

Titel:

Rechtmäßigkeit der Datenübermittlung in die USA

Normenketten:

ZPO § 253 Abs. 2 Nr. 2, § 256 Abs. 1

DSGVO Art. 6 Abs. 1 lit. b, lit. c, Art. 49 Abs. 1 lit. b, Art. 82 Abs. 1

Leitsätze:

1. Ein Feststellungsantrag, mit dem die Verpflichtung der Beklagten festgestellt werden soll, „alle zukünftigen Schäden zu ersetzen, die der Klägerseite (...) entstanden sind und/oder noch entstehen“, ist unzulässig, weil er weder erkennen lässt, ob bereits eingetretene Schäden Gegenstand des Begehrens sind, noch welche konkreten zukünftigen Schäden in Rede stehen. Damit fehlt es an der nach § 253 Abs. 2 Nr. 2 ZPO gebotenen Bestimmtheit des Streitgegenstands. (Rn. 30) (redaktioneller Leitsatz)
2. Für die Annahme eines Feststellungsinteresses genügt zwar grundsätzlich die bloße Möglichkeit des Eintritts zukünftiger Schäden, doch müssen konkrete tatsächliche Anhaltspunkte für deren Eintritt dargelegt werden. Ein rein abstraktes Risiko oder eine lediglich behauptete Gefahr ohne greifbare Grundlage reicht nicht aus. Insbesondere kann das Feststellungsinteresse nicht auf generalisierte Befürchtungen gestützt werden, die in keinem erkennbaren Zusammenhang mit dem konkret behaupteten Datenschutzverstoß stehen. (Rn. 31 – 34) (redaktioneller Leitsatz)
3. Eine Übermittlung personenbezogener Daten an Plattformbetreiber in den USA ist rechtmäßig, wenn sie zur Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO erforderlich ist. Dies gilt auch dann, wenn theoretisch ein Zugriff US-amerikanischer Behörden möglich ist, da ein solcher Zugriff – vergleichbar mit europäischen Rechtsgrundlagen – eine rechtliche Verpflichtung i.S.v. Art. 6 Abs. 1 lit. c DSGVO darstellt. Nutzer, die sich bewusst für die Teilnahme an einem globalen Netzwerk entscheiden, müssen das mit der internationalen Datenübertragung verbundene Risiko hinnehmen. Auf eine ausschließliche Speicherung und Verarbeitung innerhalb der EU besteht kein Anspruch. (Rn. 39 – 42) (redaktioneller Leitsatz)
4. Der Kläger hat darzulegen und zu beweisen, dass er infolge eines DSGVO-Verstoßes tatsächlich einen immateriellen Schaden erlitten hat oder zumindest eine begründete Befürchtung eines Missbrauchs seiner Daten besteht. Ein bloß hypothetisches Risiko oder eine abstrakte Furcht vor Missbrauch genügt nicht. Der bloße Hinweis auf ein „hohes Missbrauchspotenzial“ oder allgemein gehaltene Sorgen ersetzt nicht den erforderlichen Tatsachenvortrag. Werden zudem die angeblich angstbegründenden Dienste weiter aktiv genutzt, spricht dies entscheidend gegen die Plausibilität einer ernsthaften und begründeten Beeinträchtigung. (Rn. 45 – 51) (redaktioneller Leitsatz)

Schlagworte:

Unzulässigkeit der Klage, Beweislast, Datenschutzverstöße, Immaterieller Schaden, Unterlassungsanspruch, Auskunftsanspruch, Feststellungsinteresse

Fundstelle:

GRUR-RS 2025, 25350

Tenor

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

Beschluss

Der Streitwert wird auf 6.800,00 Euro festgesetzt.

Tatbestand

1

Die Klagepartei nimmt die Beklagte auf Schadensersatz, Unterlassung, Auskunft, Feststellung und Zahlung vorgerichtlicher Rechtsanwaltskosten aus Persönlichkeitsrechtsverletzungen und 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., 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. und I. handelt es sich um globale Online-Dienste für Kommunikation und das Teilen von Inhalten, die es den Nutzern ermöglichen sollen, mit anderen Nutzern auf der ganzen Welt auf vielfältige Weise in Kontakt zu treten und Inhalte auf verschiedene Arten zu teilen. Der Kläger unterhält auf F. und I. jeweils ein Nutzerprofil mit der E-Mail-Adresse . Er nutzt die angebotene Messenger-Dienste von F. und I. und kommuniziert über diese ausschließlich im privaten Kontext. Die Beklagte überträgt routinemäßig verschiedene Arten von Daten in die USA, dazu gehören EU-Benutzerdaten, die nicht ohnehin öffentlich einsehbar sind. Am 16.07.2020 erklärte der EuGH das P. für ungültig. Die zuständige irische Datenschutzkommission hat gegen die Beklagte eine Geldbuße von 1,2 Milliarden Euro verhängt, begründet mit einem Verstoß gegen die DSGVO. Die Beklagte hat gegen die Entscheidung Rechtsmittel eingelegt. Am 11.07.2023 ist mit dem EU-U.S. D. Framework ein neues Datenschutzabkommen zwischen der Europäischen Union (EU) und den USA in Kraft getreten.

3

Die Prozessbevollmächtigten des Klägers stellten ein außergerichtliches Auskunftersuchen an die Beklagte, das die Beklagte mit Schreiben vom 09.08.2024 beantwortete. Hierbei wurden der Klagepartei detaillierte Informationen erteilt, insbesondere wurden ihr erklärt, wie sie auf ihre F. und I.-Daten zugreifen kann. Die Beklagte hat die Klagepartei auf die maßgeblichen Abschnitte der Datenschutzrichtlinie und das verfügbare Selbstbedienungs-Tool hingewiesen, das es Nutzern ermöglicht, ihre F. bzw. I.-Daten aufzurufen und zu verwalten.

4

Die Klagepartei 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. P., das Überwachungsprogramm der ..., ermögliche der ... den Zugriff auf die Server großer Internetunternehmen, darunter auch die Beklagte. Über P. könne die ... auf Benutzerdaten zugreifen, einschließlich E-Mails, Chat-Nachrichten, Video-Chats, Fotos, Dokumente und andere Inhalte. U. sei ein weiteres Überwachungsprogramm der ..., das darauf abziele, den Internetverkehr in großem Maßstab zu überwachen. Durch U. könne die ... 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. Ziel der Überwachung sei allein Information, also keine bestimmte Person oder Einrichtung. Es bestehe ein erhebliches Risiko der Verletzung der Privatsphäre der Nutzer des sozialen Netzwerks F., da die Daten viele Informationen über deren Privatleben enthalten. Betroffene Personen seien daher auch Personen, auf deren Konten Zugriffsanträge hätten gestellt werden können. Die Zuwiderhandlung habe vorsätzlichen Charakter, da die Beklagten gegen die DSGVO verstoßen habe, obwohl sie seit dem Urteil in der Rechtssache Schrems II gewusst habe, dass die internationalen Übermittlungen der Beklagten einen Verstoß gegen die DSGVO auslösen würden. Das Datenleck sei seitens der irischen Datenschutzkommission bestätigt. Die Veröffentlichung der Daten habe weitreichende Folgen für die Klagepartei, die sich unter den betroffenen Personen befunden habe. Die Klagepartei habe einen erheblichen Kontrollverlust über ihre Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffender Daten verblieben. Die Beklagte habe den Kläger zu keinem Zeitpunkt darüber informiert, dass seine Informationen durch Dritte – ausländische Strafverfolgungsbehörden und Nachrichtendienste – eingesehen und in die USA übermittelt worden seien. Die Beklagte habe fehlerhafte Auskunft über die Empfänger der Daten erteilt. Sie habe auch nicht solche Vorkehrungen getroffen, durch die die personenbezogenen Daten für alle Personen unzugänglich gemacht wurden, die nicht zum Zugang zu den personenbezogenen Daten berechtigt gewesen seien, etwa durch Verschlüsselung. Die Beklagte habe gegen Art. 6 DSGVO verstoßen, indem sie unrechtmäßig personenbezogene Daten der Klagepartei verarbeitet habe. 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, so dass die Einwilligung nicht freiwillig erteilt worden sei.

5

Der Kläger müsse seit dem Vorfall mit der permanenten Angst leben, dass plötzlich Ermittlungen ausländischer Strafverfolgungsbehörden und Nachrichtendienste angestrengt werden könnten. Er müsse befürchten, aufgrund von sozialen Kontakten, religiösen Anschauungen, politischen Anschauungen, des Reiseverhaltens, der Postings, der Inhalte der Chat-Verläufe behördlich verfolgt zu werden bzw. jedenfalls beobachtet zu werden. Er habe insbesondere Angst, seinen Job zu verlieren, wenn er nicht mehr in die USA reisen könne oder an der Grenze der USA unverschuldet inhaftiert zu werden. Die Klagepartei behauptet weitreichende Folgen, insbesondere Gesundheitsbeeinträchtigungen, Beeinträchtigung der familiären und sozialen Beziehungen, der Arbeits- und Leistungsfähigkeit sowie der Finanzen, verschiedene Ängste, wie die Angst den Job zu verlieren, die Angst vor politischen Repressalien in den USA, die Angst, dass die persönlichen, intimen Chats von Dritten gelesen werden oder die privaten Bilder von Dritten gelesen werden sowie Symptome in Form von weichen Knien, Bauchbeschwerden, Schwindel und einem Gefühl der Unsicherheit. Hinsichtlich der Einzelheiten wird auf die Anlage K1 Bezug genommen.

6

Die Klagepartei behauptet weiter, es sei nicht ausgeschlossen, dass sie künftig infolge der Verstöße gegen die DSGVO auch materielle Schäden erleide. Unter Berücksichtigung des Umstandes, dass die im Wege des „Scrapings“ erlangten personenbezogenen Daten im Internet veröffentlicht worden seien, erscheine es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger aufgrund der Veröffentlichung der Telefonnummer und weiterer persönlicher Daten wie der Name des Klägers im Internet zu künftigen materiellen Schäden, etwa durch betrügerische Anrufe, komme. Die Daten des Klägers seien im Darknet noch abzurufen. Das Missbrauchspotenzial der streitgegenständlichen Daten sei extrem hoch. Die Datenweitergabe in die USA und an Dritte berühre sensible Daten der Klagepartei. Insofern sei es naheliegend, dass unbefugte Dritte mit den betroffenen Daten einen Vermögensschaden herbeiführen werden und können. Dieser könne sich nämlich denkllogisch jeden Tag wiederholen. Es könne nicht abgesehen werden, welche ausländischen Strafverfolgungsbehörden und Nachrichtendienste Zugriff auf die Daten der Klagepartei erhalten hätten und für welche konkreten Zwecke die Daten genutzt werden.

7

Als Marktführer im Bereich Soziale Medien mit hohen Gewinnen aus Werbung sei es der Beklagten ohne Weiteres möglich, die Daten der EU-Bürger in den EU vorzuhalten und zu separieren, ohne Datenverschickung in die USA. Eine Notwendigkeit der Datenübermittlung der EU-Bürger in die USA zur Erfüllung eines Vertrages bestehe nicht. Nicht jeder EU-Bürger habe Freunde in den USA oder Familie dort, viele EU-Bürger hätten ggf. keine über die EU hinausgehenden Interessen und möchten ggf. sich nicht mit NICHT-EU-Bürgern austauschen.

8

Die Klagepartei ist der Ansicht, die Datenübermittlung der Beklagten in die USA sei seit 16.07.2020 illegal. Die Klagepartei habe nach Art. 82 Abs. 1 DSGVO gegen die Beklagte einen Anspruch auf Schadensersatz in Höhe von 5.000 Euro nebst Zinsen gemäß §§ 288 Abs. 1, 291 BGB. Alleine der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchte, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, könne einen immateriellen Schaden darstellen. Das Verhalten der Beklagten begründe mehrere Verstöße gegen die DSGVO. Die Beklagte sei weder ihrer Informationspflicht nach Art. 34 noch nach Art. 33 DSGVO nachgekommen. Die Ersatzpflicht für die verspätete Auskunft sei mit 500 Euro bis 1.000 Euro pro Monat zu taxieren. Ein immaterieller Schadensersatzanspruch von 5.000 Euro sei vorliegend angemessen, da sowohl Datenschutzverstoß als auch mangelhafte Erfüllung des Auskunftsbegehrens kumulativ zusammen wirken. Die Beklagte sei verpflichtet, der Klagepartei alle zukünftigen Schäden zu ersetzen, die der Klagepartei durch den illegalen Zugriff der ausländischen Strafverfolgungsbehörden und Nachrichtendienste auf die persönlichen Daten entstanden sind oder noch entstehen werden. Die Klagepartei habe die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt. Das Zugänglichmachen der personenbezogenen Daten der Klagepartei an ausländische Strafverfolgungsbehörden und Nachrichtendienste sei eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO. Die Beklagte habe der Klagepartei nicht ausreichend nach Art. 13, 14 DSGVO über die (weitere) Nutzung der mitgeteilten Mobilfunknummer informiert, wodurch sie rechtswidrig

gegen Art. 13, 14 DSGVO verstoßen habe. Die Klagepartei sei in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt.

9

Die Klagepartei beantragt,

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 5000 €, nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

10

Die Beklagte wird verurteilt, es zu unterlassen,

- personenbezogene Daten der Klagepartei, namentlich die personenbezogenen Daten, die von oder über Personen generiert, geteilt und hochgeladen werden, die die Produkte und Dienste des Datenexporteurs (einschließlich F. und I.) 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 von verbundenen Unternehmen von F. und Unternehmen der F.-Familie, in die USA zu verschicken und diese Dritten, insbesondere Ermittlungsbehörden in den USA, zugänglich zu machen,

- personenbezogene Daten des Unterlassungsgläubigers, namentlich die personenbezogenen Daten, die von oder über Personen generiert, geteilt und hochgeladen werden, die die Produkte und Dienste des Datenexporteurs (einschließlich F. und I.) 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 von verbundenen von F. und Unternehmen der F.-Familie, ohne eine Einwilligung der Klagepartei zu verarbeiten.

11

Die Beklagte wird verurteilt, der Klagepartei Auskunft über die Klagepartei betreffenden personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen,

namentlich die personenbezogenen Daten, die von oder über Personen generiert, geteilt und hochgeladen werden, die die Produkte und Dienste des Datenexporteurs (einschließlich F. und I.) 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 von verbundenen Unternehmen von F. und Unternehmen der F.-Familie.

12

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.

13

Die Beklagte wird verurteilt, an die Klagepartei einen Betrag in Höhe von 1134.55 € (Rechtsanwaltskosten außergerichtlich) zu zahlen, nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz für die außergerichtliche anwaltliche Rechtsverfolgung.

14

Die Beklagte beantragt,

die Klage abzuweisen.

15

Die Beklagte behauptet, die Klage bestehe lediglich aus einer losen Aneinanderreihung von Zitaten, die Aussagen verschiedener Gerichte und Aufsichtsbehörden zusammenfassen, welche angeblich die Argumentation der Klagepartei stützen. Die Beklagte habe die Anforderungen an grenzüberschreitende Datenübermittlungen im Kapitel V der DSGVO zu jeder Zeit erfüllt. Die Beklagte habe die Datenübermittlung auf SCCs (EU Standard Contractual Clauses, standardisierte, von der Europäischen Kommission veröffentlichte Musterklauseln), gestützt (2010/87/EU vom 5. Februar 2010 seit Inkrafttreten der DSGVO bis 31.08.2021 und seither und (EU) 2021/914 vom 4. Juni 2021) und zusätzliche Maßnahmen umgesetzt, um personenbezogene Daten von EU-Nutzern ihres F.- und I.-Dienstes an die Beklagte in den USA zu übermitteln, beispielsweise werden branchenübliche Verschlüsselungsalgorithmen und -protokolle eingesetzt, um die Daten während der Übermittlung vor Zugriffen Dritter zu schützen (einschließlich U.). Staatliche Informationsanfragen würden durch die Konzernmutter systematisch geprüft, so dass sichergestellt werde, dass nur dann gegenüber Behörden auf solche Anfragen Auskunft erteilt werde, wenn die entsprechenden Anfragen rechtmäßig seien. Die Datenübermittlungen seien für die Erfüllung der Verträge mit den EU-Nutzern erforderlich gewesen. F. und I. sowie die technische Infrastruktur, auf die sie zurückgreifen, seien auf den freien Fluss personenbezogener Daten zwischen der EU und den USA zwangsläufig angewiesen. Die Datenübermittlungen seien erforderlich, damit die Beklagte ihre F.- und I.-Dienste bereitstellen und ihre vertraglichen Verpflichtungen gemäß den jeweiligen Nutzungsbedingungen erfüllen könne.

16

Die Beklagte veröffentliche detaillierte Informationen in Bezug auf die Übermittlung von EU-Nutzerdaten in die USA, beispielsweise in der Datenschutzrichtlinie der Beklagten, sie stelle Kopien der angewandten SCCs zur Verfügung, die sich online abrufen lassen und veröffentliche Informationen zu behördlichen Datenabfragen in halbjährlichen Transparenzberichten, die online verfügbar seien. Am 19.11.2020 habe die Beklagte ein Update veröffentlicht, auf dem die von der Beklagten angewandten Schutzmaßnahmen bei der Bearbeitung von Informationsanfragen durch Regierungen erläutert worden seien. Am 11.03.2021 habe die Beklagte einen Blogbeitrag veröffentlicht, der unter anderem die von der Beklagten angewandten Schutzmaßnahmen zur Sicherung der Datenübermittlung erläutere.

17

Das Risiko einer unrechtmäßigen Offenlegung von Daten bestehe nicht. Die Klagepartei habe keine spezifischen Tatsachen vorgetragen, die belegen oder darauf hindeuten, dass gerade ihre Daten Gegenstand einer gezielten Anfrage nach Section 702 FISA gewesen sein könnten. Die angeblichen „Ängste“ der Klagepartei seien völlig unbegründet.

18

Die Beklagte ist der Ansicht, die Anträge auf Zahlung immateriellen Schadensersatzes, Unterlassung, Auskunft und Feststellung seien unzulässig. Der Antrag auf Zahlung immateriellen Schadensersatzes sei unzulässig, da ein einziger Zahlungsanspruch auf eine Vielzahl angeblicher Verstöße gegen die DSGVO gestützt werde, ohne dass die Klagepartei darlege, in welchem Verhältnis die Schadensarten zu dem geltend gemachten Zahlungsanspruch stehen. Die beiden Unterlassungsanträge seien bereits mangels Bestimmtheit unzulässig, jedenfalls scheide eine Wiederholungsgefahr aus, nachdem ein neuer Angemessenheitsbeschluss durch die Europäische Kommission erlassen worden sei und die Klagepartei könne ihr Ziel durch die Löschung ihrer F. und I.-Konten einfach erreichen. Der Auskunftsantrag sei unzulässig, da der Klagepartei ein Selbstbedienungstool zur Verfügung steht, mit dem sie genau die von ihr

gewünschten Informationen erhalten könne. Der Feststellungsantrag sei unzulässig, da kein Feststellungsinteresse bestehe und der Antrag widersprüchlich und unbestimmt sei. Die hinreichende Wahrscheinlichkeit eines Schadenseintritts sei nicht substantiiert dargelegt.

19

Die Beklagte ist weiter der Ansicht, die Datenübermittlungen der Beklagten aus der EU in die USA seien nicht rechtswidrig. Der EuGH habe im Urteil vom 16.07.2020 (C-311/18) lediglich festgestellt, dass Unternehmen in der EU die Übermittlung personenbezogener Daten in die USA nicht ausschließlich auf den sogenannten Angemessenheitsbeschluss der Europäischen Kommission aus dem Jahr 2016 stützen könne ("P.-Beschluss"). Unternehmen dürften nach wie vor personenbezogene Daten in die USA übermitteln, sofern sie geeignete Garantien anwenden und/oder die in Art. 49 DSGVO vorgesehenen Ausnahmeregeln greifen. Die Datenübertragungen wären jedenfalls aufgrund der Ausnahmeregelung in Art. 49 Abs. 1 lit. b DSGVO gerechtfertigt gewesen. Der Beschluss der irischen Datenschutzbehörde vom 12.05.2023 sei für deutsche Gerichte nicht bindend. Der Beklagten sei es untersagt, Informationen über Anfragen nach Section 702 des US F. Act von 1987 gegenüber Dritten offenzulegen, sie sei gemäß § 29 Abs. 1 S. 2 BDSG und Art. 15 Abs. 4 DSGVO von der Pflicht zur Erteilung solcher Informationen entbunden. Ein Verstoß gegen die DSGVO liege nicht vor. Der Anspruch auf Auskunft sei umfassend erfüllt, ein weitergehender Anspruch bestehe nicht. Die Verstöße seien allesamt nicht substantiiert behauptet. Die Klagepartei habe nicht dargelegt oder nachgewiesen, dass sie einen nach Art. 82 Abs. 1 DSGVO ersatzfähigen Schaden erlitten habe und dass der behauptete Schaden gerade auf den vermeintlichen DSGVO-Verstoß zurückzuführen sei.

20

Die Beklagte erhebt die Einrede der Verjährung.

21

Zur Ergänzung des Sach- und Streitstandes wird auf die wechselseitigen Schriftsätze der Parteien nebst Anlagen, das Protokoll der mündlichen Verhandlung vom 29.01.2025 sowie den übrigen Akteninhalt Bezug genommen.

Entscheidungsgründe

22

Die Klage ist hinsichtlich des Antrags auf Unterlassung, Auskunft und Feststellung bereits unzulässig und jedenfalls insgesamt unbegründet.

I. Zulässigkeit

23

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

1. Zuständigkeit

24

Das Landgericht Hof ist sachlich und nach §§ 1 ZPO, 71 Abs. 1, 23 GVG, international nach Art. 79 Abs. 2 S. 2, 82 Abs. 6 DSGVO und örtlich nach § 44 Abs. 1 s. 2 BDSG zuständig.

2. Zulässigkeit des Antrags auf Schadensersatz

25

Entgegen der Auffassung der Beklagten ist der Antrag auf Zahlung immateriellen Schadensersatzanspruchs – 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 eine unzureichende Auskunft und für den Missbrauch der Daten ist weder erforderlich, noch wäre dies sachdienlich. Vielmehr handelt es sich um einen einheitlichen Streitgegenstand (vgl. hierzu BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24).

3. Unzulässigkeit des Unterlassungsanspruchs

26

Der Klageantrag ist, soweit Unterlassung begehrt wird, unzulässig. Die Beklagte weist zutreffend darauf hin, dass der Antrag zu unbestimmt formuliert ist. Zwar werden die „personenbezogenen Daten“ entgegen der Auffassung der Beklagten detailliert bezeichnet, jedoch ist die Verletzungshandlung, die die Klagepartei untersagt haben möchte, 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 (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24 m.w.N.). Soweit die Klagepartei in beiden Alternativen des Unterlassungsantrags beantragt, die Beklagte solle es Unterlassen, „...und Informationen von Drittpartnern; und Informationen von verbundenen Unternehmen von F. und Unternehmen der F.-Familie“ in die USA zu verschicken, so ist nicht klar, wer Drittpartner sein sollen, bei welchen Unternehmen es sich um verbundene Unternehmen oder Unternehmen der F.-Familie handeln soll und ebenso wenig, welche „Informationen“ hiervon umfasst sein sollen. Auch die Heranziehung des Vortrags der Klagepartei im Übrigen führt nicht dazu, dass klar wird, was genau hierunter zu verstehen ist.

27

Soweit die Klagepartei darüber hinaus in der ersten Alternative weiter beantragt, der Kläger solle es unterlassen die Informationen „...Dritten, insbesondere Ermittlungsbehörden in den USA, zugänglich zu machen,“ ist eben sowenig hinreichend klar, auch nicht unter Berücksichtigung des Klagevortrags, wer außer den beispielhaft aufgeführten Ermittlungsbehörden in den USA sonst noch „Dritter“ i.S.d. Antrags sein soll.

28

Soweit die Klagepartei in der zweiten Alternative des Unterlassungsantrags beantragt, die Beklagte solle es unterlassen „personenbezogene Daten des Unterlassungsgläubigers“ zu verarbeiten, verwundert die Terminologie zwar, dies macht den Antrag jedoch nicht unzulässig, da eine Auslegung ergeben wird, dass es sich bei dem Unterlassungsgläubiger nur um die Klagepartei handeln kann.

4. Unzulässigkeit des Antrags auf Auskunft

29

Die Beklagten weist zutreffend darauf hin, dass auch der Antrag auf Auskunft mangels Rechtsschutzbedürfnis unzulässig ist. 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 BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24). Auch wenn hierfür strenge Maßstäbe gelten, ist zu berücksichtigen, dass die Klagepartei ihr Ziel einfacher, schneller und billiger erreichen könnte, ohne Klage zu erheben, indem sie das zur Verfügung stehende Selbstbedienungstool nutzt, auf das die Beklagte sie bereits unstreitig außergerichtlich mit Schreiben vom 09.08.2024 (Anlage B14).

5. Unzulässigkeit des Feststellungsantrags

30

Der Klageantrag ist, soweit Feststellung begehrt wird, unzulässig. 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“ (Hervorhebung durch das Gericht). Auf die Widersprüchlichkeit wies die Beklagte bereits in der Klageerwiderung (Seite 45, Bl. 103 d. Akte) hin. Auch die Wiederholung des Antrags im Schriftsatz vom 18.11.2024 (dort S. 76, Bl. 183 d. Akte) führt – sicher wenig überraschend – nicht dazu, dass der Antrag zulässig wäre. In der Klagebegründung und im Schriftsatz vom 18.11.2024 ist lediglich von zukünftigen Schäden die Rede. Indes wird nicht dargelegt, dass Schäden bereits entstanden und gegebenenfalls noch nicht bekannt sein könnten.

31

Darüber hinaus ist auch kein Feststellungsinteresse dargelegt. Grundsätzlich genügt für ein Feststellungsinteresse die bloße Möglichkeit des künftigen Eintritts der geltend gemachten Schäden, eine darüberhinausgehende hinreichende Schadenswahrscheinlichkeit ist nicht erforderlich (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24).

32

Die Klagepartei führt hierzu zunächst lediglich pauschal aus, es sei nicht ausgeschlossen, dass sie künftig infolge der Verstöße gegen die DSGVO auch materielle Schäden erleide. Anhaltspunkte für diese Behauptung werden in der Folge jedoch nicht genannt. Der Klagepartei ist der Nachweis nicht gelungen, dass durch die Datenübermittlung in die USA ein materieller oder immaterieller Schaden entstanden ist (siehe dazu unten II. 1.b). Warum nunmehr Jahre später noch die Möglichkeit eines Eintritts eines materiellen oder immateriellen Schadens bestehen soll, ist nicht ersichtlich und erst recht nicht dargelegt.

33

Die Klagepartei führt weiter aus, dass unter Berücksichtigung des Umstandes, dass die im Wege des „Scrapings“ erlangten personenbezogenen Daten im Internet veröffentlicht worden seien, erscheine es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger aufgrund der Veröffentlichung der Telefonnummer und weiterer persönlicher Daten wie der Name des Klägers im Internet zu künftigen materiellen Schäden, etwa durch betrügerische Anrufe, komme. Die Daten des Klägers seien im D. noch abzurufen. Dieser Sachvortrag ist in Anbetracht der Angabe des Klägers, dass Gegenstand der Ansprüche nicht das bekannte Datenleck bei der Beklagten infolge von Scraping aus dem Jahr 2019, sondern die illegale Datenübermittlung seitens der Beklagten in die USA seit 16.07.2020 ist (Klageschrift Seite 5), schlicht falsch.

34

Die Klagepartei behauptet sodann pauschal, das Missbrauchspotenzial der streitgegenständlichen Daten sei extrem hoch. Die Datenweitergabe in die USA und an Dritte berühre sensible Daten der Klagepartei. Insofern sei es naheliegend, dass unbefugte Dritte mit den betroffenen Daten einen Vermögensschaden herbeiführen werden und können. Dieser könne sich nämlich denkllogisch jeden Tag wiederholen. Es könne nicht abgesehen werden, welche ausländischen Strafverfolgungsbehörden und Nachrichtendienste Zugriff auf die Daten der Klagepartei erhalten hätten und für welche konkreten Zwecke die Daten genutzt werden. Inwiefern Geheimdienste oder Ermittlungsbehörden – selbst wenn man einen Zugriff unterstellt – einen (materiellen oder immateriellen) Vermögensschaden herbeiführen könnten, erschließt sich dem Gericht nicht und wird auch nicht dargelegt. Im Schriftsatz vom 18.11.2024 wird sodann behauptet, es bestehe ein (allgemeines?) Risiko, aufgrund der Aktivitäten bei F. und I. staatlichen Repressalien ausgesetzt zu sein und als Beispiel Dr. R. A. aufgeführt. Dieses Beispiel lässt jeglichen Bezug zum konkreten Fall vermissen. Die Möglichkeit eines (allgemeinen) Risikos staatlicher Repressalien für den Kläger (dieser will ja die Feststellung...) wird weder dargelegt, noch ist diese ersichtlich.

35

Der vorliegende Fall unterscheidet sich insoweit maßgeblich von den Fällen der Veröffentlichung von Daten infolge Scraping aus dem Jahr 2019, bei dem die Veröffentlichung der personenbezogenen Daten fort dauert und das Risiko einer missbräuchlichen, insbesondere betrügerischen Nutzung der Daten mit der Folge eines materiellen oder immateriellen Schadens tatsächlich fortbesteht. Im vorliegenden Fall ist festzustellen, dass die Datenübermittlung aktuell (und bereits lange vor Klageerhebung) unstreitig aufgrund des Angemessenheitsbeschlusses der Kommission vom 10.07.2023 erfolgt. Dieser stellt eine taugliche Grundlage für die Datenübermittlung dar, Art. 45 Abs. 3 DSGVO. Weder ist für das Gericht ersichtlich, noch wurde dies von der Klagepartei dargelegt, dass eine unbefugte Datenweitergabe in die USA überhaupt noch erfolgt (selbst der Kläger gab im Rahmen seiner informatorischen Anhörung an, dass er davon ausgeht, dass die Datenschutzgrundsätze nun eingehalten werden) oder dass zumindest die Möglichkeit besteht, dass aus der (behaupteten) unzulässigen Datenübermittlung aktuell noch Schäden entstehen können.

II. Begründetheit

36

Die Klage war insgesamt als jedenfalls unbegründet abzuweisen. Der Klagepartei steht keiner der geltend gemachten Ansprüche gegen die Beklagte im Zusammenhang mit den behaupteten Vorwürfen im Zusammenhang mit der Datenübermittlung in die USA zu.

1. Kein Schadensersatzanspruch

37

Die Klagepartei macht Schadensersatz nach Art. 82 DSGVO geltend und behauptet, insbesondere die Beklagte habe die Anforderungen in Kapitel V der DSGVO nicht erfüllt. Sodann wird die Verletzung weiterer

„Schutzgesetze“ behauptet (Schriftsatz vom 18.11.2024 S. 29, Bl. 136 d. Akte), im weiteren Verlauf wird deutlich, dass auch ein Schadensersatzanspruch nach § 823 Abs. 2 BGB geltend gemacht werden soll. Die Klagepartei ist es weder gelungen, eine rechtswidrige Datenübermittlung darzulegen und zu beweisen, noch den Eintritt eines (immateriellen) Schadens, so dass kein Schadensersatzanspruch – egal auf welcher Rechtsgrundlage – in Betracht kommt.

38

Lediglich ergänzend sei festgestellt, dass die streitgegenständlichen Forderungen nicht verjährt sind. Die Beklagte erhebt die Einrede der Verjährung und ist für den Verjährungsbeginn darlegungs- und beweisbelastet. Der Kläger gab im Rahmen seiner informatorischen Anhörung an, er habe ca. 2021 zum ersten Mal erfahren, dass eine Datenübermittlung in die USA vorliegt. Die Klage wurde im Mai 2024 erhoben. Für eine frühere Kenntnis und damit einen früheren Verjährungsbeginn ist keinerlei Sachvortrag durch die Beklagte erfolgt, so dass diese insoweit ihrer Darlegungs- und Beweislast nicht nachgekommen ist.

a) Datenschutzverstoß

39

Ein Datenschutzverstoß liegt nicht vor, da die Übermittlung in die USA jedenfalls nach Art. 6 Abs. 1 lit. c, Art. 49 Abs. 1 lit. b DSGVO zulässig war.

40

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 Gegenbeweis bedarf es hierfür nicht. Dass 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 I.-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. 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. dergestalt 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).

41

Die Datenübermittlung ist daher grundsätzlich zur Vertragserfüllung erforderlich, Art. 6 Abs. 1 lit. b DSGVO, und damit rechtmäßig. Darauf, ob die Übermittlung auf geeignete Garantien oder eine wirksame Einwilligung gestützt wurde, kommt es daher vorliegend nicht an. Anzumerken ist insoweit lediglich, dass soweit die Klagepartei behauptet, das OLG Köln habe Verstöße seitens „M.“ (ist hiermit die Beklagte gemeint oder ihre Konzernmutter?) bei der Effektivität der zusätzlichen Schutzmaßnahmen festgestellt, dies nicht zutrifft, da das OLG Köln bekanntermaßen ein Verfahren gegen „G.“ zu entscheiden hatte.

42

Auch die potentielle Weitergabe von Daten an US-Geheimdienste oder Ermittlungsbehörden, unter anderem an die ..., begründet keinen Verstoß gegen die DSGVO. Soweit US-Regierungsbehörden einschließlich der Geheimdienste von der Konzernmutter der Beklagten nach US-amerikanischem Recht Auskünfte verlangen können, ist dies Folge der rechtmäßigen Datenübermittlung in den Herrschaftsbereich der Vereinigten Staaten von Amerika. Diese Möglichkeit steht der Gewährleistung eines im Wesentlichen gleichen Schutzniveaus nicht entgegen, da sie auch unter europäischem Datenschutzregime nach Art. 6

Abs. 1 lit. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) zulässig wäre (so 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).

43

2) Die Voraussetzungen für die Datenübermittlung in Drittländer nach Kapitel V DSGVO werden von der Beklagten eingehalten. Dies folgt bereits daraus, dass – wie vorstehend dargelegt – die Übermittlung zur Vertragserfüllung erforderlich ist, so dass eine Zulässigkeit jedenfalls nach Art. 49 Abs. 1 S. 1 lit. b) DSGVO gegeben ist. Soweit Datenschutzbehörden abweichende Auffassungen vertreten, sind diese für das Gericht jedenfalls nicht bindend.

44

3) Soweit die Klagepartei ihren Anspruch zusätzlich auf einen Verstoß gegen Benachrichtigungs- und Meldepflichten stützt, fehlt es jedenfalls an der Ursächlichkeit für den geltend gemachten Schaden (so zutreffend BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24). Dies wird bereits daraus deutlich, dass der Kläger selbst als er ca. 2021 von dem angeblichen Verstoß erfuhr, sein Verhalten nicht geändert hat. Darüber hinaus ist der Klagevortrag unstreitig geblieben, dass bereits im März 2018 The G. und The N. enthüllten, dass Cambridge Analytica F.-Daten ohne ausreichende Einwilligung der Nutzer genutzt hatte, was zu globaler Empörung führte und dazu, dass in den USA im Juli 2019 eine Rekordstrafe von 5 Milliarden US-Dollar gegen F. wegen Verstößen gegen den Datenschutz verhängt wurden. Auch dies hat den Kläger offenbar nicht davon abgehalten, F. (und I.) zu nutzen.

b) Schaden

45

Für einen Schadensersatzanspruch, insbesondere aus Art. 82 DSGVO, fehlt es zudem an einem kausalen Schaden der Klagepartei. Aus diesem Grund kommt ein Schadensersatzanspruch – gleich auf welcher Rechtsgrundlage, insbesondere auch nach § 823 Abs. 2 BGB, vorliegend nicht in Betracht. Für einen Schadensersatzanspruch (aus Art. 82 DSGVO) müsste die Klagepartei das Vorliegen eines (materiellen oder immateriellen) Schadens sowie einen Kausalzusammenhang zwischen dem Schaden und dem behaupteten Verstoß (gegen die DSGVO) darlegen und beweisen. Die Klagepartei behauptet ausschließlich immaterielle Schäden. Der Sachvortrag wurde von der Beklagten bestritten die insbesondere ausführt, dass der Vortrag der Klagepartei wortgleich von den Prozessbevollmächtigten der Klagepartei in zahlreichen nahezu identischen Verfahren ist, die Behauptung der Klagepartei, sie leide unter einer Reihe von Ängsten sei lebensfremd und die angeblichen Ängste der Klagepartei seien völlig unbegründet.

46

Der Begriff des Schadens nach Art. 82 DSGVO ist nach dem Erwägungsgrund 146 S. 3 DSGVO weit auszulegen. Ein bestimmter Schweregrad oder eine gewisse Erheblichkeit ist nicht erforderlich. Jedoch ist der Kläger verpflichtet, nachzuweisen, dass er tatsächlich einen materiellen oder immateriellen Schaden erlitten hat (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24 unter Verweis auf die st. Rspr des EuGH). Der BGH hat hierzu entschieden, dass schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Begriff des immateriellen Schadens den Nachweis zusätzlicher spürbarer negativer Folgen erfordert, wobei die Klagepartei den Nachweis erbringen muss, dass sie einen solchen – das heißt in einem bloßen Kontrollverlust als solchem bestehenden – Schaden erlitten hat, wobei die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, ausreicht, um einen Schadensersatzanspruch zu begründen (BGH a.a.O.).

47

Die Klagepartei müsste vorliegend darlegen und beweisen, dass zumindest eine begründete Befürchtung besteht und negative Folgen gegeben sind. Die bloße Behauptung einer Befürchtung ohne nachgewiesene negativen Folgen genügt ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (BGH a.a.O.). Der vorliegende Fall unterscheidet sich auch insoweit von den Fällen, in denen Daten mittels „Scraping“ abgegriffen und veröffentlicht wurden, so dass der Kontrollverlust feststeht. Dass hinsichtlich der Daten des Klägers, die in die USA übermittelt wurden, mehr als ein hypothetisches Risiko besteht, dass Geheimdienste oder Ermittlungsbehörden in den USA diese einsehen, wurde von der Klagepartei bereits nicht dargelegt. Offen bleiben kann in diesem

Zusammenhang, ob es sich hierbei überhaupt um eine „missbräuchliche Verwendung durch einen unbefugten Dritten“ handeln würde.

48

Ein darüber hinausgehender Schaden steht zur Überzeugung des Gerichts ebenfalls nicht fest.

49

Die Klagepartei behauptet weitreichende Folgen, insbesondere Gesundheitsbeeinträchtigungen, Beeinträchtigung der familiären und sozialen Beziehungen, der Arbeits- und Leistungsfähigkeit sowie der Finanzen, verschiedene Ängste, wie die Angst den Job zu verlieren, die Angst vor politischen Repressalien in den USA, die Angst, dass die persönlichen, intimen Chats von Dritten gelesen werden oder die privaten Bilder von Dritten gelesen werden sowie Symptome in Form von weichen Knien, Bauchbeschwerden, Schwindel und einem Gefühl der Unsicherheit. Die Ausführungen zur persönlichen Betroffenheit des Klägers (Klageschrift S. 24 ff., Bl. 24 ff. d. Akte und Schriftsatz vom 18.11.2024 S. 58 ff., Bl. 165 ff. d. Akte) hat der Klägervorteiler beim Kläger – nach dessen Angaben in der mündlichen Verhandlung – zunächst in Form eines Fragebogens abgefragt. Der Kläger wurde in der mündlichen Verhandlung vom 29.01.2025 ausführlich angehört. Er bestätigte zwar teilweise die Angaben, die sich aus den Schriftsätzen sowie der Anlage K1 ergeben und gab an, dass beruflich eine Reise in die USA anstünde und er Sorge habe, dass er an der Grenze festgehalten werde oder nicht einreisen dürfe und dass dies berufliche Konsequenzen habe. Die schriftsätzlich behaupteten weiteren Ängste sowie die behaupteten Symptome hat der Kläger indes auf die offene Frage des Gerichts zu den Folgen für den Kläger nicht angegeben. Die Angst des Klägers, nicht in die USA einreisen zu dürfen, oder an der Grenze festgehalten zu werden, ist für das Gericht nicht nachvollziehbar. Es fehlt jeglicher Sachvortrag und die Phantasie des Gerichts dafür, weshalb die übermittelten Daten des Klägers derartige Folgen hervorrufen könnten. Das Gericht hat sich um Aufklärung bemüht und den Kläger hierzu angehört. Dieser gab an, dass er nicht öffentlich, sondern nur für Freunde postet und auch schon immer mal etwas politisches. Ob das dann schwierig sei in den USA, wisse er auch nicht, er gehe aber davon aus, dass das dort anders gehandhabt werde, jedenfalls sei es das, was man so mitbekomme. Dass die besagten politischen Posts – haben diese denn einen Bezug zu den USA? – des Klägers dazu führen könnten, ganz allgemein Schwierigkeiten in den USA zu bekommen, erschließt sich dem Gericht nicht.

50

Hinsichtlich der Angaben des Klägers konnte sich das Gericht keine dahingehende Überzeugung bilden, dass die von der Klagepartei behaupteten Folgen tatsächlich vorliegen. Es verbleiben insoweit erhebliche Zweifel, die zu Lasten der beweisbelasteten Klagepartei gehen. Zwar konnte der Kläger darlegen, dass er aufgrund seiner Arbeit in die USA einreisen soll und Sorge hat, dort nicht einreisen zu dürfen und dass dies berufliche Konsequenzen haben könnte. Er hat jedoch beide Accounts, bei F. und I., weiter genutzt und postet auf F. auch nach wie vor bzw. nutzt die Messenger-Dienste beider Netzwerke. Als Begründung gab er an, dass er nicht wusste, ob es bei einer Löschung noch rückverfolgbar wäre, dass er dort angemeldet war. Bei den behaupteten erheblichen Sorgen und Ängsten die Priorität darauf zu legen, dass (für den angestregten Prozess) eine Nachweisbarkeit gegeben ist, lässt es für das Gericht unglaublich erscheinen, dass die in erheblicher Ausprägung Sorgen und Ängste überhaupt bestehen. Der Kläger konnte auf Nachfrage des Gerichts nicht einmal abgeben, ob er davon betroffen ist, dass seine Daten öffentlich zugänglich waren (Scraping-Vorwürfe gegen die Beklagte), oder ob lediglich die Datenübertragung in die USA seine behauptete Betroffenheit auslöste. Auch nutzt er nach eigenen Angaben insbesondere die Suchmaschine „G.“ für Suchanfragen, wobei nach den vom Klägervorteiler vielfach zitierten Urteil des OLG Köln (Urteil vom 03.11.2023, Az. 6 U 58/23) hier – obergerichtlich bestätigt – unzulässige Datenübermittlungen in die USA erfolgen. Darüber hinaus hat der Kläger nach eigenen Angaben keinen Gebrauch von der Möglichkeit gemacht, über das von der Beklagten angebotene Selbstbedienungstool für die begehrten Auskünfte die entsprechenden Informationen abzurufen, obwohl er angab, Sorgen zu haben, bei der anstehenden dienstlichen Reise in die USA seinen Job zu verlieren. Der Kläger gab an, auf I. überwiegend mit Freunden zu schreiben. Unter Berücksichtigung der behaupteten großen Sorgen und Ängste (intime, private Chats könnten mitgelesen werden) ist für das Gericht absolut unverständlich, dass dieser Kommunikationsweg beibehalten wurde, wo doch unzählige online Messenger-Dienste oder die Möglichkeit des Schreibens von E-Mails oder SMS für eine Kommunikation mit Freunden zur Auswahl stehen. Der Kläger ist nach eigenen Angaben nach wie vor in mehreren F.-Gruppen und postet für ihn interessante Artikel. Auch die Ausführungen des Klägers dahingehend, dass sich F. ja jetzt schon

verpflichtet, die Datenschutzgrundsätze einzuhalten und er davon ausgeht, dass das zukünftig nicht mehr vorkommt, überzeugen in diesem Zusammenhang nicht, da bei den behaupteten Sorgen und Ängste, insbesondere der behauptete befürchtete Jobverlust und den angeblichen körperlichen und psychischen Folgen, aus Sicht des Gerichts – von der nicht erfolgten vollständigen Abmeldung mal ganz abgesehen – eine aktive Weiternutzung nicht mehr nachvollziehbar ist. Beim Gericht verbleiben jedenfalls dahingehend, dass die behaupteten Sorgen und Ängste tatsächlich bestehen, aus den vorgenannten Gründen erhebliche Zweifel, die zu Lasten der insofern beweisbelasteten Klagepartei gehen, so dass der Kläger den entsprechenden Beweis nicht erbringen konnte. Das als weiterer Beweis angebotene Sachverständigengutachten ist insoweit ein untaugliches Beweismittel.

51

Das Risiko der Nichterweislichkeit – auch in Bezug auf das konkrete Ausmaß eines etwaigen Schadens – verbleibt bei der Klagepartei (BGH, a.a.O.). Aufgrund des Fehlens eines Schadens kommen auch vertragliche Schadensersatzansprüche oder deliktische Ansprüche nicht in Betracht.

52

Lediglich vorsorglich sei angemerkt, dass soweit die Klagepartei meint, ein immaterieller Schadensersatzanspruch von 5.000 Euro sei vorliegend angemessen, da sowohl Datenschutzverstoß als auch mangelhafte Erfüllung des Auskunftsbegehrens kumulativ zusammen wirken, dies nicht dem vom EuGH dargelegten Verständnis der DSGVO entspricht (EuGH, Urteil vom 11.4.2024, Az. C-741/21). Dem in Art. 82 Abs. 1 DSGVO niedergelegten Schadensersatzanspruch kommt ausschließlich eine Ausgleichsfunktion zu. Er erfüllt keine Abschreckungs- oder gar Straffunktion, weshalb auch das Vorliegen mehrerer auf denselben Verarbeitungsvorgang bezogener Verstöße nicht zu einer Erhöhung des Schadensersatzanspruchs führen (BGH, a.a.O.). Dies hat der BGH in einem vergleichbaren Fall entschieden, bei dem neben dem Datenschutzverstoß (im entschiedenen Fall wegen Scraping) wie hier, eine unzureichende Auskunft gerügt wurde.

53

Der Schadensersatzanspruch war daher als unbegründet abzuweisen.

2. Kein Unterlassungsanspruch

54

Soweit die Klagepartei Unterlassung begehrt, ist die Klage, wie dargelegt, bereits unzulässig, aber ebenso unbegründet. Auch ein Unterlassungsanspruch scheitert jedenfalls am Fehlen eines Verstoßes gegen die DSGVO. Soweit die Klagepartei in der zweiten Alternative des Klageantrags Unterlassung der Verarbeitung ohne Einwilligung begehrt, so besteht hierauf insbesondere kein Anspruch, da eine Verarbeitung nicht rechtswidrig ist, nur weil keine Einwilligung vorliegt, Art. 6 Abs. 1 lit. a und Art. 49 Abs. 1 lit. a DSGVO. Vielmehr genügt das Vorliegen einer der übrigen Ausnahmen nach Art. 6 Abs. 1, Art. 49 Abs. 1 DSGVO für eine Rechtmäßigkeit der Übermittlung sowie der Verarbeitung.

3. Kein Auskunftsanspruch

55

Auch soweit die Klagepartei Auskunft begehrt, ist die Klage bereits unzulässig, überdies jedoch auch unbegründet. Das Auskunftsbegehren hat die Beklagte bereits erfüllt, § 362 Abs. 1 BGB, soweit Auskunft erteilt werden konnte und durfte. Im Übrigen ist, soweit Auskunft darüber begehrt wird, ob und in welchem Umfang die Beklagte Daten gegenüber US-Geheimdiensten offengelegt hat, der Anspruch ausgeschlossen, § 29 Abs. 1 S. 2 BDSG und Art. 15 Abs. 4 DSGVO.

56

Ein auf Art. 15 DSGVO fußender Auskunftsanspruch wäre vorliegend jedenfalls erfüllt, nachdem die Beklagte dem Kläger unstreitig mit Schreiben vom 09.08.2024 (Anlage B14) ausführlich dargelegt hat, dass die entsprechenden Daten über das Selbstbedienungstool abgefragt werden können, und wie dies im Einzelnen erfolgen kann. Soweit die Klagepartei hierauf erwidert, dass sie das Tool zur Erfüllung ihres Auskunftsbegehrens nicht akzeptiert (Schriftsatz vom 18.11.2024 Seite 21, Bl. 128 d. Akte sowie wortgleich Seite 78, Bl. 185 d. Akte) und die (nicht weiter begründete) Behauptung aufstellt, es sei ausgeschlossen, sich darauf zurückzuziehen, die angeforderten Daten nur über einen Fernzugriff zur Verfügung zu stellen, führt dies nicht zur Begründetheit des Klageantrags. Entgegen der Auffassung der Klagepartei genügt Auskunftserteilung mittels Fernzugriffs auf ein elektronisches Auskunftssystem des Datenverantwortlichen

den an die Auskunftserteilung zu stellenden formellen Anforderungen (so zutreffend OLG Dresden, Urteil vom 05.12.2023, Az. 4 U 1094/23).

57

Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Grundsatzes der Verhältnismäßigkeit gegen andere Grundrechte abgewogen werden. Insbesondere ist es unter Umständen nicht möglich, Informationen über konkrete Empfänger zu erteilen, wodurch das Auskunftsrecht beschränkt werden kann (BGH, Urteil vom 18.11.2024, Az. VI ZR 10/24).

58

Hinsichtlich etwaiger an US-Geheimdienste oder Strafverfolgungsbehörden übermittelter Daten ist zunächst anzumerken, dass nach dem Verständnis des Gerichts keine Übermittlung durch die Beklagte erfolgt ist, sondern allenfalls durch die Konzernmutter der Beklagten in den USA, so dass bereits fraglich ist, ob die Beklagte diesbezüglich überhaupt passivlegitimiert ist. Sofern man davon ausgeht, dass die Beklagte die Informationen von ihrer Konzernmutter beschaffen kann und muss, kann die Konzernmutter der Beklagten und somit folglich auch die Beklagte die Auskunft jedenfalls verweigern, weil es der Konzernmutter der Beklagten nach US-Amerikanischem Recht nicht gestattet ist, Informationen über Anfragen nach Section 702 FISA dritten gegenüber offen zu halten. Es gilt zum einen eine Geheimhaltungspflicht nach US-Amerikanischem Recht und zum anderen handelt es sich um ihrem Wesen nach geheimhaltungsbedürftige Informationen handelt, Art. 23 DSGVO i.V.m. § 29 Abs. 1 S. 2 BDSG. Es versteht sich von selbst, dass die Information, ob und welche Auskünfte an Geheimdienste erteilt werden, ihrem Wesen nach geheimhaltungsbedürftig ist (so 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).

4. Kein Ersatz zukünftiger Schäden

59

Auch der Feststellungsantrag ist nicht nur unzulässig, sondern jedenfalls auch unbegründet. Wie bereits im Rahmen der Zulässigkeit dargelegt (siehe oben I.5.), ist weder für das Gericht ersichtlich, noch wurde dies von der Klagepartei dargelegt, dass eine unbefugte Datenweitergabe in die USA überhaupt noch erfolgt (selbst der Kläger gab im Rahmen seiner informatorischen Anhörung an, dass er davon ausgeht, dass die Datenschutzgrundsätze nun eingehalten werden). Der Klagepartei ist, wie bereits dargelegt, weder der Nachweis eines Verstoßes gegen die DSGVO, noch der Nachweis gelungen, dass durch die Datenübermittlung in die USA ein materieller oder immaterieller Schaden entstanden ist. Warum nunmehr Jahre später noch die Möglichkeit eines Eintritts eines materiellen oder immateriellen Schadens bestehen soll, ist nicht ersichtlich und erst recht nicht dargelegt.

5. Nebenforderungen

60

Da der Klagepartei keiner der geltend gemachten Ansprüche zusteht, ist die Klage auch in Bezug auf die Nebenforderungen (Zinsen, vorgerichtliche Rechtsanwaltskosten) abzuweisen. Lediglich ergänzend sei angemerkt, dass durch die Klagepartei keinerlei Sachvortrag dazu erfolgt ist, worin die vorgerichtliche Tätigkeit des Prozessbevollmächtigten gelegen haben soll. Lediglich aus den (unstreitigen) Ausführungen der Beklagten, die im Rahmen der Nachfrage in der mündlichen Verhandlung bestätigt wurden, wurde bekannt, dass der Klägervertreter vorgerichtlich (lediglich) eine Auskunftsanfrage an die Beklagte gerichtet hat. Anhaltspunkte dafür, dass darüber hinaus irgendwelche Ansprüche geltend gemacht worden sind, bestehen nicht. Anwaltskosten für eine solche Auskunft können indes nicht geltend gemacht werden. Bei dem erstmaligen Verlangen einer Datenauskunft nach Art. 15 DSGVO handelt es sich im Regelfall – abweichende Umstände sind hier nicht geltend gemacht – um einen Bagatellfall, für den anwaltliche Hilfe nicht erforderlich ist. Anderes mag gelten, wenn der Verantwortliche die geforderte Auskunft nicht innerhalb der Frist des Art. 12 Abs. 3 DSGVO von einem Monat erteilt und damit bereits ein Verstoß gegen den Anspruch auf Datenauskunft vorliegt oder besondere Umstände des Einzelfalles hinzutreten. Selbst wenn man eine datenschutzrechtliche Pflichtverletzung der Beklagten unterstellt, ergibt sich der Anspruch auf Erstattung der anteiligen Anwaltskosten für das Auskunftsgesuch auch nicht aus Art. 82 Abs. 1 DSGVO, der Rechtsverfolgungskosten als Teil eines materiellen Ersatzanspruchs umfassen kann. Denn zum einen bestehen schon keine durchsetzbaren Hauptansprüche und zum anderen war die anwaltliche Beauftragung

für die erstmalige Geltendmachung eines Auskunftsanspruchs – etwas anderes ist weder ersichtlich, noch dargelegt – nicht erforderlich (vgl. hierzu OLG Köln, Urteil vom 07.12.2023, Az. 15 U 67/23).

III. Kosten, vorläufige Vollstreckbarkeit

61

Die Kostenentscheidung beruht auf § 91 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf § 709 ZPO.

IV. Streitwert

62

Der Streitwert war auf 6.800,00 Euro festzusetzen. In der Klageschrift wird das Augenmerk deutlich auf die Begründung der – aus Sicht des Gerichts deutlich überhöhten – durch die Klagepartei angenommenen Streitwerte gelegt. Der Argumentation der Klagepartei kann dabei in weiten Teilen nicht gefolgt werden.

63

Der Klageantrag auf Schadensersatz war entsprechend dem von der Klagepartei begehrten Betrag auf 5.000,00 Euro festzusetzen.

64

Der Streitwert des Unterlassungsantrags als nicht vermögensrechtliche Angelegenheit ist anhand des betroffenen Interesses des Klägers zu bestimmen, wobei gemäß § 48 Abs. 2 S. 1 GKG die Umstände des Einzelfalls zu beachten sind. Dabei geht der BGH (Beschluss vom 26.11.2020, Az. III ZR 124/20) davon aus, dass in Anlehnung an § 23 Abs. 3 S. 2 RVG bei mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Streitwert von 5.000 Euro auszugehen ist. Da der Kläger selbst in der mündlichen Verhandlung angab, davon auszugehen, dass „F.“ die Datenschutzrichtlinien nunmehr einhält, wird deutlich, dass für den Kläger selbst dieser Antrag von äußerst geringem Interesse ist, was eine deutliche Abweichung nach unten rechtfertigt, so dass der Wert des Antrags auf Unterlassen auf 100 Euro festzusetzen war.

65

Der Klageantrag auf Auskunft geht wertmäßig weitgehend in den Ansprüchen auf Schadensersatz und Feststellung des Ersatzes zukünftiger Schäden auf (OLG Stuttgart, Beschluss vom 03.01.2023, Az. 4 AR 4/22) und kann daher nur mit 100 Euro berücksichtigt werden.

66

Der Feststellungsantrag war entsprechend der Ausführungen der Klagepartei auf 1.600,00 Euro festzusetzen. Der Wert orientiert sich grundsätzlich an den Vorstellungen der Klagepartei zum geltend gemachten Schadensersatzanspruch, ist jedoch nur mit einem Bruchteil zu bemessen, wobei 1.600,00 Euro angemessen erscheinen.