– Beglaubigte Abschrift –

Landgericht Hannover

Im Namen des Volkes

Urteil

13 O 88/23

Verkündet am 20.11.2023

[redacted]

In dem Rechtsstreit

[redacted]

- Kläger -

Prozessbevollmächtigte:
Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB, Eupener Str. 67, 50933 Köln
Geschäftszeichen: 8851/22 nek

gegen

Meta Platforms Ireland Ltd. (vormals: Facebook Ireland Ltd.), vertreten durch die Mitglieder des Board of Directors, Merrion Road, D04 X2K5, Dublin 4, Irland

- Beklagte -

Prozessbevollmächtigte:
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt am Main

hat das Landgericht Hannover – 13. Zivilkammer – durch den Vorsitzenden Richter am Landgericht Fischer als Einzelrichter auf die mündliche Verhandlung vom 09.10.2023 für Recht erkannt:

1. **Die Beklagte wird verurteilt, an den Kläger 500,00 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 01.06.2023 zu zahlen.**

2. **Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die ihm 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, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, 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, personenbezogene Daten des Klägers, namentlich Telefonnummer, Facebook-ID, Familiennamen, Vornamen, 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.**

4. **Im Übrigen wird die Klage abgewiesen.**

5. **Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.**

6. **Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich des Tenors zu Ziffer 1. gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages; im Übrigen gegen Sicherheitsleistung in Höhe von 5.000,00 €. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110% des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.**

und beschlossen:

Der Streitwert wird auf 7.000,00 € festgesetzt.

Tatbestand:

Der Kläger macht Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen einer Verletzung seines Persönlichkeitsrechts durch die Beklagte geltend.

Der Kläger nutzte die von der Beklagten betriebene Social Media Plattform Facebook mit seiner E-Mail-Adresse [redacted] Die Dienste der Beklagten ermöglichen es ihren Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Bei der Registrierung wurden Nutzer aufgefordert, Vor- und Nachnamen, Geburtsdatum, Geschlecht und ein entsprechendes Passwort anzugeben. In dem sich unter den genannten Angaben befindlichen Informationssegment hieß es sodann:

> *„Indem du auf „Registrieren“ klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen (...).“.*

Die genannte Datenrichtlinie – aktualisiert im April 2018 - beinhaltet Informationen dazu, welche der vom Nutzer gemachten Angaben immer öffentlich sichtbar sind und so von jedermann – also auch von Personen außerhalb der Plattform – eingesehen werden können. Hierzu gehören der Name, das Profil- sowie Titelbild, das Geschlecht, der Nutzername und die jeweilige Nutzer-ID. Bezüglich weiterer Ausführungen in der Datenrichtlinie wird auf die Anlagen B9 (Anlagenband Beklagte) verwiesen.

Darüber hinaus stand es den Nutzern frei, weitere Angaben wie z.B. zum Beziehungsstatus, zum Datum des Geburtstags und zu der eigenen Telefonnummer zu machen. Darüber informierte die Beklagte im sog. Hilfebereich, der erklärt, dass und wie Nutzer einstellen können, wer die über die immer öffentlich einsehbaren Angaben hinaus freiwillig getätigten Informationen einsehen kann (sog. Zielgruppenauswahl). Weiter wurde darüber informiert, für welche Personengruppe Nutzer anhand ihrer Telefonnummer – sofern sie hierzu im Bereich der Kontaktinformationen Angaben tätigten – im Netzwerk auffindbar sind (sog. Suchbarkeits-Einstellungen). Die Standardkonfiguration der Suchbarkeit war dabei auf „Everyone“ voreingestellt, so dass alle Personen, denen die Telefonnummer einer Nutzerin oder eines Nutzers bekannt war, diesen hierüber auch im Netzwerk finden konnten.

Die Einstellung für das Nutzerkonto die Klägerin war seit dem 13.08.2014 auf „Everyone“ gestellt (auf Anlage B17 Anlagenband Beklagte wird wegen der Einzelheiten verwiesen).

Die Beklagte betreibt neben der Facebook-Website eine Messenger-App, die von Facebook-Nutzern verwendet werden kann, um sich gegenseitig Nachrichten zu schicken. Nutzer melden sich dafür mit ihrem Facebook-Profil an. Die App und die gewöhnlichen Funktionen von Facebook sind über denselben Zugang zum Account verknüpft. Während des relevanten Zeitraums entsprachen die Einstellungen des Klägers zur Zielgruppenauswahl und Suchbarkeit im Messenger denen in seinem Facebook-Konto. Zwischen den Parteien ist streitig, ob es – wie der Kläger es behauptet und die Beklagte es bestreitet – innerhalb des Messengers eigene Einstellungsmöglichkeiten gab, die unabhängig von den Privatsphäre-Einstellungen seines Facebook-Nutzerkontos waren.

Nachdem Dritte bei der Beklagten im relevanten Zeitraum von Januar 2018 bis September 2019 mittels des sog. „Contact-Import-Tool“ Daten von Facebook-Nutzern wie u.a. Nutzer-ID, Name, Vorname, Geschlecht ausgelesen (sog. „Scraping“) und veröffentlicht hatten, berichteten Medien darüber im April 2021.

Mit außergerichtlicher E-Mail vom 04.01.2023 (Anlage K1, Anlagenband Kläger) ließ der Kläger die Beklagte durch seine Prozessbevollmächtigten zur Zahlung von 1.000,- €, zur Unterlassung der rechtswidrigen Verarbeitung der personenbezogenen Daten sowie zur Erteilung einer Auskunft, welche Daten im Zusammenhang mit dem im April 2021 bekannt gewordenen Datenschutzvorfall wann abhandengekommen seien, wo und wann diese verbreitet worden seien, ob die Sicherheitslücke durch mehrere Unbefugte ausgenutzt worden sei und welche Maßnahmen zukünftig zur Vermeidung einer Wiederholung ergriffen würden, innerhalb eines Monats auffordern. Die Beklagte ließ daraufhin mit anwaltlichem Schreiben vom 10.02.2023 Ansprüche zurückweisen und Auskunft erteilen; wegen der Einzelheiten dieses Schreibens wird auf die Anlage B16, Anlagenband Beklagte verwiesen.

Der Kläger ist der Ansicht, ihm stehe ein Schadensersatzanspruch gem. Art. 82 Abs. 1 DSGVO zu. Die Beklagte habe gegen die Informationspflichten aus Art. 13 und 14 DSGVO verstoßen, indem sie ihn nicht im ausreichenden Maße über die Verarbeitung ihn betreffender personenbezogener Daten, insbesondere über die Verwendung und Geheimhaltung seiner Telefonnummer informiert bzw. aufgeklärt habe. Die Nutzer könnten tatsächlich keine sichereren Einstellungen erreichen, weil die Einstellungen zur Telefonnummer zu undurchsichtig und zu kompliziert seien. Weiter habe die Beklagte im Jahr 2019 die personenbezogenen Daten ihrer Nutzer nicht im ausreichenden Maße den Anforderungen der DSGVO entsprechend geschützt und so gegen Art. 32 DSGVO verstoßen. Unabhängig von etwaigen Sicherheitslücken verstoße die Beklagte mit den von ihr vorgenommenen Einstellungen zur Privatsphäre auch gegen die in Art. 25 DSGVO niedergelegten Grundsätze

der „Privacy by Design“ und „Privacy by default“. Die Beklagte habe darüber hinaus weder ihn noch die zuständige Aufsichtsbehörde über den Datenschutzverstoß informiert und sei mithin ihren Informationspflichten gem. Art. 33 und 34 DSGVO und auch seinem Anspruch auf Auskunft aus Art. 15 DSGVO nicht in ausreichendem Maße nachgekommen. Durch die unbefugte Veröffentlichung seiner personenbezogenen Daten habe er einen konkreten ersatzfähigen Schaden erlitten, der darin bestehe, dass er einen erheblichen Kontrollverlust über seine Daten erlitten habe und in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten verbleibe. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen, aber auch in der ständigen Sorge, dass die veröffentlichten Daten von Kriminellen für unlautere Zwecke verwendet werden könnten. Der Kläger erachtet einen Betrag in Höhe von mindestens 1.000,00 € für angemessen.

Aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz aus dem dargestellten Schadensereignis folge auch die Pflicht, zukünftige Schäden, die aufgrund der entwendeten Daten entstünden, zu tragen.

Er habe weiter gem. §§ 1004 analog, 823 Abs. 1 und aus Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO gegen die Beklagte einen Anspruch auf Unterlassung, seine personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen. Gem. Art. 15 DSGVO könne er die geltend gemachte Auskunft beanspruchen.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000 Euro nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz,

2. festzustellen, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite 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 zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, 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 Klägerseite, namentlich Telefonnummer, Facebook-ID, Familiennamen, Vornamen, 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 Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Contact-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird,

4. die Beklagte zu verurteilen, der Klägerseite Auskunft über die Klägerseite 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 Contact-Import-Tools erlangt werden konnten.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte bestreitet mit Nichtwissen, dass der Kläger bei der Beklagten jemals ein Konto unterhalten habe, sie habe ihn anhand der angegeben Facebook-ID und beider E-Mail-Adressen nicht zuordnen können; auch anhand der E-Mail-Adresse „m.roj@m-roj.de“ lasse sich ein Facebook-Konto des Klägers nicht identifizieren und sei die Nutzer-ID auch nicht mit der E-Mail-Adresse [redacted] verknüpft. Die Beklagte meint weiter, der Kläger habe nicht substantiiert dargetan, welche Daten gescrapt worden sein sollen. Der Beklagten sei kein Datenschutzverstoß vorzuwerfen, sie habe es auch nicht unterlassen, technische Schwachstellen zu schließen. Der Kläger unterliege zum sog. Scraping einem Missverständnis. Das Ausmaß, in dem Nutzerdaten durch Scraping abgerufen werden konnten, habe von den Privatsphäre-Einstellungen des jeweiligen Nutzers abgehangen. Es seien nur öffentlich einsehbare Daten entweder von der App oder der Website durch Dritte automatisch gesammelt

und an anderer Stelle erneut zugänglich gemacht worden. Das sei nach ihren Nutzungsbedingungen untersagt gewesen und noch immer untersagt. Sie stelle allen Nutzern und auch dem Kläger alle in Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung, die sie zum Zeitpunkt der Datenerhebung im Anwendungsbereich der Datenrichtlinie durchführe. Sie ist daher der Ansicht, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe der Kläger jederzeit anpassen können.

Sie habe nicht gegen Art. 24, 32 DSGVO verstoßen, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen, um das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen. Es fehle konkreter Vortrag, welche Maßnahmen in welchem Umfang nicht genügen würden. Außerdem müsse eine solche Beurteilung ex ante und nicht ex post erfolgen. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe bei dieser Bewertung auch der zentrale Zweck von Facebook, sich mit Freunden, Familien und Gemeinschaften zu verbinden, berücksichtigt werden. Eine Melde- oder Benachrichtigungspflicht, habe nicht bestanden, da es an einer Verletzung der Sicherheit i. S. d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Schließlich fehle es an einem immateriellen Schaden. Art. 82 DSGVO umfasse schon keine Verstöße gegen Art. 13-15, 24, 25 DSGVO. Zudem fehle es an einem Verstoß gegen Art. 82 DSGVO. Ein kompensationsgeeigneter messbarer Schaden sei auch nicht dargelegt. Selbst bei einem angenommenen vorübergehenden Kontrollverlust über personenbezogene Daten des Klägers wäre dies nicht ihr zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe. Schließlich fehle es an einer schlüssigen Darlegung der Kausalität.

Die Klage ist der Beklagten am 31.05.2023 zugestellt worden.

Die Kammer hat den gem. Verfügung vom 25.08.2023 (Bl. 107 f. d.A.) persönlich geladenen Kläger im Termin am 09.10.2023 angehört; wegen des Ergebnisses der Anhörung wird auf das Protokoll der mündlichen Verhandlung verwiesen (Bl. 187 ff. d.A.).

Entscheidungsgründe:

I.

Die zulässige Klage ist in dem tenorierten Umfang begründet.

A. Die Klage ist zulässig.

1. Das Landgericht Hannover ist örtlich und sachlich, insbesondere aber auch international zuständig. Diese internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO (Brüssel Ia- VO). Es handelt sich vorliegend um eine Zivilsache, auf die die EuGVVO sachlich anwendbar ist, Art. 1 Abs. 1 EuGVVO. Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO. Die Klage eines Verbrauchers – ein solcher ist der Kläger gem. Art. 17 Abs. 1 EuGVVO – kann gegen den anderen Vertragspartner vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat, erhoben werden. Der Kläger hat seinen Wohnsitz in Wunstorf und damit im Bezirk des Landgerichts Hannover.

Danach kommt es nicht mehr darauf an, dass sich die internationale Zuständigkeit deutscher Gerichte auch aus Art. 79 Abs. 2 DSGVO ergibt.

2. Der Klageantrag zu 1. ist hinreichend bestimmt, § 253 Abs. 2 ZPO. Der Kläger hat seine Begehrensvorstellung ebenso angegeben wie er die Berechnungs- bzw. Schätzgrundlagen vorgetragen hat. Entgegen der Auffassung der Beklagten liegen dem Antrag auch nicht zwei Streitgegenstände zugrunde (Verhalten der Beklagten vor dem Scraping und die Verletzung von Benachrichtigungspflichten danach).

3. Der Kläger hat sein Feststellungsinteresse bezüglich des Antrags zu 2. hinreichend dargelegt. Ein Feststellungsantrag ist schon zulässig, wenn – wie hier - die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann. Nach der vom Kläger vorgetragenen Nutzung seiner gescrapten Daten ist zumindest nicht ausgeschlossen, dass ihm auch in Zukunft irgendein materieller oder immaterieller Schaden durch die unbefugte und unkontrollierte Verwendung der Daten entstehen könnte.

4. Schließlich ist auch der mit dem Antrag zu 4. geltend gemachte Unterlassungsantrag hinreichend bestimmt. So mag die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ – auch im Fall einer Zwangsvollstreckung - auslegungsbedürftig sein. Zur Gewährleistung effektiven Rechtsschutzes ist das indes hinzunehmen (BGH, GRUR 2015, 1237, Rn. 15, BGH NJW 2004, 2080). So wird der Kläger als Laie nicht einschätzen können, was die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen beinhalten und es wäre im Hinblick auf das Gebot der Effektivität des Rechtsschutzes aus Art. 19 GG verfehlt, vom Kläger zu verlangen, für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst ermitteln zu müssen.

B. Die Klage ist (nur) teilweise begründet.

I. Zum Zahlungsantrag zu 1.

1. Der Kläger hat einen Anspruch auf Schadensersatz in Höhe von 500,00 € aus Art. 82 DSGVO.

a. Die Beklagte hat – wie das LG Lüneburg im Urteil vom 24.01.2023, Az. 3 O 83/22 (veröffentlicht: dejure.org) ausführt -

> *„… als Verantwortliche nach Art. 4 Nr. 7 DS-GVO gegen die Vorschriften der DS-GVO verstoßen. Die Beklagte hat keine geeigneten technischen und organisatorischen Maßnahmen getroffen, um die personenbezogenen Daten der klagenden Partei zu schützen (dazu unter aa. und bb.). Über das Vorliegen der weiteren von der klagenden Partei behaupteten Verstöße der Beklagten gegen die DS-GVO braucht die Kammer nicht zu entscheiden (dazu unter cc.).*
>
> *aa) Die Beklagte hat gegen die ihr gemäß Art. 25 Abs. 1 DS-GVO auferlegte Obliegenheit verstoßen, geeignete Maßnahmen zu treffen, um die Rechte der klagenden Partei und ihre personenbezogenen Daten zu schützen.*
>
> *Nach Art. 25 Abs. 1 DS-GVO hat der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*
>
> *Unter Verarbeitung fällt nach Art. 4 Nr. 2 DS-GVO u.a. die Offenlegung personenbezogener Daten durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Hiervon werden alle Vorgänge erfasst, durch die der Verantwortliche personenbezogene Daten anderen Stellen in der Weise zugänglich macht, dass diese Kenntnis vom Informationsgehalt der betreffenden Daten erlangen können (Kühling/Buchner/Herbst, DS-GVO BDSG, 3. Auflage 2020, DS-GVO Art. 4 Nr. 2, Rn. 29).*
>
> *Unter personenbezogenen Daten versteht man nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person*

beziehen. Die durch das Scraping unstreitig abgegriffenen Daten der klagenden Partei betrafen jedenfalls die Telefonnummer und den Vor- und Nachnamen der betroffenen Person. Damit ist es möglich, die klagende Partei zu identifizieren. Es handelt sich mithin um personenbezogene Daten.

Eine Verarbeitung im vorgenannten Sinne liegt vor. Das von der Beklagten zur Verfügung gestellte Kontakt-Importer-Tool ermöglichte es unbekannten Dritten, mit den von den Dritten eingegebenen Telefonnummern Nutzerprofile aufzufinden und die darauf befindlichen öffentlich einsehbaren, personenbezogenen Daten der Nutzer abzugreifen und mit der eingegebenen Telefonnummer zu verknüpfen. Das Kontakt-Importer-Tool konnte von jedermann genutzt werden, mit der Folge, dass die Beklagte durch die Ausgestaltung dieses Tools die Daten ihrer Nutzer zum Abruf durch Dritte grundsätzlich ermöglichte und jedermann zugänglich machte.
Die von der Beklagten implementierten Sicherheitsmaßnahmen waren nicht ausreichend, um die Rechte der klagenden Partei und ihre personenbezogenen Daten insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung durch Dritte zu schützen. Dabei kann dahinstehen, ob die Beklagte die von ihr behaupteten Maßnahmen zur Bekämpfung von Scraping tatsächlich ergriffen hat, denn diese Maßnahmen waren jedenfalls für sich allein nicht geeignet, einen angemessenen Schutz der personenbezogenen Daten der klagenden Partei zu gewährleisten.

Die (angeblich) von der Beklagten implementierten Maßnahmen in Form von Ratenbegrenzung und Bot-Erkennungsmaßnahmen waren für die Zwecke des Art. 25 Abs. 1 DS-GVO nicht ausreichend, weshalb die Beklagte gegen Art. 25 Abs. 1 DS-GVO verstoßen hat. Insoweit befindet sich die Kammer im Einklang mit der irischen Datenschutzbehörde, die ebenfalls der Beklagten vorwirft, keine hinreichenden Sicherheitsmaßnahmen getroffen und damit gegen Art. 25 Abs. 1 DS-GVO verstoßen zu haben. Dabei berücksichtigt die Kammer, dass Scraping weit verbreitet und damit zum Zeitpunkt des Vorfalls unstreitig auch ein der Beklagten bekanntes Risiko gewesen ist. Hinsichtlich der von der Beklagten eingesetzten Übertragungsbeschränkungen war es nach dem eigenen Vortrag der Beklagten möglich, diese Beschränkungen zu umgehen. Trotz Kenntnis dieser Möglichkeit und auch des grundsätzlichen Risikos von „Scraping“ hat es die Beklagte indessen unterlassen, weitergehende Maßnahmen zu treffen, was hier nach Auffassung der Kammer jedoch notwendig gewesen wäre. Es wäre für die Beklagte beispielsweise möglich gewesen, das Kontakt-Importer-Tool derart auszugestalten, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern erfolgen kann. Das Tool hätte beispielsweise neben der Telefonnummer weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachname berücksichtigen können.

Dies vor allem deshalb, weil Nutzer die Telefonnummern häufig mit dem dazugehörigen Klarnamen ihres Kontakts abspeichern. Entsprechend hat die Beklagte die Funktionsweise des Tools nach Bekanntwerden des Vorfalls auch umgestaltet.“

Die Kammer schließt sich dem für den vorliegenden Fall an.

b. Weiter hat die Beklagte auch gegen Art. 25 Abs. 2 DSGVO verstoßen, indem sie keine geeigneten technischen und organisatorischen Maßnahmen getroffen hat, die sicherzustellen geeignet waren, dass personenbezogene Daten aufgrund der Voreinstellungen nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Die Suchbarkeit umfasste automatisch die Telefonnummer der Nutzer. Die Suchbarkeits-Einstellungen hatte die Beklagte im hier relevanten Zeitraum auf „Everyone“ voreingestellt, so dass Dritte mit der Telefonnummer nach einem Nutzerprofil suchen und über das Contact-Importer-Tool eine Verknüpfung zwischen Telefonnummer und dazugehörigem Nutzerprofil herstellen konnten. Das galt nur dann nicht, wenn der Nutzer nach seiner Registrierung die entsprechende Suchbarkeits-Einstellung in seinen Privatsphäre-Einstellungen aktiv änderte. Mit der Bereitstellung dieses Systems machte die Beklagte die personenbezogenen Daten des Klägers ohne dessen Eingreifen einer unbestimmten Anzahl von Personen zugänglich (vgl. LG Lüneburg a.a.O.).

c. Darauf, ob die Beklagte auch gegen Art. 5 Abs. 1 lit. a. DSGVO verstoßen hat, weil der Kläger zu seiner Auffindbarkeit keine Einwilligung gemäß Art. 6 Abs. 1 lit. a, Art. 7 Abs. 1 DSGVO erteilt hat, kommt es danach nicht mehr an.

2. Der Kläger hat einen immateriellen Schaden durch diese rechtswidrige Datenverarbeitung erlitten, für dessen Ausgleich die Kammer einen Betrag in Höhe von 500,00 € für angemessen erachtet.

a. Soweit zwar einerseits nicht allein der bloße Verstoß gegen die Bestimmungen der DSGVO zur Begründung eines Schadensersatzanspruchs ausreicht, so bedarf der erlittene Schaden andererseits nicht eines bestimmten Grades an Erheblichkeit (EuGH, Urteil vom 04.05.2023 – C-300/21 -, Rdnrn. 51, 59, curia.europa.eu). In den Erwägungsgründen 75 und 85 zur DSGVO werden einige mögliche Schäden aufgezählt, darunter Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, aber auch der Verlust der Kontrolle über die eigenen Daten sowie die Erstellung unzulässiger Persönlichkeitsprofile. Zudem benennt Erwägungsgrund 75 auch die bloße Verarbeitung einer großen Menge personenbezogener Daten einer großen Anzahl von Personen. Der Schaden ist zwar weit zu verstehen, er muss jedoch auch wirklich „erlitten“ (ErwGr. 146 S. 6) sein.

Die aufgezeigten Verstöße gegen die DSGVO sind auch kausal für den vom Kläger erlittenen Schaden.

Dazu führt das LG Paderborn mit Urteil vom 19.12.2022 – 3 O 99/22 – (unter Rn. 135 - 140, juris) aus:

> *„Der Verantwortliche haftet lediglich für kausal durch die rechtswidrige Verarbeitung verursachte Schäden (…). Eine Mitursächlichkeit des Verstoßes genügt (…).*
>
> *a) Die Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO ist kausal für den bei dem Kläger entstandenen Schaden. Gemäß vorstehender Erwägungen hat die Beklagte den Kläger bereits bei Erhebung seiner Mobilfunknummer nur unzureichend über die Verwendung seiner Mobilfunknummer im Hinblick auf das CIT aufgeklärt, sodass bezogen auf die Mobilfunknummer eine rechtswidrige Verarbeitung vorliegt. Diese ist auch kausal für den beim Kläger entstandenen Schaden, da es durch die Verwendung des CIT zu einem Kontrollverlust auf Seiten des Klägers kam.*
>
> *b) Auch der Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DSGVO ist für den eingetretenen Schaden kausal, denn durch die unzureichenden Schutzmaßnahmen ermöglichte bzw. erleichterte der Beklagten ein Ausnutzen des CIT durch "Scraping". Dieses hat einen Kontrollverlust über die personenbezogenen Daten zur Folge.*
>
> *c) Der Schaden beruht zudem kausal auf einem Verstoß gegen Art. 33 und Art 34 DSGVO. Zwar ist der geltend gemachte Kontrollverlust bereits durch das "Scraping" der Daten erstmals eingetreten. Durch die unterlassene Benachrichtigung des Klägers wurde ihm jedoch die Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren. Auch die zuständige Datenschutzbehörde konnte mangels rechtzeitiger Meldung keine Schritte zur Risikominimierung und Absicherung der Daten einleiten.“*

Die Kammer schließt sich diesen Erwägungen (so auch LG Lübeck, Urteil vom 25.05.2023 – 15 O 74/22 –, Rn. 107 f., juris) für den vorliegenden Fall übertragen auf die von ihr zugrunde gelegten Verstöße gegen die DSGVO an. Das gilt insbesondere auch dafür, dass bereits der Kontrollverlust für die Annahme eines Schadens ausreicht und es dafür auch keiner Überschreitung einer (zusätzlichen) Erheblichkeitsschwelle bedarf (so auch OLG Düsseldorf, Urteil vom 28.10.2021 – I-16 U 275/20 –, Rn. 51, juris; OLG Hamm, Urteil vom 20.01.2023 – I-

11 U 88/22 –, Rn. 112 ff., juris; a.A. OLG Hamm, Urteil vom 15.08.2023 – I-7 U 19/23 –, Rn. 150 ff., juris).

b. Die Kammer hält auch nach Anhörung des Klägers und dem dabei gewonnenen Eindruck in Ausübung des ihr durch § 287 ZPO eingeräumten Ermessens ein Schmerzensgeld von 500,00 € für angemessen, aber auch ausreichend, um einerseits der Ausgleichs- und Genugtuungsfunktion zu genügen und andererseits der auch generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung zu tragen.

aa. Der Kläger hat der Kammer glaubhaft vermittelt, dass ihn der Verlust der Kontrolle über seine Daten und deren freie Verfügbarkeit im Internet belaste. So hat er gut nachvollziehbar beschrieben, dass es beunruhigend sei, dass dann, wenn das Handy mal eine Spam nicht als solche erkenne und das Ganze glaubwürdig geschrieben sei, doch das Risiko bestehe, dass er einen Link anklicken könnte und das dann Konsequenzen habe, was auch immer dann passieren möge. Weiter hat der Kläger glaubhaft beschrieben, dass er Spams seit dem Vorfall bekomme und seine Betroffenheit auch in einer Datenbank festgestellt habe.

bb. Eine Belastung des Klägers dadurch, dass seine Telefonnummer von unbefugten Dritten verknüpft mit seinem Klarnamen, Geburtsdatum und FacebookID im Internet und ggf. sogar im sog. Darknet frei zur Verfügung gestellt wird, ist auch gut nachvollziehbar. Etwas Anderes folgt auch nicht daraus, dass der Kläger seine Telefonnummer beibehalten hat. Denn die Änderung einer Telefonnummer kann erhebliche Umstände mit sich bringen. Sämtliche Kontakte müssen informiert werden, nicht immer wird man lückenlos wissen, bei wem man seine Nummer platziert hat (Ärzte, Behörden, Dienstleister), ggf. muss der Anbieter gewechselt werden, vertragliche Bindungen zur Laufzeit können eine solche Änderung erschweren oder verzögern. Das gilt gerade auch dann, wenn es sich um eine auch im beruflichen Kontext verwendete und verbreitete Telefonnummer handelt. Im Übrigen bestehen oft auch große Interessen an der Beibehaltung der eigenen Telefonnummer, was nicht umsonst die weitverbreitete Möglichkeit der Rufnummernmitnahme und die Bereitschaft erklärt, dafür (früher sogar ganz erhebliche) Kosten aufzuwenden.

cc. Bei der Bemessung der Schadensersatzhöhe hat die Kammer daneben auch die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes berücksichtigt. Andererseits war aber auch zu berücksichtigen, dass das Allgemeininteresse im Schwerpunkt nach Art. 83 DSGVO durch die Verhängung von Bußgeldern gewahrt wird.

3. Der Kläger kann Prozesszinsen gem. §§ 291, 288 Abs. 1, 187 Abs. 1 (entspr.; vgl. BGH, Urteil vom 10.10.2017 – XI ZR 555/16 –, Rn. 21, juris) BGB, §§ 253 Abs. 1, 261 Abs. 1 ZPO ab dem auf die Zustellung der Klageschrift folgenden Tag verlangen.

II. Zum Feststellungsantrag zu 2.

Auch der Feststellungsantrag ist begründet. Es liegen die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vor. Ein haftungsrechtlich relevanter Tatbestand, der zu möglichen künftigen Schäden führen kann, ist gegeben (vgl. BGH, Beschluss vom 09.01.2007 - VI ZR 133/06, Rn. 6, beck online). Es bedarf im Rahmen der Begründetheit keiner darüberhinausgehender gewissen Wahrscheinlichkeit des Schadenseintritts. Streitgegenständlich sind die nicht von den Bestimmungen der DSGVO gedeckten Übermittlungen oder Verarbeitungen personenbezogener Daten, welche eine Verletzung des allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen können. Es reicht vorliegend bereits die nicht fernliegende Möglichkeit eines Schadens aus, der z.B. bereits darin liegen kann, dass dem Kläger durch einen späteren Wechsel der Telefonnummer Kosten entstehen.

III. Zum Unterlassungsantrag zu 3.a) und b)

Der Kläger kann Unterlassung nur wie mit dem Antrag zu 3.a) begehrt verlangen, im Übrigen aber nicht.

1. Antrag zu 3.a)

aa. Der Anspruch des Klägers folgt aus Art. 17 DSGVO ergeben, sodass dahinstehen kann, ob im Anwendungsbereich der DSGVO auf BGB-Normen zurückgegriffen werden darf.

Art. 17 DSGVO i.V.m Art. 6 DSGVO sieht in der Rechtsfolge ein Recht auf Löschung („Recht auf Vergessenwerden“) vor; nicht hingegen einen Anspruch auf Unterlassung. Nach Art. 17 Abs. 1 DSGVO kann die betroffene Person unter bestimmten Voraussetzungen von dem Verantwortlichen verlangen, dass diese sie betreffende personenbezogene Daten unverzüglich löscht. Die DSGVO definiert hingegen nicht, was unter Löschung zu verstehen ist. Jedoch lässt sich aus dem in Art. 17 Abs. 1 DSGVO normierten Recht betroffener Personen, unter gewissen Umständen vom Verantwortlichen zu verlangen, sie betreffende personenbezogene Daten unverzüglich zu löschen, auch ein Anspruch auf Unterlassung ihrer Verarbeitung für die Zukunft ableiten (Argumentum a maiore ad minus). Dies folgt grundsätzlich auch aus Art. 79 DSGVO, der der betroffenen Person einen „wirksamen gerichtlichen Rechtsbehelf“ zugesteht (LG

Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 143, beck-online). Der Kläger kann von der Beklagten mithin die begehrte Unterlassung verlangen.

bb. Ordnungsmittel sind – wie beantragt – nach § 890 Abs. 2 ZPO anzudrohen.

2. Antrag zu 3.b)

Soweit der Kläger mit dem Antrag zu 3.b) von der Beklagten auch verlangt, es zu unterlassen, seine Telefonnummer auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Contact-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, kann dahinstehen, ob die Beklagte insoweit gegen die DSGVO verstoßen und den Kläger nicht ausreichend nach Art. 13, 14 DSGVO über die Nutzung der mitgeteilten Mobilfunknummer im Zusammenhang mit dem CIT informiert hat. Diese Pflichtverletzung löst nämlich für die Zukunft keine Folgen mehr aus, da der Kläger zumindest im Verlauf des Rechtsstreits sämtliche Informationen erhalten hat, die die fragliche Art und Weise der Datenverarbeitung betreffen (vgl. LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22 –, Rn. 167 - 168, juris). Die Gefahr der Wiederholung einer Verarbeitung der Telefonnummer „auf der Grundlage einer Einwilligung“ und ohne eindeutige Information besteht danach nicht mehr. Hinzu kommt, dass nach dem klägerischen Vortrag die Verarbeitung ohne wirksame Einwilligung erfolgte und eine Verarbeitung auf der Grundlage einer Einwilligung danach ohnehin nicht in Betracht kommt.

IV. Zum Auskunftsanspruch zu 4.

Der Kläger hat keinen Auskunftsanspruch gemäß Art. 15 DSGVO.

1. Der Kläger kann nicht die Auskunft verlangen, welchen Empfängern die Daten des Klägers durch das Scraping bekannt geworden sind. Eine solche Auskunft war der Beklagten weder möglich noch war sie hierzu verpflichtet. Im Hinblick darauf, dass aufgrund des nahezu unendlichen Spektrums der möglichen Empfänger sowie des Umstandes, dass das Scraping als plattform-externer Vorgang stattgefunden hat, ist es für die Beklagte unmöglich, den Informationsfluss zurückzuverfolgen, zumal der Kläger nicht dargelegt hat, in welcher Form eine derartige Information erfolgen könnt; nichts anderes ergibt sich hinsichtlich des Zeitraumes, in welchem die Daten gescraped worden sind; die bloße Angabe des Zeitraumes durch den Kläger von dem Jahr 2019 bis zur Veröffentlichung im April 2021 vermag daran nichts zu ändern, da

die zeitliche Angabe zu unpräzise ist (vgl. LG Itzehoe, Urteil vom 27. Februar 2023 – 10 O 159/22 –, Rn. 81, juris).

2. Eine Verurteilung zu einer weitergehenden Auskunft hat der Kläger mit der Klage nicht begehrt; soweit er seinen Antrag eingangs allgemein formuliert, konkretisiert er diesen sodann („namentlich“) auf das, worauf der nach Vorstehendem keinen Anspruch hat.

II.

Der nachgelassene Schriftsatz der Beklagten vom 30.10.2023 gibt keinen Anlass, die Verhandlung gem. § 156 ZPO wiederzueröffnen.

III.

Die Kostenentscheidung beruht auf § 92 Abs. 1 Satz 1 ZPO; die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 11, 711, 709 ZPO.

IV.

Die Wertfestsetzung findet ihre Grundlage in § 3 ZPO, § 63 Abs. 2 Satz 1 GKG.

1. Für den festzusetzenden Streitwert war bezüglich des angekündigten Klagantrags zu Ziffer 1. der vom Kläger vorgestellte (Mindest-)Schadenersatzbetrag in Höhe von 1.000,00 € zu berücksichtigen.

2. Soweit der Kläger mit dem Klagantrag zu Ziffer 2. die Feststellung begehrt hat, dass die Beklagte verpflichtet ist, ihm (auch) alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten entstanden sind und/oder noch entstehen werden, so kommt diesem Antrag ein eigener wirtschaftlicher Wert zu. Dieser orientiert sich grundsätzlich an den Vorstellungen des Klägers zum Klagantrag zu 1., ist aber nur mit einem Bruchteil zu bemessen, wobei 50% und damit ein Betrag in Höhe von 500,00 € angemessen erscheint (vgl. OLG Stuttgart, Beschluss vom 03.01.2023 – 4 AR 4/22 –, Rn. 23, juris).

3. Mit den angekündigten Klageanträgen zu Ziffer 3.a) und b) hat der Kläger Unterlassung begehrt. Bei diesen nichtvermögensrechtlichen Anträgen ist es ihm darum gegangen, dass seine im Rahmen des Nutzungsverhältnisses mit der Beklagten angegebenen personenbezogenen Daten einschließlich seiner Telefonnummer künftig nicht in die Hände

unbefugter Dritter gelangen, die diese dann ggf. für illegale Aktivitäten nutzen könnten. Der Kläger hat damit effektivere Sicherheitsvorkehrungen bei der Beklagten zu erreichen angestrebt.
Der Streitwert der Unterlassungsanträge ist als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses des Klägers unter Berücksichtigung der Umstände des Einzelfalls zu bestimmen (§ 48 Abs. 2 Satz 1 GKG). Dabei ist in Anlehnung an § 23 Abs. 3 Satz 2 RVG bei mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Streitwert von 5.000,00 € auszugehen und erscheint es unter Berücksichtigung aller Umstände des vorliegenden Einzelfalls angemessen, auf die Gedanken dieser allgemeinen Wertvorschrift zurückzugreifen (vgl. OLG Stuttgart, a.a.O., Rn. 26 f.). So darf bei der Bemessung des Streitwerts das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden (vgl. BGH, Beschluss vom 26.11.2020; III ZR 124/20 Rn. 11), es erscheint unter Berücksichtigung aller Umstände des vorliegenden Einzelfalls (vgl. § 48 Abs. 2 Satz 1 GKG) hier angemessen, auf die Gedanken der allgemeinen Wertvorschrift des § 23 Abs. 3 Satz 2 RVG zurückzugreifen und – auch mangels genügender Anhaltspunkte für ein höheres oder geringeres Interesse - angemessen, von einem Wert von 5.000,00 € für das Unterlassungsbegehren in Summe auszugehen (vgl. OLG Stuttgart, a.a.O., Rn. 28).

4. Dem angekündigten Auskunftsanspruch zu Ziffer 4 ist daneben eine eher untergeordnete Bedeutung beizumessen (vgl. OLG Stuttgart, a.a.O., Rn. 29). Dessen Wert bemisst die Kammer mit einem Betrag in Höhe von 500,00 € (vgl. LG Osnabrück, Urteil vom 03.03.2023 – 11 O 834/22 –, Rn. 45, juris; LG Itzehoe, Urteil vom 27.02.2023 – 10 O 159/22 –, juris; LG Essen, Urteil vom 10.11.2022 – 6 O 111/22 –, Rn. 44, juris).

Rechtsbehelfsbelehrung

Diese Entscheidung kann hinsichtlich der Wertfestsetzung mit der Beschwerde angefochten werden. Sie ist nur zulässig, wenn sie innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache rechtskräftig geworden ist oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Hannover, Volgersweg 65, 30175 Hannover, eingeht. Wird der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung der Festsetzung bei dem Gericht eingelegt werden.
Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200,00 € übersteigt oder das Gericht die Beschwerde in diesem Beschluss zugelassen hat. Beschwerdeberechtigt ist, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist.
Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle des genannten Gerichts eingelegt. Sie kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichts erklärt werden, wobei es für die Einhaltung der Frist auf den Eingang bei dem genannten Gericht ankommt. Sie ist zu unterzeichnen. Die Einlegung kann auch mittels elektronischen Dokuments erfolgen. Informationen zu den weiteren Voraussetzungen zur Signatur und Übermittlung sind auf dem Justizportal des Bundes und der Länder (www.justiz.de) im Themenbereich zur elektronischen Kommunikation zu finden. Eine Einlegung per einfacher E-Mail ist unzulässig. Rechtsanwältinnen, Rechtsanwälte, Behörden und juristische Personen des öffentlichen Rechts einschließlich der zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse sind zur Einlegung mittels

elektronischen Dokuments verpflichtet.
Die Beschwerde muss die Bezeichnung des angefochtenen Beschlusses sowie die Erklärung enthalten, dass Beschwerde gegen diesen Beschluss eingelegt wird. Soll die Entscheidung nur zum Teil angefochten werden, so ist der Umfang der Anfechtung zu bezeichnen.

[redacted]
Vorsitzender Richter am Landgericht

Beglaubigt
Hannover, 22.11.2023

[redacted] Justizangestellte
als Urkundsbeamtin der Geschäftsstelle