

Titel:

Kenntnisnahme von Datenverarbeitungsinformationen sozialer Netzwerke obliegt dem jeweiligen Nutzer

Normenkette:

DSGVO Art. 5 Abs. 1 lit. b, Art. 15, Art. 25 Abs. 2 S. 1, S. 2, Art. 32, Art. 82 Abs. 1

Leitsätze:

1. Im Rahmen der Datenverarbeitung besteht ein Unterschied darin, ob bestimmte Daten innerhalb eines sozialen Netzwerks sichtbar sind, also für eine Person aus dem in der Zielgruppenauswahl bestimmten Personenkreis, die ein Profil aufruft, unmittelbar einsehbar sind, oder ob der Nutzer anhand dieser Daten aufgefunden werden kann, was voraussetzt, dass diese Daten der suchenden Person bereits bekannt sind. Der Anbieter eines sozialen Netzwerks hat die Nutzer in angemessener Weise über die Verarbeitung der von ihnen gespeicherten Daten zu informieren, wobei die tatsächliche Kenntnisnahme der durch ihn in angemessener Weise zur Verfügung gestellten Informationen in den Verantwortungsbereich des jeweiligen Nutzers fällt. (Rn. 28) (redaktioneller Leitsatz)

2. Nach Art. 25 Abs. 2 S. 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, wozu nach Art. 25 Abs. 2 S. 2 DSGVO auch die Zugänglichkeit der Daten gehört. Maßstab für die Auswahl der Maßnahmen ist die Erforderlichkeit für den Verarbeitungszweck. Der Verarbeitungszweck kann dabei im Rahmen der Vorgaben des Art. 5 Abs. 1 lit. b DSGVO frei gewählt werden. Es ist daher nicht zu verlangen, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. (Rn. 32) (redaktioneller Leitsatz)

3. Für den Umfang der Schutzmaßnahmen nach Art. 32 DSGVO ist eine Risikoabwägung erforderlich, die insbesondere die Art der Daten und die Wahrscheinlichkeit sowie die möglichen Folgen des Bekanntwerdens derselben miteinbezieht. (Rn. 37) (redaktioneller Leitsatz)

4. Die Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde bzw. zur Benachrichtigung der hiervon betroffenen bzw. die Auskunftspflicht nach Art. 15 DSGVO fallen nicht in den Schutzbereich des Art. 82 DSGVO, da es sich um keine Pflichten im Rahmen der Datenverarbeitung, sondern um dieser nachgelagerte Pflichten handelt. (Rn. 38) (redaktioneller Leitsatz)

Schlagworte:

Zuständigkeit, Schadensersatzanspruch, Datenverarbeitung, Einwilligung, Vertragsverhältnis, Datenübermittlung, Kausaler Schaden

Fundstelle:

GRUR-RS 2024, 16068

Tenor

1. Die Klage wird abgewiesen.
2. Die Klägerin 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 5.000,00 € festgesetzt.

Tatbestand

1

Die Klagepartei nimmt die Beklagte auf Schadensersatz, Feststellung und Auskunft wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO), insbesondere im Zusammenhang mit einem „Scraping“-Vorfall sowie wegen Datenübermittlung in die USA in Anspruch.

2

Die Beklagte betreibt das soziale Netzwerk „f.“. Die Klagepartei unterhält dort ein Nutzerprofil. Dabei sind Name, Geschlecht und Nutzer-ID stets öffentlich einsehbar, die übrigen durch den Nutzer dort hinterlegten Daten je nach gewählter Einstellung. Der Nutzer kann in seinem Profil eine Telefonnummer hinterlegen, wobei nach den Voreinstellungen (jedenfalls in dem hier in Rede stehenden Zeitraum 2018/2019) diese nicht öffentlich angezeigt wurde, der Nutzer jedoch anhand dieser gefunden werden konnte. Insbesondere war es mit dem „Contact-Import-Tool“ möglich, die auf dem Mobiltelefon eines Nutzers gespeicherten Kontakte auf „f.“ hochzuladen, so dass diese mit den bei „f.“ hinterlegten Telefonnummern abgeglichen werden und so gezielt diese Kontakte als „Freunde“ dem Profil des anfragenden Nutzers zugeordnet werden konnten, soweit diese Personen ihre Telefonnummer überhaupt bei „f.“ hinterlegt hatten und ihre Suchbarkeitseinstellungen bezüglich der Telefonnummer nicht von der Voreinstellung „alle“ auf „nur Freunde“ bzw. „Freunde von Freunden“ geändert hatten. Seit Mai 2019 ist es auch möglich, die Suchbarkeitseinstellung auf „nur ich“ zu begrenzen.

3

Im April 2021 wurden Daten (einschließlich Telefonnummer) von ca. 533 Millionen „f.“-Nutzern durch unbekannte Dritte im Internet verbreitet. Diese Daten waren in den Jahren 2018/2019 im Wege des „Scraping“ abgegriffen worden. Dabei waren die im Nutzerprofil hinterlegte Telefonnummer dem konkreten Nutzer und den in dessen „f.“-Profil hinterlegten öffentlich sichtbaren Daten zugeordnet worden. Vermutlich waren mit Hilfe des „Contact-Import-Tools“ eine Vielzahl möglicher Telefonnummern automatisiert ausprobiert und im Trefferfall das Profil des Nutzers aufgerufen und dessen öffentlich zugängliche Daten „gescraped“ worden.

4

Die Klägervertreter haben die Beklagte mit außergerichtlichem Schreiben vom 30.11.2023 (Anlage K1) zu Schadensersatz, Unterlassung und Auskunft aufgefordert. Die Beklagte hat die Ansprüche mit Schreiben vom 27.11.2023 (Anlage B16) zurückgewiesen.

5

Die Klagepartei behauptet, infolge einer Sicherheitslücke seien ihre Daten (Telefonnummer, F.-ID, Name, Vorname, Geschlecht) öffentlich zugänglich gemacht worden. Die betroffene Telefonnummer der Klagepartei laute:

6

Dies sei möglich gewesen, weil die Datenschutzeinstellungen auf „f.“ unübersichtlich und intransparent seien und die Voreinstellungen nicht datenschutzfreundlich seien. Insbesondere sei voreingestellt, dass man den Nutzer anhand seiner Telefonnummer „finden“ könne. Zudem habe die Beklagte nicht die erforderlichen Vorsichtsmaßnahmen (z.B. Einsatz von „Captchas“, Blockierung einer Vielzahl von Anfragen über dieselbe IP-Adresse bzw. von systematischen Zahlenreihen) ergriffen, um das „Scraping“ der Daten zu verhindern. Weder die betroffenen Nutzer noch die zuständige Datenschutzbehörde seien über den Vorfall informiert worden. Eine die Datenverarbeitung durch die Beklagte deckende Einwilligung der Klagepartei liege nicht vor. Die Klagepartei leide unter Kontrollverlust über ihre Daten und sei in Sorge über möglichen Missbrauch der sie betreffenden Daten. Die Klagepartei habe ihre Telefonnummer lediglich zu Sicherheitszwecken angegeben und sei davon ausgegangen, nur selbst auf diese Information zugreifen zu können. Die vorgerichtlich erteilte Auskunft der Beklagten sei unzureichend.

7

Die Beklagte habe sämtliche personenbezogenen Daten der Klägerseite aus und in Verbindung mit dem klägerischen „f.“-Account in die Vereinigten Staaten von Amerika (USA). Dies sei rechtswidrig, da die USA kein der DSGVO entsprechendes Schutzniveau gewährleisten würden. Die Daten der Klagepartei seien dem Zugriff der us-amerikanischen Geheimdienste zugänglich. Eine Einwilligung habe die Klagepartei nicht erteilt. Dadurch seien bei der Klagepartei ein Gefühl des Kontrollverlustes und der ständigen Überwachung entstanden..

8

Die Klagepartei stützt die geltend gemachten Auskunftsansprüche auf Art. 15 DSGVO, die Schadensersatzansprüche auf Art. 82 DSGVO.

9

Die Klagepartei beantragt zuletzt,

1. Die Beklagte wird verurteilt, an die Klagepartei einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 1.500,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle materiellen künftigen Schäden zu ersetzen, die der Klagepartei durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.
3. Die Beklagte wird verurteilt, der Klagepartei Auskunft über die personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch eine „Scraping“-Anwendung des Kontaktimporttools erlangt werden konnten.
4. Die Beklagte wird verurteilt, an die Klagepartei für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 1.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.
5. Die Beklagte wird verurteilt, an die Klagepartei einen immateriellen Schadensersatz für die unbefugte Datenübertragung in die USA dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 1.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.
6. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle materiellen künftigen Schäden zu ersetzen, die der Klagepartei durch die unbefugten Datenübertragung der personenbezogenen Daten in die USA, entstanden sind und/oder noch entstehen werden.
7. Die Beklagte wird verurteilt, die Klagepartei von den außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von € 1.134,55 nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz ab Rechtshängigkeit freizustellen.

10

Die Beklagte beantragt,

Klageabweisung.

11

Sie rügt die Unbestimmtheit der Klageanträge und fehlendes Feststellungsinteresse der Klagepartei. Einen Datenschutzverstoß stellt die Beklagte in Abrede. Die durch „Scraping“ erlangten Daten seien ohnehin öffentlich einsehbar gewesen. Die Transparenzpflichten würden durch die Beklagte erfüllt. Alle Nutzer würden über die Einstellungsmöglichkeiten zur Wahrung ihrer Privatsphäre (insb. Zielgruppenauswahl und Suchbarkeitseinstellungen) entsprechend der Datenrichtlinie der Beklagten hinlänglich informiert. Zweck der „f.“-Plattform sei es, andere Personen zu finden und mit ihnen in Kontakt zu treten, was durch eine Voreinstellung der Suchbarkeitseinstellungen auf „Freunde“ statt „Alle“ konterkariert werde. Die Beklagte ergreife auch angemessene technische und organisatorische Maßnahmen gegen nach ihren Richtlinien verbotenes „Scraping“ (u.a. Übertragungsbegrenzungen und Bot-Erkennung sowie Captchas) und entwickle diese laufend weiter. Gleichwohl lasse sich „Scraping“ nicht verhindern, zumal von den Tätern Umgehungsstrategien gegen die Übertragungsbeschränkungen entwickelt würden. Eine Melde- oder Benachrichtigungspflicht habe nicht bestanden. Auskunft über ihre Datenverarbeitungstätigkeit habe die

Beklagte vorgerichtlich erteilt, zu einer Auskunft über die Datenverarbeitungstätigkeit Dritter sei die Beklagte nicht verpflichtet. Eine Kopie der durch das „Scraping“ abgerufenen Rohdaten werde von der Beklagten nicht vorgehalten. Eine spürbare Beeinträchtigung habe die Klagepartei nicht erlitten; ein Kontrollverlust oder Unwohlsein stellten keinen Schaden dar.

12

Die Übermittlung von Daten durch die Beklagte an die M, Inc. in den USA erfolge auf Grundlage von Kapitel V DSGVO, des Angemessenheitsbeschlusses der Kommission 2023 und der Standardvertragsklauseln 2010 und 2021. „f.“ sei ein globaler Dienst, weswegen ein grenzüberschreitender Datenaustausch zur Vertragserfüllung erforderlich sei.

13

Das Gericht hat zur Sache am 10.06.2024 mündlich verhandelt und die Klagepartei informatorisch angehört .

14

Zur Ergänzung und Vervollständigung des Tatbestandes wird auf die gewechselten Schriftsätze nebst Anlagen sowie die Sitzungsniederschrift Bezug genommen.

Entscheidungsgründe

15

Die teilweise unzulässige Klage ist vollumfänglich unbegründet.

A.

16

Die Klage ist nur teilweise zulässig.

I. Zuständigkeit

17

Das Landgericht Passau ist international nach Art. 79 Abs. 2 S. 2, 82 Abs. 6 DSGVO und örtlich nach § 44 Abs. 1 S. 2 BDSG zuständig. Die sachliche Zuständigkeit ergibt sich infolge rügeloser Einlassung aus § 39 S. 1 ZPO.

II. „Scraping-Vorfall“

18

1. Der Streitgegenstand des geltend gemachten Schadensersatzanspruchs ist durch den klägerischen Vortrag hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Die Klagepartei hat klargestellt, dass sie den geltend gemachten Anspruch nicht alternativ, sondern kumulativ auf das Verhalten der Beklagten vor dem streitgegenständlichen Vorfall im Sinne der Nichteinhaltung gebotener Sicherungsvorkehrungen einerseits und dasjenige nach dem streitgegenständlichen Vorfall im Sinne unzureichender Information der Betroffenen andererseits stützt. Damit hat sie beide Vorwürfe zu einem einheitlich zu bewertenden (§ 287 ZPO!) Lebenssachverhalt verbunden. Einer betragsmäßigen Aufteilung des geltend gemachten Anspruchs auf beide Vorwürfe bedurfte es somit nicht. Die Klage ist insoweit hinlänglich bestimmt.

19

2. Der auf die Feststellung der Ersatzpflicht der Beklagten gegenüber der Klagepartei für künftige Schäden gerichtete Antrag ist nicht hinreichend bestimmt gem. § 253 Abs. 2 Nr. 2 ZPO. Der Antrag bezieht sich auf „künftige Schäden“, „die der Klagepartei (...) entstanden sind und/oder noch entstehen werden.“ Auch unter Berücksichtigung der Klagebegründung und des Vorbringens in der Replik ist für das Gericht nicht zu erkennen, ob sich der Antrag nur auf künftige Schäden oder auch bereits entstandene, aber ggfs. noch nicht bekannte Schäden erstrecken soll.

20

3. Hinsichtlich des Feststellungsantrags besteht auch kein ausreichendes Feststellungsinteresse (§ 256 Abs. 1 ZPO). Ein Feststellungsinteresse ist zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH NJW-RR 2007, 601). Der „Scraping“-Vorfall liegt mittlerweile über vier Jahre und die angebliche Veröffentlichung der klägerischen Daten über zwei Jahre zurück. Mit Ausnahme der Telefonnummer handelt

es sich um Daten, die die Klagepartei selbst zur Veröffentlichung bestimmt hat. Ein künftiger, den behaupteten Pflichtverletzungen der Beklagten zurechenbarer Schaden ist bei dieser Sachlage vernünftigerweise nicht zu erwarten.

III. Datenübermittlung in die USA

21

1. Der auf die Feststellung der Ersatzpflicht der Beklagten gegenüber der Klagepartei für künftige Schäden gerichtete Antrag ist nicht hinreichend bestimmt gem. § 253 Abs. 2 Nr. 2 ZPO. Auf die obigen Ausführungen unter Ziffer II. 2. wird zur Begründung Bezug genommen.

22

2. Hinsichtlich des Feststellungsantrags besteht auch kein ausreichendes Feststellungsinteresse (§ 256 Abs. 1 ZPO). Ein Feststellungsinteresse ist zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH NJW-RR 2007, 601). Welcher Schaden der Klagepartei dadurch entstehen soll, dass die Beklagte rechtswidrig Daten in die USA übermitteln sollte, ist für das Gericht nicht vorstellbar und wird auch nicht plausibel dargelegt.

23

Im Übrigen ist die Klage zulässig.

B.

24

Die Klage ist – soweit sie unzulässig ist: jedenfalls auch – unbegründet.

I. Scraping-Vorfall

25

1. Die Klagepartei hat keinen Schadensersatzanspruch gegen die Beklagte aus Art. 82 Abs. 1 DSGVO.

26

a) Es fehlt bereits an einem relevanten Verstoß gegen die Bestimmungen der DSGVO.

27

aa) Die Verarbeitung der klägerischen Daten ist rechtmäßig im Sinne von Art. 6 DSGVO.

28

(1) Zum einen hat die Klagepartei in die Datenverarbeitung (Art. 4 Nr. 2 DSGVO) durch die Beklagte eingewilligt (Art. 6 Abs. 1 Buchst. a, Art. 7 DSGVO). Die Einwilligung erfolgte auch freiwillig und in informierter Weise (Art. 4 Nr. 11 DSGVO). Das Gericht kann Vorwürfen der Klagepartei, die Datenschutzhinweise und -einstellungen auf „f.“ seien nicht hinlänglich transparent (Art. 5 Abs. 1 Buchst. a DSGVO), nicht folgen. Es werden auf „f.“ umfangreiche Hinweise und Bedienungshilfen bereitgestellt, mittels derer sich der Nutzer über sämtliche Einstellungsmöglichkeiten und deren Datenschutzrelevanz informieren kann. Hierbei stehen laut klägerischem Vortrag insbesondere im Rahmen der Seite „Privatsphäre auf einen Blick“ Informationen darüber bereit, wie andere Personen den Nutzer auf F. finden können. Die Information der Beklagten „Nur du kannst deine Nummer sehen“ ist insofern nicht irreführend. Die Telefonnummer wird zum Zeitpunkt der Angabe derselben nicht öffentlich angezeigt. Tatsächlich besteht ein Unterschied darin, ob bestimmte Daten sichtbar sind, also für eine Person aus dem in der Zielgruppenauswahl bestimmten Personenkreis, die ein Profil aufruft, unmittelbar einsehbar sind, oder ob der Nutzer anhand dieser Daten aufgefunden werden kann, was voraussetzt, dass diese Daten der suchenden Person bereits bekannt sind. Dass Zielgruppenauswahl und Suchbarekeitseinstellungen voneinander getrennt sind, ist daher nachvollziehbar. Die Beklagte informiert die Nutzer von Anfang an hinlänglich über die von ihr vorgenommene Datenverarbeitung und genügt damit ihrer Pflicht zur leicht zugänglichen Bereitstellung der entsprechenden Informationen. Die tatsächliche Kenntnisnahme obliegt dabei der Klagepartei. Was daran nicht verständlich sein soll, dass alle einen Nutzer anhand seiner Telefonnummer „finden“ können, erschließt sich dem Gericht nicht. Die Möglichkeit, durch Dritte gefunden zu werden und somit auch die Möglichkeit, dass ein missbräuchliches „Erraten“ der Telefonnummer stattfinden könnte, war daher für die Klagepartei ebenso ersichtlich wie für die Beklagte. Soweit die Klagepartei die Verletzung von Informationspflichten aus Art. 13, 14 DSGVO rügt, ist aus dem klägerischen

Vortrag nicht ersichtlich, welche der dort konkret aufgezählten Informationen der Klagepartei nicht erteilt worden sein sollen.

29

(2) Zum anderen ist die Datenverarbeitung für die Erfüllung des Vertrags zwischen den Parteien erforderlich (Art. 6 Abs. 1 Buchst. b DSGVO). Die Nutzung des „Contact-Import-Tools“ wird Nutzern im Rahmen der Nutzung von „f.“ freigestellt. Gibt der Nutzer, wie hier, seine Telefonnummer jedoch unter Einwilligung zur Nutzung des „Contact-Import-Tools“ an, so ist die Verarbeitung derselben im Rahmen dieses Tools gerade denknotwendig zur Erfüllung der resultierenden Vertragsvereinbarung, von anderen auf „f.“ gefunden zu werden. Bezüglich der übrigen, von der Klagepartei selbst veröffentlichten Daten, ist das Vorhalten dieser Nutzerdaten gerade der Zweck des zwischen den Parteien bestehenden Vertragsverhältnisses. Eine soziale Plattform wie „f.“ dient dazu, es den Nutzern zu ermöglichen, Daten miteinander auszutauschen. Zu diesem Zweck müssen diese von der Beklagten denknotwendig verarbeitet werden.

30

bb) Ein Verstoß gegen das Transparenzgebot (Art. 5 Abs. 1 Buchst. a DSGVO) ist nicht gegeben (s. bereits oben unter Buchst. aa).

31

cc) Es liegt auch kein Verstoß gegen Art. 25 Abs. 2 DSGVO (Datenschutz durch datenschutzfreundliche Voreinstellung) vor.

32

(1) Nach Art. 25 Abs. 2 S. 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, wozu nach Art. 25 Abs. 2 S. 2 DSGVO auch die Zugänglichkeit der Daten gehört. Maßstab für die Auswahl der Maßnahmen ist die Erforderlichkeit für den Verarbeitungszweck. Der Verarbeitungszweck kann dabei im Rahmen der Vorgaben des Art. 5 Abs. 1 Buchst. b DSGVO frei gewählt werden. Es ist daher nicht zu verlangen, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 18).

33

(2) Soweit die Suchbarkeitseinstellungen anhand der Telefonnummer als Voreinstellung im maßgeblichen Zeitpunkt (2018/2019) „Alle“ vorgesehen haben, war dies nicht zu beanstanden, weil der Zweck eines „sozialen Netzwerks“ generell und insbesondere des „Contact-Import-Tools“ nur dadurch erreicht werden kann, dass Nutzer dieses Netzwerks von anderen auch gefunden werden können. Wenngleich ein Auffinden auch über die manuelle Suche möglich ist, geschieht dies am effektivsten über die Telefonnummer, weil diese eine eindeutige Identifikation der Person ermöglicht, während dies beim Namen nicht der Fall ist. Wer sich als neuer Nutzer bei „f.“ anmeldet, kann selbst noch keine „Freunde“ haben und noch nicht der „Freund“ eines anderen Nutzers sein. Eine Voreinstellung auf „nur Freunde“ oder „Freunde von Freunden“ ergibt daher keinen Sinn. Wenn die Beklagte die Erforderlichkeit der Voreinstellung „Alle“ bei den Suchbarkeitseinstellungen bezüglich der Telefonnummer als für den Verarbeitungszweck erforderlich qualifiziert hat, liegt diese Entscheidung jedenfalls im Rahmen des Vertretbaren.

34

(3) Art. 25 Abs. 2 S. 3 DSGVO konkretisiert die Anforderungen dahingehend, dass insbesondere sichergestellt sein muss, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Diese Vorschrift ist jedoch auf die Suchbarkeitseinstellungen bezüglich der Telefonnummer auf „f.“ schon konzeptionell nicht anwendbar, weil die Suchbarkeit des Nutzers über seine Telefonnummer voraussetzt, dass der Suchende die Telefonnummer, nach der mittels des „Contact-Import-Tools“ gesucht wird, bereits kennt bzw. in seinen Telefonkontakten abgespeichert hat. Nichts anderes gilt, wenn die Nummer durch maschinelles Ausprobieren erraten wird. Denn auch dann wird die Nummer nicht durch die Beklagte „einer unbestimmten Zahl von natürlichen Personen“ zugänglich gemacht, sondern nur derjenigen, die die Nummer bereits erraten hat. Dass diese Person die Daten dann unbefugt weiterverarbeitet, ist jedoch nicht der Beklagten zuzurechnen, sondern stellt ein allgemeines Lebensrisiko dar, welches die Klagepartei zu tragen hat, zumal

sie selbst die Möglichkeit hatte, diesen Missbrauch durch Änderung der Suchbarkeitseinstellung (zum streitgegenständlichen Zeitpunkt auf: „nur Freunde“) zu verhindern. Es fällt nicht in den Schutzbereich der Verarbeiterpflichten nach der Datenschutzgrundverordnung, ein Datum (hier: Telefonnummer) vor jemandem geheim zu halten, der es ohnehin bereits kennt.

35

dd) Auch ein Verstoß gegen Art. 32, 25 Abs. 1, 5 Abs. 1 Buchst. f DSGVO durch die Beklagte ist nicht gegeben. Die Klagepartei kann sich nicht darauf berufen, die Beklagte habe nicht die erforderlichen Maßnahmen ergriffen, um den Schutz der klägerischen Daten zu gewährleisten.

36

(1) Die vom „Scraping“-Vorfall nach klägerischer Behauptung betroffenen Daten waren – mit Ausnahme der Telefonnummer – nach dem Willen der Klagepartei ohnehin bereits öffentlich sichtbar. Dass diese öffentlich sichtbaren Daten von Dritten kopiert und an anderer Stelle abgespeichert und veröffentlicht werden, ist ein Risiko, welches jeder, der seine Daten auf „f.“ öffentlich macht, kennt und in Kauf nimmt. Soweit dies entgegen den Nutzungsbedingungen der Beklagten maschinell und massenhaft erfolgt („Scraping“), gehört dies zum allgemeinen Lebensrisiko, das der Nutzer zu tragen hat. Bereits öffentlich zugängliche Daten müssen nicht vor dem Zugriff unbefugter Dritter geschützt werden. Diese sind vom Schutzbereich des Art. 32 DSGVO nicht erfasst (s. bereits o. Ziff. 1. a) cc) (3) der Entscheidungsgründe).

37

(2) Die Telefonnummer der Klagepartei war zwar auf dem „f.“-Profil der Klagepartei nicht öffentlich sichtbar, aufgrund der Suchbarkeitseinstellungen war jedoch das Profil anhand der Telefonnummer auffindbar. Dies ist die Folge der freiverantwortlichen Entscheidung der Klagepartei, die eigene Telefonnummer überhaupt bei „f.“ zu hinterlegen (was zur Anmeldung nicht erforderlich ist) und die diesbezüglich voreingestellte Suchbarkeitseinstellung „Alle“ nicht abzuändern. Infolgedessen war es nach klägerischem Vortrag unbekannten Dritten möglich, durch maschinelles Ausprobieren beliebiger Telefonnummern die Telefonnummer der Klagepartei deren „f.“-Profil und den dort veröffentlichten Daten zuzuordnen. Auch das findet seine Ursache darin, dass die Klagepartei zur Verwendung ihrer Telefonnummer als Suchkriterium eingewilligt und damit den unbekannten Dritten diese Möglichkeit eröffnet hat. Für Schutzmaßnahmen seitens der Beklagten bestanden – unabhängig davon, dass die Beklagte solche ergriffen zu haben behauptet – jedenfalls vor dem Zeitpunkt des Bekanntwerdens des „Scraping-Vorfalles“ (ex ante) keine Veranlassung. Wie die Beklagte zutreffend ausführt, ist für den Umfang der Schutzmaßnahmen nach Art. 32 DSGVO zudem eine Risikoabwägung erforderlich, die insbesondere die Art der Daten und die Wahrscheinlichkeit sowie die möglichen Folgen des Bekanntwerdens derselben miteinbezieht. Zum einen handelt es sich bei keinem der von der Klagepartei genannten Daten um besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO. Zum anderen sind durch das Bekanntwerden der Telefonnummer keine schwerwiegenden Nachteile für die Klagepartei zu erwarten. In Anbetracht dessen hat die Beklagte ihren Pflichten genügt, indem sie die Klagepartei auf die möglichen Einstellungen und ihre Folgen hingewiesen hat. Mehr war von der Beklagten im damaligen Zeitpunkt nicht zu erwarten (so im Ergebnis auch LG Essen GRUR-RS 2022, 34818).

38

ee) Die Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) bzw. zur Benachrichtigung der hiervon betroffenen Person (Art. 34 DSGVO) bzw. die Auskunftspflicht nach Art. 15 DSGVO fallen nicht in den Schutzbereich des Art. 82 DSGVO, da es sich um keine Pflichten im Rahmen der Datenverarbeitung (Art. 82 Abs. 2 S. 1 DSGVO), sondern um dieser nachgelagerte Pflichten handelt (Gola/Heckmann, Art. 82 Rn. 5; Ehmann/Selmayr Art. 82 Rn. 8). Jedenfalls kann durch etwaige Verletzung dieser Pflichten der Klagepartei kein zusätzlicher Schaden entstanden sein, nachdem der „Scraping“-Vorfall sich bereits ereignet hatte und der Klagepartei ohnehin keine effektiven Mittel zur Verfügung standen, der weiteren Verbreitung der Daten zu begegnen.

39

ff) Sofern die Datenschutzbehörden einen Verstoß der Beklagten gegen die Bestimmungen der DSGVO bejahen sollte, entfaltet diese keine jedenfalls Bindungswirkung für das Gericht.

40

b) Der Klagepartei ist zudem kein kausaler Schaden entstanden. Beweisbelastet für den Eintritt eines durch einen Verstoß gegen die DSGVO verursachten Schadens ist nach allgemeinen Grundsätzen die

Klagepartei. Entgegen der Auffassung der Klagepartei resultiert dabei kein Schaden aus der bloßen Verletzung der DSGVO, sondern diese muss zu einer tatsächlichen Beeinträchtigung der Klagepartei führen (vgl. EuGH, Urt. v. 4.5.2023 – C-300/21). Der Nachweis eines kausalen Schadens ist auch nach dem Beweismaßstab des § 287 ZPO nicht geführt. Die persönliche Anhörung der Klagepartei hat ergeben, dass diese gehäuft dubiose Anrufe und Kurzmitteilungen erhält. Ihre Telefonnummer hat die Klagepartei auch bei anderen Dienstleistern hinterlegt. Für einen kausalen Zusammenhang mit dem durch den „Scraping“-Vorfall nach klägerischem Vortrag veröffentlichten Datensatz gibt es keinen Beleg. So ist es allgemein bekannt, dass auch Personen, die nicht bei „f.“ angemeldet sind oder dort zumindest keine Telefonnummer hinterlegt haben, von Anrufen und Nachrichten, wie sie die Klagepartei beschreibt, geplagt werden. Soweit klägerseits ein Gefühl des Unwohlseins und Kontrollverlustes behauptet wird, bleibt der klägerische Vortrag so allgemein, dass daraus ein konkreter, der gerichtlichen Bewertung zugänglicher Schaden nicht abgeleitet werden kann. Zwar ist der Schadensbegriff weit zu verstehen, er muss jedoch auch wirklich „erlitten“, das heißt „spürbar“ und objektiv nachvollziehbar sein.

41

Woraus dieser Schaden konkret rühren soll, ist aus dem Vortrag der Klagepartei nicht zu entnehmen.

42

2. Der Antrag auf Feststellung der Ersatzpflicht bezüglich künftiger Schäden ist auch unbegründet. Es fehlt bereits an einem Verstoß gegen die Vorschriften der DSGVO, der Grundlage eines Schadensersatzanspruchs sein könnte (s.o. Ziff. 1. a). Jedenfalls ist nicht ersichtlich, welcher künftige, auf eine Pflichtverletzung der Beklagten zurückzuführende Schaden der Klagepartei entstehen können sollte.

43

3. Die Klagepartei hat auch keinen weiteren Auskunftsanspruch gegen die Beklagte aus Art. 15 DSGVO. Allgemein bekannt kann sich jeder „f.“-Nutzer die bezüglich seiner Person gespeicherten Daten herunterladen. Im vorgerichtlichen Schreiben vom 27.11.2023 (Anlage wird die Vorgehensweise nochmals beschrieben. Der Anspruch auf Datenkopie aus Art. 15 Abs. 3 DSGVO ist damit erfüllt, § 362 Abs. 1 BGB. Die weiteren Informationen nach Art. 15 Abs. 1 DSGVO finden sich in der öffentlich zugänglichen und als Anlage B20 vorgelegten Datenrichtlinie der Beklagten, sodass auch der darauf gerichtete Anspruch erfüllt ist. Im Schreiben vom 27.11.2023 (Anlage hat die Beklagte darüber hinaus (überobligatorisch) auch die ihr zur Verfügung stehenden Informationen zu dem „Scraping“-Vorfall mitgeteilt. Einen Anspruch auf Auskunft über die Datenverarbeitungstätigkeit Dritter (nämlich der Täter) hat die Klagepartei gegen die Beklagte nicht. Im Übrigen ist auch nicht schlüssig dargetan, was die Beklagte über die von ihr mitgeteilten Informationen hinaus diesbezüglich wissen, aber nicht preisgeben sollte.

44

4. Da die Beklagte ihre Auskunftspflicht nicht verletzt hat, hat die Klagepartei auch keinen Anspruch auf Schadensersatz wegen Nichterteilung der Auskunft aus Art. 82 DSGVO. Im Übrigen ist auch insoweit nicht ersichtlich, worin der Schaden der Klagepartei liegen sollte.

II. Datenübermittlung in die USA

45

1. Der Klagepartei stehen auch keine Ansprüche gegen die Beklagte im Zusammenhang mit den behaupteten Vorwürfen im Zusammenhang mit der Datenübermittlung in die USA zu.

46

a) Eine rechtswidrige Datenübermittlung kann das Gericht nicht erkennen. Die Plattform „f.“ und der M-Konzern stammen aus den USA. „F.“ ist als globale Plattform konzipiert. Um dieses weltweite Netzwerk unterhalten zu können, müssen zwangsläufig Daten international ausgetauscht werden. Dass in diesem Zusammenhang auch Daten durch die Beklagte in die USA übermittelt werden, liegt folglich nahe. Dieses Erfordernis ist auch unabhängig davon, ob die Klagepartei mit US-amerikanischen „f.“-Nutzern „befreundet“ ist oder nicht. Denn allein die Suche nach Nutzern in anderen Rechtsgebieten kann nur funktionieren, wenn ein grenzüberschreitender Datenaustausch stattfindet. All dies muss jedem „f.“-Nutzer, auch der Klagepartei, hinlänglich bekannt sein. Die Klagepartei hat keinen Anspruch darauf, dass „f.“ dergestalt betrieben wird, dass sämtliche Daten in Europa gespeichert und verarbeitet werden im Sinne eines rein europäischen „f.“. Die unternehmerische Entscheidung des Betreibers der Plattform „f.“, Daten in den

Vereinigten Staaten von Amerika zu verarbeiten, ist von den Nutzern hinzunehmen, zumal niemand dazu gezwungen wird, die Plattform „f.“ zu nutzen.

47

b) Die Datenübermittlung ist daher grundsätzlich zur Vertragserfüllung erforderlich, Art. 6 Abs. 1 Buchst. b DSGVO.

48

c) Die Voraussetzungen für die Datenübermittlung in Drittländer nach Kapitel V DSGVO werden von der Beklagten eingehalten.

49

aa) Aktuell erfolgt die Datenübermittlung aufgrund des Angemessenheitsbeschlusses der Kommission vom 10.07.2023. Dieser stellt eine taugliche Grundlage für die Datenübermittlung dar, Art. 45 Abs. 3 DSGVO. Eine weitergehende Überprüfung der Angemessenheit des Schutzniveaus erübrigt sich dadurch.

50

bb) Für den vorangegangenen Zeitraum stellen die von der Kommission erlassenen Standardvertragsklauseln 2010 und 2021 in Verbindung mit Art. 46 Abs. 1, Abs. 2 Buchst. c) DSGVO eine ausreichende Rechtsgrundlage dar. Nach Art. 46 Abs. 1 DSGVO müssen den Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, um ein dem EU-Recht gleichwertiges Schutzniveau zu gewährleisten. Wieso in den Vereinigten Staaten von Amerika kein gleichwertiger Rechtsschutz zur Verfügung gestellt werden könne, ist nicht zu erkennen.

51

cc) Schließlich ist die Datenübermittlung, wie bereits oben unter Buchst. a) ausgeführt, zur Vertragserfüllung erforderlich und damit auf Grundlage von Art. 49 Abs. 1 S. 1 b DSGVO zulässig.

52

dd) Soweit Datenschutzbehörden abweichende Auffassungen vertreten, sind diese für das Gericht nicht bindend.

53

d) Soweit US-Regierungsbehörden einschließlich der Geheimdienste von M, Inc., nach USamerikanischem 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 Buchst. c) DSGVO (Erfüllung einer rechtlichen Verpflichtung) zulässig wäre. Falls der Betroffene von einer etwaigen Auskunft an die Geheimdienste nicht informiert wird, ist dies gerechtfertigt, weil zum einen eine Geheimhaltungspflicht nach USamerikanischem Recht besteht und es sich zum anderen 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.

54

2. Für einen Schadensersatzanspruch aus Art. 82 DSGVO fehlt es zudem an einem kausalen Schaden der Klagepartei. Hinsichtlich der Datenübermittlung in die Vereinigten Staaten von Amerika machte die Klagepartei im Rahmen ihrer informatorischen Anhörung keine Angaben zu etwaigen Belastungen. Ob und in welchem Umfang Daten der Klagepartei tatsächlich dorthin übermittelt wurden, ist nicht feststellbar. Für einen konkreten Schaden der Klagepartei ist daher nichts ersichtlich.

III. Vorgerichtliche Kosten

55

Mangels zuzusprechender Hauptforderung besteht auch kein Anspruch auf Erstattung vorgerichtlicher Rechtsverfolgungskosten.

C.

56

I. Die Kostenentscheidung beruht auf § 91 ZPO.

57

II. Die vorläufige Vollstreckbarkeit ergibt sich aus § 709 ZPO.

58

III. Die Streitwertfestsetzung beruht auf §§ 39 Abs. 1, 43 Abs. 1, 48 Abs. 1 S. 1 GKG, 3 ZPO.

59

Das Gericht bewertet die Anträge wie folgt:

Ziffer Wert (€)

1. 1.500,-

2. 500,-

3. 500,-

4. 1.000,-

5. 1.000,-

6. 500,-