

Landgericht Frankfurt am Main

2-15 O 22/24



Im Namen des Volkes Urteil

In dem Rechtsstreit

[REDACTED]

- Kläger -

Prozessbevollmächtigte:

Rechtsanwälte und Rechtsanwältinnen BRR Automotive Rechtsanwaltsgesellschaft mbH, Viktoria-Luise-Platz 7, 10777 Berlin
Geschäftszeichen: DTS-005949-IUS

gegen

Meta Platforms Ireland Ltd. v.d.d. GF Yvonne Cunnane, Anne O'Leary, Genevieve Hughes, Majella Mungovan u. David Harris, Merrion Road, D04 X2K5, Dublin 4, Irland, Irland

- Beklagte -

Prozessbevollmächtigte:

Rechtsanwälte und Rechtsanwältinnen White & Case LLP, Bockenheimer Landstraße 20, 60323 Frankfurt am Main
Geschäftszeichen: 1430682-0009.VORYVON, Gerichtsfach: 350

hat das Landgericht Frankfurt am Main – 15. Zivilkammer – durch die Richterin am Landgericht [REDACTED] als Einzelrichterin auf die mündliche Verhandlung vom 01.10.2025 für Recht erkannt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 25.05.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Facebook" unter der E-Mail-Adresse [REDACTED] des Klägers verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business Tools“,

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

- E-Mail des Klägers
- Telefonnummer des Klägers
- Vorname des Klägers
- Nachname des Klägers
- Geburtsdatum des Klägers
- Geschlecht des Klägers
- Ort des Klägers
- 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 des Klägers

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 des Klägers 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 des Klägers die Beklagte seit dem 25.05.2018 zu welchem Zeitpunkt (Beginn, Dauer, Ende) in welchem Drittstaat gespeichert hat;

inwieweit die Daten des Klägers 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 verurteilt, an den Kläger 5.000,00 EUR nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 14.11.2023 zu zahlen.

3. Die Beklagte wird verurteilt, den Kläger von vorgerichtlichen Rechtsanwaltskosten i.H.v. 627,13 EUR freizustellen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits tragen der Kläger zu 1/3 und die Beklagte zu 2/3.

6. Das Urteil ist für den Kläger in Ziffer 1. vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von 5.000,00 EUR, im Übrigen gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages. Der Kläger kann die Vollstreckung durch die Beklagte durch Sicherheitsleistung in Höhe von 110 % des für die Beklagte aus dem Urteil vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung in Höhe von 110 % des zu vollstreckenden Betrages Sicherheit leistet.

7. Der Streitwert wird auf 15.000,00 EUR festgesetzt.

Tatbestand

Der Kläger macht Ansprüche aus behaupteten Datenschutzverstößen geltend.

Die Beklagte ist u.a. Betreiberin des sozialen Netzwerkes „Facebook“. Dieses Netzwerk ermöglicht es den Nutzern, persönliche Profile zu erstellen und in dem Umfang ihrer so erstellten Präsenz in diesem Netzwerk mit anderen Nutzerinnen und Nutzern in Kontakt zu treten.

Der Kläger nutzt seit dem 01.01.2015 ausschließlich zu privaten Zwecken das Netzwerk Facebook unter seiner E-Mail Adresse [REDACTED]

Zentrales Merkmal von Facebook ist die Personalisierung. Dazu nutzt die Beklagte zum ersten Daten, die der Nutzer selbst bei der Registrierung (zwingend: Benutzername, Mailadresse oder Telefonnummer, Alter) oder später angibt; zum zweiten „on-site“-Daten, die als Ergebnis der Aktivitäten des Nutzer auf Facebook gesammelt werden; und zum dritten (hier streitgegenständlich) „off-site“-Daten, die die Beklagte von Dritten erhält und die z.B. Informationen beinhalten, wie Nutzer mit den Webseiten und Apps von Drittunternehmen interagieren.

Die Beklagte ist die Entwicklerin sog. „Meta Business Tools“, namentlich „Meta Pixel“, „App Events über F.-SDK“ und „Conversions API“ sowie „App Events API“ (nachfolgend zusammenfassend genannt: „Business Tools“). Diese Business Tools werden im Einvernehmen mit der Beklagten von zahlreichen Drittunternehmen auf deren Webseiten („Meta Pixel“, „Conversions API“) oder Apps („F.-SDK“, „App Events API“) eingebunden. Dies erfolgt durch zahlreiche reichweitenstarke Webseiten und Apps in Deutschland, wie etwa zahlreiche große Nachrichtenseiten und -Apps sowie Seiten mit politischem Bezug (z.B. tagesschau.de, spiegel.de, bild.de, welt.de, faz.net, stern.de, wahl-o-mat.de), große Seiten und Apps zu Reisen und Freizeitgestaltung (z.B. bahn.de, airbnb.de, tripadvisor.de, hrs.de, holidaycheck.de, momondo.de, booking.com, chefkoch.de), Seiten und Apps, die medizinische Hilfe bieten (z.B. apotheken.de, shop-apotheke.de, docmorris.de, ärzte.de, helios-gesundheit.de, jameda.de), Dating- und Erotikseiten (z.B. parship.de, amorelie.de, orion.de, lovescout24.de), aber auch Seiten mit Inhalten aus der innersten Intimsphäre (z.B. krebshilfe.de, fertility.com, nie-wieder-alkohol.de). Eine vollständige Übersicht der betroffenen Webseiten liegt nicht vor. Die Business Tools finden sich jedoch auf den in der Anlage K2 zur Klageschrift gelisteten Websites.

Für den durchschnittlichen Internetnutzer ist nicht erkennbar, ob die von ihm besuchte Webseite mit einem Meta Business Tool ausgestattet worden ist, oder nicht.

Zweck der Business Tools ist es unter anderem, die Effektivität von Werbeanzeigen von Drittunternehmen auf den von der Beklagten angebotenen Plattformen (neben Facebook auch Instagram) zu erhöhen und zu messen.

Sobald ein Facebook-Nutzer die Homepage oder App einer Drittfirm, welche die Business Tools einsetzt, besucht, übermittelt die Drittfirm über die derart eingebundenen Business Tools die IP-Adresse des Nutzers sowie den User-Agent des Clients (d.h. vom Browser oder vom Nutzergerät abrufbare Daten, deren Verknüpfung über ein „Digital Fingerprinting“ zusammen mit der Nutzer-ID und der IP-Adresse eine Individualisierung des Nutzers erlaubt) an die Beklagte, und zwar unabhängig davon, ob der Nutzer zu diesem Zeitpunkt bei Facebook eingeloggt ist oder nicht. Auf diese Weise erkennt die Beklagte Nutzer auf Drittwebseiten unabhängig davon, ob der Nutzer in den Einstellungen seines Browsers oder in den Einstellungen bei Facebook hinsichtlich der Verwendung von Cookies Einschränkungen gemacht hat. Die Business Tools erfassen sodann, wenn der Webseiten-/Appbetreiber die Funktion „Automatische Events“ der Business Tools aktiviert hat (was die Beklagte empfiehlt), selbsttätig auch Informationen über die weiteren Aktivitäten des Nutzers auf der Drittwebsite/-

App („Events“) und übermitteln diese an die Beklagte. In welcher Weise die Beklagte diese Daten nutzt, hängt in gewissem Umfang von den Einstellungen des jeweiligen Nutzers bei Facebook ab.

Um ein Konto auf Facebook zu registrieren und zu nutzen, muss der (künftige) Nutzer den Nutzungsbedingungen (Anlage B2) zustimmen. Dort heißt es, in der Datenschutzrichtlinie der Beklagten werde erläutert, wie die Beklagte Informationen über alle Meta-Produkte hinweg erhebe, verwende und teile und wie der Nutzer auf den Einstellungen-Seiten jederzeit die Privatsphäre-Optionen überprüfen könne.

Die Facebook-Nutzer können über die dortigen Einstellungsmöglichkeiten Einfluss darauf nehmen, wie die bei der Beklagten eingehenden Daten weiterverwendet werden. In der Rubrik Einstellungen können die Nutzer entscheiden, ob sie den Einsatz von „Meta Cookies auf anderen Apps und Webseiten“ erlauben. Wenn der Nutzer durch seine Einstellungen auf Facebook den Einsatz von „Meta Cookies auf anderen Apps und Webseiten“ nicht erlaubt und/oder nicht über die Einstellung „Informationen über Aktivitäten von Werbepartnern“ einwilligt, verwendet die Beklagte Informationen dieses Nutzers, die über Business Tools auf Homepages und Apps Dritter erhoben werden, für bestimmte Zwecke gleichwohl, nicht jedoch für die Bereitstellung personalisierter Werbung.

Der Kläger hat über die Einstellung „Informationen von Werbepartnern über deine Aktivitäten“ am 30.04.2018 in die Datenverarbeitung zur Bereitstellung personalisierter Werbung eingewilligt.

Die über die Business Tools an die Beklagte übertragenen Daten werden von der Beklagten wie folgt – und teilweise in Abhängigkeit von dem Vorliegen der in den Einstellungen abgegebenen Einwilligung – weiterverarbeitet: Mittels der übertragenen technischen Standarddaten wird – soweit, wie ganz regelmäßig, technisch möglich – eine bereits von der Beklagten erfasste Person identifiziert. Der Umstand des Besuchs der die Daten übertragenden Homepage bzw. App sowie der entsprechende Zeitpunkt wird sodann dem personenbezogenen Profil dieser Person zugeordnet und gespeichert und reichert dieses Persönlichkeitsprofil entsprechend um diese personenbezogene Information weiter an. Weitere personenbezogene Daten über die Aktivitäten des Nutzers auf der Homepage bzw. App des Dritten werden jedenfalls dann gespeichert und mit den sonstigen gegebenenfalls vorhandenen Daten über den jeweiligen Nutzer zu einem personenbezogenen Profil verbunden, wenn der Nutzer in den Einstellungen seine Zustimmung zur Nutzung „optionaler Cookies“ erteilt hat. Hat der Nutzer gegenüber der Beklagten der Datenverarbeitung zur Bereitstellung personalisierter Werbung nicht zugestimmt, verwendet die Beklagte die Daten für diesen Benutzer nicht zur Bereitstellung personalisierter Werbung. Sie verwendet jedoch auch in diesem Fall die Daten, die von Drittunternehmen über Business Tools gesendet werden, für andere Zwecke. Dies sind nach Vortrag der Beklagten etwa „Sicherheits- und Integritätszwecke“, einschließlich des Zweckes „der Überwachung von versuchten Angriffen auf die Systeme von Meta“.

Die Beklagte verpflichtet die Drittunternehmen, auf deren Seiten die Business Tools eingebunden werden, zur Einhaltung der „Nutzungsbedingungen für Meta-Business-Tools“ (Anlage B5).

In ihrer Datenschutzrichtlinie (Anlage K1) räumt die Beklagte sich das Recht ein, von ihr kontrollierte personenbezogene Daten ihrer Nutzer in andere Länder weltweit zu übertragen, ohne dass insoweit hinsichtlich des datenschutzrechtlichen Schutzniveaus im betreffenden Drittstaat differenziert würde.

Mit vorgerichtlichem Anwaltsschreiben vom 16.10.2023 (Anlage K3) forderte der Kläger die Beklagte dazu auf, anzuerkennen, dass der Vertrag zwischen den Parteien nach rechtskonformer Auslegung eine Datenverarbeitung der streitgegenständlichen Drittquellendaten ohne wirksame Einwilligung grundsätzlich nicht zulasse; sich strafbewehrt zu

verpflichten, Daten nur noch gemäß ausdrücklicher Weisung des Klägers zu verarbeiten und auf Aufforderung zu löschen bzw. zu anonymisieren; bestimmte Auskunftspflichten anzuerkennen; sich strafbewehrt zur Unterlassung bestimmter Datenverarbeitungen zu verpflichten und immaterielles Schmerzensgeld i.H.v. 5.000,- EUR zu zahlen.

Der Kläger meint, die Beklagte überwache den Internetverkehr des Klägers unter grober und vorsätzlicher Missachtung des europäischen Datenschutzrechts, indem sie dessen persönliche und höchstpersönliche Daten massenweise rechtswidrig erhebe, zu einem Profil zusammenfüge, in unsichere Drittstaaten übertrage, dort unbefristet speichere und sich das Recht herausnehme, diese Daten in unbekanntem Maße auszuwerten und an Dritte weiterzugeben, ohne den Kläger hiervon zu informieren. Hierzu trägt der Kläger vor, er nutze viele Webseiten und Apps, auf denen die Business Tools aktiv seien, einschließlich Webseiten, aus deren Besuch und konkreter Verwendung direkte Rückschlüsse auf besonders sensible personenbezogene Daten gezogen werden könnten. Gegenstand der Beanstandung des Klägers sei nicht die Bereitstellung personalisierter Werbung durch die Beklagte, sondern die Tatsache, dass die auf Drittwebseiten bzw. -Apps entstehenden personenbezogenen Daten überhaupt erfasst und verarbeitet würden, gleich zu welchen Zwecken. Für die streitgegenständliche Datenverarbeitung könne sich die Beklagte nicht auf eine Einwilligung der Nutzer berufen. Die Weitergabe persönlicher Daten an unsichere Drittstaaten sei jedenfalls von 25.05.2018 bis 09.07.2023 rechtswidrig gewesen.

Die Beklagte sei für die Datenverarbeitung durch und aufgrund der Business Tools verantwortlich i.S.d. Art. 28 DSGVO.

Der Kläger trägt weiter vor, die Beklagte stelle über Facebook keine vollständige Beauskunftung gemäß Art. 15 Abs. 1, Abs. 3 DSGVO zur Verfügung. Auch eine nachträgliche Löschung der Daten durch den Nutzer sei nicht möglich. Er meint, das Recht auf Anonymisierung sei als Minus im Anspruch auf Löschung aus Art. 17 DSGVO enthalten. Dem Kläger stehe ein Entschädigungsanspruch wegen Verletzung seines Rechts auf informationelle Selbstbestimmung aus Art. 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG zu, jedenfalls aber ein Anspruch auf Schadenersatz nach Art. 82 DSGVO, und zwar jeweils mindestens in fünfstelliger Höhe.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, Auskunft nach Art. 15 Abs. 1 lit. a., c., g. und h. DGSVO darüber zu erteilen, welche personenbezogenen Daten die Beklagte seit dem 25.05.2018 verarbeitet und im Zuge dessen mit dem Nutzeraccount des Netzwerks "Facebook" unter der E-Mail-Adresse [REDACTED] der Klagepartei verknüpft hat, dies insbesondere, aber nicht ausschließlich durch die „Meta Business Tools“,

a. auf Dritt-Webseiten und -Apps die personenbezogenen Daten, die der Identifizierung der Klagepartei dienen, ob direkt oder in gehaschter 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.

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 EUR beträgt, nebst Zinsen i.H.v. fünf Prozentpunkten über dem Basiszinssatz seit dem 14.11.2023, zu zahlen.

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

Die Beklagte beantragt:

Die Klage wird abgewiesen.

Die Beklagte bezeichnet als „streitgegenständliche Datenverarbeitung“ diejenige zur Bereitstellung personalisierter Werbung. Sie meint, falls der Kläger sich gegen andere Zwecke wende, müsse er mitteilen, welche anderen Zwecke er beanstände.

Die Beklagte meint weiter, nicht sie selbst, sondern die Drittunternehmen, auf deren Webseiten bzw. Apps die Business Tools eingebunden seien, seien datenschutzrechtlich verantwortlich für die Installation und Nutzung der Business Tools, die Erhebung und Übermittlung personenbezogener Daten über diese Tools und die Einholung etwa erforderlicher Einwilligungen der Nutzer. Das sei auch in einer entsprechenden Rahmenvereinbarung zwischen der Beklagten und den Drittunternehmen i.S.d. Art. 26 DSGVO niedergelegt. Gleichwohl erklärt die Beklagte, sie stütze sich im Rahmen der streitgegenständlichen Datenverarbeitung nicht auf die über Webseiten bzw. Apps Dritter erteilte Einwilligung, sondern hole diese direkt beim Nutzer ein.

Eine erteilte Einwilligung von Nutzern in ihre Datenverarbeitung (Art. 6 Abs. 1 lit. a DSGVO) hält die Beklagte für wirksam. Wenn der Nutzer der Verwendung von Cookies auf anderen Webseiten bzw. Apps nicht zugestimmt habe, verwende sie solchermaßen erhobene Informationen „nicht für bestimmte Datenverarbeitungsvorgänge, auch nicht zur Bereitstellung personalisierter Werbung“, sondern „nur für begrenzte Zwecke, wie Sicherheits- und Integritätszwecke“.

Die „streitgegenständliche Datenverarbeitung“ umfasse keine besonderen Kategorien personenbezogener Daten i.S.d. Art. 9 DSGVO. Die Beklagte bestreitet mit Nichtwissen, dass der Kläger regelmäßig Webseiten und Apps nutzt, auf denen die Business Tools genutzt werden. Den behaupteten Umfang seiner Internetnutzung zu sensiblen Daten habe der Kläger nicht substantiiert dargelegt. Zudem verböten der Rahmenvertrag zwischen der Beklagten und den Drittunternehmen bzw. die Nutzungsbedingungen für die Meta Business Tools ausdrücklich, dass Drittunternehmen sensible Daten, insbesondere besondere Kategorien personenbezogener Daten, über die Business Tools an die Beklagte übermitteln. Die Systeme

der Beklagten seien so ausgestaltet, dass sie als potentiell unzulässig erkannte Informationen herausfilterten.

Die begehrten Auskünfte seien dem Kläger mit Schreiben vom 17.06.2024 (Anlage B8) erteilt worden. Im Übrigen könnten die Nutzer mit der Einstellung „Deine Aktivitäten außerhalb von Meta-Technologien“ auf Facebook eine Zusammenfassung der von Drittunternehmen mit der Beklagten geteilten Daten über Aktivitäten des Nutzers auf Drittwebseiten, die mit seinem Konto verknüpft seien, erhalten. Dort habe der Nutzer auch die Möglichkeit, die mit seinem Facebook-Konto verknüpften und von Drittunternehmen geteilten Informationen über Aktivitäten zu trennen. Der Antrag auf Geldentschädigung sei unzulässig, weil der Kläger in Wirklichkeit immateriellen Schadenersatz fordere und daneben für die Anwendung nationalen Rechts kein Raum sei. Den von Art. 82 DSGVO vorausgesetzten Schaden als Folge der streitgegenständlichen Datenverarbeitung habe der Kläger nicht dargelegt.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zur Akte gereichten Schriftsätze nebst Anlagen sowie auf das Protokoll vom 01.10.2025 Bezug genommen.

Entscheidungsgründe

I. Die Klage ist – mit Ausnahme des Klageantrags zu 2. – zulässig. Das Landgericht Frankfurt am Main ist insbesondere in internationaler, sachlicher und örtlicher Hinsicht zuständig.

1. Die internationale Zuständigkeit der deutschen Gerichtsbarkeit folgt aus Art. 79 Abs. 2 S. 2 DSGVO, nachdem der Kläger seinen gewöhnlichen Aufenthalt in Deutschland hat. Gemäß § 79 Abs. 2 DSGVO sind für Klagen gegen einen Verantwortlichen im Ausgangspunkt die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Nach S. 2 der Vorschrift können solche Klagen wahlweise auch bei den Gerichten des Mitgliedsstaates erhoben werden, indem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich – was vorliegend nicht der Fall ist – bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaates, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Sinn und Zweck dieser Zuständigkeitsregelung ist die Gewährleistung (und Erleichterung) eines effektiven Rechtsschutzes durch die betroffenenfreundliche Möglichkeit einer Klageerhebung am Aufenthaltsort, wobei damit nicht der „tatsächliche“, sondern der „gewöhnliche“ Aufenthaltsort gemeint ist, wie der Wortlaut der englischen Sprachfassung („habitual residence“) verdeutlicht (LG Lübeck, Urteil vom 10.01.2025 – 15 O 269/23 m.w.N.). Diese Voraussetzungen liegen hier vor, weil die Beklagte als Verantwortliche bzw. Auftragsverarbeitende i.S.d. DSGVO in Anspruch genommen wird – ob ihr diese Eigenschaft tatsächlich zukommt, ist Frage der Begründetheit der Klage – und der Kläger seinen Wohnsitz und gewöhnlichen Aufenthalt im Bezirk des erkennenden Gerichts hat.

Ob Art. 79 Abs. 2 DSGVO in seinem vorliegend eröffneten Anwendungsbereich die allgemeinen Zuständigkeitsvorschriften der EuGVVO verdrängt oder diese Vorschriften daneben anwendbar bleiben, kann offenbleiben. Denn auch nach den Vorschriften der EuGVVO ist keine abweichende ausschließliche Zuständigkeit im Sinne des Art. 24 EuGVVO begründet, sondern folgt die internationale Zuständigkeit der deutschen Gerichte vorliegend sowohl aus Art. 7 Nr. 1 lit. b als auch Art. 18 Abs. 1 Alt. 2, Art. 17 Abs. 1 lit. c EuGVVO. Nach Art. 18 EuGVVO kann ein Verbraucher gegen eine Vertragspartei, die ihre Tätigkeit auf den Mitgliedstaat, in dem der Verbraucher seinen Wohnsitz hat, ausrichtet, vor dem Gericht seines Wohnsitzes Klage erheben. Der Kläger nutzt als Privatperson die Plattform der Beklagten, die dabei gewerblich handelt (EuGH, Urteil vom 05.06.2018 – C-210/16) und ihre Tätigkeit z.B. durch entsprechende Sprachoptionen auch speziell auf das Gebiet der Bundesrepublik und hier ansässige Nutzer ausgerichtet hat.

2. In sachlicher Hinsicht ist das erkennende Gericht gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG zuständig, nachdem der Wert des Streitgegenstandes die Summe von 5.000,- EUR übersteigt.

3. Die örtliche Zuständigkeit des erkennenden Gerichts folgt sowohl aus § 44 Abs. 1 S. 2 BDSG als auch aus Art. 7 Nr. 1 lit. b EuGVVO.

Art. 79 Abs. 2 S. 1 DSGVO regelt nur die internationale, nicht auch die örtliche Zuständigkeit (LG Lübeck, Urteil vom 10.01.2025 – 15 O 269/23). Insoweit bestimmt § 44 Abs. 1 S. 2 BDSG, dass Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 oder der darin enthaltenen Rechte der betroffenen Person auch bei dem Gericht des Ortes erhoben werden dürfen, dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Diese Voraussetzungen liegen vor, nachdem der Kläger seinen gewöhnlichen Aufenthalt im Bezirk des erkennenden Gerichts hat.

4. Der Klageantrag zu 2. (Lösung und Anonymisierung) ist bereits unzulässig, da er nicht hinreichend bestimmt ist und es so an der Vollstreckbarkeit fehlt.

Der Kläger begeht mit diesem Antrag, „die Beklagte zu verpflichten, 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.“

Der Antrag ist als Antrag auf Verurteilung der Beklagten zur Lösung bzw. Anonymisierung der in Rede stehenden Daten auszulegen. Der Kläger möchte, entgegen dem Wortlaut des Antrages, eine Verpflichtung der Beklagten erkennbar nicht erst durch den Tenor begründet sehen, sondern strebt aufgrund einer nach seiner Rechtsauffassung bereits bestehenden rechtlichen Verpflichtung der Beklagten deren Verurteilung durch das Gericht an. Der so verstandene Leistungsantrag ist unzulässig, weil ein Urteilstenor des erstrebten Inhalts nicht hinreichend bestimmt wäre, um vollstreckbar zu sein.

Auf entsprechenden Hinweis im Termin hat der Kläger zwar klargestellt, dass der Klageantrag zu 2. an die abstrakte Beschreibung betroffener Daten aus dem Klageantrag zu 1. anknüpfen soll und insoweit die Lösung/Anonymisierung sämtlicher, also „aller Dateien“ begeht werde. Auch der so verstandene Leistungsantrag zu 2. ist indes nicht vollstreckbar. Solange die Beklagte die Auskunft, zu deren Erteilung sie unter Ziff. 1 des Tenors der vorliegenden Entscheidung verurteilt wird, nicht erteilt hat, ist weiterhin unklar, welche konkreten Daten gelöscht bzw. anonymisiert werden sollen. Der Leistungsantrag wird auch nicht dadurch wenigstens teilweise vollstreckbar, dass er sich zumindest auch auf solche Daten erstreckt, hinsichtlich deren die Beklagte künftig Auskunft erteilen wird. Denn ein gerichtlicher Leistungstitel muss zum Zeitpunkt seines Erlasses vollstreckbar sein. Er darf nicht in dem Sinne „blanko“ erlassen werden, dass er erst durch eine nachfolgende Handlung (hier: des Schuldners) inhaltlich konkretisiert wird (so auch: LG Mainz, Urteil vom 27.06.2025 – 3 O 29/24). Auch die Aussage in der mündlichen Verhandlung, dass die Lösung aller Daten beantragt werde, dergestalt, dass keine Daten übrig bleiben dürfen, führt nicht zu einer hinreichenden Bestimmbarkeit. Denn der Kläger begeht ja gerade nicht die Lösung sämtlicher Daten (inkl. der von ihm selbst bei Anmeldung bzw. Überarbeitung des Profils eingegebenen Daten) sondern – und dies ergibt sich explizit aus dem Antrag – nur die Lösung der gemäß des Antrags zu 1 a. seit dem 25.05.2018 gespeicherten personenbezogenen Daten. Das Problem der Abgrenzbarkeit verbleibt also.

Dem Umstand, dass der Kläger derzeit in Ermangelung der Auskunftserteilung außerstande ist, einen alle relevanten Daten umfassenden Leistungsantrag in vollstreckungsfähiger Form zu stellen hätte dieser entweder in Form einer Stufenklage (§ 254 ZPO) oder eines

Feststellungsantrags auf Verpflichtung der Beklagten zur Löschung der Daten nach vollständiger Auskunftserteilung (§ 256 ZPO) Rechnung tragen können.

Dies hat er auch auf Hinweis des Gerichts jedoch nicht – auch nicht im Wege des Hilfsantrags – getan.

II. Soweit die Klage zulässig ist, hat sich auch in der Sache ganz überwiegend Erfolg.

Auf das zwischen den Parteien bestehende Vertragsverhältnis ist deutsches Recht anzuwenden. Der Vertrag unterliegt nach Art. 3 Abs. 1, Art. 6 Abs. 2 der VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.06.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO; ABl. 2008 L 177, Seite 6) dem von den Parteien ausweislich der Nutzungsbedingungen gewählten deutschen Recht (BGH, Urteil vom 12.07.2018 – III ZR 183/17).

1. Klageantrag zu 1. – Auskunft

Die Beklagte hat dem Kläger die vom Klageantrag zu 1. erfassten Auskünfte gemäß Art. 15 Abs. 1 DSGVO zu erteilen.

a) Der sachliche und räumliche Anwendungsbereich der DSGVO ist eröffnet. Auch in zeitlicher Hinsicht ist die DSGVO auf den streitgegenständlichen Sachverhalt umfassend anwendbar. Die DSGVO ist am 25.05.2018 in Kraft getreten. Der Kläger nutzt das Netzwerk Facebook der Beklagten unbestritten seit dem 01.01.2015. Die Klageanträge beziehen sich jedoch ausschließlich auf Datenverarbeitungsvorgänge ab dem 25.05.2018.

b) Die Beklagte ist in Bezug auf die vom Antrag zu 1. erfassten Daten Verantwortliche i.S.d. Art. 15 Abs. 1 DSGVO.

Das stellt auch die Beklagte nicht in Abrede, soweit die Speicherung und Verarbeitung von Daten auf der Plattform der Beklagten selbst in Rede steht. Die Beklagte hat insoweit als Betreiberin der Plattform allein über die Zwecke und Mittel der Verarbeitung personenbezogener Daten zu entscheiden (EuGH, Urteil vom 05.06.2018 – C-210/16).

Datenschutzrechtlich (zumindest Mit-)Verantwortliche im Sinne des Art. 15 Abs. 1 DSGVO – was insoweit als Grundlage für die geltend gemachten Ansprüche genügt – ist die Beklagte aber auch insoweit, als die Erhebung der in Rede stehenden Daten durch Meta Business Tools auf Webseiten oder Apps Dritter Streitgegenstand ist. Streitgegenstand ist dabei die Summe derjenigen Datenverarbeitungsvorgänge, durch die die Beklagte personenbezogene Daten des Klägers verarbeitet und mit seinem im Klageantrag zu 1. bezeichneten Nutzeraccount des Netzwerks Facebook verknüpft hat, einschließlich personenbezogener Daten, die über Business Tools der Beklagten an sie gelangt sind. Anders als die Beklagte behauptet, beschränkt der Kläger die streitgegenständlichen Ansprüche nicht auf Datenverarbeitungsvorgänge, die einem bestimmten Zweck dienen, insbesondere nicht auf die Datenverarbeitung zur Bereitstellung personalisierter Werbung. Der Kläger trägt zwar vor, das Geschäftsmodell der Beklagten beruhe auf der Erfassung von Daten der Nutzer zu dem Zwecke, diese zu Werbezwecken nutzen zu können. Er betont aber zugleich, die Beklagte nutze die Daten und das so erstellte Persönlichkeitsprofil auch zu nicht werberelevanten Zwecken, und beanstandet dies ausdrücklich.

Es liegt auch nicht in der Macht der Beklagten, eine Einschränkung des Streitgegenstandes dahingehend vorzunehmen, dass dieser nur die Nutzung personenbezogener Daten zum Zwecke der Bereitstellung personalisierter Werbung umfasse. Zivilprozessual bestimmt der Kläger, nicht der Beklagte, den Streitgegenstand der Klage. Anders als die Beklagte meint, hat der Kläger zur Geltendmachung der streitgegenständlichen Ansprüche auch nicht zu präzisieren, welche anderen Zwecke weitergehender Datenverarbeitung er beanstandet. Der

Kläger beanstandet nicht lediglich bestimmte Datenverarbeitungszwecke. Er beanstandet vielmehr, dass die auf Drittwebseiten bzw. -Apps entstehenden personenbezogenen Daten des Klägers überhaupt erfasst und verarbeitet werden, gleich zu welchen Zwecken.

Für diese Datenverarbeitungsvorgänge ist die Beklagte Verantwortliche i.S.d. DSGVO. Verantwortlicher i.S.d. DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). Hierunter fällt hinsichtlich der streitgegenständlichen Datenverarbeitungsvorgänge jedenfalls auch die Beklagte. Die Meta Business Tools mögen durch Drittunternehmen – nicht durch die Beklagte selbst – auf den Webseiten bzw. Apps jener Drittunternehmen eingebunden werden bzw. eingebunden worden sein. Außer Streit steht aber, dass die Beklagte ihrerseits die von ihr entwickelten Business Tools den Drittunternehmen zur Einbindung auf deren Website bzw. App zur Verfügung stellt. Hierdurch nimmt die Beklagte maßgeblichen Einfluss darauf, dass und in welchem Umfang beim Besuch der Drittwebseiten bzw. -Apps durch einen Nutzer über diese Business Tools personenbezogene Daten dieses Nutzers erhoben und an die Beklagte weitergeleitet werden.

Der Verantwortlichkeit der Beklagten i.S.d. Art. 4 Nr. 7 DSGVO steht nicht entgegen, dass daneben ggf. auch das jeweilige Drittunternehmen als Betreiber der Webseite bzw. App Verantwortlicher ist. Bereits aus Art. 26 DSGVO ergibt sich, dass auch mehrere gleichzeitig und gemeinsam im Sinne der DSGVO datenschutzrechtlich verantwortlich sein können.

Die Beklagte ist ihrer datenschutzrechtlich Verantwortlichkeit nach Art. 4 Nr. 7 DSGVO auch nicht dadurch enthoben, dass sie im Rahmen einer Rahmenvereinbarung mit den Betreibern der Webseiten bzw. in ihren Nutzungsbedingungen für Meta Business Tools (Anlage B5) den Drittunternehmen die Verpflichtung auferlegt, einen stabilen und hinreichend auffälligen Hinweis für Nutzer bezüglich dem Erfassen, Teilen sowie der Verwendung der Business-Tool-Daten bereitzustellen, der näher beschriebene Mindestangaben zu enthalten hat. Zwar sollen nach Art. 26 DSGVO gemeinsam Verantwortliche „in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung erfüllt“. Eine solche Vereinbarung entbindet die gemeinsam Verantwortlichen indes nicht grundsätzlich von ihrer Verantwortlichkeit gegenüber dem Betroffenen; dies wäre ein rechtlich unbeachtlicher Vertrag zu Lasten Dritter. Sie dient primär der Effektivität der Durchsetzung der datenschutzrechtlichen Verpflichtung der mehreren Verantwortlichen. Im Übrigen wäre die Vereinbarung der Beklagten mit den Betreibern der Webseiten bzw. Apps auch inhaltlich nicht ausreichend, um die Beklagte generell aus ihrer datenschutzrechtlichen Verantwortlichkeit gegenüber ihren Nutzern für die Erhebung von Daten über die Meta Business Tools und deren weitere Nutzung zu entbinden. Die Verantwortlichkeit des Betreibers der Webseite oder App ist auf den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten beschränkt, für den/die er tatsächlich über die Zwecke und Mittel entscheidet (EuGH, Urteil vom 29.07.2019 – C-40/17). Dazu gehört die Erhebung und Weitergabe von Daten an die Beklagte, aber weder die Speicherung dieser Daten bei der Beklagten noch ihre weitere Verarbeitung durch die Beklagte, einschließlich beispielsweise ihrer Zusammenführung mit dem Nutzerprofil des Klägers bei der Beklagten oder der Weitergabe der Daten an Dritte durch die Beklagte.

c) Dass die Beklagte überhaupt personenbezogene Daten des Klägers verarbeitet, steht außer Streit. Das ist dem Grunde nach schon deshalb der Fall, weil der Kläger Inhaber eines Nutzerprofils bei Facebook ist; nach eigenem Vortrag der Beklagten ist die Personalisierung von Inhalten zentrales Merkmal des Betriebes dieser Plattform. Es steht auch außer Streit, dass die Beklagte sämtliche Daten des Klägers, die ihr über die Meta Business Tools übermittelt werden, zumindest für „bestimmte Datenverarbeitungsvorgänge“ auch dann nutzt, wenn sich der Kläger weder der Beklagten gegenüber noch dem Drittunternehmen gegenüber einverstanden erklärt hat. Diese Nutzung, wie auch die nach Behauptung der Beklagten vorgeschaltete Prüfung, ob ein Einverständnis mit der Datenverarbeitung zur Bereitstellung personalisierter Werbung vorliegt, ist Datenverarbeitung i.S.d. DSGVO.

Dass die Verarbeitung als solche insgesamt rechtswidrig ist, setzt der Auskunftsanspruch nach Art. 15 DSGVO nicht voraus. Er ist auch nicht auf die Beauskunftung rechtswidriger Datenverarbeitungsvorgänge beschränkt, soll vielmehr dem Berechtigten überhaupt erst ermöglichen, etwaige rechtswidrige Datenverarbeitungsvorgänge zu erkennen.

Der Kläger hat deshalb einen Anspruch nach Art. 15 Abs. 1 DSGVO gegen die Beklagte auf Auskunft über diese personenbezogenen Daten, wie mit der Klage näher spezifiziert. Der Anspruch erstreckt sich insbesondere auf „alle verfügbaren Informationen über die Herkunft der Daten“ (Art. 15 Abs. 1 lit. h DSGVO).

d) Bei den im Klageantrag zu 1. genannten Daten handelt es sich um personenbezogene Daten des Klägers, teils zugleich um Daten zur Herkunft der in Rede stehenden personenbezogenen Daten i.S.d. Art. 15 Abs. 1 lit. h DSGVO.

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Unzweifelhaft sind danach die E-Mail des Klägers, dessen Telefonnummer, sein Vor- und Nachname, sein Geburtsdatum, sein Geschlecht und der Ort, an dem er sich befindet, personenbezogene Daten. Ebenso handelt es sich bei der IP-Adresse des genutzten Clients um ein personenbezogenes Datum. Ferner handelt es sich auch bei der internen Klick-ID der Meta Ltd., sowie der internen Browser-ID der Meta Ltd. um personenbezogene Daten. Mit diesen Daten können die Aufrufe der Drittwebseite und die Aktionen darauf eindeutig einem bestimmten Facebook-Konto zugeordnet werden, in diesem Fall dem Konto des Klägers. Auch die URLs der Webseiten samt ihrer Unterseiten, der Zeitpunkt des Besuchs, der „Referrer“ (d.h. die Webseite, über die der Nutzer zur aktuellen Webseite gekommen ist), die vom Kläger angeklickten Buttons sowie die weiteren, von der Beklagten „Events“ genannten Daten, die die Interaktion des Klägers auf der jeweiligen Webseite dokumentieren, sind personenbezogene Daten, da sie jeweils in Verbindung mit weiteren Informationen dem Kläger zugeordnet werden können und dadurch Informationen über diesen beinhalten. So kann dadurch ermittelt werden, welche Webseiten der Kläger besuchte, wann dies geschah, von welcher Webseite er dort hingelangte, sowie welche Aktionen er dort durchgeführt hat, beispielsweise, ob er bestimmte Artikel gekauft hat. Aus den gleichen Gründen handelt es sich schließlich bei dem Namen der App, sowie dem Zeitpunkt des Besuchs, den vom Kläger in der App angeklickten Buttons, sowie den von der Beklagten „Events“ genannten Daten, die die Interaktionen des Klägers in der jeweiligen App dokumentieren, um personenbezogene Daten. Die Daten zum User-Agent des Clients stellen ebenfalls personenbezogene Daten dar. Schließlich sind auch die Lead-ID, die Abonnement-ID, die anon_id sowie die externe ID anderer Werbetreibender personenbezogene Daten. Denn als „ID“ stellen sie Identitätsdokumente bzw. Kennungen des Klägers dar bezüglich seiner Aktionen/Kontakte im Internet.

Die Auskünfte, die der Kläger mit seinem Klageantrag zu 1. in Bezug auf die vorbezeichneten personenbezogenen Daten begeht, stehen ihm gemäß Art. 15 Abs. 1 lit. a., c., g. und h. DSGVO zu.

e) Der Anspruch auf Auskunftserteilung ist nicht durch Erfüllung erloschen.

Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, 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. Der Verdacht, dass die erteilte Auskunft

unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. Die Annahme eines derartigen Erklärungsinhalts setzt jedoch voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberichtigte eine Ergänzung der Auskunft verlangen (BGH, Urteil vom 15.06.2021 – VI ZR 576/19).

Darlegungs- und beweisbelastet hinsichtlich der die Erfüllung begründenden Umstände ist die Beklagte. Die Beklagte hat ihre Auskunftspflicht weder durch ihr Schreiben vom 17.06.2024 (Anlage B8) erfüllt, noch durch ihre Bezugnahme auf dieses Schreiben im Rechtsstreit, verbunden mit der Behauptung, mit diesem Schreiben seien alle Auskünfte erteilt worden. Die Auskunft beschränkt sich auf die nach (irriger) Behauptung der Beklagten allein streitgegenständlichen Datenverarbeitungsvorgänge zur Bereitstellung personalisierter Werbung. Auch der Verweis auf das Vorhandensein von Self-Service-Tools ist nicht ausreichend. Das Tool „Deine Aktivitäten außerhalb der Meta-Technologien“ ermöglicht dem Nutzer nach unwidersprochen gebliebenem Vortrag des Klägers nur den Abruf rudimentärer Informationen, deren Umfang hinter demjenigen der begehrten Auskünfte weit zurückbleiben. Das Tool zeigt zudem – auch dies ist unstreitig – die ohnehin rudimentären Informationen nur für die jeweils letzten Monate an.

2. Klageantrag zu 2. – Löschung und Anonymisierung

Selbst bei unterstellter Zulässigkeit des Klageantrags zu 2. wäre ein Anspruch auf Anonymisierung der Daten nicht gegeben.

Ein Anspruch auf Anonymisierung von Daten ist als solcher in der DSGVO nicht ausdrücklich vorgesehen. Es handelt sich auch nicht um ein Minus gegenüber der Datenlöschung nach Art. 17 DSGVO. Die valide Datenanonymisierung, d.h. die nachträgliche Aufhebung des Personenbezuges der in Rede stehenden Daten, setzt eine komplexe Analyse der zu anonymisierenden Daten und anderer verfügbarer Datensätze voraus; denn nur eine Anonymisierung, bei der der Personenbezug nicht ohne weiteres wieder hergestellt werden kann, ist eine valide Anonymisierung i.S.d. DSGVO. Der mit dieser Analyse und dem Anonymisierungsvorgang selbst verbundene Aufwand ist einer Datenlöschung nicht notwendigerweise ebenfalls immanent. Schon aus diesem Grunde ist die Anonymisierung nicht als Minus in der Datenlöschung nach Art. 17 DSGVO enthalten. Der Betroffene hat auch kein erkennbares berechtigtes Interesse daran, dass in rechtswidriger Weise erhobenen bzw. verarbeiteten Daten in anonymisierter Form fortbestehen.

3. Klageantrag zu 3. – Entschädigung in Geld

Der Kläger hat wegen Verletzung seines Rechts auf informationelle Selbstbestimmung einen Anspruch auf eine Entschädigung in Höhe von 5.000,- EUR, § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG.

a) Seit Neufassung des Klageantrages zu 3. mit Schriftsatz vom 19.09.2024 macht der Kläger mit seinem Zahlungsbegehr vorrangig einen Entschädigungsanspruch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG geltend und stützt dieses Begehr hilfsweise auf Art. 82 DSGVO.

Dieser Klageantrag ist als unbezifferter Klageantrag zulässig. Das gilt für den Anspruch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG, weil § 253 Abs. 2 BGB die Bemessung der „billigen“ Entschädigung dem Gericht überlässt, der Kläger die für die Bemessung

maßgeblichen tatsächlichen Grundlagen vorträgt und er die ungefähre Größenordnung der begehrten Entschädigung mitgeteilt hat.

Art. 82 DSGVO schließt den Anspruch aus nationalem Recht nicht aus. Grundsätzlich haben zwar die von der DSGVO zur Verfügung gestellten Rechtsbehelfe abschließenden Charakter, wie sich insbesondere aus den Erwägungsgründen 9 und 10 der Verordnung ergibt. Dies gilt jedoch in Anbetracht des Erwägungsgrundes 146 S. 4 nicht für Art. 82 DSGVO. Dementsprechend können konkurrierende Ansprüche aus § 823 ff. BGB ebenso wie aus quasivertraglichen oder vertraglichen Sonderverbindungen (§ 280 Abs. 1, 241 Abs. 2, 311 Abs. 2 BGB bestehen (LG Ellwangen, Urteil vom 06.12.2024 – 2 O 222/24).

b) Die Voraussetzungen eines Anspruches auf Entschädigung nach § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG liegen vor.

aa) Art. 2 Abs. 1 GG gewährleistet in Verbindung mit Art. 1 Abs. 1 GG das allgemeine Persönlichkeitsrecht. Daraus ist als Schutzgut das Recht auf informationelle Selbstbestimmung herzuleiten, dass über den Schutz der Privatsphäre des einzelnen hinausgeht und ihm die Befugnis gibt, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (BVerfG, Urteil vom 15.12.1983 – 1 BvR 209/23; BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07). Es umfasst die aus dem Gedanken der Selbstbestimmung folgende Befugnis des einzelnen, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, ob ein Kommunikationsinhalt einzig dem Gesprächspartner, einem bestimmten Personenkreis oder der Öffentlichkeit zugänglich sein soll (BGH, Urteil vom 29.04.2014 – VI ZR 137/13). Davon erfasst werden alle Daten, die für Dritte erkennbar einer bestimmten Person zugeordnet sind, etwa das eigene Bild, das gesprochene und geschriebene Wort oder sonstige Einzelheiten des privaten Lebensbereiches (BGH, Urteil vom 11.06.2013 – VI ZR 209/12). Das Recht auf informationelle Selbstbestimmung schützt die Grundrechtsträger nach gefestigter höchstrichterlicher Rechtsprechung auch gegenüber Privaten in ihren Rechten, selbst zu entscheiden, welche Daten an Dritte herausgegeben werden und welche nicht.

Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die moderne Informationstechnik, insbesondere die zunehmende Verbreitung vernetzter informationstechnischer Systeme, eröffnet dem Einzelnen neue Möglichkeiten der Persönlichkeitsentfaltung, begründet aber auch neuartige Gefährdungen der Persönlichkeit. Solche Gefährdungen ergeben sich bereits daraus, dass komplexe informationstechnische Systeme ein breites Spektrum von Nutzungsmöglichkeiten eröffnen, die sämtlich mit der Erzeugung, Verarbeitung und Speicherung von Daten verbunden sind. Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07). Dieses Recht ist unter den Bedingungen der modernen und von digitalen Systemen zutiefst geprägten Massengesellschaft essenziell. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden (BVerfG, Beschluss vom 06.11.2019 – 1 BvR 16/13). Der Schutzmfang des Rechts auf informationelle Selbstbestimmung beschränkt sich auch nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb Grund rechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich

genommen nur geringen Informationsgehalt haben, kann, je nach dem Ziel des Zugriffs und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben (BVerfG, Urteil vom 27.02.2008 – 1 BvR 370/07).

bb) Eine Verletzungshandlung der Beklagten liegt durch ihre rechtswidrige Datenverarbeitung vor.

Der streitgegenständliche Datenverarbeitungsvorgang vom Erheben personenbezogener Daten über die Business Tools, das Empfangen jener Daten von den Drittwebseiten/-apps, das Speichern der Daten auf eigenen Servern der Beklagten, das Verarbeiten dieser Daten zur Profilbildung und die Weiterverwendung dieser Daten u.a. durch Weitergabe an Dritte und in Drittländer war rechtswidrig, weil nicht von einem der Rechtfertigungsgründe nach Art. 6 Abs. 1 DSGVO gedeckt.

Darlegungs- und beweisbelastet ist insoweit die Beklagte. Nicht zu folgen vermag das Gericht dem Einwand der Beklagten, sie brauche Rechtfertigungsgründe für die Erhebung und weitere Verarbeitung von personenbezogene Daten des Klägers außerhalb der Verarbeitung zum Zwecke der Bereitstellung personalisierte Werbung nicht anzuführen, weil der Kläger nicht spezifiziere, gegen welche anderen Verarbeitungszwecke er sich wenden wolle. Die Beklagte meint, es sei der konkrete Verarbeitungszweck, der eine Ermittlung der Rechtsgrundlage eines Verantwortlichen gemäß Art. 6 DSGVO bedinge, weshalb zunächst der Kläger bestimmte Verarbeitungszwecke zu beanstanden habe, bevor die Beklagte zu einer weiteren Einlassung verpflichtet sei.

Diese Argumentation der Beklagten verkennt zum ersten, dass der Kläger nicht bestimmte Verarbeitungszwecke der Beklagten, sondern die Datenverarbeitung als solche unabhängig von ihrem Zweck beanstandet. Die Argumentation der Beklagten verkennt zum zweiten, dass die vom Verantwortlichen im Sinne des § 4 Nr. 7 DSGVO verfolgten Zwecke als subjektive Merkmale für den Nutzer grundsätzlich nicht oder nur schwer erkennbar sind; es ist nicht ersichtlich, warum trotz der grundsätzlichen Darlegungslast des Verantwortlichen hinsichtlich der Rechtfertigungsgründe nach Art. 6 DSGVO gerade hinsichtlich solcher subjektiver Momente der Berechtigte zur näheren Darlegungen verpflichtet sein soll. Es ist schließlich auch nicht erkennbar, warum erst solcher Vortrag des Klägers zu bestimmten Verarbeitungszwecken, die nach seiner Vorstellung die Beklagte mit der Datenverarbeitung mutmaßlich verfolge, der Beklagten eine nähere Darlegung dergestalt ermöglichen sollte, warum die Datenverarbeitung für die Verfolgung dieser Zwecke zulässig sein soll.

Auf einen Rechtfertigungsgrund gemäß Art. 6 Abs. 1 lit. b-f DSGVO stützt die Beklagte die in Rede stehende Datenverarbeitung selbst nicht. Eine hierfür in Betracht kommende tatsächliche Grundlage ist auch für das Gericht nicht erkennbar.

Die Beklagte vermag ihre Datenverarbeitung aber auch nicht mit einer Einwilligung des Klägers gemäß Art. 6 Abs. 1 lit. a DSGVO zu rechtfertigen.

Zwar hat der Kläger über die Einstellung „Informationen von Werbepartnern über deine Aktivitäten“ am 30.04.2018 in die Datenverarbeitung zur Bereitstellung personalisierter Werbung eingewilligt. Eine Einwilligung des Klägers in die weiteren Datenverarbeitungsvorgänge seitens der Beklagten (s.o.) behauptet diese jedoch nicht einmal.

Soweit die Beklagte andeutet, zu welchen Zwecken – wenn nicht zur Bereitstellung personalisierter Werbung – sie die Daten des Klägers verarbeitet, geschieht dies nur vage unter floskelhafter Verwendung von Formulierungen, die als bloße Worthülsen schon nicht klar erkennen lassen, was genau mit den Daten des Klägers geschieht, geschweige denn, warum dies durch die von der Beklagten angedeuteten Zwecke gerechtfertigt sein soll. So behauptet die Beklagte, sie verarbeite die Daten, die von Drittunternehmen über Meta Business Tools

gesendet würden – unabhängig von der Zustimmung des Nutzers zur Datenverarbeitung zur Bereitstellung personalisierter Werbung – „zulässigerweise für andere Zwecke, z.B., um die Sicherheit ihrer Server zu schützen“. Beispielsweise wird ausgeführt, es solle sichergestellt werden, dass Kriminelle die streitgegenständlichen Business Tools nicht ausnutzen, um über diese Produkte Spam, Scraping oder andere Cyberangriffe durchzuführen. Warum eine extensive Datensammlung, wie sie die Beklagte in streitgegenständlicher Weise durchführt, dazu nützlich oder gar erforderlich sein soll, um die von ihr beispielhaft genannten Denial-of-Service-Angriffe zu verhindern, ist nicht ersichtlich. Schon gar nicht vermag dieses behauptete Ziel zu erklären, warum die Beklagte personenbezogene Daten, von denen sie erkannt hat, dass es sich nicht um Teil eines solchen Angriffes handelt, gleichwohl speichert und weiterverarbeitet. Darüber hinaus teilt die Beklagte lediglich noch pauschal und ohne nähere Substantiierung mit, sie stütze sich für die Verarbeitung der von Drittunternehmen über Meta Business Tools erhaltenen Nutzerdaten zu Sicherheit und Integritätszwecken auf die Rechtsgrundlage der vertraglichen Notwendigkeit, der berechtigten Interessen und des öffentlichen Interesses.

cc) Eine schuldhafte Verletzung des allgemeinen Persönlichkeitsrechts begründet einen Anspruch auf eine Geldentschädigung, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann. Ob eine so schwerwiegende Verletzung des Persönlichkeitsrechts vorliegt, dass die Zahlung einer Geldentschädigung erforderlich ist, kann nur aufgrund der gesamten Umstände des Einzelfalls beurteilt werden. Hierbei sind insbesondere die Bedeutung und Tragweite des Eingriffs, also das Ausmaß der Verbreitung der Veröffentlichung, die Nachhaltigkeit und Fortdauer der Interessen und/oder Rufschädigung des Verletzten, ferner Anlass und Beweggrund des Handelnden sowie der Grad seines Verschuldens zu berücksichtigen (BGH, Urteil vom 22.02.2022 – VI ZR 1175/20). Die Höhe der Geldentschädigung ist nach § 287 ZPO zu schätzen (BGH, Urteil vom 18.11.2024 – VI ZR 10/24). Auf die Vermögenslage des Beeinträchtigten kommt es zur Bemessung der Entschädigung nicht entscheidend an, aber eventuell auf die wirtschaftliche Leistungsfähigkeit des Rechtsverletzers. Für Medien muss der aufzubringende Entschädigungsbetrag einen echten Hemmungseffekt bedeuten, weniger orientiert an Prominenz oder Nichtprominenz des Betroffenen als ausgerichtet auf Art, Ausmaß und Intensität der jeweiligen Persönlichkeitsverletzung; nichts anderes kann in Fällen der vorliegenden Art gelten.

dd) Nach diesen Maßstäben gebührt vorliegend dem Kläger eine Entschädigung von 5.000,- EUR.

Die generelle Praxis der Beklagten, immer und auch ohne Einwilligung jedenfalls solche technischen Standarddaten, die der Beklagten mit hoher Wahrscheinlichkeit eine Identifizierung des jeweiligen Nutzers innerhalb der Systeme der Beklagten erlaubt, sowie das Datum, dass und wann die fragliche Drittseite mit diesem technischen Parametern aufgesucht wurde, über die Business Apps zu erheben, beeinträchtigt den Kläger in gravierendem Maße in seinem Recht auf informationelle Selbstbestimmung. Wie die Beklagte selbst nicht in Abrede stellt, führt die Vielzahl von Daten, die ihr über ihre Business Tools zur Verfügung gestellt werden, im Wege eines „Digital Fingerprinting“ dazu, dass die Beklagte den Nutzer allein hierdurch identifizieren kann, und zwar unabhängig von etwaigen browserseitigen Einschränkungen hinsichtlich der Verwendung von Third Party Cookies, ohne dass der Nutzer dazu bei den Netzwerken der Beklagten eingeloggt sein müsste und ohne dass der durchschnittliche Internetnutzer die Übertragungen von Daten an die Beklagte und deren Zusammenführung bei der Beklagten feststellen oder verhindern könnte.

Das Gericht erachtet als hinreichend dargelegt und bewiesen (§ 286 Abs. 1 ZPO), dass diese Praxis der Beklagten konkret auch den Kläger in ganz erheblicher Weise in seinem Persönlichkeitsrecht beeinträchtigt. Ohne Erfolg beanstandet die Beklagte in diesem Zusammenhang, der Kläger habe nicht genau dargelegt, welche konkreten Webseiten und Apps, auf denen Meta Business Tools aktiv seien, er im streitgegenständlichen Zeitraum genutzt habe; habe zudem auch nicht substantiiert dargelegt, dass sensible Daten des Klägers

tatsächlich über die Meta Business Tools an die Beklagte übermittelt worden seien. Solchen konkreten weiteren Vortrages des Klägers bedarf es nicht.

Zum einen ist die Beklagte dem Vortrag des Klägers nicht ausreichend entgegengetreten, dass ca. 30-40 % aller größeren Webseiten weltweit, darunter auch etliche mit hochsensiblen Themen, Business Tools nutzen (Anlagen K2, K13 und K14). Die Beklagte bestreitet das Vorbringen des Klägers lediglich als unsubstantiiert, was in der Sache unzutreffend und prozessual unzureichend ist. Hinzu kommt, dass unstreitig nur der Meta Pixel ausfindig gemacht werden kann, die anderen Meta Business Tools (Conversions API, F. SDK, Conversions API, App Events API) hingegen nicht. Es muss deshalb davon ausgegangen werden, dass die Zahl betroffener Webseiten und Apps noch deutlich größer ist. Bereits aufgrund dieser Zahlen muss bei jedem, der das Internet in üblicher Weise regelmäßig nutzt, zwangsläufig davon ausgegangen werden, dass er ebenso regelmäßig Seiten aufsucht, auf denen ein Business Tool der Beklagten installiert ist.

Der Kläger nutzt – was er im Rahmen seiner persönlichen Anhörung noch einmal deutlich gemacht hat – das Internet im Rahmen seiner täglichen Lebensführung sehr intensiv. Der Kläger hat glaubwürdig bekundet, dass er das Internet täglich mehrere Stunden nutze. So arbeite er nicht nur damit, sondern nutze es auch täglich privat. So gebe er etwa in die Google-Suchmaschine auch persönliche Fragen ein, wenn er dazu eine Hilfe oder Antwort benötige oder recherchiere zum Beispiel nach Produkten oder suche Informationen zu bestimmten Themen (zum Beispiel über Technik) oder suche nach Kontaktdaten von ansässigen Firmen. Es sei so, dass sich sein gesamter Alltag um das Internet drehe. Er nutze zum Beispiel auch Google-Nachrichten oder ChatGPT und bewege sich momentan auch vermehrt auf Parship. Es sei durchaus beängstigend, wenn man merke, dass man plötzlich persönliche Sachen angezeigt bekomme, wenn man sich im Internet bewegt hat. Da fühle er sich wie ein gläserner Mensch. Er sei durchaus besorgt bzw. verängstigt, wenn seine Gewohnheiten quasi abgespeichert würden. Es könne ja durchaus sein, dass diese Daten dann irgendwie missbraucht würden, etwa für Cyber-Attacken oder ähnliches. Die gesammelten Daten könnten ja auch für verbrecherische Sachen genutzt werden, dies insbesondere im Zeitalter von KI.

Die Darlegungen des Klägers im Rahmen seiner persönlichen Anhörung sind uneingeschränkt glaubhaft; gegen seine persönliche Glaubwürdigkeit, von der das Gericht überzeugt ist, hat auch die Beklagte keine Bedenken vorgebracht.

Die intensive Nutzung des Internets durch den Kläger in Verbindung mit der streitgegenständlichen Praxis der Beklagten führt dazu, dass die Besorgnis des Klägers absolut nachvollziehbar ist. Dies insbesondere auch hinsichtlich der von dem Kläger angesprochenen Verknüpfung der Daten mit KI.

Diese Ängste sind aber kein vages Zukunftsszenario, sondern knüpfen an präsente und schon nach dem gegenwärtigen Stand der Technik durchaus reale Befürchtungen. Zwar mag der Kläger, anders als etwa bei Datensammlungen durch den Arbeitgeber oder staatliche Stellen, unmittelbar von der Beklagten keine Sanktionen oder sonstigen Nachteile aufgrund deren Vorhaltung der gesammelten Daten und des gebildeten Profils zu besorgen haben; ein solches macht er auch nicht geltend. Andererseits geht aber die persönlichkeitsrechtsverletzende Datensammlung durch die Beklagte ihrem Umfang nach weit über jene Fälle hinaus, und sobald aber diese Daten an Dritte oder in Drittstaaten mit niedrigeren Schutzstandards weitergegeben werden oder weitergegeben worden sind, ist auch die Gefahr konkreter Nachteile nicht von der Hand zu weisen. Die exzessive Datenverarbeitung und -sammlung durch die Beklagte bedroht daher bereits jetzt die Freiheit von Inhabern von Facebook-Profilen wie dem Kläger, sich sowohl im Internet als auch in der realen Welt ungehindert nach den eigenen Bedürfnissen zu bewegen und zu verhalten.

Bei der Bemessung der Entschädigung war zu Lasten der Beklagten zu berücksichtigen, dass sich die zwei jüngeren der in Rede stehenden Business Tools, die „Conversion API“ und die

„App Events API“, von dem „Meta Pixel“ bzw. der „F. SDK“ maßgeblich dadurch unterscheiden, dass sie – unter Mitwirkung der Webseitenbetreiber und Appanbieter – alle Schutzversuche der Nutzer und Browserhersteller umgehen und die Datensammlung auch dann ermöglichen, wenn der Nutzer den Inkognito-Modus benutzt, Cookies von Drittseiten nicht zulässt und VPN benutzt. Ob dies der einzige Zweck der Einführung von „Conversion API“ und „App Events API“ gewesen ist, spielt dabei keine Rolle.

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

Insgesamt erachtet das Gericht daher eine Entschädigung von 5.000,- EUR als angemessen, aber auch erforderlich.

c) Aus Art. 82 DSGVO ergibt sich kein weitergehender Anspruch. Denn die für die Bemessung des Anspruchs aus Art. 82 DSGVO maßgeblichen Gesichtspunkte fließen sämtlich auch in die Bemessung des Anspruchs aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ein. Im Rahmen des Art. 82 DSGVO dürfen hingegen weder die Schwere des Verstoßes gegen die DSGVO, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen und ob er vorsätzlich gehandelt hat (BGH, Urteil vom 18.11.2024 – VI ZR 10/24). In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadensersatzanspruchs, wie sie in Erwägungsgrund 146 Satz 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DSGVO gestützte Entschädigung in Geld bereits dann als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 Abs. 1 DSGVO dagegen nicht erfüllen (BGH, Urteil vom 18.11.2024 – VI ZR 10/24). Soweit dem Kläger ein Anspruch auch aus Art. 82 Abs. 1 DSGVO zusteht, ist dieser von der Entschädigung nach § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 BGB umfasst (OLG Köln, Urteil vom 26.11.2020 – 15 U 39/20).

d) Der Entschädigungsanspruch des Klägers ist antragsgemäß seit dem 14.11.2023 mit 5 Prozentpunkten über dem Basiszinssatz zu verzinsen, §§ 286 Abs. 1, 288 BGB.

4. Klageantrag zu 4. – Vorgerichtliche Rechtsanwaltskosten

Der Kläger hat einen Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten, §§ 823 Abs. 1, 280 BGB.

III. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO, die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 709, 708 Nr. 11, 2. Alt., 711 ZPO.

Die Streitwertfestsetzung beruht auf § 48 GKG, 3 ZPO. Für die Anträge zu 1., 2. und 3. wird jeweils ein Betrag von 5.000,00 EUR angesetzt.



Richterin am Landgericht