Beglaubigte Abschrift

8 O 86/22

Landgericht Duisburg

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted],

Klägerin,

Prozessbevollmächtigte: Rechtsanwälte Wilde Beuger & Solmecke,
Kaiser-Wilhelm-Ring 27-29, 50672 Köln,

gegen

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

Beklagte,

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

hat die 8. Zivilkammer des Landgerichts Duisburg
auf die mündliche Verhandlung vom 03.08.2023
durch den Richter am Landgericht [redacted] als Einzelrichter

für Recht erkannt:

Die Beklagte wird verurteilt, an die Klägerin 250,00 EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 28. Juni 2022 zu zahlen.

Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerin alle künftigen materiellen und objektiv derzeit nicht vorhersehbaren immateriellen Schäden zu ersetzen, die der Klägerin durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und noch entstehen werden.

Die Beklagte wird verurteilt, an die Klägerin einen weiteren Betrag in Höhe von 159,94 EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 28. Juni 2022 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Rechtsstreits hat die Klägerin zu tragen.

Das Urteil ist vorläufig vollstreckbar, für die Beklagte jedoch nur gegen Sicherheitsleistung in Höhe von 110% des jeweils zu vollstreckenden Betrages. Die Beklagte kann die Vollstreckung der Klägerin durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die Klägerin vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrages leistet.

Tatbestand

Die Beklagte ist Anbieterin der Social Media Plattform facebook.com auf dem Gebiet der Europäischen Union. Die Dienste der Beklagten ermöglichen es ihren Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf den persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf diese Daten zugreifen können. Die Klägerin nutzt die Plattform, insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Die Beklagte bietet ihren Nutzern eine Reihe von Einstellungsmöglichkeiten bezüglich ihrer personenbezogenen Daten an. Bei der Erstellung eines Facebook-Accounts trägt der angehende Nutzer seinen Vor- und Zunamen, seine Handynummer oder E-Mail-Adresse, sein Geschlecht und sein Geburtsdatum in die Registrierungsmaske ein. Über eine Verlinkung im unteren Teil des Anmeldebereichs erreicht der Nutzer die Nutzungsbedingungen, Informationen über die Verwendung von Cookies und Datenschutzrichtlinien. Name, Geschlecht und Nutzer-ID sind sog. „immer öffentliche Nutzerinformationen“, die immer öffentlich von anderen Nutzern einsehbar sind, was durch Einstellungen nicht geändert werden kann.

Nach der Anmeldung steht dem Nutzer eine Vielzahl von Einstellungsmöglichkeiten zur Verfügung, die auf mehreren Ebenen abrufbar sind. Hierzu zählen unter anderem der Hilfebereich und die Privatsphäre-Einstellungen. Zu diesen gehören wiederum unter anderem die Zielgruppenauswahl und die Suchbarkeits-Einstellungen.

Bei der Zielgruppenauswahl kann der Nutzer festlegen, wer bestimmte Datenelemente seines Profils – Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse – einsehen kann. Möglich sind die Optionen „Alle“, „Freunde“ und „Freunde von Freunden“. Standardmäßig voreingestellt ist für die Datenelemente Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse die Option „Alle“.

In den Suchbarkeits-Einstellungen kann der Nutzer festlegen, wer das eigene Profil anhand seiner Telefonnummer finden kann. Dies funktioniert mithilfe eines sog. Kontakt-Import-Tools, das es Nutzern ermöglicht, die in ihrem Smartphone mit Telefonnummer gespeicherten Personenkontakte mit Nutzern auf Facebook zu synchronisieren. Die Funktion gleicht die im Mobiltelefon gespeicherten Telefonnummern mit den bei Facebook hinterlegten Telefonnummern ab, um dem Nutzer die hinter den Nummern stehenden Personen als Kontakte auf der Facebook-Plattform vorzuschlagen. Dies funktioniert bei einer entsprechenden Einstellung der Suchbarkeits-Einstellungen auch, wenn die im Profil hinterlegte Nummer für die Öffentlichkeit nicht einsehbar ist. Im Rahmen der Suchbarkeits-Einstellungen bestehen wiederum die Optionen „Alle“, „Freunde“ und „Freunde von Freunden.“ Seit Mai 2019 steht auch die Option „Nur ich“ zur Verfügung. Wiederum ist die voreingestellte Option „Alle“. Dies ändert sich auch nicht automatisch, wenn der Nutzer die Sichtbarkeit seiner Telefonnummer unter der Zielgruppenauswahl beschränkt.

Zudem können Nutzer den „Wer kann nach mir suchen?“-Bereich ihrer Privatsphäre-Einstellungen überprüfen und dort kontrollieren, wer ihr Facebook-Profil finden kann.

Bei den Handy-Einstellungen, die etwa eine Nutzung der Mobilnummer zur Passwortzurücksetzung ermöglichen, findet sich der Hinweis „Nur du kannst deine

Nummer sehen.“ Über einen Klick auf den Link „Mehr dazu“ findet der Nutzer Informationen zu der sog. Zwei-Faktor-Authentifizierung sowie den Hinweis „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke.“

Die Beklagte bietet zudem eine Messenger-App an. Diese dient als Schnittstelle für die Facebook-Applikation auf Mobilgeräten und bietet eine Messenger-Funktion für Nutzer an. Nutzer melden sich dafür mit ihren bestehenden Facebook-Profilen an. Die Messenger-App und die gewöhnlichen Funktionen von Facebook sind verknüpft über den Zugang zum selben Account. Auch in dieser App können Einstellungen vorgenommen werden, so auch dazu, ob Telefonkontakte mit dem Facebook-Dienst synchronisiert werden sollen.

Anfang April 2021 verbreiteten unbekannte Dritte Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern öffentlich im Internet (sog. „Scraping-Vorfall“). Die genaue Herangehensweise der unbekannten Dritten ist nicht bekannt, jedoch wird seitens der Beklagten davon ausgegangen, dass das Kontakt-Import-Tool zur Bestimmung der Telefonnummern der einzelnen Nutzer verwendet wurde. Durch die Eingabe einer Vielzahl von Kontakten in ein virtuelles Adressbuch gelang es den Unbekannten, die Telefonnummern konkreten Facebook-Profilen zuzuordnen. Von den Profilen wurden dann die öffentlich verfügbaren Daten abgeschöpft („gescrapt“). Das Datenscraping unterscheidet sich von der ordnungsgemäßen Nutzung einer Website oder App dadurch, dass die „Scraper“ Verfahren einsetzen, um Daten in großem Umfang mittels automatisierter Tools und Methoden zu sammeln. Dies war und ist nach den Nutzungsbedingungen der Beklagten untersagt. Die Beklagte hält keine Kopie der Rohdaten vor, die durch Scraping abgerufene Daten enthalten.

Unter den veröffentlichten Daten befanden sich auch solche der Klägerin.

Mit vorgerichtlichem Schreiben forderte die Klägerin die Beklagte zunächst zur Zahlung von 500,00 EUR, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen wurden (vgl. Anlage K1, Bl. 57 ff. d.A.). Die Beklagte wies eine Zahlung sowie den Unterlassungsanspruch zurück und teilte mit, dass sich unter den abgegriffenen und veröffentlichten Daten auch solche der Klägerin befanden (vgl. Anlage K2, Bl. 82 ff. d.A.). Eine Aussage darüber, welche konkreten Daten abgegriffen wurden, wann dies genau geschah oder wie viele Unbekannte die Daten der Klägerin abgegriffen hatten, enthielt das Schreiben nicht.

Die Klägerin behauptet, infolge des Scraping-Vorfalls seien auch ihre personenbezogenen Daten im Internet auf Seiten veröffentlicht worden, die illegale Aktivitäten begünstigen sollen. Die Daten würden für gezielte Phishing-Attacken genutzt. Die verbreiteten Datensätze enthielten in katalogisierter Form die Telefonnummer, Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten.

Sie habe hierdurch einen Kontrollverlust hinsichtlich ihrer persönlichen Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über den möglichen Missbrauch ihrer persönlichen Daten verblieben. Seit dem Vorfall erhalte sie regelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks. Dies habe dazu geführt, dass sie nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagiere und jedes Mal einen Betrug fürchte und Unsicherheit verspüre.

Möglich sei das Abgreifen der Daten einerseits deshalb gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorhalte, um ein Ausnutzen des bereitgestellten Tools zu verhindern, und andererseits, weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Insbesondere die Einstellungsmöglichkeiten hinsichtlich der Sichtbarkeit und Nutzbarkeit der Telefonnummer seien undurchsichtig. Die oberflächlich sicheren Einstellungen vermittelten dem Nutzer ein Gefühl der Sicherheit, während für tatsächlich sichere Einstellungen eine Vielzahl der automatisch voreingestellten Einstellungen manuell geändert werden müssten. Aufgrund der Vielzahl der Einstellungsmöglichkeiten sei wahrscheinlich, dass der Nutzer die Voreinstellungen beibehalte.

Die Beklagte habe weder sie als Nutzerin noch die zuständige Datenschutzbehörde, die Irish Data Protection Commission, über den Vorfall im Nachhinein informiert. Das Auskunftsschreiben der Beklagten sei mangels konkreter Informationen unzureichend.

Die Klägerin beantragt,

1. die Beklagte zu verurteilen, an sie 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. festzustellen, dass die Beklagte verpflichtet ist, ihr alle künftigen Schäden zu ersetzen, die ihr 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 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 zu verurteilen, ihr Auskunft über die sie 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 sie vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 EUR zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, der „Scraping-Vorfall“ beruhe nicht auf einem Datenschutzverstoß. Dies ergebe sich schon daraus, dass lediglich Daten „gescraped“ worden seien, die die Nutzer selbst der Öffentlichkeit zur Verfügung gestellt hätten.

Sie habe außerdem Maßnahmen getroffen, um das Risiko von Scraping zu unterbinden. Sie beschäftige ein Team zur Bekämpfung von Scraping. Außerdem habe sie Übertragungsbeschränkungen eingeführt, die die Anzahl von Anfragen von bestimmten Daten reduzierten. Sie gehe gegen Scraper aktiv vor und habe im relevanten Zeitraum Captcha-Anfragen genutzt. Die Klägerin erklärt sich zu diesen Maßnahmen mit Nichtwissen.

Die Beklagte ist der Ansicht, die Anträge zu 1., 2. und 3. seien zu unbestimmt und damit unzulässig. Der Schutzbereich des Art. 82 DSGVO umfasse außerdem keine Verstöße gegen die Artt. 13, 14, 15, 24, 25 und 34 DSGVO.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen.

Entscheidungsgründe

Der Antrag zu 3.b. ist unzulässig. Im Übrigen ist die Klage zulässig, jedoch nur in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Der Antrag zu 3.b. ist unzulässig.

Der Klägerin fehlt das insofern erforderliche Rechtsschutzbedürfnis, da sie ihr mit dem Antrag verfolgtes Interesse einfacher und schneller als im Klageweg erreichen kann. Die Klägerin verlangt mit dem Antrag das Unterlassen der Verarbeitung ihrer Telefonnummer auf Grundlage einer Einwilligung, die sie aus ihrer Sicht ohne die notwendigen zugrundeliegenden Informationen erteilt hat. Es ist der Klägerin aber ohne Weiteres möglich, die entsprechenden Einstellungen auf ihrem Facebook-Profil selbst vorzunehmen. Aus der Formulierung des Antrags ergibt sich bereits, dass die Klägerin inzwischen über die aus ihrer Sicht notwendigen Informationen verfügt. Der Klägerin sind auch spätestens seit dem Rechtsstreit die Möglichkeiten der Änderung der Nutzungseinstellungen bekannt.

Im Übrigen ist die Klage zulässig.

Die Anträge der Klägerin sind insbesondere hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Grundsätzlich ist ein Klageantrag hinreichend bestimmt, wenn er den erhobenen Anspruch durch Bezifferung oder gegenständliche Beschreibung so konkret bezeichnet, dass der Rahmen der gerichtlichen Entscheidungsbefugnis klar abgegrenzt ist, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung erkennbar sind, das Risiko des eventuellen teilweisen Unterliegens nicht durch vermeidbare Ungenauigkeit auf den Beklagten abgewälzt wird und keine Fortsetzung des Streits im Vollstreckungsverfahren droht (vgl. BGH, Urteil vom 21. November 2017 – II ZR 180/15). Die Anträge der Klägerin genügen diesen Anforderungen.

Mit dem Antrag zu 1. begehrt die Klägerin Schadensersatz für einen einheitlichen und abgrenzbaren Lebenssachverhalt, dessen zeitliche und inhaltliche Grenzen klar erkennbar sind, auch wenn die Klägerin sich hierbei auf verschiedene Verhaltensweisen der Beklagten über einen längeren Zeitraum stützt. Es ist in Verbindung mit der Klageschrift, die zur Auslegung des Antrags herangezogen werden kann, erkennbar, auf welches Verhalten der Beklagten in welchem Zeitraum die Klägerin sich stützt. Dass hiermit möglicherweise mehrere Verstöße gegen die DSGVO begründet werden können, ergibt sich aus der rechtlichen Würdigung des Sachverhalts und hindert nicht die Bestimmtheit des klägerischen Vortrags und Antrags. Es liegt auch kein Fall einer unzulässigen, alternativen Klagehäufung vor. Eine solche liegt vor, wenn der Kläger mehrere sich ausschließende Streitgegenstände geltend macht, ohne hierbei ein Rangverhältnis anzugeben und vom Gericht eine wahlweise Verurteilung begehrt. Die Klägerin macht jedoch einen einheitlichen Schadensersatzanspruch geltend.

Ebenso ist der Antrag zu 2. hinreichend bestimmt und auch nicht widersprüchlich. Dies ergibt sich jedenfalls aus der Zusammenschau der Anträge zu 1. und 2. Die Klägerin zielt ersichtlich darauf ab, sich wegen solcher Schäden abzusichern, die nicht über den Antrag zu 1. abgedeckt sind. Das können zum einen Schäden sein, die noch gar nicht entstanden sind, zum anderen aber auch solche, die bereits entstanden, jedoch noch unentdeckt sind. Dies liegt bei einer Verbreitung von Daten im Internet auch nahe, da eine solche naturgemäß schwierig zu überblicken ist und sich jederzeit, auch im Laufe des Rechtsstreits, fortentwickeln kann.

Der Antrag zu 3.a. ist insbesondere nicht deshalb zu unbestimmt, weil er den Begriff „Stand der Technik“ verwendet. Zwar darf ein Verbotsantrag nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts nicht erkennbar abgegrenzt sind, sich die Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was der Beklagten verboten ist, dem Vollstreckungsgericht überlassen bleibt. Eine auslegungsbedürftige Antragsformulierung ist jedoch dann hinzunehmen, wenn eine weitergehende

Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urteil vom 26. Januar 2017 – I ZR 207/14). Dies ist hier der Fall. Selbst wenn die Klägerin die aktuell möglichen Sicherheitsmaßnahmen konkret benennen könnte, würde der aktuelle Standard wegen der ständigen technischen Weiterentwicklung rasch veralten, so dass die Klägerin erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen. Zudem ist die Einrichtung der gesetzlich vorgeschriebenen Sicherheitsstandards die Aufgabe der Beklagten.

Die Klägerin verfügt zudem hinsichtlich des Antrags zu 2. über das gemäß § 256 Abs. 2 ZPO erforderliche Feststellungsinteresse. Hierfür genügt, dass eine Schadensentwicklung noch nicht abgeschlossen ist und die Klägerin deshalb ihren Anspruch noch nicht abschließend beziffern kann. Dafür reicht es, dass die Geschädigte bei verständiger Würdigung überhaupt mit dem Eintritt eines weiteren Schadens rechnen kann. Dies ist hier wegen der Unkontrollierbarkeit der Verbreitung von Daten im Internet der Fall.

II.

Die Klage ist nur teilweise, nämlich teilweise hinsichtlich der Anträge zu 1., 2. und 5., begründet und im Übrigen unbegründet.

1.

Die Klägerin hat gegen die Beklagte einen Anspruch auf immateriellen Schadensersatz in Höhe von 250,00 EUR gemäß Art. 82 Abs. 1 DSGVO. 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.

Der Klägerin ist wegen eines Verstoßes gegen die DSGVO ein Schaden entstanden.

Die Beklagte ist hierfür Verantwortliche gemäß Art. 4 Nr. 7 DSGVO.

Ein auf Art. 82 Abs. 1 DSGVO gestützter Schadensersatzanspruch kann grundsätzlich auf jeder Vorschrift der DSGVO beruhen. Der Rahmen möglicher Verstöße, die geeignet sind, eine Schadensersatzpflicht auszulösen, ist weit zu ziehen. Dies ergibt sich zum einen aus dem Wortlaut des § 82 Abs. 1 DSGVO, der allgemein von einem „Verstoß gegen die DSGVO“ spricht. Zum anderen spricht der Zweck der Vorschrift, welcher der Umsetzung des Grundziels der DSGVO dient, indem er Betroffenen einen Schadensersatzanspruch an die Hand gibt, für eine weite Auslegung. Gemäß Art. 1 Abs. 2 DSGVO soll die Verordnung die Grundrechte und

Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten schützen. Dieses Recht kann durch jeden Verstoß gegen die DSGVO berührt werden und ist dementsprechend vor jedem Verstoß zu schützen. Eine Einschränkung wegen des Wortlauts des Art. 82 Abs. 2 DSGVO ist nicht angezeigt. Dieser regelt die Haftung der an der Verarbeitung personenbezogener Daten Beteiligten, ohne dass hierdurch der Anwendungsbereich des Art. 82 Abs. 1 DSGVO auf Verstöße bei der „Verarbeitung“ beschränkt wird. Dass die Folgen eines „Verstoßes“ gegen die DSGVO und die Verantwortlichkeit für die „Verarbeitung“ in getrennten Absätzen des Art. 82 DSGVO geregelt sind, zeigt gerade, dass der Gesetzgeber hierbei eine bewusste terminologische Unterscheidung getroffen hat. Eine Einschränkung widerspräche auch dem oben genannten Schutzzweck der Vorschrift.

Die Beklagte hat gegen die Art. 25 Abs. 2, 5 Abs. 1 lit. a) und Art. 13 DSGVO verstoßen.

Gemäß Art. 25 Abs. 2 S. 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies dient dem Grundsatz der Datenminimierung, Art. 25 Abs. 1 DSGVO.

Die Voreinstellungen der von der Beklagten betriebenen Plattform genügen diesem Grundsatz nicht. Die Sichtbarkeit der Daten von Nutzern ist nach den Voreinstellungen der Beklagten mit der Registrierung auf der Plattform automatisch auf „Alle“ eingestellt. Dies steht dem Ziel der Datenminimierung entgegen. Die Voreinstellungen der Beklagten stellen gerade nicht sicher, dass nur die erforderlichen Daten verarbeitet werden. Mit der Registrierung auf der Plattform tritt eine umfassende Öffentlichkeit der angegebenen Daten ein. Der Nutzer muss keine bewusste Entscheidung im Einzelfall treffen, um die Verarbeitung bestimmter Daten zu erreichen, er muss vielmehr eine bewusste Entscheidung treffen, um einzelne Daten nachträglich der Öffentlichkeit zu entnehmen.

Diese Art der Voreinstellung lässt sich nicht durch den seitens der Beklagten behaupteten Zweck der Plattform – das Zusammenführen von Menschen – begründen. Dieses Ziel rechtfertigt jedenfalls keine allumfassende Öffentlichkeit personenbezogener Daten ab dem Zeitpunkt der Registrierung. Der Nutzer kann naturgemäß im Zeitpunkt der Registrierung noch nicht überblicken, welche Optionen ihm auf der Plattform offenstehen, vor allem, da es sich um eine Vielzahl schwierig zu überblickender Einstellungen auf verschiedenen Ebenen handelt. Der Nutzer wird auch nicht automatisch dazu angeleitet, überhaupt eine Entscheidung zu der Verbreitung seiner Daten zu treffen. Er muss selbstständig den Entschluss fassen,

sich mit den verschiedenen Einstellungen auf der Plattform auf den verschiedenen Ebenen auseinanderzusetzen. Hierbei liegt näher, dass ein Nutzer, der seine Daten nicht verbreiten möchte, eine Einstellung übersieht, als dass einem Nutzer, der mit möglichst vielen – auch unbekannten – Dritten in Kontakt treten möchte, dies wegen einschränkender Voreinstellungen nicht gelingt.

Die Beklagte hat zudem gegen das Transparenzgebot des Art. 5 Abs. 1 lit. a) DSGVO sowie gegen ihre Informationspflichten aus Art. 13 DSGVO verstoßen.

Gemäß Art. 5 Abs. 1 lit. a) DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Das Kriterium der Nachvollziehbarkeit und der Begriff Treu und Glauben stellen auf den Gedanken der Fairness und Rücksichtnahme im Rahmen der Datenverarbeitung ab.

Hiergegen verstoßen die Einstellungen der Beklagten hinsichtlich der Telefonnummern ihrer Nutzer, da diese an verschiedenen Stellen verstreut sind, ohne dass an den einzelnen Stellen erkennbar ist, dass hier jeweils keine abschließende Einstellung getroffen werden kann. Selbst wenn der Nutzer alle Stellen aufspürt, an denen er einstellen kann, dass seine Telefonnummer nicht in seinem Profil öffentlich angezeigt werden soll, besteht des Weiteren die Voreinstellung der Beklagten, die das Auffinden des Profils des Betroffenen anhand der Telefonnummer ermöglicht. Dies ist für den Nutzer erst erkennbar, sobald er zu der entsprechenden Einstellungsmöglichkeit vorgedrungen ist. Ein Nutzer, der die Sichtbarkeit seiner Telefonnummer einschränkt, muss nicht damit rechnen, dass diese aufgrund einer Einstellung an anderer Stelle zur Identifizierung seines Profils genutzt wird.

Gemäß Art. 13 Abs. 1 lit. c) DSGVO hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung personenbezogener Daten die Zwecke und die Rechtsgrundlage der Verarbeitung mitzuteilen. Hinsichtlich der Telefonnummer des Nutzers ist selbst auf Grundlage des unstreitigen Sachverhalts nicht erkennbar, dass die Beklagte dieser Verpflichtung nachkommt. Es ist nicht erkennbar, dass ein potentieller Nutzer „im Zeitpunkt der Erhebung“ seiner Telefonnummer – ggf. bereits bei der Registrierung – den Hinweis erhält, dass diese (auch) dem Zweck dient, anderen Nutzern das Auffinden seines Profils zu ermöglichen. Allenfalls erhält der Nutzer die Informationen, dass er selbst über die in seinem Telefon gespeicherten Nummern andere Nutzer finden kann, auch dies jedoch nicht im maßgeblichen Zeitpunkt der Registrierung mit der Telefonnummer.

Im Übrigen liegt aber kein weiterer Verstoß gegen das Transparenzgebot deshalb vor, weil die Informationen der Beklagten zum Datenschutz vielschichtig und

umfangreich sind. Die Notwendigkeit umfangreicher Aufklärung ergibt sich gerade aus den gesetzlichen Vorgaben; eine Aufteilung der Informationen in verschiedene Bereiche und auf mehrere Ebenen kann dem Verständnis und der Übersichtlichkeit sogar dienen, solange nicht – wie im Falle der Telefonnummer – der Eindruck vermittelt wird, es handele sich um jeweils abschließende Informationen.

Auf einen Verstoß gegen die Artt. 33, 34 und 15 DSGVO kann die Klägerin hingegen keine Schadensersatzansprüche stützen.

Die Artt. 33 und 34 DSGVO betreffen Informationspflichten der Beklagten im Nachgang von Verletzungen des Schutzes personenbezogener Daten, Art. 15 DSGVO betrifft dahingehende Auskunftspflichten. Unabhängig von einer Verletzung dieser Pflichten durch die Beklagte ist nicht ersichtlich, inwiefern die Klägerin hierdurch einen ersatzfähigen Schaden erlitten hat. Die Klägerin stützt sich zur Begründung ihres Schadens auf den erlittenen Kontrollverlust durch die Verbreitung ihrer Daten, die auch durch eine ordnungsgemäße Information der Beklagten im Anschluss nicht mehr rückgängig zu machen gewesen wäre.

Die Klägerin kann einen Schadensersatzanspruch auch nicht auf die Artt. 32 und 5 Abs. 1 lit. f) DSGVO wegen mangelnder Schutzmaßnahmen gegen die Ausnutzung der Systeme der Beklagten stützen.

Gemäß Art. 32 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu leisten. Gemäß Art. 5 Abs. 1 lit. f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Die Klägerin trägt als Anspruchstellerin die Darlegungs- und Beweislast hinsichtlich eines Verstoßes der Beklagten gegen diese Vorschriften. Den naturgemäß auftretenden Beweisschwierigkeiten bezüglich Maßnahmen aus der Sphäre der Gegenpartei kann begegnet werden, indem der Beklagten eine sekundäre Darlegungslast auferlegt wird. Dies steht auch im Einklang mit der Rechenschaftspflicht des Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO, der den Verantwortlichen zur Bereitstellung bestimmter Informationen verpflichtet, ohne hierbei eine Beweislastumkehr im Rahmen eines Schadensersatzanspruches zu

enthalten (vgl. *Quaas* in: BeckOK Datenschutzrecht, 43. Edition, Stand: 1. Februar 2023, DSGVO, Art. 82, Rn. 16).

Die Beklagte ist ihrer sekundären Darlegungslast nachgekommen, indem sie konkrete Schutzmaßnahmen ihrerseits dargelegt hat. Die Klägerin hat hierzu nicht konkret dargelegt, inwiefern diese Maßnahmen – unabhängig von ihrem tatsächlichen Vorliegen – unzureichend im Sinne einer Verletzung der DSGVO sein sollen.

Die Beklagte hat sich hinsichtlich der Verstöße gegen die DSGVO nicht entlastet. Sie trägt die Darlegungs- und Beweislast dafür, weder vorsätzlich gehandelt noch die ihr obliegende Sorgfalt, § 276 BGB, außer Acht gelassen zu haben (vgl. Art. 82 Abs. 3 DSGVO). Eine entsprechende Entlastung ist ihr nicht gelungen. Die Beklagte kann sich insbesondere nicht darauf berufen, die Klägerin selbst habe ihre Daten auf eine öffentliche Einstellung gesetzt bzw. bei dem Scraping-Vorfall seien nur öffentliche Daten der Nutzer abgegriffen worden. Die Verstöße der Beklagten liegen gerade darin begründet, dass die Klägerin aufgrund der Gegebenheiten auf der Plattform der Beklagten nicht in der Lage war, die öffentliche Verfügbarkeit ihrer Telefonnummer verlässlich einzuschätzen. Die Beklagte hat zudem die Entscheidungen bezüglich ihrer Voreinstellungen in dem Wissen getroffen, dass Dritte versuchen könnten, die automatisierten Abläufe auszunutzen. Dass dieses Problem der Beklagten bekannt war, ergibt sich daraus, dass ein solches Verhalten in ihren Nutzungsbedingungen verboten ist.

Der Klägerin ist durch die Verstöße der Beklagten gegen die DSGVO ein immaterieller Schaden entstanden, den die Kammer mit 250,00 EUR beziffert. Dieser Schaden besteht in dem Kontrollverlust hinsichtlich ihrer personenbezogenen Daten, der der Klägerin infolge der Verstöße der Beklagten gegen die DSGVO entstanden ist.

Der Begriff des Schadens ist im Rahmen des Art. 82 DSGVO in Anbetracht des Erwägungsgrundes 146 S. 3 der DSGVO weit auszulegen. Dieser besagt, dass der Schadensbegriff „im Lichte der Rechtsprechung des Gerichtshofs“ weit auf eine Art und Weise ausgelegt werden soll, die den Zielen der Verordnung, also dem Schutz personenbezogener Daten, in vollem Umfang entspricht. Notwendig ist aber jedenfalls eine Beeinträchtigung, die über den bloßen Verstoß gegen die Vorschriften der DSGVO hinausgeht. Dies ergibt sich bereits aus dem Wortlaut, nach dem ein Schaden „entstanden“ sein muss, und der Differenzierung zwischen materiellem und immateriellem Schaden in Art. 82 Abs. 1 DSGVO. Eine Erheblichkeitsschwelle hinsichtlich der Beeinträchtigung des Betroffenen ist dem Wortlaut der Vorschrift

jedoch nicht zu entnehmen und entspricht auch nicht dem Zweck der Schadensersatzpflicht des Verantwortlichen.

Ein Kontrollverlust hinsichtlich der persönlichen Daten sowie das damit begründete Gefühl des Unwohlseins im Zusammenhang mit digitalen Kontakten kann einen solchen Schaden begründen. Das durch die DSGVO geschützte Selbstbestimmungsrecht hinsichtlich der eigenen personenbezogenen Daten ist mit jedem Kontrollverlust über diese verletzt. Ein solcher Kontrollverlust zu Lasten der Klägerin liegt vor, denn dass die Daten der Klägerin im Rahmen des Scraping-Vorfalls abgegriffen wurden, ist zwischen den Parteien unstreitig.

Dieser Schaden ist auch kausal auf die Verstöße der Beklagten gegen die Artt. 25 Abs. 2, 5 Abs. 1 lit. a) und 13 DSGVO zurückzuführen. Die Voreinstellungen auf der Plattform der Beklagten, welche die Öffentlichkeit der personenbezogenen Daten begünstigen, im Zusammenhang mit den intransparenten Einstellungen hinsichtlich der Verwendung der Telefonnummer verhinderten gerade eine Kontrolle ihrer Daten durch die Klägerin selbst. Die Beklagte kann sich auch insofern nicht darauf berufen, die Klägerin selbst habe mit der Vornahme ihrer persönlichen Einstellungen das spätere Abgreifen der Daten ermöglicht. Denn wegen der Verstöße der Beklagten gegen die Vorschriften der DSGVO war es der Klägerin gerade nicht möglich, eine autonome Entscheidung hinsichtlich der Verwendung ihrer Daten zu treffen, die den Zurechnungszusammenhang zwischen den Verstößen der Beklagten und dem eingetretenen Schaden unterbrechen könnte.

Bei der Bestimmung der von der Klägerin in das Ermessen des Gerichts gestellten Höhe des Schadenersatzes gemäß § 287 Abs. 1 S. 1 ZPO sind alle Umstände des Einzelfalls zu würdigen. Die Kriterien des Art. 83 Abs. 2 DSGVO, die Anhaltspunkte für die Höhe einer von der Aufsichtsbehörde zu verhängenden Geldbuße geben, können auch für die Bemessung des immateriellen Schadenersatzes herangezogen werden (vgl. *Quaas* in: BeckOK Datenschutzrecht, 43. Edition, Stand: 1. Februar 2023, DSGVO, Art. 82 Rn. 31). Danach sind unter anderem Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der personenbezogenen Daten zu betrachten. Gemäß Erwägungsgrund 146 S. 6 zur DSGVO sollen die betroffenen Personen einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten.

Auf der Grundlage dieser Kriterien ist ein immaterieller Schadensersatz in Höhe von 250,00 EUR erforderlich und ausreichend, um den von der Klägerin erlittenen Schaden zu kompensieren. In die Abwägung einzubeziehen ist einerseits, dass die

Beklagte gegen mehrere Vorschriften der DSGVO verstoßen hat und das Zusammenspiel der Verstöße diese in ihrer Wirkung verstärkt. Der Verstoß gegen Art. 25 Abs. 2 DSGVO wiegt umso schwerer, da es dem Nutzer durch die Intransparenz der Einstellungen hinsichtlich der Telefonnummer erschwert wird, alle der Öffentlichkeit zur Verfügung gestellten Daten einer privateren Einstellung zuzuführen. Gegen die Notwendigkeit einer höheren Schadensersatzleistung spricht, dass auch auf der Grundlage des Vortrags der Klägerin nicht erkennbar ist, dass die Verstöße der Beklagten zu erheblichen, konkreten Beeinträchtigungen der Klägerin in ihrem Umgang mit ihren persönlichen Daten im Internet über das allgemeine Unwohlsein wegen des Kontrollverlustes hinaus geführt haben. Hierfür spricht entscheidend, dass die Klägerin ihr Facebook-Profil weiterhin betreibt, künftig betreiben möchte – wie sich zwanglos aus den geltend gemachten Unterlassungsansprüchen ergibt – und ihre Telefonnummer trotz der gerade mit dieser Telefonnummer verknüpften Daten nicht gewechselt hat.

Der Zinsanspruch der Klägerin ergibt sich aus §§ 291 S. 1, 288 Abs. 1 S. 1 BGB.

2.

Der Antrag zu 2. ist teilweise begründet.

a)

Die Klägerin hat einen Anspruch auf die Feststellung der Ersatzpflicht der Beklagten hinsichtlich weiterer materieller Schäden infolge der unter II. 1. dargelegten Verstöße, nicht jedoch auf die Feststellung der Ersatzpflicht hinsichtlich weiterer immaterieller Schäden.

Der Anspruch auf Feststellung der Ersatzpflicht der Beklagten hinsichtlich weiterer materieller Schäden ergibt sich aus dem Bestehen des Schadensersatzanspruchs. Unabhängig davon, ob eine derartige Feststellung der Darlegung einer gewissen Wahrscheinlichkeit eines weiteren Schadenseintritts bedarf, besteht diese ohnehin, da nicht abzusehen ist, was mit den verbreiteten Daten der Klägerin geschehen wird.

b)

Einem Feststellungsanspruch hinsichtlich weiterer immaterieller Schäden steht der Grundsatz der Einheitlichkeit des Schmerzensgeldes (vgl. BGH ZfSch 2019, 20, 21 m.w.N.) entgegen, soweit die künftige Entwicklung des Schadensbildes bereits absehbar ist. Die Festsetzung eines Schmerzensgeldanspruchs erfordert eine

Gesamtbetrachtung der Umstände, weil gerade kein objektiv messbarer Vermögensschaden auszugleichen ist. Das Schmerzensgeld hat nicht nur alle eingetretenen, sondern auch alle objektiv vorhersehbaren künftigen Schäden zu berücksichtigen. Der potentielle zukünftige Schaden ist damit als bereits bestehende Beeinträchtigung in den Schmerzensgeldanspruch einzupreisen. Gegenstand der begehrten Feststellung können demnach nur Verletzungsfolgen sein, die zum Beurteilungszeitpunkt noch nicht eingetreten waren und deren Eintritt objektiv nicht vorhersehbar ist, mit denen also noch nicht ernstlich gerechnet werden muss. Dem hat die Kammer in der Tenorierung entsprechend Rechnung getragen.

3.

Der Antrag zu 3.a. ist unbegründet.

Die Klägerin hat gegen die Beklagte keinen Anspruch auf das Unterlassen des Zugänglichmachens ihrer personenbezogenen Daten über eine Software zum Importieren von Kontakten, ohne dass die Beklagte hierbei die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorsieht, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern. Ein solcher Anspruch ergibt sich weder aus § 1004 BGB analog noch aus §§ 823 Abs. 1, 823 Abs. 2 BGB i.V.m. Artt. 6 Abs. 1, 17 DSGVO. Der von der Klägerin formulierte Unterlassungsantrag greift in den der Beklagten nach der DSGVO zustehenden Ermessensspielraum ein.

Die Klägerin zielt mit ihrem Antrag darauf ab, der Beklagten aufzugeben, bei einer Verarbeitung ihrer personenbezogenen Daten die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen – ohne Einschränkung – vorzunehmen. Hierzu ist die Beklagte nach der DSGVO nicht verpflichtet. So ist etwa gemäß Art. 32 DSGVO der Stand der Technik zu berücksichtigen, aber auch stets in Abwägung zu weiteren Faktoren (Implementierungskosten, Art, Umfang, Umstände, Zwecke der Verarbeitung, etc.) zu setzen. Die DSGVO setzt dem Verantwortlichen insofern einen Rahmen, den dieser eigenständig durch konkrete Maßnahmen ausfüllen muss und darf. Aus der oben angenommenen Verletzung hinsichtlich der Schutzmaßnahmen ergibt sich nur, dass der aktuelle Zustand unzureichend ist, ohne dass die Klägerin einen Anspruch auf eine konkrete Gegenmaßnahme hat. Insbesondere hat die Klägerin keinen Anspruch auf die Vornahme aller nach dem Stand der Technik möglichen Sicherheitsmaßnahmen.

4.

Der Antrag zu 4. ist unbegründet.

Die Klägerin hat gegen die Beklagte keinen weiteren Auskunftsanspruch. Der ursprünglich bestehende Auskunftsanspruch der Klägerin gemäß Art. 15 DSGVO ist durch Erfüllung erloschen, § 362 Abs. 1 BGB. Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (vgl. BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19). Die Beklagte hat erklärt, keine weiteren Angaben machen zu können. Sofern die Klägerin hieran Zweifel hegt, hat sie die Möglichkeit, eine eidesstattliche Versicherung zur Vollständigkeit der Auskunft gemäß § 260 Abs. 2 BGB zu verlangen oder kann ggf. Schadensersatzansprüche geltend machen, wobei sie aber jeweils darlegungs- und beweisbelastet hinsichtlich der anspruchsbegründenden Umstände ist.

5.

Der Antrag zu 5. ist teilweise begründet.

Die Klägerin hat gegen die Beklagte einen Anspruch auf Zahlung von weiteren 159,94 EUR. Die vorgerichtlichen Rechtsverfolgungskosten stellen einen Teil des ersatzfähigen Schadens dar, da nach dem Inhalt und Umfang der Sach- und Rechtslage die Hinzuziehung eines Rechtsanwalts durch die Klägerin nicht zu beanstanden ist. Der Höhe nach kann die Klägerin jedoch nur die für die Verfolgung ihrer bestehenden Ansprüche erforderlichen Kosten geltend machen. Der Zinsanspruch ergibt sich auch insoweit aus §§ 291 S. 1, 288 Abs. 1 S. 1 BGB.

III.

Die Kostenentscheidung ergibt sich aus § 92 Abs. 2 Nr. 1 ZPO analog.

Die Entscheidungen über die vorläufige Vollstreckbarkeit beruhen einerseits auf §§ 708 Nr. 11, 711 S. 1, S. 2 ZPO, andererseits auf § 709 S. 1, S. 2 ZPO.

IV.

Der Streitwert wird auf 12.000,00 EUR festgesetzt (Antrag zu 1.: 1.000,- EUR; zu 2.: 500,- EUR; zu 3.a. und 3.b. jeweils 5.000,- EUR; zu 4.: 500,- EUR).

[redacted]

Beglaubigt
Urkundsbeamter/in der Geschäftsstelle
Landgericht Duisburg

LANDGERICHT NORDRHEIN-WESTFALEN

Verkündet am 24.08.2023

[redacted], Justizbeschäftigte
als Urkundsbeamtin der Geschäftsstelle