

Titel:

Abstrakte Ängste vor einem Datenzugriff ausländischer Behörden begründen keinen datenschutzrechtlichen Schaden

Normenketten:

ZPO § 253 Abs. 2 Nr. 2, § 256 Abs. 1

DSGVO Art. 46, Art. 82

BGB § 242

Leitsätze:

1. Ein Unterlassungsantrag, der sich gegen vermeintlich unzulässige Datenübermittlungen richtet, ist unzulässig, wenn er nicht eindeutig erkennen lässt, welche konkreten Handlungen untersagt werden sollen. Das Bestimmtheitsgebot des § 253 Abs. 2 Nr. 2 ZPO verlangt, dass Art und Umfang der beanstandeten Datenverarbeitung präzise bezeichnet werden. Die bloße pauschale Bezugnahme auf „personenbezogene Daten“ genügt ebenso wenig wie ein generelles Verbot der Datenübermittlung an „Dritte“, das auch berechnigte amtliche Anfragen erfassen könnte. (Rn. 29 – 30) (redaktioneller Leitsatz)

2. Ein Auskunftsantrag ist mangels Rechtsschutzbedürfnis unzulässig, wenn der Kläger die begehrten Informationen durch einen einfacheren oder billigeren Weg erreichen kann, etwa durch die Nutzung eines von dem Verantwortlichen zur Verfügung gestellten Selbstbedienungstools, worauf er auch hingewiesen wurde. (Rn. 31 – 32) (redaktioneller Leitsatz)

3. Ein Schadensersatzanspruch nach Art. 82 DSGVO wegen einer Datenübertragung in ein Drittland, etwa die USA, scheidet aus, wenn der zugrundeliegende Datentransfer auf ausreichenden Garantien nach Art. 46 DSGVO beruht und der Kläger zudem in Kenntnis der Datenverarbeitungsmodalitäten die Dienste des Anbieters freiwillig nutzt. Wer bewusst einen globalen Kommunikationsdienst verwendet, dessen technische Funktionsweise notwendigerweise internationale Datenflüsse voraussetzt, kann sich später nicht auf eine unzulässige Datenübermittlung berufen. Das widerspricht dem Grundsatz von Treu und Glauben. (Rn. 38 – 42 und 48) (redaktioneller Leitsatz)

4. Ein immaterieller Schadensersatzanspruch nach Art. 82 DSGVO setzt eine nachvollziehbare, individualisierte Darlegung konkreter Beeinträchtigungen voraus, die kausal auf eine rechtswidrige Datenverarbeitung zurückzuführen sind. Abstrakte Ängste vor einem möglichen Zugriff ausländischer Behörden auf personenbezogene Daten genügen ebenso wenig wie pauschale, textbausteinartige Schilderungen seelischer Belastungen. Selbst wenn psychische oder körperliche Beschwerden behauptet werden, fehlt es an der haftungsrechtlichen Zurechnung, wenn die geltend gemachten Beeinträchtigungen auf allgemeine politische Entwicklungen oder das generelle Risiko staatlicher Dateneinsicht zurückgehen, nicht aber auf die konkret angegriffene Datenübermittlung. Der bloße Speicherort der Daten begründet für sich genommen keinen ersatzfähigen Schaden. (Rn. 42 – 47) (redaktioneller Leitsatz)

Schlagworte:

Drittland, Datenübertragung, Selbstbedienungstool, Treu und Glauben, Kausalität, immaterieller Schaden, Feststellungsinteresse

Fundstellen:

RDV 2025, 336

LSK 2025, 25358

ZD 2026, 223

Tenor

1. Die Klage wird abgewiesen.
2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.
3. Das Urteil ist für die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 10.000,00 € festgesetzt.

Tatbestand

1

Der Kläger nimmt die Beklagte auf Schadensersatz, Unterlassung, Auskunft, Feststellung und Zahlung vorgerichtlicher Rechtsanwaltskosten aus Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) aufgrund der Übermittlung von Daten in die USA in Anspruch.

2

Die Beklagte ist eine Gesellschaft mit Sitz in Irland, ihre Konzernmuttergesellschaft, die M. Platforms Inc., hat ihren Sitz in den USA. Die Beklagte betreibt insbesondere die sozialen Netzwerke F. und I. in Europa, der Mutterkonzern bietet solche Dienste auch im Rest der Welt an. Bei F. handelt es sich um einen globalen Online-Dienst für Kommunikation und das Teilen von Inhalten, der es den Nutzern ermöglichen soll, mit anderen Nutzern auf der ganzen Welt auf vielfältige Weise in Kontakt zu treten und Inhalte auf verschiedene Arten zu teilen. Der Kläger unterhielt auf F. ein Nutzerprofil mit der E-Mail-Adresse Er nutzte die angebotene Kommunikations-Dienste von F. jedenfalls bis in das Jahr 2024.

3

Die Beklagte überträgt routinemäßig verschiedene Arten von Daten in die USA, dazu gehören EU-Benutzerdaten, die nicht ohnehin öffentlich einsehbar sind.

4

Am 16.07.2020 erklärte der EuGH im Verfahren C-311/18 („Schrems II“) das sog. Privacy Shield für ungültig. Die zuständige irische Datenschutzkommission verhängte im Mai 2023 gegen die Beklagte wegen Vorwürfen in Zusammenhang mit der Datenübertragung eine Geldbuße von 1,2 Milliarden Euro. Die Beklagte legte gegen diese Entscheidung Rechtsmittel ein. Das Verfahren insoweit ist noch nicht rechtskräftig abgeschlossen.

5

Am 11.07.2023 trat mit dem EU-U.S. Data Privacy Framework ein neues Datenschutzabkommen zwischen der Europäischen Union (EU) und den USA in Kraft. Seit diesem Zeitpunkt stützt die Beklagte den Datentransfer in die USA auf dieses Abkommen.

6

Die Prozessbevollmächtigten des Klägers verlangten mit Schreiben vom 13.08.2024 (Anlage B15) von der Beklagten Unterlassung und Schadensersatz und stellten ein Auskunftersuchen an die Beklagte, das die nunmehrigen Prozessbevollmächtigten der Beklagten mit Schreiben vom 02.09.2024 (Anlage B16) beantwortete. Hierbei wurden dem Kläger detaillierte Informationen erteilt, insbesondere wurde ihm erklärt, wie er auf seine F.-Daten zugreifen kann. Die Beklagte verwies weiter auf die maßgeblichen Abschnitte der Datenschutzrichtlinie und das verfügbare Selbstbedienungs-Tool, welches es Nutzern ermöglicht, ihre F.-Daten aufzurufen und zu verwalten.

7

Die Beklagte erhebt die Einrede der Verjährung.

8

Der Kläger behauptet, die Beklagte habe seit 16.07.2020 bis 2023 Jahre lang wissentlich gegen die DSGVO verstoßen, um Profit zu machen. Sie übertrage Verhaltensdaten, Geräteinformationen und werbungsbezogene Daten in die USA. Die Beklagte mache personenbezogene Daten ihrer Nutzer Dritten, insbesondere den amerikanischen Ermittlungsbehörden, vorsätzlich zugänglich. PRISM, das Überwachungsprogramm der NSA, ermögliche der NSA den Zugriff auf die Server großer Internetunternehmen, darunter auch die Beklagte. Über PRISM könne die NSA auf Benutzerdaten zugreifen, einschließlich E-Mails, Chat-Nachrichten, Video-Chats, Fotos, Dokumente und andere Inhalte. UPSTREAM sei ein weiteres Überwachungsprogramm der NSA, das darauf abziele, den Internetverkehr in großem Maßstab zu überwachen. Durch UPSTREAM könne die NSA den gesamten Datenverkehr überwachen, einschließlich E-Mails, Instant Messaging, VoIP-Anrufe und andere Internetkommunikation. Es erfolge keine Autorisierung einer individuellen Überwachungsmaßnahme und auch keine Überprüfung der

Auswahl einer Zielperson. Es bestehe ein erhebliches Risiko der Verletzung der Privatsphäre der Nutzer des sozialen Netzwerks F., da die Daten viele Informationen über deren Privatleben enthalten. Die Zuwiderhandlung habe vorsätzlichen Charakter, da die Beklagte gegen die DSGVO verstoßen habe, obwohl sie seit dem Urteil in der Rechtssache Schrems II gewusst habe, dass die internationale Übermittlung der Daten seitens der Beklagten einen Verstoß gegen die DSGVO darstelle.

9

Der Kläger trägt weiter vor, die Veröffentlichung der Daten habe weitreichende Folgen für ihn (Anmerkung des Gerichts: Dies entspricht dem Sachvortrag des Klägers in der Klageschrift S. 10. Nach Auffassung des Gerichts dürfte es sich um einen nicht passenden Textbaustein aus einem Scraping-Verfahren handeln). Er habe einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten verblieben. Seit er erfahren habe, dass seine Daten illegal in die USA übermittelt worden seien, habe sich sein Leben grundlegend verändert. Er habe zunächst bei sich körperliche Beschwerden wie Kälteschauer, Schwitzen und Schwindel bemerkt. Dies mache es für ihn schwer, seinen Alltag zu bewältigen. Er fühle sich häufig benommen und unsicher. Er müsse seither mit der permanenten Angst leben, dass plötzlich Ermittlungen ausländischer Strafverfolgungsbehörden angestrengt werden könnten. Seine Freude am Reisen und sein berufliches Fortkommen sei stark eingeschränkt.

10

Der Kläger ist der Rechtsauffassung, die Datenübertragung seitens der Beklagten in die USA könne in der Zeit vom 16.07.2020 bis zum 11.07.2023 nicht auf einen Erlaubnistatbestand der DSGVO gestützt werden. Eine Übermittlung könne insbesondere nicht auf Art. 46 DSGVO gestützt werden aufgrund des Fehlens geeigneter Garantien für ein angemessenes Datenschutzniveau in den USA. Eine Notwendigkeit der Datenübermittlung zur Vertragserfüllung (Art. 49 DS-GVO) scheide auch aus. Er habe aus Art. 82 DSGVO Anspruch auf einen angemessenen immateriellen Schadensersatz, der mit 3.000 € zu bemessen sei. Er könne zudem die Feststellung der Ersatzpflicht der Beklagten für seine aus dem Datenschutzverstoß resultierenden künftigen Schäden verlangen. Zudem habe er einen Anspruch auf Unterlassung der unrechtmäßigen Verarbeitung seiner Daten sowie auf Auskunft aus Art. 15 DSGVO.

11

Der Kläger meint weiter, die in Frage kommende Rechtsgrundlage der Einwilligung erfordere, dass der Betroffene hinlänglich informiert worden sei. An einer solchen Information fehle es in den Belehrungen der Beklagten, sodass die Einwilligung nicht freiwillig erteilt worden sei.

12

Der Kläger beantragt:

13

Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, mindestens jedoch 3000 €, nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

14

Die Beklagte wird verurteilt, es zu unterlassen,

a) personenbezogene Daten der Klagepartei,

hilfsweise sämtliche von der Beklagten verarbeiteten Daten der Klagepartei,

die von oder über Personen generiert, geteilt und hochgeladen werden, die die Produkte und Dienste des Datenexporteurs (einschließlich F.) besuchen, darauf zugreifen, sie nutzen oder anderweitig mit ihnen interagieren; Informationen im Zusammenhang mit den Handlungen der Nutzer und den Informationen, die die Nutzer bei der Nutzung der Dienste bereitstellen; Informationen im Zusammenhang mit den Daten, die von anderen Nutzern der Produkte und Dienste zur Verfügung gestellt werden; Informationen über Netzwerke und Verbindungen von Nutzern; Informationen über Zahlungen; Informationen über Geräte, auf denen Nutzer Software installieren, die vom Datenexporteur bereitgestellt wird, oder die auf Produkte und Dienste des Datenexporteurs zugreifen; Informationen von Websites und Apps, die Produkte und Dienste des Datenexporteurs nutzen, die einen „Gefällt mir“- oder „Kommentar“-Button oder andere

Dienstintegrationen verwenden; und Informationen von Drittpartnern, und Informationen hinsichtlich der Dienste der Beklagten, F. sowie die Messenger Dienste von F.,

aa) in die USA zu verschicken und

bb) diese Dritten, insbesondere Ermittlungsbehörden in den USA, zugänglich zu machen.

b) personenbezogene Daten der Klagepartei,

hilfsweise sämtliche von der Beklagten verarbeiteten Daten der Klagepartei,

die von oder über Personen generiert, geteilt und hochgeladen werden, die die Produkte und Dienste des Datenexporteurs besuchen, darauf zugreifen, sie nutzen oder anderweitig mit ihnen interagieren; Informationen im Zusammenhang mit den Handlungen der Nutzer und den Informationen, die die Nutzer bei der Nutzung der Dienste bereitstellen; Informationen im Zusammenhang mit den Daten, die von anderen Nutzern der Produkte und Dienste zur Verfügung gestellt werden; Informationen über Netzwerke und Verbindungen von Nutzern, wie Verbindungen eines Nutzers zu Gruppen, Seiten und anderen Nutzern; Informationen über Zahlungen; Informationen über Geräte, auf denen Nutzer Software installieren, die vom Datenexporteur bereitgestellt wird, oder die auf Produkte und Dienste des Datenexporteurs zugreifen; Informationen von Websites und Apps, die Produkte und Dienste des Datenexporteurs nutzen, die einen „Gefällt mir“- oder „Kommentar“-Button oder andere Dienstintegrationen verwenden; und Informationen von Drittpartnern, und Informationen hinsichtlich der Dienste der Beklagten, F. sowie die Messenger Dienste von F.,

ohne eine Einwilligung der Klagepartei zu verarbeiten.

15

Die Beklagte wird verurteilt,

a) der Klagepartei Auskunft zu erteilen darüber, welche der die Klagepartei betreffenden personenbezogenen Daten, betreffend die Dienste der Beklagten, F. sowie die Messenger Dienste von F., hilfsweise sämtliche von der Beklagten verarbeiteten Daten der Klagepartei, durch die Beklagte in der Zeit vom 16.7.2020 bis zum 10.7.2023 in die USA versendet wurden oder zugänglich gemacht wurden.

b) der Klagepartei Auskunft zu erteilen darüber, welche der personenbezogenen Daten betreffend die Dienste der Beklagten, F. sowie die Messenger Dienste von F., hilfsweise sämtliche von der Beklagten verarbeiteten Daten der Klagepartei, durch die Beklagte Dritten zugänglich gemacht wurden oder solchen Dritten übersendet/übermittelt wurden.

c) der Klagepartei Auskunft zu erteilen darüber, welche Dritte gegebenenfalls Zugang zu den personenbezogenen Daten betreffend die Dienste der Beklagten, F. sowie die Messenger Dienste von F., hilfsweise sämtlichen von der Beklagten verarbeiteten Daten der, hatten oder diese von der Beklagten erhalten haben.

d) der Klagepartei Auskunft zu erteilen, wie lange solche personenbezogenen Daten betreffend die Dienste der Beklagten, F. sowie die Messenger Dienste von F., hilfsweise sämtliche von der Beklagten verarbeiteten Daten der Klagepartei, in den USA gespeichert bleiben, wo diese gespeichert sind und ob eine Löschung der Daten in den USA vorgesehen ist.

16

Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle zukünftigen Schäden zu ersetzen, die der Klägerseite durch die unbefugte Datenverschickung in die USA und die Zugänglichmachung gegenüber Dritten, insbesondere Ermittlungsbehörden in den USA, seitens der Beklagten entstanden sind und/oder noch entstehen.

17

Die Beklagte wird verurteilt, an die Klagepartei einen Betrag in Höhe von 973,66 € (Rechtsanwaltskosten außergerichtlich) zu zahlen, nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz für die außergerichtliche anwaltliche Rechtsverfolgung.

18

Die Beklagte beantragt

Klageabweisung.

19

Die Beklagte ist der Rechtsauffassung, der EuGH habe im Schrems II-Urteil keine Aussage zur Rechtmäßigkeit der Datenübermittlung der Beklagten getroffen, sondern lediglich festgestellt, dass eine solche Datenübermittlung nicht auf den Privacy Shield gestützt werden könne. Die Beklagte habe sich aber auf vereinbarte Standardvertragsklauseln (Standard Contractual Clauses, „SCC“) nach Art. 46 DSGVO gestützt. Zudem könne die Beklagte sich auf Art. 49 Abs. 1 lit. b DS-GVO stützen, da die Datenübermittlung erforderlich sei, um die Verträge mit den EU-Nutzern zu erfüllen.

20

Die Beklagte meint weiter, der Antrag des Klägers auf Zahlung von immateriellen Schadensersatz sei bereits nicht bestimmt genug, weil ein einziger Zahlungsanspruch geltend gemacht werde, dieser jedoch auf eine Vielzahl angeblicher DSGVO-Verstöße gestützt werde. Im Übrigen sei der Anspruch auch unbegründet. Der Kläger habe keinen konkreten Schaden, den er durch den angeblichen Verstoß der Beklagten gegen die DSGVO erlitten habe, nachgewiesen. Auch an der Kausalität eines etwaigen Verstoßes der Beklagten gegen die DSGVO und des behaupteten Schadens fehle es. Der Auskunftsantrag sei mangels Rechtsschutzbedürfnisses unzulässig, jedenfalls aber unbegründet, da sie die gewünschten Auskünfte bereits erteilt habe. Soweit sich das Auskunftersuchen des Klägers auf Anfragen nach Section 702 des US Foreign Intelligence Surveillance Act von 1978 („Section 702 FISA“) beziehe, sei es Anbietern elektronischer Kommunikationsdienste, die Anfragen nach Section 702 FISA erhalten, nach US-amerikanischem Recht untersagt, Informationen über diese Anfragen Dritten gegenüber offenzulegen. Die Beklagte sei deshalb u.a. gemäß § 29 Abs. 1 Satz 2 BDSG und Art. 15 Abs. 4 DSGVO von der Pflicht zur Erteilung solcher Informationen entbunden. Die Unterlassungsanträge seien aufgrund fehlender hinreichender Bestimmtheit unzulässig, im Übrigen auch unbegründet. Insbesondere habe sich die Beklagte zur Rechtfertigung der Datenübertragung nie auf eine Einwilligung des Nutzers gestützt, so dass sie insoweit auch keine Einwilligung des Nutzers einholen müsse.

21

Die Beklagte ist ferner der Rechtsansicht, der Kläger sei in jedem Fall verpflichtet, die Datenübermittlung in die USA gemäß § 242 BGB zu dulden. Der Kläger verhalte sich widersprüchlich, weil er einerseits die von der Beklagten erbrachten Leistungen nutze und auch weiterhin nutzen möchte, andererseits aber die Datenübertragung in die USA verhindern wolle, obwohl die Beklagte die Dienstleistung ohne eine solche Übermittlung nicht erbringen könne.

22

Der Kläger repliziert, es sei zu bestreiten, dass zwischen der Beklagten und ihrer Konzernmutter stets wirksame Datenübermittlungs- und verarbeitungsverträge bestanden hätten und dass diese exakt den Inhalt hatten, den die EU-Kommission vorgegeben habe. Ohnehin komme es hierauf aber nicht an, da auch bei ordnungsgemäßen Verträgen mit Standardvertragsklauseln es erforderlich sei, dass die Beklagte zusätzliche Maßnahmen ergreifen müsse, um sicherzustellen, dass die SSCs gültig seien. Solche Maßnahmen habe die Beklagte nicht ergriffen und insbesondere auch nicht die nötige „Transfer-Folgenabschätzung“ (TIA) getätigt.

23

Die Beklagte dupliziert, sie habe eine Transfer-Folgenabschätzung (TIA) durchaus vorgenommen. Ohnehin führe ein Versäumnis, eine solche durchzuführen, aber nicht zu einem Schadensersatzanspruch. Sie habe auch umfassende technische und organisatorische Sicherheitsvorkehrungen getroffen, um die Integrität der Datenübermittlung sicherzustellen, etwa systematisch alle Auskunftersuchen der US-amerikanischen Behörden auf deren Berechtigung geprüft und die Daten durchgehend verschlüsselt.

24

Das Gericht hat den Kläger im Termin zur mündlichen Verhandlung vom 27.08.2025 informatorisch angehört. Hinsichtlich des Ergebnisses der informatorischen Anhörung wird auf das Protokoll über die mündliche Verhandlung vom 27.08.2025 Bezug genommen.

25

Zur Ergänzung des Sachverhalts wird Bezug genommen auf die gewechselten Schriftsätze der Parteien nebst Anlagen sowie das Protokoll über die mündliche Verhandlung vom 27.08.2025.

Entscheidungsgründe

26

Die Klage ist hinsichtlich der Anträge auf Unterlassung, Auskunft und Feststellung bereits unzulässig, im Übrigen insgesamt unbegründet.

A.

Zulässigkeit

27

Die Klage war teilweise, soweit Unterlassung, Auskunft und Feststellung beantragt werden, als unzulässig abzuweisen. Im Übrigen, soweit Zahlung von Schadensersatz und vorgerichtlicher Rechtsanwaltskosten begehrt wird, ist die Klage zulässig.

28

I. Entgegen der Auffassung der Beklagten ist der Antrag auf Zahlung immateriellen Schadensersatzes – die Klagepartei hat sich nicht die Mühe gemacht, die Anträge zu nummerieren – bestimmt genug. Die Klagepartei macht einen einheitlichen Anspruch auf Ersatz eines immateriellen Schadens geltend, der sich aus mehreren Datenschutzverstößen ergeben soll. Es handelt sich dabei nicht um unzulässige Alternativen, eine Aufspaltung in Schadensersatz für die jeweils geltend gemachten einzelnen DSGVO-Verstöße ist weder erforderlich, noch wäre dies sachdienlich. Vielmehr handelt es sich um einen einheitlichen Streitgegenstand (vgl. hierzu Bundesgerichtshof, Urteil vom 18.11.2024, Az.: VI ZR 10/24).

29

II. Der Klageantrag ist, soweit Unterlassung begehrt wird, unzulässig. Die Beklagte weist zutreffend darauf hin, dass der Antrag zu unbestimmt formuliert ist. Die Verletzungshandlung, welche der Kläger untersagt haben möchte, ist nicht hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Ein Unterlassungsanspruch darf nicht derart undeutlich gefasst sein, dass die Entscheidung darüber, was der Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (Bundesgerichtshof, Urteil vom 18.11.2024, Az.: VI ZR 10/24 m.w.N.).

30

Es ist schon nicht klar, welches personenbezogenen Daten von dem Unterlassungsbegehren erfasst sein sollen. Darüber hinaus ist nicht klar, an welche Dritte der Beklagten die Übermittlung von Daten untersagt werden soll – nach dem Wortlaut wären etwa auch berechtigte Ermittlungsersuchen der nationalen und auch von ausländischen Strafverfolgungsbehörden erfasst.

31

III. Auch die gestellten Auskunftsanträge erweisen sich als unzulässig. Den Anträgen fehlt jedenfalls das Rechtsschutzbedürfnis. Ein fehlendes Rechtsschutzbedürfnis, das zur Unzulässigkeit des Klageantrags führt, kann angenommen werden, wenn ein einfacherer oder billigerer Weg zur Erreichung des Rechtsschutzziels besteht (vgl. auch hierzu Bundesgerichtshof, Urteil vom 18.11.2024, Az.: VI ZR 10/24).

32

Ein entsprechender einfacherer Weg steht dem Kläger zur Verfügung, weil sich der Kläger über das von der Beklagten zur Verfügung gestellte Selbstbedienungstool diese Informationen einfacher beschaffen könnte, worauf er durch die Beklagte bereits mit dem außergerichtlichen Schreiben (Anlage B16) hingewiesen wurde.

33

IV. Der Feststellungsantrag gerichtet auf die Verpflichtung der Beklagten, dem Kläger künftige Schäden zu ersetzen, ist ebenfalls unzulässig.

34

Der Antrag genügt, worauf die Beklagte zutreffend hinwies, nicht den Anforderungen des § 253 Abs. 2 Nr. 2 ZPO sowie des § 256 Abs. 1 ZPO, nachdem die Klagepartei festgestellt haben möchte, dass die Beklagte verpflichtet ist, „alle zukünftigen Schäden zu ersetzen, die der Klägerseite (...) entstanden sind und/oder noch entstehen“. In der Klageschrift führt der Kläger lediglich zu zukünftigen Schäden aus. Es wird nicht dargelegt, dass entsprechende Schäden bereits entstanden seien und ggf. noch nicht bekannt sein könnten.

35

Hinsichtlich zukünftiger Schäden fehlt es auch am Feststellungsinteresse. Grundsätzlich genügt dafür zwar die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden, eine darüber hinausgehende hinreichende Schadenswahrscheinlichkeit ist nicht erforderlich (vgl. auch hierzu Bundesgerichtshof, Urteil vom 18.11.2024, Az.: VI ZR 10/24). Der Kläger beschränkt sich jedoch auf lediglich völlig pauschales Vorbringen zu ihm noch aus der behauptet rechtswidrigen Datenübermittlung drohenden Schäden. Da dem Kläger schon nicht der Beweis gelungen ist, dass ihm überhaupt bisher ersatzfähige Schäden entstanden sind (siehe dazu unten), ist erst recht nicht zu erkennen, wie dem Kläger jetzt noch zwei Jahre nach der Datenübertragung, welche er für rechtswidrig hält, Schäden entstehen sollen, die tatsächlich adäquat kausal auf die behauptete rechtswidrige Datenübertragung zurückzuführen wären.

B.

36

Soweit die Klage zulässig ist, erweist sie sich als vollumfänglich unbegründet.

37

I. Dem Kläger steht kein Anspruch auf Zahlung eines Betrags von 3.000 € oder einer niedrigeren Summe nach Art. 82 DSGVO zu.

38

1. Bereits im Ausgangspunkt steht dem Kläger kein Schadensersatzanspruch zu, weil die Übertragung der Daten des Klägers in die USA entgegen der Rechtsauffassung des Klägers auch in der Zeit vom 16.07.2020 bis zum 11.07.2023 nicht rechtswidrig war.

39

a) Die Beklagte konnte sich für den Datenübertrag auf Art. 46 Abs. 1 DSGVO stützen. Zwischen der Beklagten und ihrem Mutterkonzern waren Standarddatenschutzklauseln vereinbart, die unter Art. 46 Abs. 2 lit. C DSGVO fallen. Solche ausreichenden Standardvertragsklauseln stellen nach Art. 46 DSGVO unter den dort genannten Bedingungen ausreichende Garantien des Verantwortlichen bzw. des Auftragsdatenverarbeiters dar. Es ist davon auszugehen, dass auch in den USA dem Betroffenen wirksame Rechtsbehelfe zur Durchsetzung seiner Rechte zur Verfügung stehen. Neben einer zivilrechtlichen Klage gegen den Mutterkonzern der Beklagten, soweit dieser aus Sicht des Klägers Daten unrechtmäßig verarbeitet, steht dem Kläger auch die Möglichkeit offen, die US-amerikanischen Datenschutzbehörden einzuschalten.

40

b) Zuletzt konnte sich die Beklagte für die Datenübermittlung auch Art. 49 Abs. 1 lit. c DSGVO stützen.

41

Insofern hat das Landgericht Hof in seinem Endurteil vom 19.02.2025, Az.: 12 O 144/24 ausgeführt was folgt:

„1) Der Klagepartei ist es nicht gelungen, eine rechtswidrige Datenübermittlung substantiiert darzulegen und zu beweisen. Die Plattformen „F.“ und „I.“ sowie die Konzernmutter der Beklagten stammen aus den USA. Beide Plattformen sind gerade global konzipiert. Um diese weltweiten Netzwerke unterhalten zu können, müssen zwangsläufig Daten international ausgetauscht werden, auch wenn die Klagepartei dies bestreitet. Der Einholung des von der Klagepartei angebotenen Sachverständigengutachtens für einen Gegenbeweisbedarf es hierfür nicht. Das in diesem Zusammenhang auch Daten durch die Beklagte in die USA übermittelt werden, ist unerlässlich. Dieses Erfordernis ist auch unabhängig davon, ob die Klagepartei mit US-amerikanischen F.- oder -Nutzern „befreundet“ ist oder sein möchte oder von der Tatsache, dass nicht jeder EU-Bürger Freunde in den USA oder Familie dort hat oder ob viele EU-Bürger ggf. keine über die EU hinausgehenden Interessen haben und sich ggf. sich nicht mit NICHT-EU-Bürgern austauschen wollen. F. und I. sind weltweite Netzwerke. Jeder Nutzer kann selbst entscheiden, ob er die beiden Plattformen nutzen möchte oder nicht. Allein die weltweite Suche nach Nutzern, die von F. und I. angeboten wird, kann nur funktionieren, wenn ein grenzüberschreitender Datenaustausch stattfindet. All dies ist jedem Nutzer der Plattformen, auch der Klagepartei, hinlänglich bekannt. Die Klagepartei hat keinen Anspruch darauf, dass F. und I. der gestalt betrieben werden, dass sämtliche Daten in Europa gespeichert und verarbeitet werden im Sinne einer rein europäischen Plattform. Die unternehmerische Entscheidung der Beklagten sowie ihrer Konzernmutter als Betreiberin der Plattformen, ein weltweites Netzwerk mit

entsprechender Vernetzung anzubieten und Daten in den USA zu verarbeiten, ist von den Nutzern, die sich freiwillig für eine entsprechende Nutzung entscheiden, hinzunehmen (so i.E. auch zutreffend LG Passau, Urteil vom 16.02.2024, Az. 1 O 616/23 sowie LG Bochum, Urteil vom 15.05.2024, Az. 5 O 334/23).“

42

Dem ist uneingeschränkt beizutreten.

43

2. Darüber hinaus vermochte der Kläger ein ihm durch den Datenübertrag in die USA entstandenen Schaden auch nicht zur Überzeugung des Gerichts darzulegen.

44

Der Kläger legt schriftsätzlich zwar umfangreiche Beeinträchtigungen durch den Datenübertrag dar. Während die Angaben dazu auf S. 10 der Klageschrift noch ein offensichtlicher Textbaustein sind, der gerichtsbekannt in zahlreichen Datenschutzverfahren ohne jegliche Individualisierung vorgebracht wird, zitiert der Schriftsatz auf S. 11 aus einem offenbar ausgefüllten Fragebogen und trägt einen individuellen Sachverhalt vor. Die Beklagte bestritt das Vorbringen des Klägers zu seiner Beeinträchtigung mit Nichtwissen.

45

In seiner informatorischen Anhörung legte der Kläger dem Gericht umfangreiche, auch körperliche, Beeinträchtigungen aufgrund seiner Kenntnis eines Datenübertrags seitens der Beklagten in die USA dar. Auf Nachfrage des Gerichts, weil es dem Gericht nur schwer nachvollziehbar erschien, dass ein Nutzer von F. vom Datenübertrag erst 2024 Kenntnis erlangt haben soll, erläuterte der Kläger seine Beeinträchtigungen weiter dahingehend, dass für ihn v.a. belastend sei die Kenntnis, dass auch Dritte in den USA Kenntnis von seiner Kommunikation erlangen könnten.

46

Für das Gericht ist im Grundsatz noch verständlich, dass sich Nutzer der Beklagten Sorgen machen wegen eines Zugriffs etwa der US-Geheimdienste oder der Grenzbehörden der USA auf ihre Posts etc. auf der Kommunikationsplattform der Beklagten. Diesen Punkt vermag das Gericht dem Kläger zu glauben, der auch anschaulich seine Ängste beschrieb. Zumindest sehr ungewöhnlich erscheinen dem Gericht allerdings die geklagten auch körperlichen Beeinträchtigungen des Klägers in Kenntnis des Datenübertrags bzw. eines Zugriffs von US-Behörden hierauf. Es handelt sich nach Einschätzung des Gerichts zunächst einmal um ein abstraktes Risiko, allzumal ein konkreter Schaden (etwa gegen ihn bisher eingeleitete Maßnahmen der US-Behörden) vom Kläger nicht angegeben wurde. Hierauf gleich mit körperlichen Beschwerden wie Schlaflosigkeit zu reagieren, erscheint dem Gericht zumindest sehr ungewöhnlich.

47

Letztlich scheidet ein Schaden des Klägers, die vom Kläger genannten Beeinträchtigungen für einmal als zutreffend unterstellt, aber an der fehlenden Kausalität der Datenübertragung seitens der Beklagten in die USA hierfür: Es kann zwar ohne weiteres Medienberichten entnommen werden, dass die USA seit Amtseinführung der Trump II-Administration eine verschärfte Politik gegenüber Einwanderern (darunter auch Einwanderern, die über legale Kanäle ins Land kommen wollen wie z.B. für Studien- oder Forschungsaufenthalte) ergriffen haben. Des Weiteren ist auch zutreffend, dass die US-amerikanischen Grenzbehörden nach Medienberichten ein verschärftes Vorgehen gegenüber Personen, die (auch nur kurzfristig) in die USA einreisen wollen, an den Tag legen. Hier sollen nach Medienberichten auch in sozialen Medien gepostete Inhalte von Relevanz sein. Allerdings ist dieses Vorgehen unabhängig vom Datenübertrag seitens der Beklagten in die USA. Es ist schlichtweg eine Folge einer massiv geänderten Politik der USA gegenüber Einwanderern und sonstigen Ausländern. Für dieses Vorgehen spielt jedoch der Datenübertrag in die USA keine Rolle. Selbst wenn die Beklagte einen solchen Datenübertrag nicht vornehmen sollte, könnten sich die US-amerikanischen Behörden die geposteten Inhalte anzeigen lassen, etwa in dem sie selber F.-Profile unterhalten oder Einwanderungs – sowie Einreisewillige dazu zwingen, ihnen den Zugang zu Profilen in den sozialen Medien zu eröffnen. Letzteres ist nach Medienberichten bereits vorgekommen und völlig unabhängig vom Speicherort der F.-Kommunikation des Klägers. Das Gericht kann zwar ohne weiteres nachfühlen, dass dies insbesondere für Personen, die sich zur Zeit für eine Reise in die USA bzw. einen Aufenthalt dort interessieren (wie vom Kläger angegeben) sehr unangenehm und bedrohlich ist. Dies ist aber eine Folge der politischen Entwicklung in den USA, nicht des Speicherorts der Daten. Hinzu tritt, dass – sollte der Kläger tatsächlich eine solche Vorstellung gehabt

haben – es schon immer eine unrealistische Annahme war, dass Dritte auf die von der Beklagten gespeicherten Daten ihrer Nutzer nie zugreifen könnten. Ein solcher Zugriff war schon lange und auch in Deutschland nach den einschlägigen gesetzlichen Bestimmungen möglich, etwa für Staatsanwaltschaften und Gerichte im Rahmen von Strafverfolgungsmaßnahmen nach der StPO und für den Verfassungsschutz nach den für die jeweilige Behörde geltenden Vorschriften. Ähnliche Möglichkeiten bestehen, wie von den Parteien dargelegt, für die US-amerikanischen Dienste. Und auch die anderen EU-Staaten werden im Rahmen vergleichbarer Regeln wie der deutschen auf bei F. vorhandene Daten zugreifen können – rechtlich ist das unabhängig vom Speicherort. Neu ist insoweit allenfalls die Bereitschaft US-amerikanischer Behörden und Dienste, hiervon massiv Gebrauch zu machen (und hierbei bestehende gesetzliche Schranken sehr eng zu sehen bzw. die Befugnisse sehr weit) und die gewonnenen Erkenntnisse dann auch zum Zwecke politischer Differenzierung auch hinsichtlich von Äußerungen zu verwenden, die auch nach dem US-Recht ohne weiteres zulässig wären. Auch diese geänderte Politik der US-Behörden ist aber eine Folge der allgemein geänderten politischen Verhältnisse in den USA, nicht aber des Speicherorts der Daten der Beklagten.

48

3. Zuletzt besteht auch kein Schadensersatzanspruch des Klägers gegen die Beklagte, weil dessen Geltendmachung gegen das Gebot von Treu und Glauben verstößt (§ 242 BGB). Der Kläger verlangt von der Beklagten Schadensersatz für eine Datenübertragung in die USA. Es ist jedoch allgemein bekannt – und war nach Überzeugung des Gerichts auch dem Kläger bekannt – dass die Beklagte einen Dienst zur weltweiten Kommunikation anbietet und Tochter eines US-amerikanischen Unternehmens ist. Schon allein, um die Dienste der Beklagten weltweit anbieten zu können, ist es offensichtlich erforderlich, Daten aus der EU in das Nicht-EU-Ausland zu übertragen. Nach Überzeugung des Gerichts war auch den Nutzern der Dienste der Beklagten für den hier gegenständlichen Zeitraum bewusst, dass ihre Daten auch in die USA übertragen werden. Über die entsprechende Datenübertragung wurde schon vor dem Privacy Shield-Urteil des EuGH öffentlich berichtet. Spätestens aber anlässlich der Schrems II-Entscheidung wurde öffentlich breit über den Transfer von Daten seitens der Beklagten berichtet. Auch die Frage eines Zugriffs US-amerikanischer Behörden auf Daten ist bereits infolge der Snowden-Berichterstattung allgemein bekannt. Dennoch hat der Kläger die Dienste der Beklagten benutzt. Es erscheint mit dem Gebot von Treu und Glauben nicht zu vereinbaren, einerseits in Kenntnis des behaupteten Rechtsverstoßes den Dienst der Beklagten (mit dem bekannten Datenübertrag in die USA) zu nutzen, andererseits aber die Beklagte gerade für das Anbieten des Dienstes auf Schadensersatz in Anspruch nehmen zu wollen.

49

Aus Sicht des Gerichts zeigt die vorliegende Klage, dass es dem Kläger nicht um den Ersatz tatsächlich erlittener Schäden geht, sondern er einen ihn tatsächlich nur eingeschränkt betreffenden Vorgang (die Datenübertragung in die USA) nutzen will, um hierfür eine Geldentschädigung zu erlangen. Fühlte sich der Kläger tatsächlich so schwer beeinträchtigt durch den Datentransfer in die USA, so hätte es sich angeboten, nicht nur F. schon ursprünglich nicht zu nutzen, jedenfalls aber die Nutzung zu stoppen (letzteres gibt der Kläger auch an), sondern ebenso die Nutzung des Dienstes I., der ebenfalls von der Beklagten betrieben wird und bei dem sich mutmaßlich ein ähnliches Problem wie bei F. ergibt. Die Geltendmachung von Schadensersatz ohne tatsächlich erlittene Schäden kann ebensowenig Sinn und Zweck eines Anspruchs aus Art. 82 DSGVO sein wie die massenhafte Geltendmachung von Schadensersatz- und weiteren Ansprüchen durch die Prozessbevollmächtigten des Klägers durch weitgehend aus Textbausteinen bestehende Klagen, um durch diese Klagen und ggf. noch weiter zu führende Rechtsmittelverfahren ein hohes Maß an Gebühren für die Rechtsanwälte zu generieren, wobei es dabei sogar unerheblich ist, wie diese Verfahren im Ergebnis ausgehen.

50

II. Anspruch auf Zinsen aus der Hauptforderung hat der Kläger schon mangels Anspruchs in der Hauptsache nicht.

51

III. Anspruch auf die Erstattung vorgerichtlicher Rechtsanwaltskosten nebst Zinsen hat der Kläger mangels Anspruchs in der Hauptsache nicht.

52

IV. Die Unterlassungsanträge wären, wenn sie zulässig wären, ebenfalls unbegründet.

53

1. Der Unterlassungsanspruch hinsichtlich eines Datenübertrags in die USA besteht nicht, weil die Beklagte zu einem solchen Datenübertrag berechtigt ist (s.o.).

54

2. Der Unterlassungsanspruch bezüglich des Zugänglichmachens besteht ebenfalls nicht. Sollte dieser dahingehend zu verstehen sein, dass es um die in die USA übertragenen Daten geht, so wäre die die Daten übertragende Stelle auf dieser Stufe schon nicht die Beklagte, sondern deren Konzernmutter. Sollte es dem Kläger auch um das Verhältnis der Beklagten zu den europäischen Behörden gehen, besteht ein Unterlassungsanspruch nicht, weil es in der deutschen Rechtsordnung (und mutmaßlich auch in allen anderen EU-Staaten) öffentlich-rechtliche Normen gibt, welche die Beklagte zur Auskunftserteilung unter bestimmten Umständen verpflichten. Entsprechenden berechtigten Ersuchen muss die Beklagte nachkommen, kann also einer entsprechenden Unterlassungsverpflichtung nicht nachkommen.

55

3. Der Unterlassungsanspruch bezüglich der Verarbeitung der Daten ist, wie bereits oben im Rahmen der Zulässigkeit angeführt, vollkommen unklar. Sollte es dem Kläger tatsächlich um die allgemeine Verarbeitung seiner Daten gehen, so besteht kein Unterlassungsanspruch. Es ist gerichtsbekannt, dass die Nutzer der Dienste der Beklagten bei Anmeldung eines Benutzerkontos bestimmte Erklärungen abgeben müssen. Mit der Nutzung der Dienste ist es auch offensichtlich nicht vereinbar, mit einer Verarbeitung der Nutzerdaten durch die Beklagte in keiner Weise einverstanden zu sein.

56

V. Die Auskunftsanträge des Beklagten wären durch die vorgerichtlich erteilte Antwort der Beklagten (Anlage B16) und den Verweis auf das Selbstbedienungstool jedenfalls erfüllt (§ 362 BGB).

C.

57

I. Die Entscheidung über die Kosten erfolgte nach § 91 ZPO. Über die vorläufige Vollstreckbarkeit war nach § 709 ZPO zu entscheiden.

58

II. Hinsichtlich der Streitwertfestsetzung folgt das Gericht den Angaben zur Streitwertbemessung in der Klageschrift von 27.12.2024.