LG Landshut, Endurteil v. 25.10.2024 – 54 O 2373/23

Titel:

Schlüssiger Sachvortrag erfordert mehr als Behauptungen ins Blaue hinein

Normenketten:

DS-GVO Art. 82

ZPO § 253 Abs. 2 Nr. 2

Leitsätze:

1. Wer einen Unterlassungsanspruch wegen angeblich unzulässiger Datenverarbeitung geltend macht, muss den zugrunde liegenden Sachverhalt in sich widerspruchsfrei, konkret und nachvollziehbar darlegen; bloße Behauptungen „ins Blaue hinein“, die sich weder aus vorgelegten Anlagen noch aus einer Auseinandersetzung mit dem substantiierten Vortrag des Gegners ergeben, genügen der Substantiierungspflicht nicht. (Rn. 14 – 22 und 26) (redaktioneller Leitsatz)

2. Die bloße Zurverfügungstellung von Tracking- und Messwerkzeugen (Meta Business Tools, Meta-Pixel, Conversion-API) macht den Anbieter nicht automatisch zum Verantwortlichen für die Datenverarbeitung der Drittunternehmen. Für die Einholung wirksamer Einwilligungen und die datenschutzkonforme Erfassung sind die Drittunternehmen verantwortlich. (Rn. 19 und 22 – 25) (redaktioneller Leitsatz)

3. Behauptet ein Kläger einen unzulässigen internationalen Datentransfer, ohne sich mit entgegenstehenden Angemessenheitsbeschlüssen der Europäischen Kommission auseinanderzusetzen, und legt er keinen fühlbaren und messbaren Schaden dar, scheiden sowohl Unterlassungs- als auch Schadensersatzansprüche nach der DS-GVO aus. Der bloße – zudem unsubstantiiert behauptete – Verstoß gegen die Verordnung genügt nicht. (Rn. 29 – 32) (redaktioneller Leitsatz)

Schlagworte:

Feststellungsinteresse, Vorrang der Leistungsklage, Unzulässige Datenverarbeitung, Schlüssigkeitsprüfung, Datenschutzverletzung, Schadensersatzanspruch

Fundstelle:

GRUR-RS 2024, 48072

Tenor

1. Die Klage wird abgewiesen.

2. Die Kosten des Rechtsstreits trägt die Klägerin.

3. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

4. Der Streitwert wird auf 9.500,-- € festgesetzt.

Tatbestand

1

Die Klägerin macht Unterlassung- und Schadensersatzansprüche wegen Datenverarbeitung geltend.

2

Die Beklagte betreibt das soziale Netzwerk ..., über welches die Nutzer Fotos und Videos teilen können. Die Klägerin nutzt ... seit dem ... .

3

Die Beklagte ist darüber hinaus Urheberin der sogenannten Meta Business Tools, welche die Beklagte für Drittunternehmen zum Einbau auf deren Webseiten anbietet.

4

Die Klägerin behauptet, die Beklagte würde die Meta Business Tools, insbesondere die Conversions API sowie das sogenannte Meta Pixel dazu einsetzen, um über die Webseiten Dritter Daten ihrer Nutzer

einzusammeln, obwohl eine hinreichende Einwilligung der jeweiligen Nutzer nicht vorhanden sei. Dadurch sei es der Beklagten möglich, ein detailliertes Nutzungsprofil für die jeweiligen ...-Kunden anzulegen. Diese Daten würden darüber hinaus weltweit weiter versandt, auch in Länder mit einem niedrigen Datenschutzniveau, wie beispielsweise die Vereinigten Staaten von Amerika. Der Klägerin sei dadurch ein Schaden entstanden. Zum Zwecke der Datensammlung nutze die Beklagte das sogenannte Digital Fingerprinting, so dass Nutzungsdaten und personenbezogene Daten der jeweiligen ...-Mitglieder auch dann gesammelt werden könnten, wenn sie nicht während der Nutzung des Internets beim Netzwerk der Beklagten eingeloggt sind. Mittels der sogenannten Conversions API könne die Beklagte auch Daten sammeln, wenn eine Zustimmung zur Datennutzung durch den jeweiligen Nutzer nicht vorhanden sei. Durch die Meta Business Tools sei es möglich, Inkognito-Modi der Webbrowser zu umgehen und den Browser zu erkennen, um weiter detaillierte Daten über die Internetnutzer zusammen, auch wenn diese einer Datennutzung nicht zugestimmt haben. Beim sogenannten Meta Pixel käme es zu einer Datenweitergabe an die Beklagte bereits dann, wenn das Pixel geladen wird, ohne dass es auf die Bestätigung der Datennutzung im sogenannten Cookie Banner ankommen würde.

5
Die Klägerin beantragt zuletzt,

1. Es wird festgestellt, dass der Nutzungsvertrag der Parteien zur Nutzung des Netzwerks „...“ unter dem Benutzernamen „...“ die Verarbeitung von folgenden personenbezogenen Daten in folgendem Umfang seit dem 25.05.2018 nicht gestattet:

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

- E-Mail der Klagepartei

- Telefonnummer der Klagepartei

- Vorname der Klagepartei

- Nachname der Klagepartei

- Geburtsdatum der Klagepartei

- Geschlecht der Klagepartei

- Ort der Klagepartei

- Externe IDs anderer Werbetreibender (von der „external_ID” genannt)

- IP-Adresse des Clients

- User-Agent des Clients (d. h. gesammelte Browserinformationen)

- interne Klick-ID der ...

- interne Browser-ID der ...

- Abonnement-ID

- Lead-ID

- Anon_id

sowie folgende personenbezogene Daten der Klagepartei

b) auf Webseiten

- die URLs der Webseiten samt ihrer Unterseiten

- der Zeitpunkt des Besuchs

- der „Referrer“ (die Webseite, über die der Benutzer zur aktuellen Webseite gekommen ist),

- die von der Klagepartei auf der Webseite angeklickten Buttons sowie

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

c) in mobilen Dritt-Apps

- der Name der App sowie

- der Zeitpunkt des Besuchs

- die von der Klagepartei in der App angeklickten Buttons sowie

- die von der ... „Events“ genannte Daten, die die Interaktionen der Klagepartei in der jeweiligen App dokumentieren.

2. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, auf Drittseiten und -Apps außerhalb der Netzwerke der Beklagten personenbezogene Daten gem. des Antrags zu 1. zu verarbeiten.

3. Die Beklagte wird verurteilt, die weitere Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO sämtlicher unter dem Antrag zu 1 a., b. und c. aufgeführten, seit dem 25.05.2018 bereits von der Beklagten verarbeiteten personenbezogenen Daten bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 Euro, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, insbesondere diese nicht an Dritte weiterzugeben, bis die Klagepartei die Beklagte zur Löschung auffordert, spätestens jedoch sechs Monate nach rechtskräftigem Abschuss des Verfahrens.

4. Die Beklagte wird verpflichtet, sämtliche gem. dem Antrag zu 1 a. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten der Klagepartei auf ihre Aufforderung hin, spätestens jedoch sechs Monate nach rechtskräft igem Abschluss des Verfahrens, vollständig zu löschen und der Klagepartei die Löschung zu bestätigen sowie sämtliche gem. dem Antrag zu 1 b. sowie c. seit dem 25.05.2018 bereits gespeicherten personenbezogenen Daten vollständig zu anonymisieren.

5. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, der aber mindestens 5.000,00 Euro beträgt, nebst Zinsen i. H. v. fünf Prozentpunkten über dem Basiszinssatz seit dem ..., zu zahlen.

6. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten i.H.v. 973,66 Euro freizustellen.

6
Die Beklagte beantragt,

die Klage abzuweisen.

7
Die Beklagte behauptet, eine Datenverarbeitung ihrer Nutzer würde nur mit entsprechender Einwilligung der Kunden erfolgen. Die Meta Business Tools würden allein der Integration der Metaprodukte und der Messung der Effektivität von Werbeanzeigen dienen, eine systematische Datensammlung der Internetnutzer sei durch die Beklagte nicht angestrebt. Bei einer Nutzung der Meta Business Tools, insbesondere durch die Drittunternehmen, seien diese auf Grund der Nutzervereinbarung zwischen der Beklagten und den Drittunternehmen verpflichtet, vor Weitergabe von Daten an die Beklagte eine entsprechende Einwilligung einzuholen. Im Vortrag der Klägerin sei bereits nicht dargelegt worden, welche Daten überhaupt übermittelt worden seien. Eine systematische Überwachung der Nutzer gäbe es nicht. Die Weitergabe von Daten ins Ausland beruhe auf den Grundlagen der Datenschutzgrundverordnung (DSGVO) und dem Angemessenheitsbeschluss der Europäischen Kommission. Ein Schaden werde durch die Beklagte bestritten. Entgegen der Auffassung der Klägerin würden die Business Tools den jeweiligen Dritten als Feedback für die Effektivität ihrer Werbeanzeigen im Netzwerk der Beklagten dienen. Im übrigen sei es den Nutzern der Beklagten möglich, der Nutzung von sogenannten Offsite-Daten, also bei Drittunternehmen erhobenen Daten, zu widersprechen. In den aktuellen Datenschutzeinstellungen der Beklagten sei eine

Nutzung bei Neuanmeldung abgeschaltet, d. h. die Nutzer müssten aktiv einer solchen Nutzung zustimmen. Die Beklagte stelle auch ausreichend Möglichkeiten zur Verfügung, die erhobenen Daten von Dritten zu kontrollieren und gegebenenfalls zu löschen.

8
Eine Beweisaufnahme hat nicht stattgefunden.

9
Zur Vervollständigung des Tatbestands wird verwiesen auf sämtliche Schriftsätze der Parteien nebst Anlagen sowie sonstigen Aktenteile.

Entscheidungsgründe

10
Die Klage ist teilweise unzulässig, im Übrigen unbegründet.

I.

11
Der Klageantrag Ziffer 1 (stets bezogen auf die Anträge in der Replik vom ...) ist unzulässig, weil kein Feststellungsinteresse der Klägerin besteht. Es herrscht der Grundsatz des Vorrangs der Leistungsklage, was vorliegend die Unterlassung im Sinne von Ziffer 2 der Klageanträge ist. Warum die Klägerin vorab einen Feststellungsantrag geltend macht, um in Anschluss daran die entsprechende Unterlassung zu verlangen, erschließt sich nicht und wird von ihr auch nicht hinreichend genau begründet.

12
Ob die Klageanträge 3 und 4 zulässig sind, kann vorliegend dahinstehen, weil sie jedenfalls unbegründet sind.

II.

13
Im Übrigen ist die Klage unbegründet, da die Klägerin bereits nicht schlüssig darlegt, dass die Beklagte unzulässigerweise und unter Verstoß gegen die DSGVO Daten erheben und verarbeiten würde.

14
1. Streitgegenstand im Sinne des § 253 Abs. 2 Nr. 2 ZPO ist nach dem ausdrücklichen Vortrag der Klägerin im Schriftsatz vom ..., die Untersagung von Datensammlungen bei Drittunternehmen, insbesondere die Verarbeitung personenbezogener Daten der Klägerin über die Meta Business Tools durch die Beklagte (Seite 9 des Schriftsatzes, Bl. 398 d.A.). Entgegen der Auffassung der Klägerin sieht die Beklagten diesen Streitgegenstand ebenfalls als eng umrissen an, da sich der Vortrag der Beklagten (von der Beklagten als „streitgegenständliche Datenverarbeitung“ bezeichnet) stets mit dem Meta Pixel und den Meta Business Tools befasst. Es ist nicht ersichtlich, dass die Beklagte (abgesehen von einer abweichenden Rechtsauffassung) einen anderen Streitgegenstand definiert bzw. in ihren Schriftsätzen behandelt.

15
2. Die Unbegründetheit der Klage folgt daraus, dass die Klägerin nicht schlüssig darlegt, dass bei der Beklagten unzulässigerweise Daten gesammelt und verarbeitet werden. Denn insbesondere unter Berücksichtigung des Vortrags der Beklagten, auf den die Klägerin nicht näher eingeht, sondern schlicht als falsch zurückweist, ist eine Schlüssigkeit nicht gegeben (MüKo-ZPO/Prütting, 6. A., § 284, Rn. 11; Musielak-Voit/Foerste, ZPO, 21. A., § 284, Rn. 1).

16
Es ist bereits kaum möglich, den Vortrag der Klägerin bei einer Schlüssigkeitsprüfung als wahr zu unterstellen, da er erhebliche Widersprüche und Inkonsistenzen aufweist, die mit den beigelegten Anlagen nicht in Übereinklang zu bringen sind, insbesondere unter Berücksichtigung des Vortrags der Beklagten erhebliche Zweifel an der Richtigkeit des klägerischen Vortrags aufwirft und man somit einen solchen, steten Widersprüchen unterliegenden Vortrag nicht einmal einer sachverständigen Begutachtung zuführen kann.

17

3. Im Kern trägt die Klägerin drei Sachverhalte vor, aus welchen sich eine unerlaubte Datenverarbeitung der Beklagten in Bezug auf ihre Kunden ergeben soll.

18
a) Die Klägerin behauptet, die Beklagte würde mittels „digital fingerprinting“ Daten der jeweiligen Nutzer zur jeweiligen ... zuordnen können, dies unabhängig davon, ob der jeweilige Kunde bei der Beklagten eingeloggt ist oder nicht. Der Beklagten sei es durch modernste Techniken möglich, auch ohne das Setzen von Cookies den jeweiligen Nutzer vor dem PC wiederzuerkennen. Als Hinweis darauf legt die Klägerin Anlage K7, einen Artikel des ...- Onlinemagazins vor, das auf Forschungsergebnisse einer Universität in den USA verweist. Allerdings bleibt es das Geheimnis der Klägerin, woraus sich ein Rückschluss ergeben soll, dass diese Technik von der Beklagten eingesetzt wird. Aus Anlage K7 ergibt sich dies jedenfalls nicht. Die Beklagte hat bestritten, dass sie derartige Techniken einsetzt. Darüber hinaus stellt sich die Frage, wenn bereits 2017 eine derartige Technik stark verbreitet wäre, warum die Beklagte sich noch mit „primitiven“ Techniken wie Setzen von Cookies oder Nutzung des Meta-Pixels abgeben sollte, wenn sie auf die in Anlage K7 erwähnte „Webbrowser Fingerprintingmethode“ zurückgreifen könnte.

19
b) Eine weitere, von der Klägerin beanstandete Datenverarbeitung ist das behauptete Setzen von Cookies für die Drittunternehmen, wenn der ...-Nutzer innerhalb des -Netzwerks (beispielsweise bei ...) auf eine Werbeanzeige klickt und die Beklagte dann die Tatsache dieses Werbeklicks an das Drittunternehmen weiterleitet. Hier bleibt bereits offen, was das mit den im Klageantrag genannten Daten, welche von den Drittunternehmen angeblich an ... geschickt werden, zu tun haben soll. Ebenso wenig kann die Klägerin nicht darlegen, warum die Beklagte sich nicht an die Datenschutzeinstellungen ihrer Nutzer halten soll. Hier handelt es sich um eine reine Behauptung ins Blaue hinein, die Beklagte würde eine unzulässige Datenverarbeitung vornehmen, ohne dass erkennbar ist, dass ein Datenstrom von den Drittunternehmen zu Beklagten gerichtet ist. Die Tatsache, dass die Beklagte Daten an die Drittunternehmen schickt (also in die umgekehrte Richtung), um diesen ein Feedback zu geben, dass der ...-Nutzer auf eine Werbeanzeige innerhalb des ...-Netzwerks geklickt hat, rechtfertigt noch nicht die Annahme, die Beklagte würde dies in allen Fällen unabhängig einer eventuellen Einwilligung vornehmen. Darüber hinaus ergibt sich aus dem Vortrag der Klägerin insoweit nicht, dass tatsächlich personenbezogene Daten verarbeitet werden. Insbesondere erklärt sich nicht, inwieweit die beiden Cookies, welche die Klägerin auf Seite 15 der Replik vom ... erwähnt, tatsächlich mit dem jeweiligen Nutzerkonto in Verbindung gebracht werden können. Die Klägerin belässt es bei der bloßen Behauptung, ohne dies näher darzulegen, das Meta-Pixel würde diese beiden Cookies zusammenführen und dann Daten an die Beklagte übersenden. Im Vortrag der Klägerin ist ein Zusammenhang mit einer von den Business Tools generierten ID die Rede und einer Klick-ID, die mit dem Klick innerhalb des ...-Netzwerks in Zusammenhang steht. Wie ein Zusammenhang mit dem jeweiligen Nutzer beim Drittunternehmen oder bei der Beklagten hergestellt wird, bleibt offen. Vielmehr erkennt die Webseite des Drittanbieters (!) den Besucher anhand der Cookies wieder, von der Beklagten ist aber nicht die Rede. Dies untermauert vielmehr den Vortrag der Beklagten, die Meta Business Tools dienten der Messung der Effizienz der Werbekampagnen innerhalb des ...-Netzwerks. Denn anhand dieses Cookies kann die Seite des Drittunternehmens nachvollziehen, ob der Besucher der Seite auch schon einmal auf eine Werbeanzeige geklickt hat. Die Identität des Besuchers kann aber nicht festgestellt werden, da die Klägerin nicht behauptet, ein Zusammenhang mit der ...-ID werde hergestellt. Konkret auf die ...- Seite im Beispiel des Klägerin bezogen, wird bei Klick auf eine Anzeige des ... auf dem Computer der Klägerin in einem Cookie von ... (!) hinterlegt, dass ein (!) Nutzer dieses Computers mal eine Werbeanzeige vom ... angeklickt hat. Besucht dieser Nutzer (bzw. dessen Computer) nochmals die ...-Homepage, erkennt diese (und nicht die Beklagte) diese Tatsache wieder. Sofern die Klägerin dies aber für unzulässig hält, muss sie sich an den jeweiligen Betreiber der Seite wenden, denn mit dieser Form der Datenerhebung und -verarbeitung hat die Beklagte nichts zu tun. Allein die Programmierung und Zurverfügungstellung der Software, die eine solche Datenverarbeitung ermöglicht, macht die Beklagte nicht zur Verantwortlichen dieser Datenverarbeitung. Das kann auch der Fashion-ID-Entscheidung des EuGH (Urteil vom 29.07.2019, Az. C-40/17) nicht entnommen werden, da dort Daten vom „Gefällt-mir-Button“ an ... übersandt wurden, was hier gerade nicht ersichtlich ist.

20
Inwieweit ein Rückschluss auf den jeweiligen Nutzer möglich ist erschließt sich somit nicht und wird von der Klägerin nicht erklärt. Ob sich dies aus Anlage K6 ergibt kann dahinstehen, da diese in Englisch abgefasst

ist und es nicht Aufgabe des Gerichts ist, sich aus irgendwelchen Anlagen einzelne Informationen, welche mit Schriftsätzen schlüssig dargelegt sein müssen, zusammenzusuchen.

21
Im Übrigen erklärt die Klägerin auch nicht, wie dieser Datenstrom funktionieren soll, wenn die Beklagte eine Nutzung von Offsitedaten (wozu diese Klick-ID-Informationen werden, wenn das Drittunternehmen sie wieder an die Beklagte zurückgeschickt) nur mit Einwilligung des Nutzers durchführt. Die Beklagte hat darüber hinaus auf Seite 26 des Schriftsatzes vom ... substantiiert und konkret dargelegt, dass die Cookies _fbp und _fbc nicht von der Beklagten kontrolliert und gesetzt werden, sondern allein von den Drittunternehmen, die sich für eine Nutzung von Meta Businesstools entschieden haben. Wenn also das Drittunternehmen zwar im Netzwerk der Beklagten wirbt, Meta Business Tools allerdings nicht nutzt, werden offenbar diese beiden Cookies auch nicht gesetzt. Es handelt sich also nicht um Drittanbieter-Cookies, sondern um Erstanbieter-Cookies aus Sicht der Drittunternehmen. Diese mögen zwar im Zusammenhang mit den Meta Business Tools stehen und von der Beklagten „erfunden“ sein, von einer Datenverarbeitung der Beklagten kann in diesem Zusammenhang allerdings nicht gesprochen werden (s.o.).

22
c) Ebenso wenig kann die Klägerin näher darlegen, es käme zu einem systematischen Ausspionieren und somit zu einer unzulässigen Datenverarbeitung durch die Nutzung des sogenannten Meta-Pixels bei den Drittunternehmen. Insbesondere reicht in diesem Zusammenhang nicht aus, die Entscheidung des Bundeskartellamts vom 06.02.2019 zu zitieren, vielmehr wäre es erforderlich, selbst den Sachverhalt so darzustellen, dass er in sich schlüssig wäre. Die Beklagte hat nachvollziehbar und technisch korrekt dargelegt, dass allein aus einem Datenstrom, der durch das Laden des Metapixels beim Aufruf der entsprechenden Seite (zum Beispiel www....de) anfällt, nicht geschlossen werden kann, dass unzulässigerweise Daten des jeweiligen Internetnutzers an die Beklagte übertragen wird. Wer beispielsweise die ... -Homepage aufruft, wird zu Beginn sofort von einem Cookiebanner begrüßt, in welchem man die Wahl hat, entweder mit dem kostenpflichtigen ...-Abonnement fortzufahren oder mit Werbung die ...- Homepage zu lesen. Bevor man aber zur eigentlichen Homepage gelangt muss man den Cookies gegebenenfalls zustimmen oder diese ablehnen. Wer die entsprechende Einwilligung näher studiert, wird dort auch das Meta-Pixel finden, in welches man einwilligen kann oder nicht.

23
Dies unterstreicht aber den Vortrag der Beklagten, dass es die Drittunternehmen sind, welche dafür verantwortlich sind, die entsprechende Einwilligung der Nutzer einzuholen, bevor sie Daten an die Beklagte übertragen. Daran ändert auch die Fashion-ID-Entscheidung des EuGH (s.o.) nichts. Der EuGH hat damals lediglich festgestellt, dass zumindest auch das Drittunternehmen für die entsprechende Datenverarbeitung mitverantwortlich ist. Aus der Entscheidung kann nicht geschlossen werden, dass das Drittunternehmen alleine oder dass die Beklagte alleine verantwortlich ist.

24
Unbeachtet blieb allerdings in der damaligen Entscheidung, dass die Beklagte keinen Einfluss darauf hat, ob sich ein Drittunternehmen für die Nutzung des Meta-Pixels bzw. der übrigen Meta Business Tools entscheidet. Diese werden von der Beklagten zur Nutzung angeboten, die Klägerin trägt aber nicht vor, die Beklagte hätte konkrete Kenntnis darüber ob und in welchem Umfang Dritte die Meta Business Tools zum Einsatz bringen. Wie bereits ausgeführt unterscheidet sich das Meta Pixel vom „Gefällt-mir-Button“ dadurch, dass nicht ohne weitere Daten an die Beklagte übertragen werden, da dies nach dem nachvollziehbaren substantiierten Vortrag der Beklagte nur der Fall ist bzw. sein darf, wenn die Drittunternehmen eine entsprechende Einwilligung einholen, da auch nur dort eine solche sinnvoll ist. Dann sind aber die Drittunternehmen dafür verantwortlich. Wenn die Klägerin daher der Meinung ist, es würden ohne ausreichende Einwilligung Daten von den Drittunternehmen an die Beklagte übersandt, muss sie die Drittunternehmen in Anspruch nehmen.

25
Damit ist es der Beklagten nur möglich, eine datenschutzkonforme Datenverarbeitung durchzuführen, indem sie eine Datenübertragung an sie nur dann ermöglicht, wenn die Drittunternehmen die entsprechende Einwilligung der Nutzer einholen. Diese sind für diesen Teil alleinverantwortlich, dies ergibt sich auch eindeutig aus den Bedingungen für die Drittunternehmen, welche die Beklagte in Anlage B5 vorlegt. Es ist für die Beklagte mangels leeren Vortrags der Klägerin diesbezüglich auch offensichtlich nicht möglich zu

kontrollieren, ob sich die Drittunternehmen an die einschlägigen Regelungen der Datenschutzgrundverordnung halten oder nicht. Die Klägerin kann auch nicht aufzeigen, wie die Beklagte eine solche regelwidrige Nutzung der Meta Business Tools überhaupt erkennen und gegebenenfalls unterbinden können soll.

26
d) Auch der Vortrag der Klägerin zur sogenannten Conversion API zeigt eine unzulässige Datenverarbeitung durch die Beklagte nicht auf. In Anlage K 10 ergibt sich dazu nichts. Während die Klägerin reißerisch behauptet, die Beklagte würde mit Stasi-Methoden die Nutzer des Internets systematisch aufhorchen und versuchen, persönlichen Bewegungsprofile der Nutzer zu erstellen, kann eine solche Datenkontrolle insbesondere den vorgelegten Unterlagen zur Conversion API gerade nicht entnommen werden. Wie sich aus Anlage K 10 ergibt, dient die Conversion API dazu, den Drittunternehmen eine Kontrolle über ihre bei der im Netzwerk der Beklagten (kostenpflichtig) geschalteten Werbeanzeigen zu überprüfen und den Erfolg der Werbekampagne zu kontrollieren. Auch die Klägerin kann nicht näher darlegen, dass eine Datenverarbeitung für solche Daten, soweit sie in diesem Zusammenhang von den Drittunternehmen an die Beklagte geschickt werden, ohne Einwilligung der jeweiligen Nutzer erfolgt. Das bloße Bestreiten der Klägerin ist in diesem Zusammenhang unbeachtlich, da es auf den Vortrag der Beklagten nicht eingeht und diesen schlicht als falsch darlegt und die Einwilligung als „nicht ausreichend und freiwillig“ abqualifiziert, ohne dies näher zu erläutern. Die Beklagte hat ausführlich dargelegt, wie die jeweiligen Dialoge zur Erlangung einer Einwilligung zur Nutzung von Offsitedaten bei Drittunternehmen gestaltet sind und wie der Begleittext dieser Einwilligungserklärungen lautet.

27
Es mag für den jeweiligen ...– oder ...-Nutzer mühselig sein, sich durch diese Vielzahl von Einstellungen zu klicken, andererseits scheint es der Klägerin im Hinblick auf den Datenschutz ja besonders wichtig zu sein, dass ihre Daten nicht missbraucht werden oder unzulässig einer Datenverarbeitung unterworfen werden. Von daher kann gerade in so einem Fall vor einem verständigen Internetnutzer wie der Klägerin erwartet werden, dass sie sich die Mühe macht, sich in dieses Thema einzuarbeiten und die Vielzahl von Einstellungen einer kritischen Überprüfung zu unterwerfen. Dies umso mehr, als die Nutzung von Offsitedaten nach dem nicht widersprochenen Vortrag der Beklagten als Standardeinstellung ausgeschaltet ist und der Nutzer daher konkret zustimmen muss, dass diese Offsitedaten auch verwendet werden. Auch die von der Beklagten aufgezeigten Möglichkeiten, die bereits erhobenen bzw. verarbeiteten Offsitedaten zu kontrollieren hält das Gericht für ausreichend und in sich nachvollziehbar.

28
Beim Vortrag, aus Anlage K10 würde sich ergeben, die Conversion API sei für „Nutzer gedacht, die nicht der Datennutzung zugestimmt haben“, übersieht die Klägerin, dass ausweislich der Fußnote 12 auf Seite 23 der Anlage K10 dies nur ...-Kunden ab einem bestimmten ...-Versionsstand gilt (also für Inhaber von ...-Geräten), offensichtlich ist dies bei ...-Geräten nicht relevant. Davon abgesehen, dass die Klägerin nirgends bestreitet, dass das Drittunternehmen vorab die Einwilligung einholen muss und sich dies auch nicht aus der besagten Stelle in Anlage K10 ergibt, hat die Beklagte nachvollziehbar dargelegt (S. 34 des Schriftsatzes vom ..., Bl. 310 d. A.), dass es bei dieser Aussage überhaupt nicht um eine Datenverarbeitung bei der Beklagten in Bezug auf Offsitedaten der ...-Nutzer geht, sondern allein um das Messen der Effektivität von Werbekampagnen, wie die Conversions API stets beworben wird. Außerdem erklärt die Klägerin nicht, dass die Beklagte tatsächlich bei Nutzern, welche sich gegen die Nutzung ihrer Daten entschieden haben (opt out bzw. fehlendes opt in), tatsächlich personenbezogene Daten dieser Nutzer erhält bzw. verarbeitet. Auf Seite 23 der Anlage K10 sind im unteren Bereich sechs Schritte beschrieben, wie die Events (die Aktionen der jeweiligen Nutzer auf der jeweiligen Webseite des jeweiligen Drittunternehmens) aggregiert werden, um den Erfolg einer Werbekampagne zu messen. In keinem dieser sechs Schritte ist zu erkennen, dass personenbezogene Daten an die Beklagte übersandt werden. In Schritt 3 ist die Rede von Anzeigen, welche an eine Testgruppe (was auch immer das darstellen soll) ausgeliefert wird, in Schritt 4 werden Conversion-Daten aus der Kampagne über die Conversions API an Meta gesendet, wo dann (Schritt 5) die Events unter Wahrung der Privatsphäre verarbeitet werden. Woraus sich ergibt, dass personenbezogene Daten übertragen werden erschließt sich nicht. Allein die Tatsache, dass anonyme (!) Eventdaten aggregiert werden und zur Auswertung an ... übersandt werden, lässt nicht den Schluss zu, es würden personenbezogene Daten der jeweiligen Nutzer an die Beklagte übermittelt und könnten dort einer Datenverarbeitung in Bezug auf die jeweilige Nutzungs-ID bei der Beklagten zugeführt

werden. Vielmehr ist dieser Vortrag der Klägerin ein Beispiel dafür, dass der gesamte Vortrag sich auf Schlagworte beschränkt, die genutzt werden sollen, um angebliche Datenschutzverletzungen der Beklagten darzulegen. Substanz haben diese Vorwürfe nicht. Darüber hinaus wäre es äußerst ungeschickt von der Beklagten, Datenschutzverstöße wie angeblich auf Seite 23 der Anlage K 10, frei ins Internet zu stellen und damit denjenigen einen Angriffspunkt zu liefern, die offenkundig sehr um die Sicherheit ihrer Daten bemüht sind.

29
4. Soweit die Klägerin behauptet, die Beklagte würde unzulässigerweise Daten in die USA übertragen und damit gegen einschlägige EuGH Rechtsprechung verstoßen, verweist die Beklagte auf die stets nach den EuGH-Entscheidungen ergangenen Angemessenheitsbeschlüsse der Europäischen Kommission und auf die fehlende Rückwirkung der EuGH-Entscheidungen. Darauf geht die Klägerin überhaupt nicht mehr ein. Es ist daher unstreitig, dass die Angemessenheitsbeschlüsse einen Datentransfer in die USA erlauben.

30
5. Somit kommen Unterlassungsansprüche von vornherein nicht in Betracht.

III.

31
Ein Schadensersatzanspruch ist ohnehin unbegründet, da die Klägerin einen irgendwie gearteten materiellen oder immateriellen Schaden nicht darzustellen vermag. Die Klägerin sieht die Beklagte bereits schadensersatzpflichtig, da diese gegen Vorschriften der DSGVO verstößt. Dies allein reicht jedoch nicht aus. Der Vortrag der Klägerin auf Blatt 187 ff. d. A. (S. 37 ff. der Replik vom ...) ist denkbar ungefähr, wie es in Schriftsätzen betreffend die DSGVO auf Klägerseite stets der Fall ist. Individuellen Vortrag findet man dort nicht, der Vortrag ist in allen Fällen stets der gleiche. Im Übrigen erklärt die Klägerin auch nicht, warum sie sich nicht bei ... abmeldet, wenn die Beklagte permanent Daten von ihr abgreift und einer unzulässigen Datenverarbeitung unterwirft.

32
In der Rechtsprechung des EuGH ist mittlerweile hinreichend geklärt, ab wann Schadenersatz bei Verstößen gegen Datenschutzgrundverordnung zu leisten ist. Wie bereits ausgeführt, reicht der bloße Verstoß gegen die Datenschutzgrundverordnung (der hier ohnehin nicht substantiiert dargelegt ist) nicht aus (Urteil vom 20.06.2024, Az. C-182/22 und C-189/22; NJW 2024, 2599). Es bedarf eines fühlbaren und messbaren Schadens, den die Klägerin hier gerade nicht vorzutragen vermag (Urteil vom 13.12.2018, Az. C-150/17; Urteil vom 14.12.2023, Az. C-340/21).

IV.

33
Nachdem die Klägerin schon nicht darstellen kann, welche unzulässige Datenverarbeitung die Beklagte durchführen soll, bestehen auch keine Ansprüche auf Speicherung oder Anonymisierung oder Löschung von Daten.

V.

34
Mangels Hauptansprüche besteht auch kein Anspruch auf Ersatz außergerichtlicher Kosten.

VI.

35
Die Kostenfolge ergibt sich aus § 91 ZPO. Die vorläufige Vollstreckbarkeit resultiert aus § 709 ZPO. Der Streitwert wurde wie folgt festgesetzt: Ziffer 1: 1.500 €, Ziffer 2 und 3 jeweils 1.000 €, Ziffer 4: 1.000 € und Ziffer 5: 5.000 €.