LG Passau, Endurteil v. 16.02.2024 – 1 O 616/23

Titel:

Erfolglose Schadensersatzklage wegen Verbreitung personenbezogener Nutzerdaten durch Dritte

Normenketten:

BGB § 823, § 1004
ZPO § 253, § 256
DSGVO Art. 4, Art. 5, Art. 6, Art. 15, Art. 17, Art. 18, Art. 82

Leitsätze:

1. Nach Art. 25 Abs. 2 DSGVO kann nicht verlangt werden, dass ein Plattformbetreiber stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft; der Plattformbetreiber entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. (Rn. 42) (redaktioneller Leitsatz)
2. Soweit die Suchbarkeitseinstellungen auf der hier gegenständlichen Internetplattform (Social-Media) anhand der Telefonnummer des Nutzers als Voreinstellung „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. (Rn. 43) (redaktioneller Leitsatz)

Schlagwort:

Datenschutz

Fundstellen:

ZD 2024, 411
LSK 2024, 3875
GRUR-RS 2024, 3875

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 23.000,00 € festgesetzt.

Tatbestand

1
Die Klagepartei nimmt die Beklagte auf Schadensersatz, Unterlassung, Löschung und Auskunft wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO), insbesondere im Zusammenhang mit einem „Scraping“-Vorfall sowie wegen Überwachung des F.-Messenger-Dienstes, Verarbeitung von „Off-F.-Daten“ und 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
Bestandteil von „f.“ ist auch ein Messenger-Dienst, über den die „f.“-Nutzer Nachrichten und Dateien miteinander austauschen können.

5
Die Klägervertreter haben die Beklagte mit außergerichtlichem Schreiben vom 15.02.2023 (Anlage K15) zu Schadensersatz, Unterlassung und Auskunft aufgefordert. Die Beklagte hat die Ansprüche mit Schreiben vom 20.09.2023 (Anlage B 15) zurückgewiesen.

6
Wegen der Vorwürfe bezüglich des „f.“-Messengers, der „Off-F.-Daten“ und der Datenübermittlung in die USA traten die Klägervertreter außergerichtlich ebenfalls an die Beklagte heran. Die Beklagte ließ die Ansprüche mit Schreiben vom 19.12.2023 (Anlage B33) zurückweisen.

7
Die Klagepartei behauptet, infolge einer Sicherheitslücke seien ihre Daten (Telefonnummer, F.-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt sowie Beziehungsstatus u.a.) öffentlich zugänglich gemacht worden. Die betroffene Telefonnummer der Klagepartei laute:

…

8
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.

9
Darüber hinaus werde der Messenger-Dienst von „f.“ systematisch und automatisiert überwacht („crawling“ der Inhalte). Dies könne nutzerseitig nicht deaktiviert werden und sei zur Vertragserfüllung nicht notwendig.

10
Daten, die Aktivitäten außerhalb des sozialen Netzwerks betreffen („Off-F.-Daten“), würden durch „f.“ massenhaft gesammelt, gespeichert und ausgewertet und innerhalb des M.-Konzerns weitergegeben. Eine Einwilligung der Nutzer werde nicht eingefordert.

11

Die Beklagte habe sämtliche personenbezogenen Daten der Klägerseite aus und in Verbindung mit dem klägerischen „f.“-Account in die Vereinigten Staaten von Amerika (USA), insbesondere an die National Security Agency (NSA) zur anlasslosen Überprüfung und Untersuchung weitergeleitet. Dies sei rechtwidrig, da die USA kein der DSGVO entsprechendes Schutzniveau gewährleisten würden. Auch habe die Klagepartei nicht in die Weitergabe ihrer Daten eingewilligt. Inhaltlich würden die in enormer Menge übermittelten Daten praktisch das gesamte soziale Leben des Nutzers abbilden. Dadurch seien bei der Klagepartei erhebliche Ängste und Stress entstanden.

12
Die Klagepartei stützt die geltend gemachten Auskunfts-, Unterlassungs- und Löschungsansprüche auf Art. 15, 17 und 18 DSGVO, §§ 1004 analog, 823 Abs. 1, 823 Abs. 2 BGB i.V.m. Art. 6 DSGVO, die Schadensersatzansprüche auf Art. 82 DSGVO.

13
Die Klagepartei beantragt zuletzt,

1. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Telefonnummer sowie weiterer personenbezogener Daten der Klägerseite zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens 2.000,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 10.02.2023

2. Die Beklagte wird weiter verurteilt, an die Klagepartei immateriellen Schadenser satz als Ausgleich für Datenschutzverstöße hinsichtlich der anlasslosen Überwachung von im Wege des F.-Messenger-Dienstes versandten und erhaltenen Chat-Nachrichten der Klagepartei sowie der Sammlung, Nutzung und Auswertung der „Off-F.-Daten“ der Klagepartei an die Klägerseite zu zahlen, dessen Hö he in das Ermessen des Gerichts gestellt wird, jedoch mindestens 1.500,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit.

3. Die Beklagte wird weiter verurteilt, an die Klagepartei immateriellen Schadenser satz als Ausgleich für Datenschutzverstöße hinsichtlich der Weitergabe und Übermittlung personenbezogener Daten der Klägerseite in die USA, insbesondere an die dortige Nation Security Agency (NSA) zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens 1.500,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit.

4. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle zukünftigen Schäden zu ersetzen, die der Klagepartei

a) durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussagen der Beklagten im Jahr 2019 erfolgte und

b) durch die anlasslose Überwachung von im Wege des F.-Messenger-Dienstes versandten und erhaltenen Chat-Nachrichten der Klagepartei sowie der Sammlung, Nutzung und Auswertung der „Off-F.-Daten“ sowie

c) durch die Weitergabe und Übermittlung personenbezogener Daten der Klägerseite in die USA, insbesondere an die dortige Nation Security Agency (NSA) entstanden sind und / oder noch entstehen werden.

5. Die Beklagte wird verurteilt, an die Klägerseite für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft im Sinne des Art. 15 DS-GVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit Rechtshängigkeit zu bezahlen.

6. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogene Daten der Klagepartei, namentlich Telefonnummer, F.-ID, Familienname, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klagepartei auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Information darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontakt-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der F.-Messenger-App, hier ebenfalls die Berechtigung verweigert wird.

7. Die Beklagte wird weiter verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) Chat-Nachrichten der Klagepartei, welche mittels des „F.-Messenger“-Dienstes versandt werden und wurden, anlasslos zu überwachen,

b) „Off-F.-Daten“ der Klagepartei zu sammeln, nutzen und auszuwerten,

c) personenbezogene Daten der Klagepartei in die USA, insbesondere die National Security Agency (NSA) zu übermitteln.

8. Die Beklagte wird verurteilt, der Klagepartei Auskunft

a) über die Klagepartei betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontakt-Import-Tools erlangt werden konnten,

b) über die überwachten, ausgewerteten und gespeicherten Daten aus der Überwachung des F.-Messengers zu erteilen, namentlich Chat-Protokolle vorzulegen und deren interne Bewertung offenzulegen, sowie diese, sofern anlasslos gespeichert, zu löschen,

c) zu erteilen, welche „Off-F.-Daten“ durch die Beklagte an der IP-Adresse der Klägerseite gesammelt wurden und zu welchem Zweck diese gespeichert und verwendet wurden, sowie diese, sofern anlasslos gespeichert, zu löschen,

d) zu erteilen, in welcher konkreten Hinsicht die Klägerseite von der Übermittlung der personenbezogenen Daten der Klägerseite in die USA, insbesondere an die dortige National Security Agency (NSA) betroffen war, also wer wann auf welche Daten der Klägerseite zugegriffen hat und welche genauen personenbezogenen Daten der Klägerseite von wem eingesehen wurden.

9. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.398,25 EUR gegenüber der Fachanwaltskanzlei Seehofer frei – zustellen.

14
Die Beklagte beantragt,

Klageabweisung.

15
Sie rügt die Unbestimmtheit der Klageanträge und fehlendes Feststellungsinteresse und Rechtsschutzbedürfnis 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.

16
Die Beklagte trägt des Weiteren vor, sie behandle alle über den Messenger-Dienst übertragenen Nachrichten vertraulich. Die ePrivacy-Richtlinie werde von der Beklagten befolgt. Die Beklagte führe gemäß Art. 3 der CSAM-Verordnung ein sog. CSAM-Scanning durch, um kinderpornographische Inhalte zu identifizieren. Die Datenverarbeitung im Zusammenhang mit dem Messenger-Dienst werde in der Datenschutzrichtlinie der Beklagten dargelegt.

„Off-F.-Daten“, also Informationen über Aktivitäten außerhalb der M.-Technologien, erhalte die Beklagte von Drittanbietern, welche dafür verantwortlich seien, dass die Erfassung und Übermittlung von Daten auf einer gültigen Rechtsgrundlage beruhe, insbesondere eine etwa erforderliche Einwilligung einzuholen. Zusätzlich verwende die Beklagte die Daten nur, wenn der Nutzer über ein Cookie-Banner zugestimmt habe, es sei denn die Verarbeitung sei für Zwecke der Sicherheit und Integrität erforderlich. Die Einstellungen könnten nachträglich geändert werden.

17
Die Übermittlung von Daten durch die Beklagte an die M. Platforms, 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. Gezielte Anfragen von US-Regierungsbehörden nach Section 702 des Foreign Surveillance Act (FISA) würden vor Beantwortung auf Rechtmäßigkeit geprüft. Da es der M. Platforms, Inc. nach US-amerikanischem Recht untersagt sei, Informationen über derartige Anfragen offenzulegen, sei auch die Beklagte hierzu nicht verpflichtet.

18
Die Beklagte rügt die fehlende Bestimmtheit der Klageanträge und das fehlende Rechtsschutzbedürfnis bzw. Feststellungsinteresse der Klagepartei. Sie erhebt die Einrede der Verjährung.

19
Das Gericht hat zur Sache am 12.02.2024 mündlich verhandelt und die Klagepartei informatorisch angehört (Bl. 404/406 d.A.).

20
Zur Ergänzung und Vervollständigung des Tatbestandes wird auf die gewechselten Schriftsätze nebst Anlagen sowie die Sitzungsniederschrift Bezug genommen.

Entscheidungsgründe

21
Die teilweise unzulässige Klage ist vollumfänglich unbegründet.

A.

22
Die Klage ist nur teilweise zulässig.

I. Zuständigkeit

23
Das Landgericht Passau ist sachlich 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.

II. „Scraping-Vorfall“

24
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.

25
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 Klägerseite (…) 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.

26
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 Veröf1 O 616/23 – Seite – fentlichung bestimmt hat. Ein künftiger, den behaupteten Pflichtverletzungen der Beklagten zurechenbarer Schaden ist bei dieser Sachlage vernünftigerweise nicht zu erwarten.

27
4. Die Unterlassungsanträge sind hinlänglich bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Soweit darin Bezug genommen wird auf den „Stand der Technik“ handelt es sich hierbei um den Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt; Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein (BMJ, Handbuch der Rechtsförmlichkeit, 3. Aufl., Teil B, Ziff. 4.5.1, Rn. 256). Der genaueren Beschreibung der nach diesen Grundsätzen zu erwartenden Sicherheitsmaßnahmen bedurfte es nicht.

28
5. Hinsichtlich der Unterlassungsanträge kann das Gericht jedoch kein Rechtsschutzinteresse erkennen. Der Klagepartei steht ein einfacherer Weg zur Verfügung, um das mit diesen Anträgen gewünschte Ziel zu erreichen. Sie kann in den Suchbarkeitseinstellungen bezüglich der Telefonnummer „nur ich“ wählen oder die Telefonnummer gänzlich löschen. Dadurch kann sie die Verarbeitung der Telefonnummer in der von ihr missbilligten Weise unterbinden. Ein rechtlich geschütztes Interesse daran, dass die Beklagte die Klagepartei so behandelt, als wäre bei den Suchbarkeitseinstellungen „nur ich“ eingestellt, obwohl die Klagepartei diesen ihr jedenfalls aufgrund der Aufbereitung im gegenständlichen Rechtsstreit positiv bekannten und einfach zu beschreitenden Weg nicht gehen will, vermag das Gericht nicht zu sehen (so auch LG Osnabrück GRUR-RS 2023, 3281).

III. Messenger-Dienst, „Off-F.-Daten“, Datenübermittlung in die USA

29
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 2. wird zur Begründung Bezug genommen.

30

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 seine Messenger-Nachrichten überwacht, Off-F.-Daten verarbeitet und Daten in die USA übermitteln sollte, ist für das Gericht nicht vorstellbar und wird auch nicht plausibel dargelegt.

31
3. Der Unterlassungsantrag zu Ziff. 7 a) der Klageanträge ist nicht hinlänglich bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Das Wort „anlasslos“ schränkt das Unterlassungsbegehren in objektiv nicht abgrenzbarer Weise ein. Ein entsprechender Ausspruch wäre nicht vollstreckungsfähig.

32
4. Hinsichtlich des Unterlassungsantrags zu Ziff. b) fehlt der Klagepartei das Rechtsschutzbedürfnis. Die Klagepartei hat die Möglichkeit, über die Einstellungen die Behandlung der „Off-F.-Daten“ bzw. „Aktivitäten außerhalb der M.-Technologien“ selbst zu steuern. Dies muss der Klagepartei spätestens aufgrund des Beklagtenvortrags im Rechtsstreit auch bekannt sein. Da ihr ein einfacherer Weg zur Erreichung ihres Rechtsschutzziels zur Verfügung steht, fehlt ihr für eine Unterlassungsklage das Rechtsschutzbedürfnis.

33
5. Der Antrag auf Löschung „anlasslos gespeicherter“ Daten (Ziff. 8 b und c der Klageanträge) ist aus den oben unter Ziff. 3 genannten Erwägungen wegen Unbestimmtheit unzulässig.

34
6. Im Übrigen ist die Klage zulässig.

B.

35
Die Klage ist – soweit sie unzulässig ist: jedenfalls auch – unbegründet.

I. Scraping-Vorfall

36
1. Die Klagepartei hat keinen Schadensersatzanspruch gegen die Beklagte aus Art. 82 Abs. 1 DSGVO.

37
a) Es fehlt bereits an einem relevanten Verstoß gegen die Bestimmungen der DSGVO. aa) Die Verarbeitung der klägerischen Daten ist rechtmäßig im Sinne von Art. 6 DSGVO.

38
(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 Telefonnum1 O 616/23 – Seite – mer 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 Suchbarkeitseinstellungen 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.

39
(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.

40
bb) Ein Verstoß gegen das Transparenzgebot (Art. 5 Abs. 1 Buchst. a DSGVO) ist nicht gegeben (s. bereits oben unter Buchst. aa).

41
cc) Es liegt auch kein Verstoß gegen Art. 25 Abs. 2 DSGVO (Datenschutz durch datenschutzfreundliche Voreinstellung) vor.

42
(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, DS-GVO Art. 25 Rn. 18).

43
(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.

44
(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.

45
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.

46
(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).

47
(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 veröffentlichen 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-Vorfalls“ (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 – Seite – 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).

48
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.

49
ff) Sofern die Datenschutzbehörden einen Verstoß der Beklagten gegen die Bestimmungen der DSGVO bejahen sollte, entfaltet diese keine jedenfalls Bindungswirkung für das Gericht.

50

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 Nachrichten über E-Mail, SMS und F.-Messenger erhalten habe sowie Anrufe von Unbekannten, diese auch über WhatsApp, die die Klagepartei nicht beantwortet habe. Die Klagepartei hat ihre Telefonnummer und Anschrift auf der öffentlich zugänglichen Homepage hinterlegt. Die E-Mail-Adresse der Klagepartei ist schon nach ihrem eigenen Vortrag gar nicht in dem sie betreffenden Datensatz enthalten. Für einen kausalen Zusammenhang mit dem durch den „Scraping"-Vorfall nach klägerischem Vortrag veröffentlichen 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. Woraus dieser Schaden konkret rühren soll, ist aus dem Vortrag der Klagepartei nicht zu entnehmen.

51
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.

52
3. Die geltend gemachten Unterlassungsansprüche ergeben sich nicht aus entsprechender Anwendung von § 1004 BGB in Verbindung mit dem Recht auf informationelle Selbstbestimmung und den Vorschriften der DSGVO.

53
a) Es liegt bereits kein Verstoß gegen Vorschriften der DSGVO vor, der einen Unterlassungsanspruch zu begründen geeignet wäre (s.o. Ziff. 1. a).

54
b) Der Unterlassungsantrag zu Ziffer 4. a) der Antragsformel, der darauf gerichtet ist, die Beklagte zu verpflichten, es zu unterlassen, personenbezogene Daten der Klägerseite über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern, scheitert auch daran, dass die Klagepartei es selbst in der Hand hat, durch Anpassung ihrer Einstellungen über die Verarbeitung ihrer Daten zu disponieren. Die Klagepartei weiß spätestens seit dem gegenständlichen Rechtsstreit, wie die Suchbarkeitseinstellung funktioniert. Sie kann jederzeit ihre Telefonnummer löschen oder in den Suchbarkeitseinstellungen insoweit die Option „nur ich" wählen. Wenn sie dies nicht tut und die Dienste der Beklagten gleichwohl weiterhin in Anspruch nimmt, willigt sie in die Datenverarbeitung durch die Beklagte – und zwar in Kenntnis aller Umstände – ein. Dann kann sie nicht mehr mit einem Unterlassungsanspruch gegen Beklagte vorgehen.

55
c) Hinsichtlich des Unterlassungsantrags zu Ziffer 4. b), der darauf gerichtet ist, die Beklagte zu verpflichten, es zu unterlassen, die Telefonnummer der Klägerseite auf Grundlage einer auf nicht hinlänglicher Information beruhenden Einwilligung zu verarbeiten, gilt insoweit das Nämliche: Die Klagepartei kann nicht einerseits ihre Einstellungen so belassen wie sie sind und andererseits von der Beklagten verlangen, dass sie die Daten nicht auf Basis dieser Einstellungen verarbeitet (so im Ergebnis auch LG Bielefeld GRUR-RS, 2022, 38375).

56
4. 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 19.06.2023 (Anlage B16) 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 DS- GVO 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 19.06.2023 (Anlage B16) 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.

Messenger-Dienst, „Off-F.-Daten", Datenübermittlung in die USA

57
1. Der Klagepartei stehen keine Ansprüche gegen die Beklagte im Zusammenhang mit den behaupteten Vorwürfen hinsichtlich des F.-Messenger-Dienstes zu. Es fehlt bereits an einem relevanten Verstoß gegen die Bestimmungen der DSGVO.

58
Die Klagepartei hat nicht schlüssig dargelegt, woraus sich ergeben soll, dass die Beklagte die über den F.-Messenger-Dienst ausgetauschten Inhalte systematisch automatisiert überwacht im Sinne eines „crawlings" der Inhalte. Aus der Datenschutzrichtlinie der Beklagten ergibt sich solches jedenfalls nicht. Die Beklagte hat vielmehr plausibel dargelegt, dass sie die übertragenen Nachrichten entsprechend der gesetzlichen Vorgaben, insbesondere der ePrivacy-Richtlinie, behandelt und ein zulässiges CSAM (child sexual abuse material)-Scanning zur Identifikation kinderpornographischer Inhalte durchführt. Soweit die Klagepartei die Länge und Unübersichtlichkeit der Datenschutzrichtlinie der Beklagten rügt, lässt sich kein Verstoß gegen Art. 13, 14 DSGVO erkennen. Die umfangreichen datenschutzrechtlichen Anforderungen, die von Rechts wegen an die Beklagte gestellt werden, in Verbindung mit der Komplexität der von der Beklagten zur Verfügung gestellten Dienstleistungen lassen keine knappere oder einfachere Darstellung der datenschutzrechtlichen Rahmenbedingungen zu. Dass die Beklagte die über den Messenger-Dienst ausgetauschten Inhalte als solche speichert und an den Adressaten übermittelt, ist zur Bereitstellung dieser Dienstleistung unumgänglich, Art. 6 Abs. 1 Buchst. b DSGVO. Für einen Verstoß gegen das Gebot der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) sieht das Gericht deswegen ebenfalls keine Anhaltspunkte. Das CSAM-Scanning ist von Art. 6 Abs. 1 Buchst. f DSGVO gedeckt. Im Übrigen ist es der Klagepartei – wie jedem „f."-Nutzer selbst überlassen, ob sie den Messenger-Dienst überhaupt verwenden will oder nicht.

59
2. Der Klagepartei stehen auch keine Ansprüche gegen die Beklagte im Zusammenhang mit den behaupteten Vorwürfen hinsichtlich der „Off-F.-Daten" zu.

60
a) Auch insoweit ist kein datenschutzrechtlicher Verstoß ersichtlich. Die Verarbeitung von Daten im Zusammenhang mit „Aktivitäten außerhalb der M.-Technologien" („Off-F.-Daten") ist durch die Einwilligung des Nutzers gedeckt, Art. 6 Abs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a DSGVO. Nach dem Vortrag der Beklagten, an dessen Richtigkeit das Gericht keine Zweifel hat, holt sie die Einwilligung der Nutzer mittels eines im Schriftsatz vom 15.01.2024 auf S. 11 abgebildeten Cookie-Banners ein. Die entsprechenden Einstellungen werden durch Hinweise nachvollziehbar beschrieben und können vom Benutzer nachträglich abgeändert werden. Die Klagepartei ist bei „f." angemeldet, so dass sie selbst die entsprechenden Einstellungen vornehmen kann. Wie es sich bei Personen verhält, die nicht bei „f." angemeldet sind, kann dahinstehen, weil die Klagepartei nicht zu diesem Personenkreis gehört. Dass die Schaltfläche „Alle Cookies erlauben" blau eingefärbt ist, stellt keinen Verstoß gegen Art. 25 Abs. 2 DSGVO (datenschutzfreundliche Voreinstellung) dar. Denn es handelt sich um keine „Voreinstellung", sondern um eine übliche und erlaubte optische Hervorhebung, die die aktive Entscheidungsmöglichkeit des Nutzers unberührt lässt. Soweit die Beklagte Informationen von Cookies und ähnlichen Technologien von Dritten erhält, verarbeitet sie sie nach eigenen Angaben ohne Zustimmung des Nutzers nur zu Sicherheits- und Integritätszwecken, was durch Art. 6 Abs. 1 Buchst. b ff. DSGVO bzw. Art. 9 Abs. 2 Buchst. b ff. DSGVO gedeckt ist. Substanziell Entgegenstehendes wurde durch die Klagepartei nicht in den Rechtsstreit getragen.

61
b) Soweit die Beklagte bis zum Beschluss des Bundeskartellamts vom 06.02.2019 (s. Pressemitteilung vom 07.02.2019, Anlage K-E-4) die „Off-F.-Daten“ ohne eine erforderliche Einwilligung verarbeitet haben sollte, wird schon nicht vorgetragen, dass die Beklagte „Off-F.-Daten“ aus diesem Zeitraum bezogen auf die Klagepartei überhaupt noch vorhält. Im Übrigen wären daraus resultierende Ansprüche der Klagepartei jedenfalls verjährt, §§ 195, 199 Abs. 1, 214 Abs. 1 BGB. Die Klagepartei musste jedenfalls infolge der vorgenannten Pressemitteilung die tatsächlichen Anspruchsvoraussetzungen kennen oder sich dem Vorwurf grob fahrlässiger Unkenntnis aussetzen. Verjährung wäre somit zum Ende des Jahres 2022 eingetreten.

62
3. Der Klagepartei stehen schließlich keine Ansprüche gegen die Beklagte im Zusammenhang mit den behaupteten Vorwürfen im Zusammenhang mit der Datenübermittlung in die USA zu.

63
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 konzi1 O 616/23 piert. 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 USamerikanischen „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.

64
b) Die Datenübermittlung ist daher grundsätzlich zur Vertragserfüllung erforderlich, Art. 6 Abs. 1 Buchst. b DSGVO. Dafür dass die Beklagte, was die Klagepartei letztlich behauptet, darüber hinaus ihren gesamten Datenbestand dem amerikanischen Auslandsgeheimdienst voraussetzungslos zur freien Verfügung stellt, gibt es keine hinreichenden tatsächlichen Anhaltspunkte. Was die USamerikanische Regierung insoweit „zugegeben“ haben soll, wird klägerseits nicht konkret dargelegt. Die Beklagte jedenfalls hat solches bestritten und Beweis wurde klägerseits nicht geführt.

65
c) Die Voraussetzungen für die Datenübermittlung in Drittländer nach Kapitel V DSGVO werden von der Beklagten eingehalten.

66
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.

67
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. Die Klagepartei rügt insoweit, dass der USamerikanische Rechtsbehelfsmechanismus auf einer Verordnung der Regierung und nicht auf formellem Gesetz beruhe. Auch bei einer Verordnung handelt es sich aber um ein Gesetz im materiellen Sinne. Wieso hierdurch kein gleichwertiger Rechtsschutz zur Verfügung gestellt werden kön1 O 616/23 ne, ist nicht zu erkennen.

68
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.

69

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

70
d) Für eine Verletzung von Art. 5 Abs. 1 Buchst. f bzw. Art. 32 DSGVO ist schlüssig nichts vorgetragen. Wieso Anlass zur Annahme bestehen sollte, dass die Beklagte die Daten der Klagepartei in technischer oder organisatorischer Hinsicht nicht hinlänglich schützt, ergibt sich aus dem Klagevortrag nicht.

71
e) Eine Verletzung von Art. 13 DSGVO kann das Gericht ebenfalls nicht erkennen. Die Beklagte hat die Fundstellen genannt, unter denen sich der Nutzer über die Notwendigkeit der Datenübermittlung an ausländische Unternehmen, namentlich die M. Platforms, Inc., wie auch über die Beauskunftung von Regierungsanfragen informieren kann. Dass die Beklagte ihrer Informationspflicht nicht nachgekommen wäre, ist nicht ersichtlich.

72
f) Soweit US-Regierungsbehörden einschließlich der Geheimdienste von M. Platforms, Inc., 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 Buchst. c DSGVO (Erfüllung einer rechtlichen Verpflichtung) zulässig wäre.

73
4. Für einen Schadensersatzanspruch aus Art. 82 DSGVO fehlt es zudem an einem kausalen Schaden der Klagepartei. Diese gab im Rahmen ihrer informatorischen Anhörung lediglich an, dass sie erst durch die Klägervertreter auf etwaige Datenschutzverstöße im Zusammenhang mit dem F. Messenger gebracht worden sei. Diesen nutze sie nicht aktiv, sondern sie antworte nur, wenn sie von Bekannten darüber angeschrieben werde. Von irgendwelchen Ängsten berichtete die Klagepartei nichts, ebensowenig von irgendwelchen sonstigen Folgen. Für einen Schaden der Klagepartei ist daher nichts ersichtlich.

74
5. Auskunftsansprüche nach Art. 15 DSGVO stehen der Klagepartei gegen die Beklagte nicht zu.

75
a) Soweit begehrt wird Auskunft bezüglich der Daten „aus der Überwachung des F.-Messengers“ zu erteilen, „Chat-Protokolle vorzulegen und deren interne Bewertung offenzulegen“, können die Chat-Verläufe durch die Klagepartei selbst heruntergeladen werden, wie von der Beklagten in ihrem vorgerichtlichen Schreiben (Anlage B33) umfassend beschrieben wird. Der Auskunftsanspruch ist dadurch erfüllt, § 362 Abs. 1 BGB. Was unter einer „internen Bewertung“ zu verstehen sein soll, erschließt sich dem Gericht nicht; eine Subsumtion unter eine der Kategorien des Art. 15 Abs. 1 DSGVO ist insoweit nicht möglich.

76
b) Soweit Auskunft begehrt wird, welche „Off-F.-Daten“ durch die Beklagte an der IP-Adresse der Klägerseite gesammelt und zu welchem Zweck sie gespeichert und verwendet wurden, verweist die Beklagte in ihrem vorgerichtlichen Schreiben (B33) ebenfalls zu Recht auf die von ihr zur Verfügung gestellte Selbstauskunftsmöglichkeit und hinsichtlich der Verarbeitungszwecke auf eine bestimmte Seite im Hilfebereich. Die Auskunft ist damit erteilt, § 362 Abs. 1 BGB.

77
c) Hinsichtlich etwaiger an die NSA übermittelter Daten kann die Beklagte die Auskunft verweigern, weil zum einen eine Geheimhaltungspflicht nach USamerikanischem Rechts 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, wobei sich letztgenannte Vorschrift entgegen der Auffassung der Klagepartei schon dem Wortlaut nach nicht auf Berufsgeheimnisträger beschränkt. Es versteht sich von selbst, dass die Information, ob und welche Auskünfte an Geheimdienste erteilt werden, ihrem Wesen nach geheimhaltungsbedürftig ist. Im Übrigen erfolgt die Beauskunftung an die NSA nicht durch die Beklagte, sondern durch die M. Platforms, Inc., so dass die Beklagte hinsichtlich eines Auskunftsanspruchs auch nicht passivlegitimiert wäre.

78
6. Die Löschanträge nach Art. 17 DSGVO (Ziff. 8 b und c der Klageanträge) gehen ins Leere, weil sie unter der Voraussetzung gestellt sind, dass die Datenverarbeitung „anlasslos“ erfolgt. Selbst wenn man diesem Begriff die Bedeutung „nicht notwendig“ (Art. 17 Abs. 1 Buchst. a DSGVO), „ohne Rechtsgrundlage“ (Art. 17 Abs. 1 Buchst. b DSGVO), oder „unrechtmäßig“ (Art. 17 Abs. 1 Buchst. d DSGVO) beimessen wollte, liegen diese Voraussetzungen, wie unter Ziffer 1. bis 2. ausgeführt, nicht vor.

79
7. Sämtliche Unterlassungsansprüche scheitern am Fehlen eines Verstoßes gegen die DSGVO, s.o. Ziff. 1 bis 3. Bezüglich der „Off-F.-Daten“ tritt hinzu, dass es der Nutzer selbst in der Hand hat, die diesbezüglichen Einstellungen zu verwalten. Die Klagepartei handelt widersprüchlich, wenn sie die Einstellungen so belässt, wie sie sind, und andererseits von der Beklagten verlangt, die Daten nicht auf Grundlage dieser Einstellungen zu verarbeiten.

80
III. Vorgerichtliche Kosten Mangels zuzusprechender Hauptforderung besteht auch kein Anspruch auf Erstattung vorgerichtlicher Rechtsverfolgungskosten.

C.

81
Die Kostenentscheidung beruht auf § 91 ZPO.

82
Die vorläufige Vollstreckbarkeit ergibt sich aus § 709 ZPO.

83
Die Streitwertfestsetzung beruht auf §§ 39 Abs. 1, 43 Abs. 1, 48 Abs. 1 S. 1 GKG, 3 ZPO.

84
Das Gericht bewertet die Anträge wie folgt:

Ziffer	Wert
1.	2.000,-
2.	1.500,-
3.	1.500,-
4. a)	500,-
4. b)	500,-
4. c)	500,-
5.	2.000,-
6. a)	2.500,-
6. b)	2.500,-
7. a)	2.500,-
7. b)	2.500,-
7. c)	2.500,-
8. a)	500,-
8. b)	500,-
8. c)	500,-
8. d)	500,-