10 O 34/23

Landgericht Duisburg

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

,

Klägers,

Prozessbevollmächtigte: Wilde, Beuger, Solmecke Rechtsanwälte
Partnerschaft mbB,
Eupener Straße 67, 50933 Köln,

gegen

die Meta Platforms Ireland Limited, vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

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

hat die 10. Zivilkammer des Landgerichts Duisburg
im schriftlichen Verfahren mit Schriftsatzfrist bis zum 26.01.2024
durch die Richterin als Einzelrichterin

für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerseite als Ausgleich für Datenschutzverstöße einen immateriellen Schadensersatz in Höhe von 500,00 EUR, nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 29.03.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite sämtliche materiellen künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten („Facebook-Datenleak“), der nach Aussage der Beklagten im Jahr 2019 erfolgte, künftig entstehen werden.

3. Die Beklagte wird verurteilt, an die Klagepartei außergerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit 29.03.2023 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits trägt die Klagepartei zu 6/7 und die Beklagte zu 1/7.

6. Das Urteil ist vorläufig vollstreckbar. Beide Parteien können die Vollstreckung durch die jeweils andere Partei durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die vollstreckende Partei vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrags leistet.

Tatbestand:

Die Klagepartei macht gegen die Beklagte Schadensersatz-, Unterlassungs- und Auskunftsansprüche im Zusammenhang mit einem sog. „*Scraping-Vorfall*“ geltend.

Die Beklagte mit Sitz in Dublin, Irland, betreibt die Social-Media-Plattform *Facebook*, die unter anderem über die Website-URL *www.facebook.com* abrufbar ist. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu ihrer Person machen und im von der Beklagten

vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

Im Rahmen der Registrierung – nach Eingabe einer E-Mail-Adresse oder einer Telefonnummer – müssen die Nutzer für ihr Profil zwingend einen Namen und ein Geschlecht angeben. Darüberhinausgehende Informationen sind optional. Jeder Nutzer verfügt zudem über eine Nutzer-ID.

Bei den verpflichtend bei der Registrierung anzugebenden Nutzerdaten für das Nutzerprofil – Name und Geschlecht – sowie auch bei der Nutzer-ID handelt es sich um immer öffentliche Nutzerinformationen, die für jedermann, auch für Nicht-Nutzer der Plattform, auf dem Profil des jeweiligen Nutzers einsehbar sind. Die Öffentlichkeit der darüberhinausgehenden Daten – wie z. B. der Telefonnummer, des Wohnorts, des Beziehungsstatus, des Geburtstags und der E-Mail-Adresse – ist durch den jeweiligen Nutzer steuerbar. Durch die *Zielgruppenauswahl* kann der Nutzer auswählen, wer einzelne Informationen im Facebook-Profil eines Nutzers sehen kann, z. B. *„Nur ich“*, „*Freunde“*, „*Freunde von Freunden*“ und „*Alle*“. Unter „*Freunden*“ sind dabei andere Nutzer zu verstehen, mit denen sich der Betroffene bereits auf der Plattform vernetzt hat. In den *Suchbarkeits-Einstellungen* kann der Nutzer auswählen, für wen sein Nutzerprofil auffindbar ist. Die Sichtbarkeit nach der Zielgruppenauswahl und die Suchbarkeit bzw. Auffindbarkeit können also unabhängig voneinander eingestellt werden und müssen nicht übereinstimmen.

Jedenfalls im Jahr 2019 bestand für die Nutzer zudem die Möglichkeit, eine Telefonnummer zu ihrem Profil hinzuzufügen. Über das sog. *Contact-Import-Tool* (nachfolgend: CIT) der Beklagten war es dann möglich, die im Smartphone eines Nutzers gespeicherten Kontakte mit den Nutzern der Plattform der Beklagten – soweit diese ihre Telefonnummern ebenfalls hinterlegt und die Auffindbarkeit innerhalb der Suchbarkeits-Einstellungen aktiviert hatten – abzugleichen und sich darüber mit den gefundenen Nutzern zu vernetzen.

Zudem bot die Beklagte unter Verwendung der Telefonnummer eine sog. *Zwei-Faktor-Authentifizierung* an, die der Sicherung des Nutzerkontos dienen sollte.

Soweit keine individuellen Einstellungen getroffen wurden, richteten sich die Sichtbarkeit und die Suchbarkeit nach den Standardeinstellungen der Beklagten. Für den Fall der Angabe einer Telefonnummer war die Suchbarkeits-Einstellung auf „*Alle*“ voreingestellt.

Die Plattform der Beklagten verfügt über einen allgemein zugänglichen Hilfebereich, in dem über die vorgenannten Einstellungsmöglichkeiten informiert wird. Darin befinden sich unter anderem Anleitungen, wie man eine Anpassung der Zielgruppenauswahl und der Suchbarkeits-Einstellungen vornehmen kann, Anlagen B2 – B5 zur Klageerwiderung. Sie verfügt zudem über einen sog. *Privatsphäre-Check*, der es den Nutzern ermöglicht, die eigenen Privatsphäre-Einstellungen zu kontrollieren. Auch können Nutzer über das Tool „*Wer kann nach mir suchen?*“ überprüfen, wer ihr Profil finden kann.

Von der Beklagten wird zudem noch eine Messenger-App betrieben, die eine Versendung von kurzen Nachrichten der Nutzer der Plattform ermöglicht. Nutzer melden sich dafür mit ihren bei der Beklagten bereits bestehenden Nutzerkonten an.

Die Klagepartei ist registrierter Nutzer der von der Beklagten betriebenen Plattform. Das klägerische Profil konnte aufgrund der hinterlegten Telefonnummer und der auf „*Alle*“ standardmäßig eingestellten Suchbarkeit von jedem Nutzer gefunden werden, der die Nummer der Klagepartei in das CIT hochlud, Anlage B 17, Bl. 294 d. A.

Jedenfalls auch im Jahr 2019 griffen Dritte auf die bei der Plattform der Beklagten hinterlegten Daten zu und schöpften diese ab (sog. „*Scraping-Vorfall*“). In welchem Umfang die Daten abgeschöpft – „*gescraped*“ – wurden ist zwischen den Parteien streitig. In Hinblick auf den Abschöpfungsvorgang gehen die Parteien übereinstimmend davon aus, dass Dritte das auf der Plattform der Beklagten hinterlegte CIT verwendeten, um einzelne Telefonnummern den Profilen einzelner Nutzer zuzuordnen, ohne dass diese auf den Profilen der Nutzer öffentlich einsehbar waren. Hierzu wurden Nummern in ein virtuelles Telefonbuch hochgeladen und dann über das CIT mit den auf der Plattform der Beklagten hinterlegten Telefonnummern synchronisiert. Das jeweils ausgeworfene Profil wurde daraufhin durch die Dritten besucht, die darauf befindlichen öffentlichen Daten abgeschöpft und dann mit der verwendeten Telefonnummer korreliert. Einer Sichtbarkeit der Telefonnummer auf dem Profil des jeweiligen Nutzers bedurfte es dafür nicht.

Eine Unterrichtung der Klagepartei über den Vorfall erfolgte seitens der Beklagten zunächst nicht.

Anfang April 2021 wurden die in diesem Vorgang abgeschöpften Daten von ca. 533 Millionen Facebook-Nutzern im Internet veröffentlicht. Darunter befanden sich auch Daten der Klagepartei, wobei der genaue Umfang der abgeschöpften Daten zwischen den Parteien streitig ist.

Mit E-Mail vom 13.09.2022 forderte die Klagepartei die Beklagte zur Zahlung von Schadensersatz, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zu einer Auskunft darüber auf, welche konkreten Daten abgegriffen und veröffentlicht worden seien. Wegen der Einzelheiten wird auf die Anlage 1 zur Klageschrift, Bl. 53 ff. d. A., verwiesen.

Die Beklagte wies das Schadensersatz- und Unterlassungsbegehren der Klagepartei mit Schreiben vom 12.10.2022, Anlage B 16, Bl. 274 ff. d. A., zurück. Mit demselben Schreiben teilte die Beklagte der Klagepartei mit, dass es ihr nicht gelungen sei, der Nutzer ID der Klagepartei Informationen aus den durch Scraping abgerufenen Daten zuzuordnen. Für die Details wird auf das Schreiben der Beklagtenseite vom 12.10.2022, Anlage B 16, Bl. 274 ff. d. A., verwiesen.

Im November 2022 verhängte die irische Datenschutzbehörde DPC gegen die Beklagte eine Geldbuße in Höhe von 265 Mio. € mit der Begründung, die Beklagte habe es nicht hinreichend verhindert, dass etwa 533 Mio. Datensätze mit persönlichen Informationen von Facebook-Nutzern abgegriffen und veröffentlicht worden seien.

Die Klagepartei behauptet, sie habe ihre Telefonnummer nur aufgrund der Zwei-Faktor-Authentifizierung angegeben. Diese habe dann aufgrund einer Sicherheitslücke bei der Beklagten mit den restlichen Personendaten korreliert werden können, obwohl die bei den entsprechenden Profilen hinterlegten Telefonnummern öffentlich nicht freigegeben gewesen seien. Die Beklagte habe im Zeitpunkt des Vorfalls keinerlei Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des CIT zu verhindern.

Zudem seien die Sicherheitseinstellungen auf der Webseite der Beklagten so kompliziert und verwirrend gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Nutzer würden mit einer Vielzahl an Informationen hinsichtlich der Nutzungsbedingungen, der Verwendung von Cookies und Datenschutzrichtlinien konfrontiert. Aufgrund dieser Vielzahl an Einstellungsmöglichkeiten behielten Nutzer, die durch die Beklagte vorbestimmten Standardeinstellungen zum größten Teil oder auch gänzlich bei. Hierzu verweist die Klagepartei auf einzelne Screenshots von der Plattform der Beklagten, Bl. 10 ff. d. A. Hinzu kämen separate Einstellmöglichkeiten betreffend die durch die Beklagte vorgehaltene Messenger-App.

Die Klagepartei ist der Ansicht, die Vertraulichkeit der Telefonnummer des jeweiligen Nutzers sei besonders schützenswert. Sie behauptet hierzu, nicht darauf hingewiesen worden zu sein, dass durch die angegebene Nummer in irgendeiner Weise das Profil des Nutzers identifiziert werden könne.

Die Veröffentlichung der Daten habe weitreichende Folgen für die Klagepartei. Die Zuordnung von Telefonnummern zu weiteren Daten wie Vor- und Nachnamen, E-Mail-Adresse oder Anschrift eröffne Kriminellen die Möglichkeit des „*Identitätsdiebstahls*“, der Übernahme von Accounts und gezielter „*Phishing*“-Nachrichten. Aufgrund der Veröffentlichung im Internat habe die Klagepartei einen erheblichen Kontrollverlust erlitten, sie fühle sich unwohl und sorge sich über möglichen Missbrauch der abgeschöpften Daten. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Adressen und Nummern. Die Klägerseite erhalte seit dem Vorfall betrügerische Kontaktversuche. Sie könne daher nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren, da sie jedes Mal einen Betrug fürchten müsse und Unsicherheit verspüre. Die unterlassene Information durch die Beklagte habe zudem zu einer Intensivierung des Schadens geführt.

Die Klagepartei ist der Ansicht, dass die Datenverarbeitung durch die Beklagte ohne Rechtsgrundlage erfolgt sei und die Beklagte sie nicht im ausreichenden Maße über die Verarbeitung sie betreffender Daten informiert bzw. aufgeklärt habe; dies gelte insbesondere im Hinblick auf die fehlende Aufklärung über die Verwendung und Geheimhaltung ihrer Telefonnummer. Darüber hinaus seien die Daten der Klagepartei durch die Beklagte nicht im ausreichenden Maße geschützt worden. Zudem sei die Beklagte ihrer Informationspflicht nicht nachgekommen, da sie die Klagepartei nicht über den Datenschutzverstoß informiert habe. Das Antwortschreiben der Beklagten auf das Auskunftsersuchen der Klagepartei sei außerdem insgesamt unzureichend.

Sie ist weiter der Ansicht, dass die Beklagte die Darlegungs- und Beweislast im Hinblick darauf trage, dass sie keine Pflichten aus der DSGVO verletzt habe. Zudem führe bereits die Verletzung der DSGVO zu einem auszugleichenden immateriellen Schaden, ein darüber hinaus entstandener Schaden sei durch die Klagepartei nicht darzulegen.

Die Klagepartei beantragt,

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

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

   a. personenbezogenen Daten der Klägerseite, 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. 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 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 wird verurteilt 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 Kontaktimporttools erlangt werden konnten.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, der klägerische Vortrag zum „*Scraping-Vorfall*“ beruhe auf einem Missverständnis. Es sei nicht substantiiert vorgetragen, welche Daten der Klagepartei genau abgeschöpft worden seien. Der Vorfall sei nicht Folge eines Datenschutzverstoßes durch die Beklagte oder einer technischen Schwachstelle, vielmehr seien – so behauptet die Beklagte – lediglich automatisch gesammelte öffentlich einsehbare Daten „gescraped“ worden. Die Telefonnummer hätten Dritte durch die Verwendung einer Telefonnummeraufzählung erhalten und nicht bei der Beklagten abgeschöpft.

Die Beklagte stelle darüber hinaus ihren Nutzern alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung. 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 Nutzerkonto hinterlegt habe, einsehen könne.

Im Einklang mit der Marktpraxis habe die Beklagte während des relevanten Zeitraums sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt. Die Beklagte entwickle ihre Maßnahmen zur Verringerung von „*Scraping*“ und als Reaktion auf sich ständig ändernde Bedrohungen fortlaufend weiter. Sie beschäftige hierzu ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren (External Data Misuse-Team, EDM-Team). Die Beklagte habe auch auf die Verwendung des CIT durch „*Scraper*“ reagiert und eine Verknüpfung mit den Telefonnummern der Nutzer sei auf diesem Wege nun nicht mehr möglich. Auch

nutze die Beklagte Captcha-Abfragen, die dazu genutzt würden, herauszufinden, ob hinter einer Anfrage ein menschlicher Nutzer stehe oder nicht.

Eine weitergehende Auskunft als in dem an die Klagepartei gerichteten Antwortschreiben sei der Beklagten nicht möglich, da sie über keine Kopie der Rohdaten, welche die durch „*Scraping*“ abgerufenen Daten enthalte, verfüge.

Entscheidungsgründe:

Die zulässige Klage ist in dem im Tenor ersichtlichen Umfang begründet.

A.

Die Klage ist zulässig.

I.

Das Landgericht Duisburg ist in internationaler, örtlicher und sachlicher Hinsicht zuständig.

1.

Die internationale und örtliche Zuständigkeit des Landgerichts Duisburg folgt aus Artt. 79 Abs. 2 Satz 2, 28 Abs. 4 DSGVO und § 44 Abs. 1 Satz 2 BDSG sowie aus Art. 17 Abs. 1 lit. c) EuGVVO i. V. m. Art. 18 Abs. 1 EuGVVO, jeweils i. V. m. §§ 12, 13 ZPO. Da die Vorschriften dieselbe internationale und örtliche Zuständigkeit begründen, kann vorliegend dahinstehen, in welchem Verhältnis diese zueinanderstehen, wobei von einem Vorrang des besonderen Gerichtsstands des Art. 79 Abs. 2 Satz 2 DSGVO als lex specialis gegenüber den Gerichtsständen der EuGVVO auszugehen sein dürfte, vgl. Art. 67 EuGVVO und Erwägungsgrund 147 DSGVO.

Nach Art. 79 Abs. 2 DSGVO und § 44 Abs. 1 Satz 2 BDSG sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter die Gerichte des Mitgliedsstaats zuständig, in dem der Verantwortliche oder Auftragsverarbeiter seine Niederlassung hat; wahlweise können solche Klagen auch bei den Gerichten des Mitgliedsstaates erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse

tätig geworden ist. Dabei spricht eine Vermutung dafür, dass es sich bei einem bestehenden Wohnsitz um den Aufenthaltsort der Klagepartei im Sinne der Norm handelt (*Mundil* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.11.2021, DS-GVO Art. 79, Rn. 18). Die Klagepartei mit Wohnsitz im Landgerichtsbezirk Duisburg richtet ihre Klage gegen die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Die diesbezügliche Behauptung reicht in Anbetracht des Vorliegens einer doppeltrelevanten Tatsache zur Begründung der Zuständigkeit aus.

Nach Art. 18 Abs. 1 EuGVVO kann darüber hinaus die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Nach Art. 17 Abs. 1 EuGVVO gilt Art. 18 EuGVVO, wenn Gegenstand des Verfahrens ein Vertrag oder Ansprüche aus einem Vertrag sind, den eine Person, der Verbraucher, zu einem Zweck geschlossen hat, der nicht der beruflichen oder gewerblichen Tätigkeit dieser Person zugerechnet werden kann und wenn – lit. c) – der andere Vertragspartner im Mitgliedsstaat, in dessen Hoheitsgebiet der Verbraucher seinen Wohnsitz hat, eine berufliche oder gewerbliche Tätigkeit ausübt oder eine solche auf irgendeinem Wege auf diesen Mietgliedstaat oder auf mehrere Staaten, einschließlich dieses Mitgliedstaates, ausrichtet und der Vertrag in den Bereich dieser Tätigkeit fällt. Die Beschränkung des EuGVVO auf die Erbringung von Dienstleistungen und die Lieferung beweglicher Sachen ist damit entfallen (*Stadler* in: Musielak/Voit, ZPO, 19. Aufl. 2022, EuGVVO Art. 17 Rn. 6).

Vorliegend ist nach den klägerischen Behauptungen zwischen den Parteien jedenfalls ein Nutzungsvertrag über die durch die Beklagte betriebene Plattform zustande gekommen, §§ 133, 157 BGB. Wer dem Verbraucher die Bereitstellung digitaler Inhalte gegen die Preisgabe von Daten anbietet, sei es die Nutzung einer Social-Media-Plattform oder einer Suchmaschine, unterbreitet typischerweise ein Angebot auf Abschluss eines Vertrags, welches innerhalb der AGB in der Regel konkretisiert wird (*Metzger* in: MüKo, BGB, 9. Aufl. 2022, BGB § 327 Rn. 17).

Die Klagepartei ist hier als Verbraucherin aufgetreten. Der geschlossene Nutzungsvertrag diente weder ihrer gewerblichen noch beruflichen Tätigkeit. Die Klagepartei hat ihren Wohnsitz zudem im Gerichtsbezirk des Landgerichts Duisburg, § 13 ZPO.

Darüber hinaus findet Art. 18 Abs. 1 EuGVVO auch Anwendung auf deliktische Ansprüche nach §§ 823 ff. BGB. Nach der Rechtsprechung des EuGH ist für die Einbeziehung deliktischer Ansprüche in das Verbraucherschutzregime der Art. 17 ff. erforderlich, dass die deliktische Klage „*untrennbar mit einem zwischen dem Verbraucher und dem Gewerbetreibenden tatsächlich geschlossenen Vertrag verbunden ist*“ (*Stadler* in: Musielak/Voit, 19. Aufl. 2022, EuGVVO Art. 17 Rn. 1e). Die durch die Klagepartei geltend gemachten Verletzungen beziehen sich allesamt auf solche, die im Zusammenhang mit dem vorliegend geschlossenen Nutzungsvertrag stehen.

2.

Die sachliche Zuständigkeit des Landgerichts Duisburg folgt aus § 1 ZPO i. V. m. §§ 23 Nr. 1, 71 Abs. 1 ZPO, da der Zuständigkeitsstreitwert vorliegend jedenfalls über 5.000,00 € liegt.

II.

Die Klageanträge zu 1), 2) und 3) sind auch hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO.

1.

Der Zulässigkeit des Klageantrags zu 1) steht weder entgegen, dass der Schadensersatzanspruch nicht hinreichend beziffert worden sei, noch die von der Beklagten eingewandte Alternativität der zugrunde gelegten Lebenssachverhalte.

Die Bezifferung eines Geldzahlungsantrages kann dann unterbleiben, wenn statt der Bezifferung jedenfalls die Größenordnung des Betrags angegeben wird oder sich aus dem übrigen Klagevortrag ergibt. Das Gericht muss in die Lage versetzt werden, auf der Grundlage des klägerischen Vortrags eine Entscheidung über die Anspruchshöhe im Sinne des § 287 ZPO treffen zu können. Die Klagepartei hat in ihrem Antrag einen Mindestbetrag in Höhe von 1.000,00 € aufgenommen und der Entscheidung des Gerichts zulässigerweise zugrunde gelegt.

Entgegen des Beklagtenvortrags liegt der Streitsache auch ein einheitlich zu bewertender Lebenssachverhalt zugrunde; eine unzulässige Alternativität ist nicht festzustellen. Die Klagepartei stützt ihr Klagevorbringen zwar auf – von ihr behauptete – unterschiedliche Datenschutzverletzungen, diese sind aber innerhalb eines Lebenssachverhaltes danach zu bewerten, ob die von der Klagepartei

angegebenen Daten vor dem „*Scraping-Vorfall*“ hinreichend geschützt und die Nutzer zuvor hinreichend informiert wurden. Eine Aufspaltung des Antrags nach einzelnen Datenschutzverstößen würde den Streitgegenstand hingegen unnatürlich aufspalten.

2.

Auch der Klageantrag zu 2) ist hinreichend bestimmt. Es lässt sich ein hinreichender Bezug zu dem durch die Klagepartei behaupteten Datenleak und der behaupteten Betroffenheit eigener Rechtsgüter herstellen.

3.

Der Bestimmtheit des Klageantrags zu 3) steht nicht entgegen, dass die Klagepartei hierin Bezug auf die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen nimmt. Auch wenn es sich hierbei um einen auslegungsbedürftigen Begriff handelt und daraus resultierende Vollstreckungsprobleme denkbar sind, so ist dies zur Gewährleistung eines effektiven Rechtsschutzes hinzunehmen (LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 mit Verweis auf BGH, Urteil vom 04.03.2004 – I ZR 221/01, NJW 2004, 2080).

Dies muss nicht zuletzt deshalb gelten, weil sich aus der DSGVO schon kein Anspruch auf bestimmte Sicherungsmaßnahmen ableiten lässt und dem Störer insoweit ein Wahlrecht zukommt, Art. 32 DSGVO.

III.

Die Klagepartei hat im Hinblick auf den Klageantrag zu 2) auch ein hinreichendes Feststellungsinteresse, § 256 Abs. 1 ZPO.

Das Feststellungsinteresse wäre nur dann zu verneinen, wenn aus der Sicht der Klagepartei bei verständiger Würdigung kein Grund bestehen würde, mit dem Eintritt eines Schadens wenigstens zu rechnen (LG Essen, *aaO* mit Verweis auf BGH, Beschluss vom 09.01.2007 – VI ZR 133/06, juris). Nach dem vorliegenden Klagevortrag im Hinblick auf eine mögliche Verwendung der Daten durch Dritte, die der Öffentlichkeit zur Verfügung stehen, ist bei lebensnaher Betrachtung nicht völlig ausgeschlossen, dass solche durch Dritte schädigend verwendet werden und der Klagepartei hieraus ein künftiger Schaden entstehen könnte (vgl. LG München I, Urteil vom 09.12.2021 – 31 O 16606/20, GRUR-RS 2021, 41707).

B.

Die Klage ist in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Der Antrag zu 1. ist, soweit er immateriellen Schadensersatz wegen Datenschutzverstößen im Zusammenhang mit dem Scraping von Daten im Jahr 2019 betrifft, in Höhe von 500 € begründet. Die Klägerseite kann von der Beklagten aus Art. 82 DSGVO Zahlung von 500 € verlangen.

Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

1.

Die Beklagte hat als Verantwortliche gegen mehrere Vorschriften der DSGVO verstoßen.

Verantwortlicher ist nach der Legaldefinition in Art. 4 Nr. 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Personenbezogene Daten sind nach der Legaldefinition in Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Unter Verarbeitung ist nach Art. 4 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung

Hier hat die Beklagte als juristische Person von der Klägerseite personenbezogene Daten, nämlich neben den immer anzugebenden Daten wie Vor- und Nachnamen sowie Geschlecht insbesondere die Telefonnummer, erhoben und diese Daten danach für die Zwecke ihrer Plattform verwendet. Somit hat sie diese Daten als Verantwortliche verarbeitet.

Die Beklagte trägt – entgegen des allgemeinen zivilprozessualen Grundsatzes – die Darlegungs- und Beweislast dafür, dass ihr kein Verstoß gegen die DSGVO zu Last zu legen ist (so auch EuGH (Große Kammer), Urt. v. 4.7.2023 – C-252/21 (Meta Platforms Inc. ua/Bundeskartellamt); OLG Hamm, Urt. v. 15.8.2023 – 7 U 19/23). Dies folgt aus der spezifischen Beweislastregel in Art. 5 Abs. 2 DSGVO, nach der der Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO niedergelegten Grundsätze der Datenverarbeitung verantwortlich ist und deren Einhaltung nachweisen können muss („Rechenschaftspflicht“).

Gemessen daran hat die Beklagte weder schlüssig dargelegt noch bewiesen, dass ihre streitgegenständliche, zum Scraping-Vorfall bei der Klägerpartei führende Verarbeitung entgegen dem klägerischen Vorbringen nicht gegen die in Art. 5 Abs. 1 DSGVO normierten Grundsätze verstoßen hat.

a.

Die Beklagte hat nicht dargelegt und bewiesen, dass sie bei der Datenverarbeitung nicht gegen Art. 5 Abs. 1, Art. 6 Abs. 1 DSGVO verstoßen hat. Nach diesen Vorschriften ist eine Datenverarbeitung nur rechtmäßig, wenn eine der in Art. 6 Abs. 1 DSGVO genannten Bedingungen vorliegt. Dies bedeutet, jegliche Verarbeitung personenbezogener Daten, wie z.B. Erhebung, Verwendung, Verarbeitung etc. ist zunächst verboten, steht aber unter dem Erlaubnisvorbehalt des Art. 6 Abs. 1 DSGVO, der verschiedene Rechtfertigungsgründe normiert (Verbot mit Erlaubnisvorbehalt).

Hier hat die Beklagte mit der Telefonnummer der Klagepartei, die nach den Voreinstellungen für „alle“ auffindbar war, personenbezogene Daten der Klagepartei verarbeitet, indem sie sie abgefragt und für „alle“ Plattformnutzer auffindbar bereitgestellt hat.

Zu dieser Verarbeitung war sie nicht nach i.S.d. Art. 6 Abs. 1 DSGVO berechtigt.

aa.

Die Beklagte beruft sich im Hinblick auf die Datenverarbeitung ausdrücklich nicht auf eine Einwilligung der Klägerseite (vgl. Duplik der Beklagten vom 02.11.2023, Bl. 607 d. A.). Aber selbst wenn sie dies täte, läge keine wirksame Einwilligung der Klägerseite i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO in die Nutzung ihrer nicht öffentlich geteilten Mobilfunknummer für die Auffindbarkeit durch Dritte vor.

Nach Art. 6 I UAbs. 1 Buchst. a DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung für einen oder mehrere bestimmte Zwecke freiwillig in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung in informierter Weise und unmissverständlich i.S.v. Art. 4 Nr. 11 DSGVO erteilt hat. Dabei ist auch der Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a Var. 3 DSGVO zu berücksichtigen. Wie sich der eindeutigen Formulierung in Art. 4 Nr. 11 DSGVO entnehmen lässt, setzt eine Einwilligung ein aktives Handeln voraus. Zudem ergibt sich auch aus Erwägungsgrund 32 Satz 3 der DSGVO, dass aus Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit der betroffenen Person gerade keine Einwilligung folgt.

Vor diesem Hintergrund ist hier nicht von einer Einwilligung der Klagepartei auszugehen, dass ihre Telefonnummer für „alle“ öffentlich auffindbar war. Aus dem Umstand, dass die Suchbarkeit für Dritte anhand der Mobilfunknummer voreingestellt war, kann nach den oben dargestellten Grundsätzen der DSGVO keine wirksame Einwilligung hergeleitet werden, weil es insoweit an einer aktiven Handlung der Klagepartei fehlte. Weiterer Vortrag dazu, wodurch die Klägerseite in der erforderlichen aktiven Weise ihre Einwilligung zu der gegebenen Nutzung erteilt haben könnte, liegt nicht vor. Insbesondere ist kein Vortrag dahingehend feststellbar, dass die Klagepartei im Kontext der Erstregistrierung durch Klick auf den Button „Registrieren“ eine entsprechende Einwilligung abgegeben hat. Zwar wurde die Klägerseite in diesem Kontext unstreitig auf die Nutzungsbedingungen und die Datenschutzrichtlinie der Beklagten hingewiesen. Dass in einer dieser beiden Dokumente die hier streitgegenständliche Funktionalität auch nur Erwähnung findet, trägt die Beklagte jedoch nicht vor. Insoweit kann dem Registrierungsvorgang auch kein Erklärungswert beigemessen werden. Auch der Verweis auf Seite 6 der Datenschutzrichtlinie und den dortigen Link („Mehr dazu, wie Du die Informationen über dich kontrollieren kannst, die du mit diesen Apps und Webseiten teilst bzw. die andere teilen.“) führt nicht weiter. Denn es ist nicht vorgetragen, wohin dieser Link führt und welche Informationen dort aufzufinden sind. Selbst wenn unter diesem Link Informationen zu der hier streitgegenständlichen Funktionalität abrufbar wären, läge

jedenfalls keine informierte Einwilligung vor. In „informierter Weise“ ist eine Zustimmung nämlich nur dann, wenn die Informationen „leicht zugänglich und deutlich von anderen Sachverhalten klar zu unterscheiden sind. Insbesondere dürfen die Informationen nicht in AGB „versteckt“ werden (BeckOK DatenschutzR/Albers/Veit, 42. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 29-39). Davon kann hier keine Rede sein, wenn sich die Information (wenn überhaupt) nur unter einem Unterlink finden lässt, der aus der Datenschutzrichtlinie heraus führt und der zudem nach der gewählten Bezeichnung („Mehr dazu, wie Du die Informationen über dich kontrollieren kannst, die du mit diesen Apps und Webseiten teilst bzw. die andere teilen“) keinerlei Anhaltspunkte dahingehend enthält, dass dort auch Informationen zur Nutzung der Mobilfunknummer aufzufinden sein könnten, von der zum Zeitpunkt der Registrierung gerade nicht anzunehmen war, dass diese öffentlich geteilt würde (LG Lübeck, Urteil vom 7. Dezember 2023 – 15 O 73/23).

bb.

Die Datenverarbeitung war mit Blick auf die Suchbarkeit der Telefonnummer und insbesondere die Voreinstellung der Suchbarkeit auf „alle“ auch nicht für die Erfüllung des Vertrags i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO erforderlich. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Vorschrift angesehen werden kann, muss sie objektiv unerlässlich sein, 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 (EuGH (Große Kammer), Urt. v. 4.7.2023 – C-252/21 (Meta Platforms Inc. ua/Bundeskartellamt)). Nicht ausreichend ist, dass die Verarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist. Vielmehr muss die Datenverarbeitung für die ordnungsgemäße Erfüllung des Vertrags so wesentlich sein, dass keine praktikablen und weniger einschneidenden Alternativen zur Verfügung stehen.

Daran fehlte es hier. Dass die Auffindbarkeit der Telefonnummer für „alle“ nicht erforderlich war, zeigt sich bereits daran, dass die Beklagte es im streitgegenständlichen Zeitpunkt – auch wenn die Voreinstellung auf „*alle*“ lautete – den Nutzern freigestellt hat, die Telefonnummer als nur für „*Freunde von Freunden*“ oder „*Freunde*“ suchbar einzustellen. Ab 2019 stand den Nutzern auch die Option

„*Nur ich*“ zur Verfügung, mit der verhindert wird, dass irgendjemand anders das entsprechende Profil so finden kann.

cc.

Die Auffindbarkeit der Telefonnummer für „*alle*“ war auch nicht zur Wahrung der berechtigten Interessen der Beklagte erforderlich i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Selbst wenn man vor dem Hintergrund des von der Beklagten angegebenen Zwecks, „Menschen miteinander in Verbindung zu bringen“ die Auffindbarkeit der Telefonnummer für alle anderen Nutzer als berechtigtes Interesse bewerten würde, da diese Grundlage des CIT war, würde es jedenfalls an der Erforderlichkeit fehlen. Dies ergibt sich bereits daraus, dass das CIT mittlerweile ersatzlos gelöscht worden ist.

b.

Des Weiteren hat die Beklagte gegen das in Art. 25 Abs. 2 DSGVO niedergelegte Gebot verstoßen, durch Technikgestaltung und datenschutzfreundliche Voreinstellungen vor und bei der Datenverarbeitung zur Einhaltung der Datenschutzgrundsätze beizutragen und sicherzustellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Nach Art. 25 Abs. 2 DSGVO soll im Grundsatz ein Produkt oder Dienst für den Nutzer bereits ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen; der Verantwortliche ist verpflichtet, geeignete technisch-organisatorische Maßnahmen zu treffen (Hartung in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 24 f.). Nach Art. 25 Abs. 2 Satz 3 DSGVO muss durch entsprechende Voreinstellungen sichergestellt werden, dass personenbezogene Daten nicht ohne Eingreifen einer Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Dieser Grundsatz gilt auch und gerade für soziale Netzwerke; er muss allerdings dort seine Grenze haben, wo ein Dienst die öffentlich zugängliche Verbreitung – z. B. Blogs, Kommentarfunktionen – gerade beabsichtigt und dies auch hinreichend transparent ist (Hartung in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 26; Baumgartner in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2 Aufl. 2018, DS-GVO Art. 25 Rn. 20).

Hier war zwar nach dem Zweck der Beklagten, ein soziales Netzwerk zu betreiben, die öffentlich zugängliche Verbreitung der Telefonnummer über die Einstellung Auffindbarkeit für „*alle*“ beabsichtigt. Die Verwendung der Telefonnummer zu diesem Zweck wurde jedoch gerade nicht hinreichend transparent gemacht. Wie bereits oben näher ausgeführt, fehlt es hier an Vortrag der Beklagten dazu, dass die Klagepartei im Registrierungsprozess überhaupt oder jedenfalls in informierter Weise über die streitgegenständliche Funktionalität informiert worden ist. Das hier auch nach Inkrafttreten der DSGVO beibehaltene sog. „Opt-out-System“, bei dem die Klagepartei aktiv die datenschutzunfreundliche Suchbarkeitseinstellung „*alle*“ abwählen muss, genügt nicht den Anforderungen des Art. 25 DSGVO (so auch OLG Hamm, Urt. v. 15.8.2023 – 7 U 19/23). Diese datenschutzunfreundlichen Suchbarkeitseinstellungen haben es auch ermöglicht, dass die Telefonnummer der Klagepartei ohne deren Eingreifen mit ihren öffentlich sichtbaren personenbezogenen Daten zu einem neuen Datensatz zusammengefügt und mit der Verbreitung im Internet einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht worden ist.

c.

Die Beklagte hat auch gegen ihre aus Art. 32 DSGVO folgende Pflicht zur Ergreifung geeigneter technischer und organisatorischer Schutzmaßnahmen verstoßen. Nach dieser Vorschrift haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die von der Beklagten ergriffenen Maßnahmen waren technisch und organisatorisch ungeeignet i.S.d. 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.

Zwar folgt allein aus dem Umstand, dass Scraper durch unzulässige Nutzung des CIT die Telefonnummer der Klägerseite mit den öffentlich einsehbaren personenbezogenen Daten zu einem neuen Datensatz verbinden konnten und damit unbefugt als Dritte i.S.d. Art. 4 Nr. 10 DSGVO auf diesen zugreifen konnten, noch

nicht, dass die von der Beklagten getroffenen Maßnahmen nicht i.S.d. Art. 32 DSGVO geeignet waren (vgl. EuGH, Rs. C-340/21, VB gegen Natsionalna agentsia za prihodite, Rn. 39).

Denn die DSGVO geht nicht davon aus, dass durch geeignete technische und organisatorische Maßnahmen Verletzungen des Schutzes personenbezogener Daten gänzlich vermieden werden können und sie sieht in Art. 24 DSGVO ausdrücklich vor, dass der Verantwortliche den Nachweis dafür erbringen können muss, dass die von ihm umgesetzten Maßnahmen im Einklang mit der DSGVO stehen. Diese Möglichkeit bliebe ihm jedoch verwehrt, wenn aufgrund des unbefugten Zugangs von Dritten zu personenbezogenen Daten bereits eine unwiderlegliche Vermutung für die Ungeeignetheit der Maßnahmen angenommen würde (EuGH, Rs. C-340/21, VB gegen Natsionalna agentsia za prihodite, Rn. 30 ff.). Zudem schreibt Art. 32 DSGVO gerade keine konkreten Maßnahmen vor, sondern gesteht dem Verantwortlichen bei der Wahl der Mittel einen gewissen Beurteilungsspielraum zu (vgl. GA Pitruzzella GRUR-RS 2023, 8707 Rn. 38–44).

Vorliegend ist jedoch auch unter Berücksichtigung des Beurteilungsspielraums der Beklagten davon auszugehen, dass diese keine geeignete und gebotene Maßnahme gegen die Zusammenfügung der Telefonnummer mit den öffentlich sichtbaren Daten getroffen hat.

Soweit die Beklagte vorträgt, sie sei nicht verpflichtet gewesen, für die Vertraulichkeit solcher Informationen zu sorgen, die auf dem Profil der Klagepartei immer öffentlich einsehbar waren (Facebook-ID, Vorname, Nachname und Geschlecht), greift diese Argumentation zu kurz. Denn durch den Scraping-Vorfall sind gerade nicht lediglich diese – bereits öffentlichen – Daten veröffentlicht worden, sondern es ist zu einer Zusammenfügung dieser Daten mit der nicht öffentlich sichtbaren Telefonnummer, in deren Suchbarkeit die Klagepartei nicht eingewilligt hat, gekommen. Das Zustandekommen und den Zugang zu diesem neu entstandenen Datensatz hätte die Beklagte verhindern müssen.

Es 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 genügten nicht den Anforderungen des Art. 32 DSGVO. Zu berücksichtigten ist, 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 des Gerichts jedoch notwendig gewesen wäre. Es wäre für die Beklagte beispielsweise möglich gewesen, das CIT derart auszugestalten, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern hätte erfolgen können. Das Tool hätte beispielsweise neben der Telefonnummer weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachname berücksichtigen können (so auch LG Lüneburg, Urteil v. 24.01.2023, 3 O 82/22).. 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.

Soweit die Beklagte darüber hinaus vorträgt, sie gehe nun mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor, handelt es sich bei diesen Maßnahmen um solche, die erst nach dem erfolgten Scraping-Vorfall ergriffen wurden und die demnach zum hier streitgegenständlichen Zeitpunkt noch nicht im Einsatz waren. Diese Maßnahmen genügen daher bereits aus diesem Grund nicht den Anforderungen des Art. 32 DSGVO, da es diese Vorschrift erfordert, bereits vor und bei der Datenverarbeitung und nicht erst im Nachhinein angemessene Schutzvorkehrungen zu treffen (so auch LG Lübeck, Urteil vom 07.12.2023 – 15 O 73/23).

Soweit die Beklagte vorträgt, den „Social Connection Check“ eingeführt oder das CIT durch die PYMK-Funktion ersetzt zu haben, handelt es sich um solche Maßnahmen, welche nach ihrem Vortrag ebenfalls erst im Nachgang und damit nach dem streitgegenständlichen Vorfall ergriffen wurden. Weiterhin enthält der Vortrag der Beklagten diesbezüglich keine hinreichende Auseinandersetzung damit, aus welchen Gründen diese Maßnahmen nicht bereits vor dem streitgegenständlichen Vorfall ergriffen worden sind. Dies ist insbesondere auch unter dem Gesichtspunkt relevant, dass der Beklagten – wie oben bereits dargelegt – das Problem des Scrapings als „gängige Taktik“ bekannt war (so auch LG Lübeck, Urteil vom 07.12.2023 – 15 O 73/23; LG Frankfurt am Main, Urteil vom 21. März 2023 – 2-18 O 114/22-, nicht veröffentlicht).

d.

Ob die Beklagte darüber hinaus gegen Informationspflichten (Artt. 13, 14 DSGVO), Auskunftspflichten (Art. 15 DSGVO) und Meldepflichten (Artt. 33, 34 DSGVO) verstoßen hat, kann dahinstehen. Denn diese Pflichten sind zum einen bereits nicht vom Anwendungsbereich der Art. 82 DSGVO umfasst, der eine Verarbeitung personenbezogener Daten voraussetzt (aa.). Zum anderen ist auch nicht ersichtlich, wie ein Verstoß gegen diese Vorschriften kausal für den von der Klagepartei behaupteten Schaden geworden sein soll (bb.).

aa.

Der Anwendungsbereich des Art. 82 Abs. 1 DSGVO umfasst allein solche Verstöße gegen die DSGVO, die auf einer Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO beruhen, Art. 82 Abs. 2 Satz 1 DSGVO (so auch LG Essen, *aaO*; LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, juris; AG Straußberg, Urteil vom 13.10.2022 – 25 C 95/21, BeckRS 2022, 27811; LG Düsseldorf, Urteil vom 28.10.2021 – 16 O 128/20, ZD 2022, 48; andere Ansicht OLG Köln, Urteil vom 14.07.2022 – 15 U 137/21, ZD 2022, 617; *Quaas* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.08.2022, DS-VO Art. 82 Rn. 14 *mwN*).

Auch wenn der Wortlaut des Art. 82 Abs. 1 DSGVO allein auf einen Verstoß „*gegen diese Verordnung*“ Bezug nimmt, ergibt sich aus Art. 82 Abs. 2 DSGVO eindeutig, dass eine Haftung nur für solche Schäden entstehen soll, die durch eine nicht der DSGVO entsprechenden *Verarbeitung* verursacht wurden. Diese Auslegung steht auch im Einklang mit den Erwägungsgründen 146 und 75 der DSGVO. Der Erwägungsgrund 146 stellt auf eine *Verarbeitung* der personenbezogenen Daten ab. Der Erwägungsgrund 75 beschreibt beispielhaft Risiken, die aus der *Verarbeitung* personenbezogener Daten resultieren und aus denen materielle und immaterielle Schäden entstehen können, welche gerade über Art. 82 Abs. 1 DSGVO Ersatz finden sollen. Die dort benannten Risiken wie z. B. Diskriminierung, „Identitätsdiebstahl“ oder -betrug, finanzieller Verlust, Rufschädigung und der Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten gehen alle mit der *Verarbeitung* personenbezogener Daten einher.

Das Verhalten der Beklagten, durch welches sie möglicherweise ihre Auskunfts-, Informations- oder Benachrichtigungspflichten verletzt hat, stellt keine Verarbeitung im Sinne der oben genannten Legaldefinition in Art. 4 DSGVO dar und löst deshalb auch keinen Schadensersatzanspruch gemäß Art. 82 Abs. 1 DS-GVO aus.

Die genannten Pflichten aus Artt. 13, 14, 15, 33 und 34 DSGVO knüpfen nicht unmittelbar an eine Datenverarbeitung an, sondern stehen mit einer solchen allenfalls in Zusammenhang. So liegt in der von Art. 13 und 14 DSGVO geforderten Informationserteilung selbst keine Datenverarbeitung i.S.d. DSGVO. Insbesondere handelt es sich bei einer unterlassenen Information nicht um eine Datenverarbeitung. Auch die in Art. 15 DSGVO normierte Auskunftspflicht stellt selbst keine Datenverarbeitung dar, sondern knüpft höchstens an eine bereits erfolgte Verarbeitung an. Dasselbe gilt für die Meldepflichten aus Art. 33 und 34 DSGVO, die den Verantwortlichen zu einer Meldung an die zuständige Behörde sowie die betroffene Person verpflichten, wenn es zu einer Verletzung personenbezogener Daten gekommen ist.

bb.

Selbst wenn man davon ausginge, dass ein Verstoß gegen die genannten Pflichten vom Schutzbereich des Art. 82 DSGVO umfasst wäre, so hätte die Klagepartei jedenfalls nicht dargelegt, inwiefern die behaupteten Verstöße kausal für den von ihr angeblich erlittenen Schaden geworden sein sollen. Vielmehr ist das streitgegenständliche Scraping der Daten mit der öffentlichen Einstellung der Daten im Internet erstmals offenbar geworden. Dass eine in der Folge unterlassene Information hierüber entgegen Artt. 33, 34 DSGVO den behaupteten, damit bereits eingetretenen, Schaden in Gestalt der Befürchtung eines Datenmissbrauchs und des Kontrollverlusts über die Daten konkret weiter vertieft hätte, lässt sich bei dieser Sachlage nicht feststellen. Dafür, dass die Klagepartei bei vorheriger Information und Auskunft über die verarbeiteten Daten nach Artt. 13 – 15 DSGVO durch die Beklagte „Schritte zur Risikominimierung und Absicherung“ ergriffen hätte, ist sie mangels eines entsprechenden Beweisangebotes beweisfällig geblieben.

2.

Die Beklagte hat sich nicht gemäß Art. 82 Abs. 3 DSGVO von der vermuteten Haftung befreit. Die Verantwortung des Anspruchsverpflichteten wird zunächst grundsätzlich vermutet. Nach Art. 82 Abs. 3 DSGVO wird der Anspruchsverpflichtete von der Haftung befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Vorliegend kann dahingestellt bleiben, ob der Begriff der Verantwortlichkeit i.S.d. Art. 82 DSGVO mit dem Begriff des Verschuldens nach der deutschen Rechtsterminologie gleichzusetzen ist oder ob

er als Gefährdungshaftungstatbestand zu verstehen ist, mit der Folge, dass eine Haftung des Verantwortlichen nur bei atypischen Kausalverläufen oder bei höherer Gewalt entfiele. Denn selbst wenn Art. 82 DSGVO eine Exkulpationsmöglichkeit enthielte, wäre der Beklagten eine solche Exkulpation nicht gelungen.

Eine Haftungsbefreiung greift nämlich nur dann ein, wenn der Verantwortliche sämtliche Sorgfaltsanforderungen erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist (vgl. AG Hildesheim, Urteil vom 5. Oktober 2020 – 43 C 145/19; Spindler/Schuster/Spindler/Horváth, Recht der elektronischen Medien, 4. Auflage 2019, DS-GVO Art. 82 Haftung und Recht auf Schadensersatz, Rn. 11).

Im Hinblick auf die rechtwidrige Verarbeitung der Telefonnummer der Klägerseite ist nichts zu erkennen, was die Beklagte zu Exkulpation vortragen könnte. Vielmehr hat sie zumindest fahrlässig gehandelt. Der Beklagten war das Risiko von „Scraping“ und der Umstand bekannt, dass Übertragungsbeschränkungen umgangen werden können. Genauso war ihr bekannt, dass die Suchbarkeit der Telefonnummer der Klagepartei für „*alle*“ aufgrund ihrer Voreinstellungen selbst dann gegeben war, wenn die Klagepartei bezüglich der Sichtbarkeit der Telefonnummer die Zielgruppenauswahl auf privat einstellte. Die Beklagte hätte deshalb erkennen können, dass Dritte das CIT wie geschehen ausnutzen würden.

Die Beklagte kann sich auch nicht unter Hinweis auf ein mögliches Mitverschulden seitens der klagenden Partei von ihrer Haftung befreien. Denn da die klagende Partei nicht datenschutzkonform über die Suchbarkeit ihrer Telefonnummer für „*alle*“ informiert war und sie in diese auch nicht eingewilligt hat, kann es ihr nicht angelastet werden, dass sie diese datenschutzwidrige Voreinstellung nicht umgestellt hat.

3.

Die Klagepartei hat aufgrund der Verstöße auch einen Schaden i.S.d. Art. 82 DSGVO erlitten.

Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schäden. Ein materieller Vermögensschaden wurde von der insoweit darlegungs- und beweisbelasteten Klägerseite nicht vorgetragen. Sie beruft sich jedoch erfolgreich auf das Vorliegen eines immateriellen Schadens.

Die von der DSGVO verwandten Begriffe „immaterieller“ und „materieller“ Schaden sind unionsautonom auszulegen und setzen nach dem Wortlaut der Norm, der Systematik und Telos des Art. 82 Abs. 2, Abs. 1 DSGVO sowie der Art. 77 bis 84

DSGVO und den Erwgr. 75, 85 und 146 DSGVO einen über den schlichten Verstoß gegen die DSGVO hinausgehenden Schaden voraus (so EuGH GRUR 2023, 980 Rn. 29–42; GA Campos Sánchez-Bordona GRUR-RS 2022, 26562 Rn. 117).

Das heißt, dass im Rahmen des haftungsbegründenden Tatbestands des Art. 82 Abs. 2, Abs. 1 DSGVO zunächst zwischen einem haftungsrelevanten Datenschutzverstoß einerseits und einem – materiellen oder immateriellen – Schaden andererseits zu differenzieren ist. Beide sind nicht deckungsgleich, sondern selbstständige Voraussetzungen im Rahmen des Art. 82 DSGVO, die kumulativ vorliegen müssen.

Ein immaterieller Schaden i.S.d. Art. 82 DSGVO setzt – entgegen möglicherweise bestehendem innerstaatlichen Recht (vgl. für das deutsche Deliktsrecht zuletzt etwa BGH NJW 2023, 983 Rn. 18 mwN) – nach Wortlaut, Erwgr. 10, 146 DSGVO und Telos nicht voraus, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (so EuGH GRUR 2023, 980 Rn. 44–51 – Österreichische Post; vgl. auch BAG NZA 2021, 1713 Rn. 33; offengelassen BVerfG NJW 2021, 1005 Rn. 19 ff.; s. zu Störungen und Belästigungen sowie Zorn und Ärger in Abgrenzung gegenüber Schäden GA Campos Sánchez-Bordona GRUR-RS 2022, 26562 Rn. 111 ff.; GA Pitruzzella GRUR-RS 2023, 8707 Rn. 79 ff. und insbes. Rn. 83 zur von den nationalen Gerichten zu beantwortenden Frage des Schadens im Einzelfall).

Vielmehr kann nach der Rechtsprechung des EuGH bereits der Kontrollverlust über die Daten und/oder die Befürchtung genügen, dass künftig aufgrund des Verstoßes gegen die DSGVO eine missbräuchliche Verwendung der personenbezogenen Daten durch Dritte erfolgt (EuGH, Rs- C-340/21, VB gegen Natsionalna agentsia za prihodite, Rn. 80). Zur Begründung führt der EuGH aus, dass – auch ausweislich des Erwägungsgrunds 146 – eine solche weite Auslegung geboten sei, um den Zielen der DSGVO, ein hohes Datenschutzniveau zu gewährleisten, Rechnung zu tragen. Dass bereits der bloße Kontrollverlust über die Daten einen immateriellen Schaden i.S.d. Art. 82 DSGVO darstellen könne, ergebe sich darüber hinaus aus Erwägungsgrund 85 der DSGVO, nach dem „eine Verletzung des Schutzes personenbezogener Daten […] einen […] immateriellen Schaden für natürliche Personen nach sich ziehen [könne], wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten […]“.Aus dieser beispielhaften Aufzählung der „Schäden“, die den betroffenen Personen entstehen können, gehe hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen „Verlust der Kontrolle“ über ihre eigenen Daten infolge eines Verstoßes gegen die

DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte.

Eine derartige – von dem Verstoß gegen die DSGVO selbst – zu trennende Rechtsgutverletzung liegt hier vor.

Diese ergibt sich bereits aus dem Kontrollverlust der Klagepartei über ihre Daten, die mit dem unbefugten Abschöpfen durch die Scraper und der nachfolgenden Veröffentlichung der Datensätze im Internet einhergeht. Infolge der obigen Verstöße gegen die einschlägigen Bestimmungen der DSGVO war es den Scrapern möglich, die Telefonnummer der Klagepartei mit ihren öffentlich sichtbaren Daten zu einem Datensatz zusammenzufügen und für eigene oder fremde Zwecke weiterzuverwenden. Hierdurch wurde das Recht der Klägerseite verletzt, selbst zu entscheiden, wo und ob sie diese Daten im Zusammenhang auf Dauer verfügbar machen möchte (so auch LG Lübeck, Urteil vom 7. Dezember 2023 – 15 O 73/23 –, juris). Aufgrund der abgegriffenen und veröffentlichen Daten besteht für die Klagepartei ein Risiko, dass diese Daten unbefugt benutzt werden. Die negativen Folgen können dabei vielfältig sein und schwere Nachteile mit sich bringen, wie zum Beispiel die Belästigung durch Spam- und Werbenachrichten, die Zusendung von Viren oder vermögenswirksame Handlungen zu Lasten der klagenden Partei, sodass ein Schadensersatzanspruch gerechtfertigt ist. Etwas Anderes ergibt sich auch nicht aus dem Urteil des EuGH in der Rechtssache C-456/22 (VX, AT gegen Gemeinde Ummendorf), in dem der EuGH den „kurzzeitigen Verlust der Hoheit über personenbezogene Daten“ als solchen nicht als ausreichend erachtet hat, um einen immateriellen Schaden zu bejahen, solange die betroffene Person nicht darlegt, inwiefern ihr über diesen „kurzzeitigen Verlust“ hinaus ein Schaden entstanden ist (EuGH, C-456/22, Rn. 23). Denn die dieser Rechtssache zugrundeliegende Situation ist bereits nicht mit der hier vorliegenden vergleichbar. Während in der Rechtssache C-456/22 die Daten der Kläger (Vorname, Name und Adresse) lediglich für 3 Tage auf der Internetseite der Gemeinde veröffentlicht waren, ist der Datensatz der Klagepartei im hiesigen Verfahren dauerhaft im Internet verfügbar und kann dementsprechend nach wie vor für unlautere Machenschaften verwendet werden. Der von der Klagepartei insoweit hinreichend dargelegte immaterielle Schaden besteht daher im nicht nur kurzzeitigen, sondern vielmehr dauerhaften Kontrollverlust, der die oben genannten Gefahren mit sich bringt. Dieser Schaden ist insoweit auch von dem bloßen Verstoß gegen die DSGVO zu unterscheiden.

Vor diesem Hintergrund kann es dahinstehen, ob die Klagepartei zusätzlich – was von der Beklagten bestritten wird – in einem Zustand des Unwohlseins und Sorge über einen möglichen Missbrauch ihrer Daten verbleibt.

4.

Der Schaden beruht auch kausal auf den oben dargestellten Verstößen. Im Hinblick auf die datenschutzwidrige Verarbeitung der Telefonnummer der Klagepartei folgt dies daraus, dass es nicht zu dem Schaden gekommen wäre, wenn die Beklagte die Telefonnummer der Klagepartei nicht ohne Rechtfertigung nach Art. 6 DSGVO über das CIT für „*alle*“ zur Verfügung gestellt hätte. Die Kausalität zu den Verstößen gegen Art. 25 DSGVO und Art. 32 DSGVO ist ebenfalls gegeben, da es nicht zu einer unbefugten Verknüpfung der Telefonnummer mit den öffentlichen Informationen der Klagepartei gekommen wäre, wenn die Suchbarkeitseinstelllungen nicht durch die Beklagte auf „*alle*“ voreingestellt gewesen wäre und die Beklagte angemessene Maßnahmen getroffen hätte, um ein unbefugtes Ausnutzen des CIT zu verhindern.

5.

Das Gericht erachtet vorliegend einen Schadensersatz in Höhe von 500,00 € als angemessen.

Art. 82 Abs. 1 DS-GVO macht bezüglich der Höhe des Schadensersatzanspruchs keine Vorgaben, sodass die Ermittlung gemäß § 287 ZPO dem Gericht obliegt. Dabei ist das Ziel des Schadensersatzanspruchs nach Art. 82 Abs. 1 DSGVO zu berücksichtigen, Verstöße gegen die DS-GVO effektiv und abschreckend zu sanktionieren. Für die Bemessung der Höhe des Schadensersatzes können die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden, wie etwa die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs und des Zwecks der betreffenden Verarbeitung, weiterhin das Ausmaß des von der klagenden Partei erlittenen Schadens sowie die betroffenen Kategorien personenbezogener Daten (vgl. LG München I, Urteil vom 09.12.2021 – 31 O 16606/20, Rn. 44 - juris; BeckOK Datenschutzrecht, Wolff/Brink/Quaas, a.a.O., Rn. 31). Wesentlich für die Bemessung der Höhe des Schadensersatzes sind die konkreten Umstände des Einzelfalls.

Vorliegend muss bei der Bemessung der Höhe des immateriellen Schadensersatzes der klagenden Partei zunächst berücksichtigt werden, dass der Kontrollverlust über

die Daten hier zwar tatsächlich eingetreten ist und die oben beispielhaft dargestellten Risiken für die klagende Partei birgt. Allerdings ist auch zu berücksichtigen, dass die Gefahr von Spam- oder Fishing-SMS, sowie von mit krimineller Intention geführten Telefongesprächen auch zum allgemeinen Lebensrisiko gehört, mit welcher auch ohne den Verstoß gegen die DSGVO gerechnet werden muss. Eine gesunde Skepsis gegenüber SMS und Anrufen ist damit in gewisser Weise ohnehin berechtigt. In ganz erheblichem Maße wirkt sich vorliegend auch aus, dass die klagende Partei den Kontrollverlust ihrer Daten durch einen Wechsel ihrer Telefonnummer, die mit vergleichsweise wenig Umständen und Kosten verbunden ist, beseitigen kann. Berücksichtigt werden muss daneben für die Bemessung der Schadensersatzhöhe auch die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes, wobei das Gericht die hohe Abschreckungswirkung insbesondere in der Gesamtsumme aller immateriellen Schadensersatzansprüche gegen die Beklagte erblickt und berücksichtigt, dass das Allgemeininteresse im Schwerpunkt nach Art. 83 DSGVO durch die Verhängung von Bußgeldern gewahrt wird. Die Höhe des von vom Gericht angesetzten immateriellen Schadensersatzanspruchs berücksichtigt danach auch den Grundsatz der Verhältnismäßigkeit. Unter Abwägung dieser gesamten Gesichtspunkte erachtet das Gericht einen (immateriellen) Schadensersatz in Höhe von 500,00 Euro für angemessen, aber auch ausreichend.

II.

Die Entscheidung über die Zinsen folgt aus § 291, § 288 Abs. 1 BGB beginnend ab dem Tag nach Klagezustellung, hier der 29.03.2023.

III.

Der Klageantrag zu 2. ist begründet. Die Klägerseite hat Anspruch auf Feststellung der Eintrittspflicht für künftige materielle Schäden.

Ein Feststellungsantrag ist begründet, wenn die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vorliegen, also ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann (vgl. BGH, Beschluss vom 9. 1. 2007 - VI ZR 133/06).

Wie unter I. näher dargestellt, liegen diese Voraussetzungen hier vor. Entgegen der Auffassung der Beklagten ist darüber hinaus nicht erforderlich, dass eine gewisse Wahrscheinlichkeit für einen Schadenseintritt besteht. Der BGH hat klargestellt, dass jedenfalls in Fällen, in denen die Verletzung eines u.a. durch § 823 Abs. 1 BGB geschützten absoluten Rechtsguts und darüber hinaus ein daraus resultierender Vermögensschaden bereits eingetreten sind, die Begründetheit einer Klage, die auf die Feststellung der Ersatzpflicht für weitere, künftige Schäden gerichtet ist, nicht von der Wahrscheinlichkeit des Eintritts dieser Schäden abhängig ist (BGH, Urteil vom 17.10.2017 – VI ZR 423/16 –, NJW 2018, 1242 Rz. 49). Für den hier bereits eingetretenen immateriellen Schaden aufgrund des Kontrollverlusts über die Daten, der auch als Verletzung des allgemeinen Persönlichkeitsrechts eingeordnet werden kann und somit auch über § 823 Abs. 1 BGB geschützt wäre, kann nichts Anderes gelten. Demnach reicht vorliegend bereits die Möglichkeit eines Schadens aus. Es liegen, wie dargelegt, die Voraussetzungen des Schadensersatzanspruches aus Art. 82 Abs. 1 DSGVO vor. Auch die Möglichkeit künftiger materieller Schäden ist zu bejahen. Diese Möglichkeit folgt daraus, dass nicht absehbar ist, welche Dritte möglicherweise Zugriff auf die Daten erhalten haben und für welche kriminellen Zwecke diese möglicherweise missbraucht werden. Es erscheint eben nicht von vorneherein ausgeschlossen, dass die klagende Partei z.B. betrügerische Anrufe erhält, mit denen unter Vortäuschung falscher Identitäten sensible Daten abgegriffen werden.

IV.

Die mit dem Klageantrag zu 3. a und b geltend gemachten Unterlassungsansprüche sind unbegründet.

Entsprechende Ansprüche der Klagepartei ergeben sich weder aus § 1004 Abs. 1 S. 2, § 823 Abs. 1 BGB noch aus § 1004 Abs. 1 S. 2, § 823 Abs. 2 BGB i.V.m. Art. 25 Abs. 1 u. 2 DS-GVO.

Es kann dahinstehen, ob diese Ansprüche überhaupt anwendbar sind oder ob die DSGVO als vereinheitlichtes Datenschutzrecht, das in Art. 17 DSGVO und Art. 82 DSGVO lediglich einen Löschungs- und Schadensersatzanspruch vorsieht, insoweit eine Sperrwirkung entfaltet (so wohl BGH, Urteil vom 3. Mai 2022 – VI ZR 832/20). Denn die Voraussetzungen der Unterlassungsansprüche nach nationalem Recht sind vorliegend nicht gegeben.

Voraussetzung eines jeden vorbeugenden Unterlassungsanspruch ist die Wiederholungsgefahr (vgl. BGH, Urteil vom 19. Oktober 2004 – VI ZR 292/03 –, Rn. 17, juris, mwN). An dieser fehlt es jedoch vorliegend. Zwar begründet eine vorausgegangene, rechtswidrige Beeinträchtigung eines von § 823 Abs. 1 BGB geschützten absoluten Rechts eine tatsächliche Vermutung für die Wiederholungsgefahr, an deren Widerlegung hohe Anforderungen zu stellen sind (vgl. BGH, Urteil vom 30. Oktober 1998 – V ZR 64/98 –, BGHZ 140, 1-11, Rn. 20). Hier wäre die rechtswidrige Beeinträchtigung darin zu sehen, dass die Beklagte durch ihr datenschutzwidriges Verhalten zu einem Kontrollverlust der Klagepartei über ihre Daten beigetragen und dies dadurch in ihrem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1, Art. 1 Abs. 1 GG als sonstiges Recht i.S.d. § 823 Abs. 1 BGB verletzt hat.

Vorliegend kann die Wiederholungsgefahr aber zum einen vollständig dadurch abgewendet werden, dass die klagende Partei die Suchbarkeit ihrer Telefonnummer auf der streitgegenständlichen Plattform der Beklagten auf „privat“ einstellt. Wie oben ausgeführt, liegt der von der klagenden Partei gerügte und festgestellte Verstoß gegen die DSGVO durch die Beklagte allein darin, dass es Dritten möglich war, die Telefonnummer der klagenden Partei mit den auf ihrem Profil ohnehin öffentlich zugänglichen Daten durch einen Missbrauch des Kontakt-Importer-Tools zu verknüpfen, weil die Suchbarkeit der Telefonnummer auf „für alle“ voreingestellt war, die Beklagte hierüber nicht hinreichend informiert und keine Maßnahmen ergriffen hat, um den Missbrauch zu verhindern. Der Wiederholung dieses Verstoßes kann die klagende Partei aber ganz einfach selbst dadurch begegnen, dass sie ihre Telefonnummer auch hinsichtlich der Suchbarkeit auf „*Nur ich*“ einstellt, was seit 2019 unstreitig möglich ist. Eines vollstreckbaren Unterlassungsanspruchs gegen die Beklagte bedarf es insoweit nicht.

Zum anderen dürfte eine Wiederholungsgefahr hinsichtlich des gleichen Missbrauchs des CIT durch die mittlerweile ergriffenen Maßnahmen der Beklagten auch gering bis ausgeschlossen sein. So hat die Beklagte vorgetragen, dass sie im ersten Schritt das CIT derart geändert habe, dass wenn ein Nutzer seine Kontaktliste von seinem Mobiltelefon über das CIT auf die Plattform hochgeladen habe, der übereinstimmende Nutzer nur dann dem importierenden Nutzer angezeigt worden sei, wenn dieser zugleich einen Namen sowie die Telefonnummer für den hochgeladenen Kontakt importiert habe, der dem Namen des übereinstimmenden Nutzers geähnelt habe oder der übereinstimmende Nutzer den importierenden Nutzer bereits in seinen Kontakten gehabt habe (vgl. Duplik der Beklagten vom

02.11.2023, Bl. 587 ff. d. A.). Schließlich habe sie das CIT dergestalt überarbeitet, dass nach dem Import der Kontakte nur noch eine Liste von Personen angezeigt werde, die die importierende Person kennen könnte, deren Telefonnummern aber nicht zwingend mit den importierten Kontakten übereinstimme („Menschen, die du kennen könntest“ - „people you may know-Funktion“, PYMK-Funktion; Duplik aaO). Diese Maßnahmen sind ohne Weiteres überprüfbar. Die Klagepartei ist diesen ausführlichen Darlegungen nicht hinreichend entgegengetreten.

Soweit die Unterlassungsanträge über den oben unter I. festgestellten, konkreten Verstoß gegen die DSGVO hinausgehen, indem sie allgemeiner formuliert sind, fehlt es bereits an der Erstbegehung und damit an der tatsächlichen Vermutung der Wiederholungsgefahr. Insoweit besteht auch keine erstmalige konkret drohende Beeinträchtigung (vgl. zu diesem Erfordernis BGH, Urteil vom 5. Juli 2019 – V ZR 96/18 – , Rn. 28, juris; Urteil vom 17. September 2004 – V ZR 230/03 –, BGHZ 160, 232-240, Rn. 11). Dies gilt etwa für die Formulierung „personenbezogene Daten der Klägerseite, namentlich FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen“ gemäß dem Klageantrag zu 3. a. Denn soweit dieser Antrag über die Telefonnummer hinausgehende, personenbezogene Daten benennt, ist er jedenfalls deswegen unbegründet, weil keine Erstbegehung vorliegt. Dafür, dass andere Daten als die jeweilige Telefonnummer datenschutzwidrig verarbeitet wurden, ist die klagende Partei beweisfällig geblieben.

V.

Der Klageantrag zu 4. ist unbegründet.

Die Klagepartei hat gegen die Beklagte keinen (weitergehenden) Auskunftsanspruch aus Art. 15 DSGVO. Der Auskunftsanspruch wurde mit dem Antwortschreiben der Beklagten vom 12.10.2022 erfüllt und ist vollständig erloschen, § 362 Abs. 1 BGB. Der Klagepartei steht auch kein Anspruch auf Auskunft über die abgegriffenen Daten sowie die Personen, die die Daten abgegriffen haben, zu, da diese Informationen bereits bekannt oder für die Beklagte unmöglich zu beschaffen sind. Soweit die Klagepartei ihren Auskunftsanspruch darauf stützt, dass die Auskunft unvollständig gewesen sei, weil die Beklagte keine konkrete Auskunft zum in Rede stehenden Datenschutzvorfall erteilt und insbesondere nicht darüber informiert habe, wer auf die

Daten zugegriffen habe und welche Daten genau auf diesem Weg abgegriffen worden seien, vermag sie hiermit nicht durchzudringen.

Die Beklagte hat in ihrem Antwortschreiben vom 12.10.2022 bereits mitgeteilt, dass es ihr nicht gelungen sei, anhand der Nutzer ID festzustellen, welche Daten der Klagepartei aufgrund des Scraping-Vorfalls mit der Telefonnummer korreliert werden konnten. Um welche Daten es sich gehandelt hat, dürfte der Klagepartei aber selbst bekannt sein, da es sich um diejenigen Daten handelte, die zum Zeitpunkt des Scraping-Vorfalls öffentlich sichtbar waren. Hierbei handelt es sich unstreitig zumindest um den Vor- und Familiennamen, das Geschlecht und die Facebook-ID-Nummer. Welche Daten darüber hinaus öffentlich sichtbar waren und somit mittels Ausnutzung des CIT und anschließendem Scraping der Telefonnummer der Klagepartei zugeordnet werden konnten, hängt von den damaligen Profileinstellungen ab, über die die Klagepartei selbst verfügen konnte und die ihr deswegen bekannt waren.

Soweit die Klagepartei geltend macht, die Beklagte habe ihr zu Unrecht keine Auskunft darüber erteilt, wer auf die Daten zugegriffen habe, so verkennt sie, dass es der Beklagten unmöglich war und ist, eine solche Auskunft zu erteilen. Denn da sie den Scrapern die Daten unstreitig jedenfalls nicht freiwillig offengelegt hat, fehlt und fehlte es ihr an der Kenntnis deren Identität.

VI.

Als Teil des der klagenden Partei zustehenden Schadensersatzanspruchs hat sie gegen die Beklagte einen Anspruch auf Zahlung der außergerichtlichen Rechtsanwaltskosten. Ausgehend von einem Wert des berechtigten Verlangens der Klägerseite von bis zu 1.000,00 € zum Zeitpunkt der außergerichtlichen Tätigkeit ergibt dies Kosten in Höhe von 159,94 € (1,3 Geschäftsgebühr Nr. 2300, 1008 VV RVG: 114,40 €; Auslagen Nr. 7001 u. 7002 VV RVG: 20,00 €; 19% MwSt: 25,54 €).

VIII.

Der Zinsanspruch ergibt sich bezüglich der außergerichtlichen Rechtsanwaltskosten aus §§ 291, 288 BGB seit dem Tag nach Rechtshängigkeit, hier der 29.03.2023.

Die Kostenentscheidung folgt aus § 92 Abs. 1 Satz 1 ZPO.

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt hinsichtlich beider Parteien jeweils aus §§ 708 Nr. 11, 711 ZPO.

Der Streitwert wird auf 7.000,00 EUR festgesetzt.

Klageantrag zu 1): 1.000,00 €

Klageantrag zu 2): 500,00 €

Klageantrag zu 3): 5.000,00 €

Klageantrag zu 4): 500,00 €

Die Streitwertbemessung folgt aus §§ 3 ff. ZPO, § 48 GKG. Die Werte der einzelnen Klageanträge waren danach zu addieren.

Für den Klageantrag zu 1) bemisst sich die Höhe des Streitwertes nach dem durch die Klagepartei bezifferten Mindestschaden in Höhe von 1.000,00 €.

Im Hinblick auf den Klageantrag zu 2) ist ein Streitwert in Höhe von 500,00 € angemessen. Dabei ist insbesondere zu berücksichtigen, dass der Vorfall sich bereits im April 2019 ereignet haben soll. Zudem ist - da es sich vorliegend um eine Feststellungsklage handelt - ein Abschlag von 20 % vorzunehmen.

Bezogen auf die Klageanträge zu 3.) a. und b. ist ein Streitwert von 5.000,00 € anzusetzen. Da es sich um eine nichtvermögensrechtlichen Streitigkeit handelt, ist nach § 48 Abs. 2 GKG der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen zu bestimmen. Bei mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse ist von einem Streitwert von 5.000,00 € auszugehen (BGH, Beschluss vom 28.01.2021, III ZR 162/20, juris, Rn. 9). Ein solcher Fall ist vorliegend gegeben, Anhaltspunkte für ein geringeres oder höheres Interesse sind nicht gegeben. Die beiden Unterlassungsanträge sind wertmäßig als Einheit zu betrachten sind, weil sie letztlich auf dasselbe Ziel gerichtet sind, die Beklagte zu einem besseren Schutz der überlassenen Daten zu verpflichten (OLG Düsseldorf, Beschluss vom 13.07.2023 – I-16 W 51/23, n. v.).

Für den Klageantrag zu 4.) ist ein Streitwert von 500,00 € angemessen (vgl. OLG Köln NJOZ 2018, 1120; LAG Berlin/Brandenburg, NZA-RR 2021, 269 m. w. N.).