4 O 148/22

Verkündet am 11.01.2024

, Justizbeschäftigte

als Urkundsbeamter

der Geschäftsstelle

# Landgericht Dortmund

## IM NAMEN DES VOLKES

## Urteil

In dem Rechtsstreit

des ,

Klägers,

Prozessbevollmächtigte: Rechtsanwälte WBS.LEGAL,
Eupener Straße 67, 50933 Köln,

gegen

Meta Platforms Ireland Limited, vertr. d. d. Gf. Gareth Lambe, 4 Grand Canal , Square Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields, Bruckhaus, Deringer,
Bockenheimer Anlage 44, 60322 Frankfurt,

hat die 4. Zivilkammer des Landgerichts Dortmund
auf die mündliche Verhandlung vom 25.10.2023
durch die Vorsitzende Richterin am Landgericht als Einzelrichterin

für Recht erkannt:

Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 500,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 15.12.2022 zu zahlen.

Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen materiellen und nicht vorhersehbaren immateriellen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten in der Zeit vom 25.05.2018 bis zum 06.09.2019 entstanden sind und/oder noch entstehen werden, soweit die Ansprüche nicht auf Sozialversicherungsträger oder sonstige Dritte übergegangen sind oder übergehen werden.

Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,93 € zuzüglich Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit dem 15.12.2022 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Rechtsstreits tragen der Kläger zu 2/3 und die Beklagte zu 1/3.

Das Urteil ist vorläufig vollstreckbar.

Die Parteien können die Zwangsvollstreckung der Gegenseite durch Sicherheitsleistung i. H. v. 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Gegenseite vor der Zwangsvollstreckung Sicherheit i. H. v. 110% des zu jeweils zu vollstreckenden Betrags leistet.

**Tatbestand**

Der Kläger macht gegen die Beklagte Ansprüche wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (DSGVO) im Zusammenhang mit einem sogenannten "Scraping-Vorfall" geltend.

Die Beklagte betreibt in der Europäischen Union die Social Media-Plattform Facebook, die über die Website www.facebook.com sowie Apps abrufbar ist. Das von der Beklagten auf dieser Seite angebotene soziale Netzwerk ermöglicht es den Nutzern, persönliche Profile zu erstellen und in dem Umfang ihrer so erstellten Präsenz in diesem Netzwerk mit anderen Nutzern in Kontakt zu treten. Der Zugang zu der Plattform erfolgt auf der Grundlage eines Nutzungsvertrages, den die Nutzer durch Betätigung der Schaltfläche "Registrieren" abschließen und - mittlerweile - den Allgemeinen Nutzungsbedingungen zustimmen. Diese verweisen auf die Richtlinien der Beklagten für die Verwendung von Daten und Cookies, mit denen die Beklagte nutzer- und gerätebezogene Daten über Nutzeraktivitäten innerhalb und außerhalb des sozialen Netzwerks erfasst. So sind detaillierte Rückschlüsse auf die Präferenzen und Interessen des Nutzers möglich.

Bei der Registrierung sind bestimmte Informationen über den jeweiligen Nutzer zu hinterlegen, nämlich Vorname, Nachname, Benutzer-ID, Nutzername, Geschlecht. Diese Daten sind im Internet für jedermann sicht- und suchbar, ohne dass der Suchende ein eigenes Nutzerprofil bei der Beklagten anlegen müsste. Wenn der Nutzer weitere Information, wie z.B. die Telefonnummer, den Wohnort, den Beziehungsstatus und/oder den Geburtstag einstellte, waren sie im streitgegenständlichen Zeitraum nur allgemein sichtbar, wenn als Zielgruppe "öffentlich" gewählt worden war. Anstelle der Einstellung "öffentlich" konnten Nutzer auswählen, dass nur "Freunde" oder "Freunde von Freunden" die weiteren Informationen einsehen konnten.

Neben diesem Profil, je nach Zielgruppe sichtbar, stellte die Beklagte in ihren sogenannten Suchbarkeits-Einstellungen Funktionen zur Verfügung, um Kontakte zu finden. Als Standardeinstellung war vorgegeben, dass eine Suchbarkeit durch "alle" („everyone“) möglich sein sollte. Ein registrierter Nutzer war daraufhin in der Lage,

mit der Eingabe einer Telefonnummer in die Suchfunktion einen anderen Nutzer zu finden, selbst wenn dieser die Telefonnummer im Rahmen des Nutzerprofils nicht als "öffentlich" hinterlegt hatte. Ebenso war es über die Kontaktimportfunktion („CIT“ oder „KIT“) für Nutzer möglich, ihre eigenen Kontakte mit Telefonnummern auf die Plattform bzw. den Messenger hochzuladen und so über die Telefonnummer andere Nutzer zu finden/identifizieren.

Wie der - nicht bindenden - Entscheidung der Irischen Datenschutzbehörde (DPC) vom 28.11.2022 (eGA II-299 ff.) zu entnehmen ist, kam es seit spätestens Januar 2018 bis zum 06.09.2019 zu dem das soziale Netzwerk der Beklagten betreffenden "Scraping-Vorfall". Die Scraper machten sich zunächst die Suchfunktion auf der Plattform zu Nutze, indem sie sich unter Vorgabe fremder oder nichtexistierender Identitäten bei der Beklagten als Nutzer registrierten und über die Eingabe von Rufnummern nach den passenden Nutzern suchten und sodann Telefonnummer und Nutzer zuordneten. Diese Funktion wurde seitens der Beklagten im April 2018 deaktiviert. Nutzbar blieb die Kontaktimportfunktion, mit der die Scraper ihre fiktiven Kontakte hochladen konnten und sodann über die Telefonnummern ihre vermeintlichen Kontakte angezeigt erhielten. Auch mit dieser Funktion konnten Telefonnummern bis dahin unbekannten Nutzern zugeordnet werden. Die Kontaktimportfunktion deaktivierte die Beklagte auf der Plattform am 10.10.2018 und beim Facebook Messenger am 06.09.2019. Sowohl auf der Plattform als auch beim Facebook-Messenger ersetzte sie jeweils die Kontaktimportfunktion durch die sogenannte "People-You-May-Know"-Funktion. Bei dieser Funktion kann ein Nutzer der Beklagten seine Kontakte mitsamt Telefonnummer ebenfalls hochladen. Das System der Beklagten zeigt ihm aber allein aufgrund der Telefonnummer nicht mehr nur den einen passenden Nutzer an, sondern nur noch eine Liste von mehreren Personen, die aufgrund anderer zusätzlicher Zuordnungskriterien der hochgeladenen Kontakte, z.B. des Namens, zuzuordnen sein könnten. Das "Friend Centre" wurde bereits am 11.12.2018 in ähnlicher Weise geändert. Dies alles ist gerichtsbekannt geworden durch die Entscheidung des OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris und von den Parteien bei der Erörterung in der mündlichen Verhandlung nicht mehr streitig gestellt worden.

Im April 2021 ist bekannt gegeben worden, dass die von den Scrapern erbeuteten Daten im Internet veröffentlicht worden waren.

Die Parteien streiten darüber, ob auch der Kläger von dem Scraping-Vorfall betroffen war.

Mit vorgerichtlicher E-Mail der Prozessbevollmächtigten vom 16.12.2021 machte der Kläger wegen datenschutzrechtlicher Verstöße Schadensersatz-, Unterlassungs- und Auskunftsansprüche sowie den Ersatz vorgerichtlicher Anwaltskosten gegenüber der Beklagten geltend (Anlage K1, Bl. 53 ff. d.A.). Die Beklagte erklärte daraufhin über ihre Prozessbevollmächtigten unter dem 14.01.2022, dass Meta Ireland nicht in der Lage sei, das angebliche Facebook-Konto des Klägers anhand der bereitgestellten Informationen zu identifizieren. Bevor diese Angelegenheit weiter geprüft werden könne, werde der Kläger aufgefordert gemäß Art. 12 Abs. 6 DSGVO zusätzliche Informationen, die zur Bestätigung der Identität erforderlich seien, einschließlich der mit dem Facebook-Konto verbundenen E-Mail-Adresse oder URL, bereitzustellen. (Anlage B17, Bl. 282 ff. d.A.).

Der Kläger verfolgt sein Begehren weiter. Er behauptet, er habe bei der Beklagten ein Nutzerkonto unterhalten und sei im maßgeblichen Zeitraum, das genaue Datum könne er nicht angeben, von dem Sprapingvorfall betroffen worden. Dass er ein Nutzerkonto unterhalten habe, ergebe sich aus der überreichten Profilinformationen (vgl. Bl. 687/2015.F d.A.). In der u.a. im Darknet für jedermann abrufbaren Datenbank seien nachfolgende personenbezogene Daten von ihm enthalten:

Dabei handele es sich um seine Telefonnummer, die Facebook-ID, den Namen und sein Geschlecht.

Seine Telefonnummer sei in der sogenannten Zielgruppenauswahl auf nicht "öffentlich" und damit als nicht allgemein sichtbar eingestellt gewesen. In der sogenannten Suchbarkeits-Einstellung hingegen habe die Einstellung auf "alle" gestanden, sodass seine Mobilfunktelefonnummer ihm auf die dargestellte Art und Weise habe zugeordnet werden können. Er habe seine Telefonnummer stets

bewusst und zielgerichtet weitergegeben und diese nicht wahl- und grundlos der Öffentlichkeit zugänglich gemacht, wie etwa im Internet.

Die Zuordnung von Telefonnummern zu den Profildaten der Nutzer eröffne nunmehr böswilligen Akteuren eine weite Bandbreite an Möglichkeiten, wie z.B. einen Identitätsdiebstahl, die Übernahme von Accounts oder gezieltes Phishing. Er habe dadurch einen erheblichen Kontrollverlust über die persönlichen Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch der Daten gewesen. Dies habe sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen manifestiert. Seit dem Vorfall komme es zu dem deutlich vermehrten und unregelmäßigen Erhalt unbekannter Kontaktversuche via SMS und E-Mail auf sein Mobiltelefon. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks. Er habe mittlerweile sein Benutzerkonto bei Facebook gelöscht.

Der Kläger meint, die Beklagte habe in vielfältiger Hinsicht im Vor- und im Nachgang zum streitgegenständlichen Scarping-Vorfall gegen die DSGVO verstoßen.

Er behauptet, die Beklagte habe nicht die erforderlichen Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen insbesondere der Kontaktimportfunktion zu verhindern. So seien keine Sicherheitscaptchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage gehandelt habe. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden. Der massenhafte Zugriff auf die Facebook-Profile mit auffälligen Telefonnummernabfragen wäre durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination verschiedener Maßnahmen erforderlich und üblich gewesen. Zudem sei die Einführung einer Begrenzung der abgleichbaren Rufnummern oder die Nutzung des Kontaktimporttools für „Freunde von Freunden“ möglich gewesen.

Insbesondere seien die Einstellungen zur Sicherheit der Telefonnummer undurchsichtig und zu kompliziert gestaltet gewesen. Es habe jeglicher Hinweis zur

Suchbarkeit per Telefonnummer gefehlt. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten gewesen, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte, die zur Gefährdung der Daten geführt habe.

Er meint, den Voreinstellungen komme besondere Bedeutung zu, ein „opt-out“ genüge nicht. Es müsse die datenschutzfreundlichste Variante als Standardeinstellung vorgesehen werden, dies folge dem Grundsatz der „*privacy by default*“.

Ein Verstoß liege auch darin, dass die Beklagte die zuständige Behörde zu keinem Zeitpunkt darüber informiert habe, dass die persönlichen Informationen durch Dritte entwendet und veröffentlicht worden seien.

Schließlich vertritt der Kläger die Auffassung, dass das vorgerichtliche Auskunftsschreiben der Beklagten unzureichend sei. Es enthalte nämlich insbesondere keinerlei konkrete Aussagen dazu, welche persönlichen Daten von unbekannten Dritten abgegriffen worden seien.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an ihn immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 € nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz;

2. festzustellen, dass die Beklagte verpflichtet ist, ihm alle künftigen materiellen und nicht vorhersehbaren immateriellen 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 zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu

250.000,00 €, 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) personenbezogenen Daten von ihm, namentlich Telefonnummer, FacebookID, 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) 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 Kontaktimporttools 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, ihm Auskunft über ihn 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 Kontaktimporttools erlangt werden konnten;

5. die Beklagte zu verurteilen, an ihn vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, die Klage sei bereits unzulässig.

Der Klageantrag zu Ziffer 1. sei nicht hinreichend bestimmt, da der Schadensersatz für mehrere, zeitlich auseinanderfallende angebliche Verstöße geltend gemacht werde.

Für den Feststellungsantrag zu Ziffer 2. sei weder das festzustellende Rechtsverhältnis hinreichend genau bezeichnet, noch ein Feststellungsinteresse dargelegt.

Der Klageantrag zu Ziffer 3. sei deshalb unzulässig, weil er die immer öffentlichen Nutzerinformationen nicht ausnehme und die zu unterlassenden Verhaltensweisen zu ungenau beschreibe. Bezüglich der Telefonnummer fehle es überdies am Rechtsschutzbedürfnis, da der Kläger hier das gewünschte Ergebnis durch eine Änderung seiner Profileinstellungen selbst erreichen könne.

Darüber hinaus – so die Auffassung der Beklagten – sei die Klage unbegründet.

Die Beklagte bestreitet, für den Kläger während des relevanten Zeitraums oder überhaupt jemals ein mit der eMail-Adresse oder einer Telefonnummer des Klägers verknüpftes Nutzerkonto geführt zu haben. Entweder habe es ein solches Konto nie gegeben oder ein solches Konto habe existiert, aber alle relevanten persönlichen Daten, die eine Identifizierung des Klägers ermöglichten, seien mittlerweile dauerhaft und unwiderruflich gelöscht worden. Dann könne sie weder bestätigen, dass ein solches Konto jemals existiert habe noch könne sie nähere Angaben zu den mit diesem Konto verbundenen Daten machen. Zudem werde mit Nichtwissen bestritten, dass die Daten, welche der Kläger in der Klageschrift nenne (dort, S. 6), in dieses angebliche Nutzerkonto eingestellt worden seien.

Soweit der Kläger in der Replik zu einer vermeintlich in einer nicht näher spezifizierten „im Darknet für jedermann abrufbaren Datenbank“ enthaltenen Facebook Nutzer-ID (die angebliche Nutzer-ID) vortrage, sei darauf hinzuweisen, dass die angebliche Nutzer-ID nicht mit der E-Mail-Adresse verknüpft

sei, die der Kläger in dem vorgerichtlichen Auskunftsersuchen (Anlage K 1) angegeben habe. In Anbetracht der Tatsache, dass er in verschiedenen Phasen des Verfahrens unterschiedliche Angaben gemacht habe, sei unklar auf welches Facebook-Nutzerkonto sich die vorliegende Klage bezieht. Eine eindeutige Zuordnung des Klägers zu einem Facebook-Nutzerkonto sei aufgrund der widersprüchlichen Angaben des Klägers nicht möglich. Er möge ausdrücklich klarstellen, ob – entgegen der bisherigen Angaben im vorgerichtlichen Auskunftsersuchen und in der Klageschrift – nunmehr das mit der angeblichen Nutzer-ID verknüpfte Facebook-Nutzerkonto streitgegenständlich sein solle.

Die Beklagte bestreitet, dass die Daten des Klägers gescrapt worden seien.

Hilfsweise ist die Beklagte der Ansicht, dass das erfolgte „*Scraping*“ keinen Datenschutzverstoß begründe, da lediglich öffentlich zugängliche Profilinformationen des Klägers abgerufen und auch keine spezifischen Sicherheitsmaßnahmen oder Zugriffsberechtigungen dafür umgangen oder überwunden worden seien (wie beim „*Hacking*“). Es habe insoweit weder eine Sicherheitsverletzung noch eine unbefugte Offenlegung von personenbezogenen Daten gegeben. Gegebenenfalls sei die hergestellte Verknüpfung zwischen der Telefonnummer des Klägers und seinem Nutzerkonto auf die seinerzeit von ihm selbst gewählte Suchbarkeitseinstellung zurückzuführen.

Zu den wählbaren Profileinstellungen stelle sie, die Beklagte, ihren Nutzern alle in Art. 13 DSGVO festgelegten Informationen zur Verfügung, insbesondere informiere sie umfassend und transparent über die Möglichkeiten zur Einstellung der Suchbarkeit und Zielgruppenauswahl. Die gewünschten Informationen seien durch entsprechende Überschriften leicht zu finden und einfach aufzurufen.

Die Beklagte behauptet, sie verwende sowohl Captchas als auch geänderte Einstellungen, die ein automatisches Verknüpfen über das Kontakt-Importer-Tool nicht mehr ermöglichten, obwohl dadurch eine legitime und nützliche Funktion für ihre Nutzer entfallen sei. Die Beklagte ist der Auffassung, dass sie nicht dazu verpflichtet sei, darüber hinaus weitergehende Schutzvorkehrungen gegen eine Erhebung der immer öffentlich zugänglichen Informationen eines Nutzerprofils durch

Dritte zu ergreifen. Soweit es dazu komme, gehe sie mit Unterlassungs- und Beseitigungsaufforderungen sowie Kontosperrungen gegen die Scraper vor. Es gebe jedoch keine formellen oder vorgeschriebenen Branchen- oder Industriestandards zur Bekämpfung von Scraping.

Die Beklagte macht geltend, dass ein kompensationsgeeigneter und messbarer Schaden des Klägers nicht dargelegt sei. Dabei beruft sie sich darauf, dass selbst ein angenommener vorübergehender Kontrollverlust über personenbezogene Daten nicht ihr zuzurechnen sei, weil die öffentliche Einsehbarkeit der Privatsphäre-Einstellungen entsprochen habe. Mindestens fehle es an der Kausalität und an einem Verschulden ihrerseits.

Die Beklagte ist der Ansicht, dass eine Melde- oder Benachrichtigungspflicht gegenüber der zuständigen Behörde schon mangels einer Verletzung von Vorschriften der DSGVO nicht bestanden habe.

Für einen Unterlassungsanspruch sei keine Anspruchsgrundlage ersichtlich. Die insoweit abschließenden Regelungen der DSGVO sähen gerade keinen Unterlassungsanspruch vor.

Die Beklagte behauptet ferner, es sei unzutreffend, dass sie auf den Scraping-Vorfall nicht reagiert habe. Über die technischen Anpassungen hinaus widme sie in ihrem Hilfebereich einen eigenen Abschnitt der Information, wie der Nutzer sich vor nicht autorisiertem Scraping schützen könne.

Bezüglich des geltend gemachten Auskunftsanspruches meint die Beklagte, dass sie zur Erteilung weitergehender Auskünfte, insbesondere über eine etwaige Datenverarbeitung durch Dritte, weder imstande noch nach Art. 15 DSGVO rechtlich verpflichtet sei.

Die Beklagte meint, es handele sich schon nicht um eine unbefugte Offenlegung, weil die abgerufenen und veröffentlichten Informationen aufgrund der Einstellungen,

die der Kläger vorgenommen habe, bereits öffentlich einsehbar gewesen seien. Auch wenn die Art des Abrufs der Daten gegen die Nutzungsbedingungen verstoßen habe, gelte dies nicht für den Zugang als solchen. Weiter habe es dem Hauptzweck von Facebook, nämlich den Nutzern zu helfen, einander zu finden und sich mit Freunden, der Familie und bedeutsamen Gemeinschaften zu verbinden, entsprochen, die Einstellung für die Suchbarkeit von Telefonnummern auf „alle“ als Standard-Einstellung vorzusehen. Die Verarbeitung von Kontaktdaten, wie E-Mail-Adresse oder Telefonnummer sei erforderlich, um diesen Verarbeitungszweck, nämlich die gegenseitige Auffindbarkeit und Vernetzung, zu erreichen.

Wegen der weiteren Einzelheiten wird auf die zwischen den Parteien gewechselten Schriftsätze Bezug genommen.

Die Kammer hat der Kläger persönlich angehört. Wegen des Ergebnisses der Anhörung wird Bezug genommen auf das Protokoll der mündlichen Verhandlung vom 25.10.2023.

## Entscheidungsgründe

Der Klageantrag zu 1. ist zulässig und teilweise begründet.

Der Klageantrag zu 2. ist zulässig und begründet.

Die Klageanträge zu 3.a. und der Klageantrag zu 3.b. sind bereits unzulässig.

Der Klageantrag zu 4. ist zulässig, aber unbegründet.

Der Klageantrag zu 5. ist zulässig und teilweise begründet.

Die Kammer folgt insofern nach eigener Prüfung in weiten Teilen der Entscheidung des OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris.

Klageantrag zu 1.

Die mit dem Klageantrag zu 1. verfolgte Leistungsklage gerichtet auf den Ersatz immateriellen Schadens ist zulässig und teilweise begründet.

1.

Die Leistungsklage ist zulässig.

a)

Nach den Erörterungen in der mündlichen Verhandlung vom 25.10.2023 geht das Gericht davon aus, dass der Kläger einen Verstoß rügt, den er zeitlich nicht genau einordnen kann, der sich aber nach Geltung der DSGVO zugetragen haben soll.

b)

Die internationale Zuständigkeit der deutschen Gerichte folgt vorliegend im zeitlichen Anwendungsbereich der DSGVO nach Art. 99 Abs. 2 DSGVO ab dem 25.05.2018 aus Art. 79 Abs. 2 Satz 1 DSGVO in Verbindung mit Erwägungsgrund 22 DSGVO sowie aus Art. 79 Abs. 2 Satz 2 Hs. 1 DSGVO, jeweils als unmittelbar geltendes Recht (Art. 288 Abs. 2 AEUV), und § 44 Abs. 1 Satz 2 BDSG, da die Beklagte in Deutschland eine Niederlassung und der Kläger als betroffene Person im Sinne von Art. 4 Nr. 1 DSGVO ihren gewöhnlichen Aufenthalt in Deutschland haben (vgl. BGH Urt. v. 27.7.2020 - VI ZR 405/18, BGHZ 226, 28 Rn. 16 m. w. N.; BGH Urt. v. 23.5.2023 - VI ZR 476/18, GRUR-RS 2023, 16479 Rn. 27).

c)

Soweit die Kammer aufgrund des Streitwertes sachlich nicht zuständig ist (§ 23 Nr. 1 GVG), hat sich die Beklagte nach entsprechender Erörterung rügelos eingelassen.

d)

Der Klageantrag zu 1. ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Ein Klageantrag ist hinreichend bestimmt, wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abwälzt und schließlich eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21.11.2017 – II ZR 180/15, juris).

Das Gericht hat keine Zweifel, dass der Leistungsantrag den Erfordernissen genügt. Abgesehen davon, dass eine konkret bezifferte Mindestentschädigung begehrt wird, wird eindeutig klar, dass sämtliche auf Grund des Scraping-Vorfalls gerügten Datenschutzverstöße und Persönlichkeitsverletzungen des Klägers nach Geltung der DSGVO und der dadurch bis zum Schluss der letzten mündlichen Verhandlung entstandene immaterielle (Gesamt)Schaden umfassend und abschließend rechtshängig geworden sind und einer rechtskräftigen Entscheidung zugeführt werden sollen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

2.

Die Leistungsklage ist teilweise begründet.

Das Gericht geht von einem Verstoß der Beklagten gegen die DSGVO aus, der einen Anspruch des Klägers aus Art. 82 Abs. 2, Abs. 1 DSGVO (in Verbindung mit Art. 288 Abs. 2 AEUV) begründet.

a)

Das Gericht ist davon überzeugt, dass der Kläger bei der Beklagten ein Nutzerkonto unterhalten hatte. Der Kläger hat nicht nur mit der Replik einen Auszug seiner Profilinformationen eingereicht, sondern diesen Auszug auch in der mündlichen Verhandlung vom 25.10.2023 vorgelegt und dazu glaubhaft erklärt, dass dies der Auszug sei, den er von der Beklagten auf Anforderung und anlässlich der Löschung des Kontos selbst erhalten habe. Der Umstand, dass er das Konto gelöscht hat,

passt auch zu den eigenen Ausführungen der Beklagten, dass sie in diesem Fall die Kontoinformationen nicht mehr aufrufen könne.

Die Klage ist auch nicht etwa deshalb unbegründet, weil der Kläger vorprozessual mitgeteilt hatte, dass das Benutzerkonto über eine eMail-Adresse verknüpft sei und er nunmehr auf eine Mobilfunknummer Bezug nimmt. Mit der Replik hat er spätestens auch diese in den Rechtsstreit eingeführt und dies durch Vorlage der Profilinformationen in der mündlichen Verhandlung bekräftigt. Auf die gewährte Frist zur Stellungnahme ist kein weiterer Vortrag der Beklagtenseite erfolgt. Die Angaben des Klägers zu seinem Benutzerkonto sind uneingeschränkt glaubhaft.

b)

Das Gericht ist ebenso davon überzeugt, dass der Kläger mit seinem Benutzerkonto von dem Scarping-Vorfall betroffen war, weil er bei seinem Konto die zur Verfügung gestellten Grundeinstellungen genutzt hatte. Der Kläger hat konkret dargelegt, welche Daten im Internet zu ersehen sind, und zwar über die öffentlich zugänglichen Daten hinaus seine Mobilfunknummer. Dem ist die Beklagte nicht hinreichend entgegengetreten (§ 139 Abs. 3 ZPO).

c)

Der zeitliche, sachliche und räumliche Anwendungsbereich der DSGVO ist damit gegeben.

(aa) Der zeitliche Anwendungsbereich der DSGVO ist eröffnet. Wie bereits im Rahmen der Zulässigkeit dargelegt, geht das Gericht von einem behaupteten Verstoß seit der Geltung der DSGVO, also ab dem 25.05.2018 aus. Die Beklagte wiederum hat ihrer aus § 138 Abs. 2 ZPO abgeleiteten sekundären Darlegungslast bezüglich des genauen Zeitpunkts dieses Scraping-Vorgangs nicht genügt, so dass die Kammer davon ausgeht, dass sich der Vorfall tatsächlich ab dem 25.05.2018 zugetragen hat.

Eine sekundäre Darlegungslast trifft den Prozessgegner der primär darlegungsbelasteten Partei, wenn diese keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Bestreitende alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen. Genügt der Anspruchsgegner seiner sekundären Darlegungslast nicht, gilt die Behauptung des Anspruchstellers nach § 138 Abs. 3 ZPO als zugestanden (vgl. zur ständigen Rechtsprechung etwa BGH Urt. v. 25.5.2020 - VI ZR 252/19, NJW 2020, 1962 Rn. 37 m. w. N.).

Die sekundäre Darlegungslast der Beklagten ergibt sich bereits daraus, dass die Scraping-Vorfälle ausschließlich der Sphäre der Beklagten zuzuordnen sind und sie nach Art. 5 Abs. 2, Art. 15 DSGVO eine umfassende Rechenschafts- und Auskunftspflicht zu Verarbeitungszweck, -art und insbesondere auch zur Offenlegung / Zugänglichmachung der Daten gegenüber Dritten trifft. So muss sie auch nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, führen. Insbesondere aber trägt die Beklagte nach Art. 5 Abs. 2 DSGVO als Verantwortliche die Beweislast dafür, dass die Daten unter anderem für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (so EuGH Urt. v. 4.7.2023 - C-252/21, GRUR 2023, 1131 Rn. 95; OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Für die zeitliche Verortung des Scraping-Vorfalls nach dem 24.05.2018 streitet zudem der Umstand, dass die Deaktivierung der Suchbarkeit über die Mobilfunktelefonnummer über die Kontaktimportfunktion im Facebook-Messenger erst im September 2019 erfolgt ist, so dass also bis September 2019 ein Scraping möglich war. Dass die Daten des Klägers vor dem 25.05.2018 den Scrapern offengelegt wurden, ist weder von der Beklagten konkret dargetan noch sonst ersichtlich.

Selbst wenn Verstöße im Rahmen des Anmeldeprozesses aus dem zeitlichen Anwendungsbereich der DSGVO herausfallen, da der Kläger den Registrierungsprozess bereits vor Geltung der DSGVO vorgenommen hat und der Beklagten damit kein Verstoß gegen Art. 13 DSGVO zur Last gelegt werden kann, so

unterfällt doch die Weiterverarbeitung der Daten ab dem 25.05.2018 den Anforderungen der DSGVO. Denn aus Erwägungsgrund 171 Satz 2 DSGVO, aus Art. 4 Nr. 2 DSGVO und Art. 24 Abs. 1, insbesondere Satz 2 DSGVO ergibt sich die Pflicht, die Datenverarbeitungen, die zum Zeitpunkt der Anwendung der DSGVO bereits begonnen hatten, bis zum 25.05.2018 in Einklang mit der Verordnung zu bringen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Zudem folgt aus Erwägungsgrund 171 Satz 3 DSGVO, dass die Beklagte zum 25.05.2018 zur Einholung neuer Einwilligungen verpflichtet war, soweit bereits bestehende Einwilligungen nicht den Anforderungen an diese Verordnung entsprachen. Daher ist die Frage einer hinreichenden Information - ganz oder teilweise deckungsgleich mit der nach Art. 13 DSGVO - (nur) entscheidend für die Frage der Wirksamkeit einer ursprünglich erteilten Einwilligung und deren Fortgeltung über den 25.05.2018 hinaus (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Soweit der Kläger einen Verstoß der Beklagten gegen Art. 35 DSGVO rügt, die keine Datenschutz-Folgenabschätzung vorgenommen haben soll, fällt ein solcher Verstoß nicht in den zeitlichen Anwendungsbereich der DSGVO. Letztendlich kann auch dahinstehen, ob die Beklagte jedenfalls im Hinblick auf Art. 35 Abs. 11 DSGVO nach der Feststellung der ersten Scraping-Vorfälle spätestens im März 2018 zur Erstellung einer Datenschutz-Folgenabschätzung ab dem 25.05.2018 verpflichtet war. Denn durch einen etwaigen Verstoß gegen Art. 35 Abs. 11 DSGVO kann kein zusätzlicher Schaden entstanden oder ein entstandener Schaden vertieft worden sein.

(bb) Der sachliche Anwendungsbereich der DSGVO ist ebenfalls eröffnet.

Der Betrieb eines sozialen Netzwerkes durch Sammlung / Speicherung jedenfalls des Namens und Geschlechts von Mitgliedern und die automatisierte Vernetzung der Mitglieder sowie deren Beschickung mit individualisierter Werbung fällt in den sachlichen Anwendungsbereich der DSGVO im Sinne des Art. 2 Abs. 1 DSGVO; die Tätigkeit unterfällt - was die Beklagte aber auch schon nicht in Anspruch nimmt - keinem Ausnahmetatbestand im Sinne von Art. 2 Abs. 2 bis Abs. 4 DSGVO oder der

Öffnungsklausel nach Art. 85 Abs. 2 DSGVO (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Bei den hier in Rede stehenden Daten (Telefonnummer, Facebook-ID, Familienname, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus) handelt es sich unzweifelhaft um personenbezogene Daten im Sinne der Art. 5 Abs. 1 lit. a Var. 1, Art. 6 Abs. 1 Unterabs. 1 lit. a, Art. 7, Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1 DSGVO.

Die personenbezogenen Daten (konkret jedenfalls Telefonnummer, Facebook-ID, Familienname, Vorname sowie Geschlecht) hat die Beklagte auch unzweifelhaft im Sinne von Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 2 DSGVO automatisiert verarbeitet.

(cc) Der räumliche Anwendungsbereich der DSGVO ist ebenfalls eröffnet.

Die Beklagte ist unzweifelhaft Verantwortliche der Verarbeitung im Sinne von Art. 4 Nr. 7 DSGVO (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.). Sie hat ihren Sitz in Irland, betreibt jedenfalls für die Tätigkeit ihrer Datenverarbeitung eine Niederlassung in Irland, also innerhalb der Union (vgl. auch BGH Urt. v. 27.7.2020 - VI ZR 405/18, BGHZ 226, 28 Rn. 15).

d) Das Gericht ist von einem Verstoß gegen die DSGVO überzeugt.

Wie bereits dargelegt ist der Kläger vom Scraping-Vorfall betroffen. Damit traf die Beklagte die Darlegungslast dahin, seine betroffenen personenbezogenen Daten entsprechend der DSGVO verarbeitet zu haben. Denn die DSGVO enthält in Art. 5 Abs. 2 DSGVO eine spezifische Beweislastregelung. Danach ist nämlich der für die Datenverarbeitung Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO enthaltenen Grundsätze der Datenverarbeitung verantwortlich und muss deren Einhaltung nachweisen können ("Rechenschaftspflicht").

Er muss damit also generell - und entgegen dem Ansatz der Beklagten auch im Zivilprozess - nach dem in Art. 5 Abs. 2 DSGVO verankerten Grundsatz der Rechenschaftspflicht nachweisen können, dass er die in Abs. 1 dieses Artikels festgelegten Grundsätze für die Verarbeitung personenbezogener Daten einhält (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Gemessen daran hat die Beklagte als die für die Datenverarbeitung Verantwortliche weder schlüssig dargelegt noch gar bewiesen, dass ihre streitgegenständliche, zum Scraping-Vorfall bei dem Kläger führende Verarbeitung nicht gegen die in Art. 5 Abs. 1 DSGVO normierten Grundsätze verstoßen hat.

Namentlich hat sie insbesondere nicht schlüssig dargelegt, dass sie die personenbezogenen Daten des Klägers rechtmäßig im Sinne des Art. 6 Abs. 1 DSGVO verarbeitet hat.

Konkret nicht ausgeräumt hat die Beklagte neben Verstößen gegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 Unterabs. 1 DSGVO zudem auch solche gegen Art. 5 Abs. 1 lit. b, Art. 25 Abs. 1 und Abs. 2 DSGVO und Art. 5 Abs. 1 lit. f, Art. 32 DSGVO. Auch insoweit folgt die Kammer der Entscheidung des OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris.

Im Einzelnen:

(aa) Zunächst war die Datenverarbeitung mit Blick auf die Suchbarkeit eines Nutzerprofils über die Mobilfunktelefonnummer per Such- und Kontaktimportfunktion und insbesondere die diesbezügliche Voreinstellung der Suchbarkeit für "alle" - entgegen der Ansicht der Beklagten - nicht zur Vertragszweckerfüllung erforderlich und damit nicht gemäß Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO gerechtfertigt.

Voraussetzung ist nämlich, dass eine Verarbeitung personenbezogener Daten objektiv unerlässlich sein muss, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte. Der etwaige

Umstand, dass eine solche Verarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist, ist insoweit für sich genommen unerheblich. Dabei ist im Fall eines Vertrages, der mehrere Dienstleistungen oder mehrere eigenständige Elemente einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit von Art. 6 Abs. 1 Unterabs. 1 lit. b DSGVO für jede dieser Dienstleistungen gesondert zu beurteilen (EuGH Urt. v. 4.7.2023 - C-252/21, GRUR-RS 2023, 15772 Rn. 98).

Demzufolge ergibt sich schon allein aus dem Umstand, dass die Beklagte nur hinsichtlich bestimmter personenbezogener Daten vorgab und -gibt, dass diese "immer öffentlich", also zwecks Vernetzung sichtbar und damit suchbar sein müssen, und dem Umstand, dass sie den Nutzern im Rahmen der Zielgruppenauswahl und der Suchbarkeitseinstellungen freistellt, ob und wem die nicht "immer öffentlichen" Daten gezeigt werden bzw. ob und wer nach ihnen suchen kann, dass diese Daten nicht objektiv unerlässlich waren und sind, um eine (hinreichende) Verknüpfung der Nutzer der Beklagten zu ermöglichen. Dass dies (unter Umständen) für die Nutzer (und vor allem im Hinblick auf die Werbezweckrichtung und damit das Geschäftsmodell der Beklagten) wünschenswert gewesen sein mag, reicht gerade nicht. Ob der einzelne Nutzer (sich) diesen Wunsch erfüllen mochte, musste ihm vielmehr im Rahmen einer informierten Einwilligung selbst überlassen bleiben (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Dass die Suchbarkeit über die Telefonnummer auf den verschiedenen Ebenen, insbesondere per Kontaktimportfunktion von Facebook oder im Facebook-Messenger, nicht erforderlich ist und war, wird dadurch belegt, dass diese Funktion zum 06.09.2019 endgültig und vollständig aus allen Anwendungsbereichen eliminiert wurde.

Zudem ist die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem sogenannten Grundsatz der "Datenminimierung" zu prüfen, der in Art. 5 Abs. 1 lit. c DSGVO verankert ist und verlangt, dass personenbezogene Daten "dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" sind (EuGH Urt. v. 4.7.2023 - C-252/21, GRUR-RS 2023, 15772 Rn. 109).

(bb) Auch eine Rechtfertigung über Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO scheidet aus, da die erschöpfende und abschließende Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann, nicht eingreift. Wie bereits dargestellt, fehlt es an einer Erforderlichkeit der Gestaltung.

(cc) Die Beklagte kann sich zur Rechtfertigung der Verarbeitung der personenbezogenen Daten des Klägers auch nicht auf seine Einwilligung im Sinne des Art. 5 Abs. 1 lit. a Var. 1, Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO berufen. Denn eine wirksame Einwilligung im Sinne von Art. 6 Abs. 1 Unterabs. 1 lit. a, Art. 7 DSGVO in die Suchbarkeit des Nutzerprofils über die Mobilfunktelefonnummer lag nicht vor (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Nach Art. 6 Abs. 1 Unterabs. 1 lit. a DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung für einen oder mehrere bestimmte Zwecke freiwillig in informierter Weise und unmissverständlich im Sinne von Art. 4 Nr. 11 DSGVO erteilt hat (vgl. EuGH Urt. v. 4.7.2023 - C-252/21, GRUR-RS 2023, 15772 Rn. 91 f.; EuGH Urt. v. 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f.). Dabei gilt es, auch den Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a Var. 3 DSGVO zu berücksichtigen.

Soweit der Kläger möglicherweise vor dem 25.05.2018 in die Suchbarkeit seines Profils über die Mobilfunknummer eingewilligt hat, konnte eine solche Einwilligung unter Geltung der DSGVO jedenfalls keine rechtfertigende Wirkung mehr entfalten; denn nach Erwägungsgrund 171 Satz 3 DSGVO musste eine vorab erteilte Einwilligung bereits den Bedingungen der DSGVO entsprechen, um fortzugelten. Daran fehlt es vorliegend, weil auch die im April 2018 von der Beklagten der Klagepartei mit Blick auf den Geltungsbeginn der DSGVO zur Verfügung gestellten neuen Nutzungsbedingungen vom 19.04.2018 (Anl. B19) und die zur Verfügung gestellte neue Datenrichtlinie vom 19.04.2018 (Anl. B20) den Anforderungen der DSGVO nicht genügen.

So wie das OLG Hamm (Urteil vom 15.08.2023 - 7 U 19/23-, juris) zur historischen Entwicklung der Datenschutz-Richtlinie (im Folgenden: DSRL) zur DSGVO ausführt, erfordert eine wirksame Einwilligung seit dem 25.05.2018 ein aktives Verhalten des Einwilligenden. Entsprechend Erwägungsgrund 32 Satz 3 DSGVO folgt aus Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung mehr (vgl. EuGH Urt. v. 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f.; siehe auch EuGH Urt. v. 1.10.2019 - C-673/17, NJW 2019, 3433 Rn. 51 ff., insbesondere Rn. 61 f.).

Gemessen daran kann die Beklagte schon allein auf Grund des Umstandes, dass sie mit ihrer Voreinstellung "alle" zur Suchbarkeit zum Zeitpunkt der Bedingungsänderungen am 19.04.2018 unverändert eine "Opt-Out-Einwilligung" vorsah, keine wirksame Einwilligung vorweisen.

Folglich hat die Beklagte nicht wie geboten sichergestellt, dass das - wie auch bei dem Kläger - voreingestellte und ab dem 25.05.2018 unzulässige Opt-Out entfiel und die fortgesetzte Datenverarbeitung durch eine der DSGVO entsprechende Einwilligung gedeckt wurde. Da - wie bereits ausgeführt - zudem ab dem 25.05.2018 eine Einwilligung nur durch ein aktives Tun und nicht durch stillschweigendes Akzeptieren von Voreinstellungen erfolgen kann, hätte die Beklagte die Nutzer im Rahmen der Änderung der Nutzungsbedingungen etc. mithin sämtliche bisherigen Voreinstellungen durchlaufen lassen müssen, die Einstellungen - wie erst seit Mai 2019 möglich - auf "nur ich" voreinstellen und die aktive Einwilligung nach umfassender Information zu hiervon abweichenden neuen Einstellungen einholen müssen.

(dd) Weiterhin hat die Beklagte nicht dargelegt, dass ihre Datenverarbeitung den Anforderungen der Art. 5 Abs. 1 lit. f, Art. 32 DSGVO entsprach.

Die Beklagte hat trotz der sie treffenden Darlegungs- und Beweislast konkret weder substantiiert dargelegt noch bewiesen, dass sie den Vorgaben des Art. 32 DSGVO zur Sicherheit der Verarbeitung genügt hätte.

Ohne die automatisierte Datenverarbeitung der Beklagten hätten die Scraper die Nutzerinformationen nicht zusammenstellen und veröffentlichen können. Offenlegung und Zugangsgewährung geschahen auch unbefugt, was die Beklagte auch gar nicht in Abrede stellt.

Tatsächlich waren die im Zeitpunkt des Scraping-Vorfalls bestehenden Maßnahmen unter Zugrundelegung des unstreitigen und streitigen Vortrags der Beklagten technisch und organisatorisch ungeeignet im Sinne des Art. 32 Abs. 1 Hs. 1 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, obwohl es in Bezug auf die Kontaktimportfunktionen bei Facebook und im Facebook-Messenger geeignete Maßnahmen gab.

Das Gericht verkennt insoweit zunächst nicht, dass allein die Tatsache, dass es zum Scraping-Vorfall gekommen ist, kein Beweis dafür ist, dass die Beklagte im Vorfeld ungeeignete Maßnahmen ergriffen hätte. Vorliegend hat die Beklagte jedoch bei einer ex-ante-Betrachtung trotz ihres Beurteilungsspielraums unter Abwägung der widerstreitenden Interessen spätestens ab April 2018 keine geeignete und gebotene Maßnahme gegen das Scraping getroffen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris). Denn es war ihr ohne Weiteres möglich und im Hinblick auf die Datensicherheit ihrer Nutzer geboten sowie zumutbar, die Kontaktimportfunktion auf Facebook, im Friend Center und im Facebook-Messenger unverzüglich einzuschränken und somit einen massiven weiteren Datenverlust an Unbefugte zu unterbinden, nachdem das Scraping aufgefallen war. So erfolgte die Deaktivierung der Suchfunktion im April 2018 binnen weniger Monate nach Kenntniserlangung vom Vorfall, während die vollständige Deaktivierung der Kontaktimportfunktionen aber noch weitere rund sechzehn Monate dauerte.

Auch die Umstellung auf die aktuelle Funktion "People-You-May-Know" zeigt, dass weitere Möglichkeiten bestanden hätten, das Scrapen zu erschweren.

(ee) Ob die Beklagte ihrer Darlegungslast mit Blick auf mögliche weitere Verstöße gegen die DSGVO zeitlich nach dem Scraping-Vorfall und der Veröffentlichung im Darknet nachgekommen ist, kann dahinstehen; denn hinsichtlich der seitens des Klägers gerügten Verstöße gegen die Meldepflicht nach Art. 33 DSGVO, die

Benachrichtigungspflicht nach Art. 34 DSGVO sowie die Nicht- bzw. Schlechterfüllung des Auskunftsrechts nach Art. 15 DSGVO hat der Kläger keinen konkreten auf die fehlenden Informationen zurückzuführenden Schaden dargelegt noch ist ein solcher sonst ersichtlich (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

e)

Aufgrund der aufgezeigten, nicht widerlegten Verstöße der Beklagten gegen die DSGVO steht dem Kläger die begehrte Entschädigung jedenfalls teilweise zu.

Die von der DSGVO verwandten Begriffe "immaterieller" und "materieller" Schaden sind unionsautonom auszulegen und setzen - entgegen dem Ansatz des Klägers - nach dem Wortlaut der Norm, der Systematik und Telos des Art. 82 Abs. 2, Abs. 1 DSGVO sowie der Art. 77-84 DSGVO und den Erwägungsgründen 75, 85 und 146 DSGVO einen über den schlichten Verstoß gegen die DSGVO hinausgehenden Schaden voraus. Ein solcher Schaden setzt nach Wortlaut, Erwägungsgründen 10, 146 DSGVO und Telos nicht voraus, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Auch wenn es keine Erheblichkeitsschwelle gibt, so bedeutet dies indes nicht, dass die aus dem Datenschutzverstoß resultierenden negativen Folgen per se einen haftungsbegründenden Schaden darstellen; denn der EuGH führt hierzu explizit aus, dass diese Auslegung nicht bedeutet, "dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 dieser Verordnung darstellen" (EuGH Urt. v. 4.5.2023 - C-300/21, GRUR-RS 2023, 8972 Rn. 50 und das in dem Bewusstsein der konkret vom ÖOGH zum Kontrollverlust aufgeworfenen Frage, vgl. Rn. 17). Entsprechend stellt der EuGH auch darauf ab, dass die "konkret erlittenen Schäden" vollständig ausgeglichen werden müssen (vgl. EuGH Urt. v. 4.5.2023 - C-300/21, GRUR-RS 2023, 8972 Rn. 58). Die Annahme eines solchen konkreten Schadens setzt in unionsautonomer Auslegung nach ständiger Rechtsprechung des EuGH voraus, dass dieser

"tatsächlich und sicher" besteht (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Der Kontrollverlust in Form des unkontrollierten Abrufs der Daten durch die Scraper und der anschließenden Veröffentlichung des Leak-Datensatzes im Darknet waren lediglich die zwangsläufige und generelle Folge der unrechtmäßigen bzw. unzureichend geschützten Datenverarbeitung durch die Beklagte (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris). Daraus folgt, dass es über den Kontrollverlust als Realisierung des generellen Risikos hinaus eines tatsächlichen materiellen oder immateriellen Schadens im konkreten Einzelfall bedarf. Damit deckt sich, dass der völlige Kontrollverlust als solcher nicht per se ein immaterieller Schaden ist.

Unter Berücksichtigung dieser Gesamtkriterien und unter Anwendung des Beweismaßstabes des § 286 ZPO, der keine absolute oder unumstößliche Gewissheit und auch keine an Sicherheit grenzende Wahrscheinlichkeit erfordert, sondern nur einen für das praktische Leben brauchbaren Grad von Gewissheit, der Zweifeln Schweigen gebietet (BGH Urt. v. 23.6.2020 - VI ZR 435/19, VersR 2021, 1497 Rn. 13), ist das Gericht von einem kausalen Zusammenhang zwischen den vermehrten Spamnachrichten auf dem Mobiltelefon des Klägers mit den streitgegenständlichen Scraping-Vorfällen überzeugt. Dabei teilt das Gericht nicht die Auffassung des OLG Hamm (Urteil vom 15.08.2023 - 7 U 19/23-, juris), dass es aufgrund der für eine Vielzahl an Fällen formulierten Klageschrift an einer schlüssigen Schadensdarlegung im Einzelfall fehle und es eine Anhörung des Klägers nicht bedürfe. So hat auch die Anhörung des Klägers gezeigt, dass seine schriftsätzlich vorgetragenen Beeinträchtigungen von ihm konkret und glaubhaft bestätigt werden konnten.

Der Kläger hat auf seinem Handy zeigen können, dass er Spam-Nachrichten erhält. Dies allein vermag allerdings keinen kausalen Schaden zu begründen, denn es ist gerichtsbekannt, dass auch Mobiltelefonnutzer, die über keinen Facebook Zugang verfügen, wiederkehrend mit Spam-Nachrichten konfrontiert werden. Deshalb hat das Gericht in Parallelverfahren bislang auch nicht die Überzeugung eines Schadens gewinnen können. Der vorliegende Fall ist anders zu beurteilen. Der Kläger hat

glaubhaft dargestellt, dass er selbst in einem Unternehmen im Bereich des Datenschutzes tätig ist und schon immer dafür sensibilisiert war. Dass dies glaubhaft ist, zeigt sich darin, dass er der erste Nutzer ist, den das Gericht sieht, der nach dem Scraping-Vorfall konsequent sein Benutzerkonto bei der Beklagten gelöscht und sich die für ihn vorliegenden Daten hat aushändigen lassen. Hinzukommt, dass der Kläger glaubhaft eine Strategie entwickelt hat, seine Mobilfunknummer gerade nicht anzugeben, sondern er, wenn es zwingend erforderlich ist, auf seine Festnetznummer zurückgreift. Vor dem Hintergrund seiner beruflichen Aufgaben und aufgrund des persönlichen Eindrucks erachtet das Gericht die Schilderung für glaubhaft und ist mithin davon überzeugt, dass die vermehrten Spam-Meldungen auf die Veröffentlichung seiner Mobilfunknummer im Rahmen des Scarping-Vorfalls zurückzuführen sind. Insgesamt erachtet das Gericht aber aufgrund des Eindrucks des Klägers und der doch geringen Beeinträchtigungen einen immateriellen Schadensersatz in Höhe von 500,00 € für angemessen und ausreichend. Insoweit war dem Klageantrag zu 1. stattzugeben

Klageantrag zu 2.

Die mit dem Klageantrag zu 2. verfolgte Feststellungsklage ist zulässig und begründet.

1.

Der Antrag ist dahingehend klargestellt worden, dass zwischen den künftigen materiellen und immateriellen Schäden unterschieden wird.

Dem Begehren fehlt auch nicht das Feststellungsinteresse im Sinne des § 256 Abs. 1 ZPO. Das Gericht schließt sich der Rechtsprechung der Entscheidung des OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris insoweit nicht an.

Die Zulässigkeit der Feststellungsklage ist nur bei reinen Vermögensschäden von der Wahrscheinlichkeit eines auf die Verletzungshandlung zurückzuführenden

Schadenseintritts abhängig. Geht es jedoch nicht um reine Vermögensschäden, sondern um Schäden, die aus der behaupteten Verletzung des allgemeinen Persönlichkeitsrechts, also eines sonstigen absolut geschützten Rechtsguts im Sinne von § 823 Abs. 1 BGB, resultieren, reicht bereits die Möglichkeit materieller oder weiterer immaterieller Schäden für die Annahme eines Feststellungsinteresses aus (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Diese Rechtsprechung zum allgemeinen Persönlichkeitsrecht ist unter dem Gesichtspunkt von Äquivalenz und Effektivität (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.) auf den vorliegenden Fall der Verletzung des nach Art. 82 DSGVO absolut geschützten Rechtsguts Datenschutz als (abschließende) europarechtliche Ausformung des deutschen allgemeinen Persönlichkeitsrechts zu übertragen.

Ein Feststellungsinteresse ist also nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen. Das Gericht kann der Einschätzung des OLG Hamm (Urteil vom 15.08.2023 - 7 U 19/23-, juris), dass die Möglichkeit eines Schadenseintritts durch den Kläger nicht hinreichend dargelegt sei, nicht folgen. Welche kriminellen oder sonstigen beeinträchtigenden Möglichkeiten im und außerhalb des Internets künftig noch zur Verfügung stehen, nachdem in unzulässiger Weise die Mobilfunknummer des Klägers erbeutet und veröffentlicht worden ist, vermag das Gericht nicht abzuschätzen. Dass die Beweislage in der Zukunft eine schwierige ist, schließt einen Feststellungsanspruch nicht aus.

2.

Der Antrag ist auch begründet. Insoweit wird auf die Ausführungen zu den nicht widerlegten Verstößen der Beklagten gegen die DSGVO bei dem Klageantrag zu 1. verwiesen.

Klageantrag zu 3.a.

Das mit dem Klageantrag zu 3.a. verfolgte Unterlassungsbegehren, ist bereits unzulässig, da es sich tatsächlich um eine verdeckte Leistungsklage handelt (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

1.

So enthält der Klageantrag mit der geforderten Androhung nach § 890 Abs. 2 ZPO ein unzulässiges Antragsbegehren.

Die Titulierung einer Unterlassungsverpflichtung kann - auch unter Berücksichtigung der Grundsätze der Effektivität und Äquivalenz - eine gleichfalls nach § 890 ZPO vollstreckbare Verpflichtung zur Handlung nur beinhalten, wenn der Schuldner der Pflicht zur Unterlassung ausschließlich genügen kann, indem er die hierfür erforderliche positive Handlung vornimmt. Ob ein Titel Handlungspflichten auferlegt oder Unterlassung fordert, ist im Wege der Auslegung mit Blick auf den Schwerpunkt der jeweils in Rede stehenden Verpflichtung zu beurteilen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.*).*

Vorliegend fordert der Kläger mit dem Antrag zu 3.a. im Schwerpunkt ein aktives Tun, das nicht nach § 890 ZPO, sondern als vertretbare Handlung nach § 887 ZPO zu vollstrecken ist - nämlich zukünftig Kontaktimportfunktionen nur im Einklang mit den einzuhaltenden Sicherheitsvorkehrungen "freizuschalten", um Zugriffe unbefugter Dritter nach Möglichkeit von vorneherein zu verhindern - so wie es die DSGVO verlangt. Der Kläger will gar kein Unterlassen der Nutzung der Kontaktimportfunktion, was er durch eine schlichte Umstellung der Suchbarkeitseinstellungen hätte erreichen können, sondern er will, dass er die bzw. zukünftig irgendeine andere Kontaktimportfunktion unter Wahrung der Sicherheitsanforderungen nutzen kann (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

2.

Die Klage ist aber auch im Übrigen im Hinblick auf § 259 ZPO insgesamt unzulässig.

a)

Da der Antrag tatsächlich auf ein zukünftiges aktives Tun gerichtet ist, ist er an § 259 ZPO zu messen, dessen Voraussetzung der Besorgnis nicht rechtzeitiger Leistung offensichtlich nicht gegeben ist (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Der Kläger hat einen gesetzlichen Anspruch gegen die Beklagte aus Art. 25 Abs. 1 und Art. 32 DSGVO auf Wahrung der Sicherheitsanforderungen. Dieser ist aber nach ihrem eigenen erstinstanzlichen Vortrag erfüllt. Er ist auch tatsächlich allein deshalb erfüllt, weil es die Such- und Kontaktimportfunktion hinsichtlich der Mobilfunktelefonnummer seit dem 06.09.2019 gar nicht mehr gibt, sondern nur noch die "People-You-May-Know"-Funktion. Die Klage ist also auf zukünftige Leistung der Beklagten für den Fall gerichtet, dass es droht, dass die Scraper Wege finden, die neue Funktion zu umgehen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Insoweit besteht bis heute und bestand auch bei Klageerhebung aber den Umständen nach keine Besorgnis nicht rechtzeitiger Leistung im Sinne des § 259 ZPO. Die Beklagte hat nach (interner) Aufdeckung des Scraping-Vorfalls am 06.09.2019 die streitgegenständliche Funktion eliminiert. Es ist seitdem nicht wieder zu einem Vorfall gekommen. Die Beklagte hat zu keinem Zeitpunkt geltend gemacht, sie brauche nicht zu leisten oder sie wolle den gegen sie erhobenen, gesetzlichen Anspruch nicht erfüllen (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

b)

Das Feststellungsinteresse des Klägers fehlt aber insbesondere, weil er selbst das Benutzerverhältnis gekündigt hat und seine Daten für eine Kontaktimporterfunktion nicht mehr zur Verfügung stehen.

3.

Ob und wann eine Umdeutung der Leistungsklage in eine Feststellungsklage nach § 256 Abs. 1 ZPO in Betracht kommt, kann hier offenbleiben, weil für eine

Feststellungsklage jedenfalls kein Rechtsschutzinteresse besteht. Die Beklagte ist ohnehin an die gesetzlichen Vorgaben der Art. 25 Abs. 1 und Art. 32 DSGVO gebunden, was nicht weiter festgestellt werden muss, zumal eine Vollstreckung aus einem entsprechenden Feststellungsurteil nicht möglich ist (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Klageantrag zu 3.b.

Die mit dem Klageantrag zu 3.b. verfolgte Unterlassungsklage ist bereits unzulässig.

1.

Zunächst liegt nach dem Schwerpunkt des Rechtsschutzbegehrens in der Sache erneut kein Unterlassen, das nach § 890 Abs. 2 ZPO vollstreckt werden könnte, sondern eine Leistungsklage, gerichtet auf ein aktives Tun vor (siehe schon oben zum Antrag zu 3.a.). Denn die Klage ist auf ein aktives Tun gerichtet, zukünftig die Mobilfunktelefonnummer nur nach Maßgabe einer infolge ausreichender Information wirksam erteilten Einwilligung im Rahmen einer Suchfunktion zu verarbeiten (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

2.

Diese verdeckte Leistungsklage wahrt nicht die Grenzen des § 259 ZPO. Auch insoweit gilt - wie bezüglich des Antrags zu 3.a. ausgeführt -, dass wegen der endgültigen Abschaffung der Such- / Kontaktimportfunktionen am 06.09.2019 bereits seit Klageerhebung schon keine Besorgnis der Leistungsverweigerung mehr bestand und mangels anderer Anhaltspunkte auch heute nicht besteht (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris).

Insbesondere aber hat der Kläger sein Benutzerprofil gelöscht, sodass eine Nutzung seiner Mobilfunknummer nicht mehr im Raum steht.

Klageantrag zu 4.

Die mit dem Klageantrag zu 4. verfolgte Auskunftsklage ist zulässig, aber unbegründet.

Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung (so auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23-, juris m.w.N.).

Diese Daten sind dem Kläger ausgehändigt worden. Er hat mit der Replik und in der mündlichen Verhandlung einen Ausdruck seiner Profilinformationen vorgelegt. Ferner ist den Prozessbevollmächtigten des Klägers und damit auch zurechenbar auch dem Kläger bekannt, dass die Beklagte angibt – und damit Auskunft erteilt hat – dass ihr keine Rohdaten zu den abgerufenen Daten vorliegen und Hinweise auf das Handeln mehrerer Scraper, nicht eines Scrapers vorliegen.

Klageantrag zu 5.

Soweit der Kläger mit dem Klageantrag zu 5. den Ersatz vorgerichtlicher Rechtsanwaltskosten begehrt, ist die Klage teilweise begründet, nämlich soweit er mit den Klageanträgen zu 1. und 2. (teilweise) obsiegt.

Es wird auf die Ausführungen zum Klageantrag zu 1. verwiesen, dass die Beklagte einen Verstoß gegen die DSGVO nicht widerlegt hat. Der dem Kläger zustehende Schadensersatzanspruch nach Art. 82 Abs. 2, Abs. 1 DSGVO umfasst auch die notwendigen Kosten zur Rechtsverfolgung. Es bestehen keine Zweifel, dass es zur Verfolgung von Ansprüchen gegen ein Großunternehmen wie der Beklagten erforderlich war, einen Rechtsanwalt einzuschalten.

Bei der Bemessung des erforderlichen Honorars hat das Gericht 1.000,00 € berücksichtigt und den Umstand, dass die Klägervertreter bekanntlich die Ansprüche mit Anspruchsschreiben verfolgen, die für eine Vielzahl an Fällen vorformuliert sind. Gerechtfertigt ist daher nur eine 1,3-fache Geschäftsgebühr nebst Auslagenpauschale und Umsatzsteuer. Es ergibt sich ein zu erstattender Betrag von 159,93 €.

Zinsen gemäß § 291 BGB waren einen Tag nach der Verteidigungsanzeige des Beklagtenvertreters am 14.12.2022 zuzusprechen. Der Rückschein zur Klagezustellung ist nicht zur Akte gelangt, sodass sich eine frühere Zustellung nicht feststellen lässt.

IV.

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO und berücksichtigt entsprechend des angenommenen Streitwertes das teilweise Obsiegen und Unterliegen der Parteien. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 11, 711 ZPO.