vornehmen. Zu den sonstigen Rechtfertigungsgründen innerhalb von Art. 6 DSGVO wurde ebenfalls nicht hinreichend vorgetragen. Da es bereits an diesen Voraussetzungen fehlt, sind erst Recht die strengeren Anforderungen nach Art. 9 DSGVO nicht erfüllt. Im Übrigen verstößt das Vorgehen der Beklagten 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, Ur. v. 4.10.2024, Az. C-446/21, NJW 2025, 207 Rn. 55). 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 (EuGH, a.a.O, NJW 2023, 2997).

Auch Art. 6 Abs. 1 lit. f DSGVO rechtfertigt die Datenverarbeitungen nicht. Die Interessensabwägung gemäß Art. 6 Abs. 1 lit. f DSGVO fällt nicht zugunsten der Beklagten aus. Zwar hat die Beklagte ein berechtigtes Interesse an einem profitablen Dienst, jedoch überwiegen die Interessen der Klägerin an Datensicherheit und -minimierung sowie an informationeller Selbstbestimmung. Obwohl die Nutzung des Netzwerks der Beklagten unentgeltlich ist, musste die Klägerin nicht damit rechnen, dass die Beklagte ihre personenbezogenen Daten, die auf Webseiten von Drittunternehmen erhoben wurden, ohne Einwilligung verarbeitet.

Für die Verarbeitung von Daten besonderer Kategorien gemäß Art. 9 Abs. 1 DSGVO stellt Art. 6 Abs. 1 lit. f DSGVO bereits keine Rechtsgrundlage dar. Die Beklagte verarbeitet personenbezogene Daten besonderer Kategorien der Klägerin. Die Klägerin hat hinreichend dargelegt, dass sie Webseiten zu den Themen Politik, Sexualität, Gesundheit und Liebe besucht, die mit einem Meta Business Tool der Beklagten ausgestattet sind. Dies hat die Beklagte nicht qualifiziert bestrit-

ten. Aufgrund der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO ist die Beklagte verpflichtet, eine umfassende Dokumentation von Verarbeitungsvorgängen zu führen. Ein qualifiziertes Bestreiten wäre ihr somit auch möglich gewesen.

3. Zahlung

Die Klägerin hat gegen die Beklagte einen Anspruch auf Zahlung von 5.000.- € Schadensersatz aus Art. 82 DSGVO.

Der Schadensersatzanspruch besteht dem Grunde nach. Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Ein Schadenersatzanspruch besteht laut gefestigter Rechtsprechung des EuGH, wenn eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO erfolgt und kausal zum Entstehen eines materiellen oder immateriellen Schadens der betroffenen Person führt (EuGH, Urt. vom 04.05.2023 – C-300/21, Urt. vom 14.12.2023 – C-340/21, Urt. vom 21.12.2023 – C-667/21).

Die Klägerin ist anspruchsberechtigt. Sie ist durch die Datenverarbeitungen der Beklagten individuell betroffen. Die Beklagte ist (Mit)Verantwortliche der Datenverarbeitung und war an dieser beteiligt. Es liegt ein Verstoß gegen Art. 6 Abs. 1 DSGVO vor. Die Datenverarbeitungen erfolgten ohne Rechtsgrundlage (s.o. unter 2.).

Der Klägerin ist ein kausaler immaterieller Schaden entstanden. Gemäß Art. 82 DSGVO sind sowohl materielle als auch immaterielle Schäden zu ersetzen. Der bloße Verstoß gegen die DSGVO reicht zwar selbst noch nicht für die Begründung eines Schadensersatzanspruchs aus (EuGH, Urt. v. 4.5.2023, Az. C-300/21, GRUR-RS 2023, 8972 Ls. 1), es gibt jedoch umgekehrt auch keine Erheblichkeitsschwelle, deren Überschreitung es festzustellen gilt (siehe nur EuGH, a.a.O., GRUR-RS 2023, 8972). Als Schäden sind insbesondere in der Rspr. bereits anerkannt der Verlust von Kontrolle über personenbezogene Daten oder die Befürchtung der missbräuchlichen Verwendung der eigenen Daten (BGH, Urt. v. 18.11.2024, Az. VI ZR 10/24, GRUR-RS 2024, 31967 Rn. 30 u.a. mit Verweis auf den 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., GRUR-RS 2024, 31967 Rn. 31).

Nach dem der Klage zugrundeliegenden Tatbestand wurde nahezu das gesamte Online-Verhal-

ten der Klägerin dokumentiert und in Persönlichkeitsprofilen ausgewertet. Damit ist auch der unantastbare Kernbereich der privaten Lebensgestaltung der Klägerin 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 Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft (LG Ellwangen (Jagst), a.a.O., S. 42 f.). 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 EuGHs bereits abstrakt möglich, dass beim Nutzer das Gefühl einer kontinuierlichen Überwachung verursacht wird (EuGH, a.a.O., GRUR 2023, 1131, Rn. 118).

Die Klägerin hat substantiiert dargelegt, dass sie die weitreichende Überwachung ihres Privatle-

bens durch die Beklagte als äußerst beunruhigend empfindet und dass es für sie eine erhebliche Hürde darstellt, die Kontrolle über diese Daten wiederzuerlangen, da ihre Daten in unsichere Drittstaaten wie die USA übermittelt werden.

Der Verstoß gegen Art. 6 Abs. 1 DSGVO war auch geeignet den Schaden auszulösen. Unbefugte Datenverarbeitungen können zu einem Gefühl des Beobachtetwerdens und der Hilflosigkeit führen, was die betroffenen Personen zu einem reinen Objekt der Datenverarbeitung degradiert.

Der Schadensersatzanspruch ist in Höhe von 5.000 € gerechtfertigt.

Nach der Rspr. des EuGHs ermöglicht die DSGVO ausschließlich einen Schadensersatz zum Zwecke des Ausgleichs, nicht auch zur Genugtuung. Die Vorschrift verlangt nicht, dass der Grad der Schwere und die Vorsatzform des Verantwortlichen bei der Schadensbemessung berücksichtigt werden. Im Gegenzug gibt der EuGH den nationalen Gerichten jedoch vor, dass die Höhe des geschuldeten immateriellen Schadensersatzes „seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung“ (zum Ganzen EuGH, Urt. v. 20.6.2024, Az. C-182/22, C-189/22, NJW 2024, 2599 sowie LG Leipzig, a.a.O.). Im Einzelnen:

Der EuGH stellt klar, dass die Art. 83 und 84 DSGVO, welche im Wesentlichen Strafzwecke erfüllen, nicht im Rahmen von Art. 82 DSGVO herangezogen werden dürfen, da die Vorschrift auf den Ausgleich für erlittene Einbußen abzielt (EuGH, a.a.O., NJW 2024, 2599 Rn. 22). Abschreckungs- und Strafzwecke sind der Vorschrift damit nicht zugänglich, sodass ein sog. Strafschadensersatz ausscheidet.

In Ermangelung eigener europäischer Regelungen zur Bestimmung der Höhe des Anspruchs nach Art. 82 DSGVO haben die nationalen Gerichte nach der Rspr. des EuGHs die bestehenden nationalen Vorschriften im Lichte der Äquivalenz und Effektivität des Unionsrechts anzuwenden (EuGH, a.a.O., NJW 2024, 2599 Rn. 27).

Soweit es der EuGH ausschließt, dass im Rahmen der Ausgleichsfunktion des Schadensersatzanspruchs i.S.v. Art. 82 DSGVO ein möglicher Vorsatz des Verantwortlichen oder der Grad der Schwere des Verstoßes berücksichtigt wird, gibt er jedoch auch zu erkennen, dass der Schadensersatz der Höhe nach den konkret erlittenen Schaden vollständig ausgleichen muss (EuGH, a.a.O., NJW 2024, 2599 Rn. 29).

Mit Blick auf den Vergleich physischer, materieller und immaterieller Schäden rekurriert der EuGH auf den 146. Erwägungsgrund der DSGVO und weist insoweit darauf hin, dass „[d]er Begriff des Schadens ... im Lichte der Rechtsprechung des EuGH weit auf eine Art und Weise ausgelegt

werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht“, und dass „[d]ie betroffenen Personen ... einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten [sollten]“ (EuGH, a.a.O., NJW 2024, 2599 Rn. 36). Weiterhin führt er aus, dass durch die nationalen Vorschriften zur Umsetzung des immateriellen Schadensersatzanspruchs die Ausübung der durch das Unionsrecht verliehenen Rechte, insbesondere der DSGVO, nicht unmöglich gemacht oder übermäßig erschwert werden darf (EuGH, a.a.O., NJW 2024, 2599 Rn. 34.)

Hiermit bringt der EuGH zum Ausdruck, dass an der deutschen Rechtsprechung, die bislang immateriellen Schadensersatz bei Persönlichkeitsrechtsverletzungen grundsätzlich nur höchst ausnahmsweise und insgesamt lediglich in geringem Umfang zugesprochen hat, bei der Anwendung der DSGVO nicht festgehalten werden darf (LG Leipzig, a.a.O., so auch Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18a; Ehmann/Selmayr/Nemitz, 3. Aufl. 2024, DS-GVO Art. 82 Rn. 38). Daraus folgt nicht zuletzt, dass trotz der Beschränkung auf den bloßen Ausgleich der erlittenen Nachteile, die Höhe des Schmerzensgeldes über die in der nationalen Rechtsprechungspraxis etablierten Beträge aus Schmerzensgeldtabellen o.ä. hinausgehen kann (so auch Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18d m.w.N.). Ein „Sich-Einfügen“ in die bisherige nationale Rechtsprechungspraxis stünde geradezu im Widerspruch zur europarechtsautonomen Auslegung des Schadensersatzanspruchs gem. Art. 82 DSGVO.

Der EuGH betont bei alledem, 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, a.a.O., NJW 2024, 1561 Rn. 62).

Die Höhe des Schadensersatzanspruchs ist nach der nationalen Vorschrift des § 287 ZPO zu schätzen. Nach § 287 Abs. 1 S. 1 ZPO entscheidet das Gericht nach Würdigung aller Umstände nach freier Überzeugung. Hierbei handelt es sich um das Einfallstor für die o.g. europarechtlichen Vorgaben.

Anknüpfungspunkte für die Bemessung eines immateriellen Schadensersatzanspruchs muss hier 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 (OLG Dresden, Ur. v. 10.12.2024, Az. 4 U 808/24, ZD 2025, 221 Rn. 20). Zudem sind vor allem der Umfang der gesammelten Daten und die Dauer des Verstoßes zu berücksichtigen. Hierbei handelt es sich um Kategorien zur Feststellung der Schaden-

stiefe bzw. -intensität, die nicht gleichzusetzen sind mit dem Grad der Schwere des Verstoßes, den der EuGH für nicht berücksichtigungsfähig erklärt (EuGH, a.a.O., NJW 2024, 2599 Rn. 26). Darüber hinaus kann die Möglichkeit des Betroffenen an der Wiedererlangung seiner Daten bzw. der Kontrolle über diese eine Rolle spielen (OLG Dresden, a.a.O., ZD 2025, 221, Rn. 20).

Weiterhin hat das LG Leipzig (a.a.O.) bei der Schadensschätzung für den Wert der personenbezogenen Daten einen entsprechenden Anknüpfungspunkt festgelegt. Hierfür hat es auf den Wert personenbezogener Daten für die Beklagte – soweit dieser geschätzt werden konnte – abgestellt, zudem auf den allgemeinen Wert personenbezogener Daten auf dem hierfür relevanten legalen oder auch illegalen Markt. Die Berücksichtigung des Wertes der Daten für den Verletzer wird jedenfalls im Bereich der kommerziellen Nutzung auch in der Literatur gefordert (Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DS-GVO Art. 82 Rn. 31, m.w.N.).

Für das Ausmaß und den Umfang der betroffenen Daten wird auf die Ausführungen oben verwiesen, auch für die Grundrechtssensibilität der betroffenen Daten. Hinzutritt, dass es aufgrund des bis zum Schluss der mündlichen Verhandlung bestehenden Schweigens der Beklagten zur streitgegenständlichen Datenverarbeitung aussichtslos erscheint, dass die Klägerin konkrete Kenntnis davon erhält, ob sie die Kontrolle der Daten durch Löschung o.ä. wiedererlangen könnte. Zudem ist über die Geständnisfiktion hinaus rein tatsächlich nicht feststellbar, ob und in welchem Umfang die Daten bereits an Dritte weitergegeben wurden und eine Datensicherung auch aus diesem Grund ausgeschlossen ist.

Erschwerend kommt hinzu, dass sogar wenn die Klägerin in Bezug auf die Erhebung und Verarbeitung von Daten zu Zwecken personalisierter Werbung die von der Beklagten vorgesehene Einwilligung abgegeben hätte, diese unwirksam gewesen wäre, da die allgemeine und unterschiedslose Sammlung von Daten u.a. gegen den Grundsatz der Datenminimierung verstößt und die unbegrenzte Speicherung personenbezogener Daten zu Zwecke der zielgerichteten Werbung unverhältnismäßig ist (siehe nur EuGH, a.a.O., NJW 2025, 207 Rn. 58 ff.).

Für den Wert der Daten für die Beklagte hat das LG Leipzig (a.a.O.) auf die Feststellungen des BKartA (Beschl. v. 2.5.2022, Az. B 6-27/21, BeckRS 2022, 47486 Rn. 432) 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 (BKartA a.a.O., Rn. 7). 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 ihn aufgrund seines persönlichen Konsumverhaltens, seiner Interessen und seiner Lebenssituation interessieren könnte (BKartA a.a.O., Rn. 53). 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. Der finanzielle Wert eines einzigen Nutzerprofils, in dem sämtliche Daten über die Person gespeichert sind, ist für Teilnehmer datenverarbeitender Märkte enorm. Dass die Wertbemessung auch der Wahrnehmung in der Gesellschaft entspricht, bestätigen diverse Studien (siehe nur die Studie „Der Wert persönlicher Daten – Ist Datenhandel der bessere Datenschutz?“, Berlin, 2016, im Auftrag des Sachverständigenrats für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz; Infografik „Preis, den Erwachsene in den USA für personenbezogene Daten aufrufen würden (in US-Dollar)“, Statista mit Quelldaten von Morning ... Consult aus dem Jahr 2019, abgerufen unter <https://cdn.statcdn.com/Infographic/images/normal/18449.jpeg>).

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. Kühling/Buchner/Bergt, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 18b, beck-online).

Obwohl der BGH in seiner Rspr. (BGH, a.a.O., GRUR-RS 2024, 31967 Rn. 31) 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 der Klägerin, da sich die Klägerin 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 Urt. v. 4.10.2024, a.a.O., NJW 2025, 207 Rn. 62) 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.

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, Beschl. v. 27.9.2017, 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 der Klägerin zu verzichten. Bei einer Anhörung der Klägerin 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 der klägerischen Partei 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 wird, kann sich die Erwartung oder Befürchtung der Klägerin nicht auf ein bestimmtes Verhalten konkretisieren. Dies kann und darf ihr nicht zum Nachteil gereichen.

Wie der EuGH in seiner Rechtsprechung jenseits des Datenschutzrechts, bspw. 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, Ur. v. 29.4.2004, Az. C-456/01 P und C-457/01 P, GRUR Int 2004, 631, Rn. 35; Ur. v. 8.10.2020, Az. C-456/19, GRUR 2020, 1195, Rn. 32). 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 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 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 Kontrollverlust für angemessen erachtet wird (siehe nur OLG Dresden, a.a.O., ZD 2025, 221 Rn. 20 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 Rspr. des EuGHs per se einen schweren Eingriff in die durch Art. 7 und 8 GrCh gewährleisteten Rechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten dar

(EuGH, a.a.O., NJW 2025, 207 Rn. 63), 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 Durchschnittsbetroffene 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 (s.o. zur Wahrnehmung der Gesellschaft hinsichtlich der Werthaltigkeit von Daten). 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 gezwungener Maßen 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, Urt. v. 30.11.2021, 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.

Nicht anspruchsmindernd i.S.e. widersprüchlichen Verhaltens wirkt sich aus, dass die Klägerin die Nutzung der Dienste der Beklagten auch nach Kenntniserlangung über die Datenverarbeitung weiter in Anspruch nimmt. Die Beklagte nimmt im Bereich der Social-Media-Plattformen eine überragende marktübergreifende Stellung ein, welche bereits das Bundeskartellamt i.S.v. § 19a GWB festgestellt hat (BKartA, Beschl. v. 02.05.2022, Az. B6-27/21). Gerade für die Teilhabe am gesellschaftlichen Leben handelt es sich 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 (zu-

sammenfassend zu den Hintergründen siehe Mohr, EuZW 2019, 265 unter Bezugnahme auf die F.-Entscheidung des Bundeskartellamts vom 06.02.2019). Auch wenn die Nutzerin Kenntnis von den Datenschutzverletzungen der Beklagten erlangt, ist es ihr deshalb nicht zuzumuten, dass sie sämtliche Profile bei der Beklagten löscht und seine Nutzung beendet. Vielmehr muss die Beklagte gewährleisten, dass die Klägerin ihre Netzwerke DSGVOkonform (auch in Zukunft) nutzen kann. Gerade durch die hiesige Klage bringt die Klägerin zum Ausdruck, dass ihr die Datenschutzverstöße der Beklagten nicht egal sind, sondern sie eine DSGVO-konforme Nutzung durchsetzen will. Anders als in den Scraping-Fällen war es der Klägerin hier zudem – bis auf die vollständige Löschung der Profile – nicht möglich, ihr Nutzerverhalten auf den Plattformen der Beklagten so anzupassen, dass weitere Datenschutzverletzungen verhindert werden (vgl. Paal, ZfDR 2023, 325).

Art und Umfang des Schadensersatzanspruchs richten sich nach den nationalen Vorschriften in §§ 249 ff. und § 287 ZPO. Im Sinne des Effektivitätsgrundsatzes muss der Umfang des Schadensersatzanspruchs seiner Höhe nach den vollständigen und wirksamen Ersatz des erlittenen Schadens sicherstellen, abschreckend wirken und weitere Verstöße gegen die DSGVO unattraktiv machen, Erwägungsgrund 146 S. 3 DSGVO. Zur Festlegung der Höhe des Schadensersatzes können daher auch die Kriterien zur Bußgeldbemessung gemäß Art. 83 DSGVO herangezogen werden. Die Beklagte hat über einen langen Zeitraum unbestimmte Mengen personenbezogener Daten der Klägerin unrechtmäßig verarbeitet. Der Verstoß wiegt besonders schwer, da die Beklagte auch personenbezogene Daten besonderer Kategorien nach Art. 9 Abs. 1 DSGVO unrechtmäßig verarbeitet hat. Eine Wiedererlangung der Kontrolle über die personenbezogenen Daten der Klägerin ist nur schwer möglich. Bei der Bezifferung eines Schadens infolge eines Kontrollverlusts ist zu berücksichtigen, ob die Kontrolle über die personenbezogenen Daten wiederhergestellt werden kann. Die Beklagte hat die Auskunftserteilung gegenüber der Klägerin hinausgezögert und pauschal auf ihr „Self-Service“- Tool verwiesen, das keine vollumfängliche Auskunft erteilen kann. Zudem übermittelt die Beklagte die personenbezogenen Daten der Klägerin in Drittstaaten wie die USA.

4. Vorgerichtliche Kosten

Die Klägerin hat einen Anspruch auf Freistellung gegen die Beklagte in Höhe von 367,23 €. Die Klägerin kann im Rahmen des ihr zustehenden Schadensersatzanspruchs nach Art. 82 Abs. 1 DSGVO die Freistellung von vorgerichtlich angefallenen Rechtsanwaltsgebühren beanspruchen. Zu einem Streitwert von bis zu 5.000 € fiel eine 0,9 Geschäftsgebühr von 300,60 € an, der sich die Auslagenpauschale von 20 € und die Umsatzsteuer von 60,91 € hinzugesellen, was

zusammen 381,51 € ergibt, also mehr als die Klägerin begehrt.

5. Zinsen

Die Klägerin hat einen Anspruch auf Zinszahlung in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 11.12.2024 aus §§ 291, 288 BGB.

Die Klägerin hat aus §§ 286, 288 BGB keinen Anspruch auf Zinszahlung in Höhe von 5 Prozentpunkten über dem Basiszinssatz bereits seit dem 16.04.2024. Sie hat die Beklagte nicht in Verzug gesetzt. Den für die Überprüfung der Rechtmäßigkeit der geltend gemachten Ansprüche notwendigen – korrekt geschriebenen – Nutzernamen hat die Klägerin der Beklagten erst im gerichtlichen Verfahren mitgeteilt.

Die Kostenentscheidung folgt aus § 91 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit ergeht auf Grundlage des § 709 Satz 1 und 2 ZPO.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung kann das Rechtsmittel der Berufung eingelegt werden. Die Berufung ist nur zulässig, wenn der Wert des Beschwerdegegenstands 600 Euro übersteigt oder das Gericht des ersten Rechtszuges die Berufung im Urteil zugelassen hat.

Die Berufung ist binnen einer Notfrist von **einem Monat** bei dem

Landgericht Berlin II
Littenstraße 12-17
10179 Berlin

einzulegen.

Die Frist beginnt mit der Zustellung der vollständigen Entscheidung, spätestens mit Ablauf von fünf Monaten nach der Verkündung der Entscheidung.

Die Berufung muss mit Schriftsatz durch eine Rechtsanwältin oder einen Rechtsanwalt eingelegt werden. Die Berufungsschrift muss die Bezeichnung der angefochtenen Entscheidung und die Erklärung enthalten, dass Berufung eingelegt werde.

Die Berufung muss binnen zwei Monaten mit Anwaltsschriftsatz begründet werden. Auch diese Frist beginnt mit der Zustellung der vollständigen Entscheidung.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Erstatteinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.


Elektronische Dokumente müssen

- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:

- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

Dr. 
Richter am Amtsgericht