Beglaubigte Abschrift

Landgericht München I

Az.: 15 O 4507/22

IM NAMEN DES VOLKES

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde Beuger Solmecke**, Rechtsanwälte Partnerschaft mbB, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.: [redacted]

gegen

Meta Platforms Ireland Limited (zuvor: Facebook Ireland Ltd.), vertr. d. d. GF (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer**, Rechtsanwälte Steuerberater PartG mbB, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.: [redacted]

wegen Forderung

erlässt das Landgericht München I - 15. Zivilkammer - durch die Richterin am Landgericht [redacted] als Einzelrichterin am 20.04.2023 aufgrund der mündlichen Verhandlung vom 10.02.2023 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an den Kläger 600,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 08.06.2022 sowie weitere 280,60 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 08.06.2022 zu zahlen.

2. 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,

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.

3. Im Übrigen wird die Klage abgewiesen.

4. Von den Kosten des Rechtsstreits haben der Kläger 63 % und die Beklagte 37 % zu tragen.

5. Das Urteil ist in Ziffer 1. und 4. vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung des Klägers durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet. Der Kläger kann die Vollstreckung der Beklagten aus Ziffer 4. durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.
Das Urteil ist in Ziffer 2. gegen Sicherheitsleistung in Höhe von 2.000 € vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 4.300,00 € festgesetzt.

Tatbestand

Die Parteien streiten um Schadensersatz, Auskunfts- und Unterlassungsansprüche nach einem Daten-Scraping.

Die Klagepartei ist Nutzer des sozialen Netzwerks Facebook. Für Nutzer im Gebiet der Europäischen Union ist die Beklagte Anbieterin dieser Plattform.

Anfang April 2021 wurden Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet durch unbekannte Dritte öffentlich verbreitet. Bei den Datensätzen handelte es sich um Telefonnummer, Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere Daten.

Teile der von dem Vorfall betroffenen Daten wurden in den Jahren 2018 und 2019 bei der Beklagten mittels des Facebook-Tools Kontakt-Importer (CIT, Contact-Import-Tool) „gescraped“, d.h. aus zum Teil öffentlich zugänglichen Daten durch automatisierte Abfragen in großer Zahl ausgelesen. Bei dem Scraping-Vorgang wurden durch die unbekannten Täter virtuelle Adressbücher mit einer großen Zahl an willkürlich gewählten Telefonnummern erstellt (nach Angabe der Klagepartei etwa für den Rufnummernblock eines deutschen Mobilfunkanbieters ca. 10 Millionen Rufnummern; dies wurde durch die Beklagte mit Nichtwissen bestritten), um sodann über das Kontakt-Importer-Tool (CIT) automatisiert herauszufinden, ob bei der Beklagten zu diesen Telefonnummern Facebook-Profile bestanden. Wurde hierbei ein Facebook-Profil gefunden, so fragten die unbekannten Täter die bei Facebook zum Profil gespeicherten (öffentlich einsehbaren) Daten ab und exportierten diese.

Automatisierte Scraping-Aktivitäten ohne Erlaubnis der Beklagten waren während des hier gegenständlichen Zeitraums durch die Nutzungsbedingungen für die Facebook-Plattform verboten und sind auch weiterhin untersagt.

Unabhängig von etwaigen Einstellungen sind auf der Plattform der Beklagten die Nutzerdaten Name, Facebook ID und Geschlecht immer öffentlich einsehbar. Einstellungen bzgl. der Telefonnummer konnten Facebook-Nutzer an zwei Orten vornehmen. Im Rahmen der „Privatsphäre-Einstellungen“ konnten unter den von der Beklagtenseite so bezeichneten Bereichen „Zielgruppenauswahl“ und „Suchbarkeits-Einstellungen“ Einstellungen vorgenommen werden. In Bezug auf die Telefonnummer konnte zum einen eingestellt werden, wer die Telefonnummer auf dem Facebook-Profil des Nutzers sehen könne („Zielgruppenauswahl“), wobei die Optionen „öffentlich“, „Freunde“ und „Freunde von Freunden“ möglich waren. Zum andere konnte eingestellt werden, wer den Nutzer über die Telefonnummer finden könne (Suchbarkeits-Einstellungen). Insofern war als Voreinstellung eingestellt, dass „alle/jeder“ den Nutzer über die Telefonnummer finden könne. In den Suchbarkeits-Einstellungen im Profil der Klagepartei war die Einstellung hinsichtlich der Te-

lefonnummer auf „alle“ eingestellt und nicht verändert seit 21.02.2018 (Screenshot Anlage B16).

Mit vorgerichtlicher E-Mail vom 11.06.2021 forderte die Klagepartei die Beklagte zur Zahlung von 500,00 EUR Schadensersatz nach Art. 82 Abs.1 DSGVO, zur Unterlassung zukünftiger Zugänglichmachung der Daten der Klagepartei an unbefugte Dritte sowie zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden seien (Anlage K 1)

Mit Schreiben vom 23.08.2021 (Anlage K 2) wies die Beklagte Ansprüche auf Schadensersatz und Unterlassung zurück und erteilte der Klagepartei Auskünfte. Mit Schreiben vom 09.09.2021 (Anlage B 15) erteilte die beklagte Partei ebenfalls Auskünfte.

Die Klagepartei trägt vor, neben den Einstellmöglichkeiten an zwei verschiedenen Orten auf der Facebook-Plattform seien in der Messenger-App separate Sicherheitseinstellungen möglich. Die App diene als Schnittstelle für Facebook-Applikationen auf Mobilgeräten. Sicherheitseinstellungen seien dort unabhängig vom sonstigen Facebook-Dienst möglich. Die Einstellung, dass Telefonkontakte mit dem Facebook-Dienst synchronisiert würden, sei möglich. Eine Anfrage zur Synchronisierung erfolge bei der Erstanmeldung. Hierbei erfolge keine Information über Risiken über die Verwendung der Telefonnummer bei Verwendung des Kontakt-Import-Tools.

Zudem werde durch die Beklagte angeboten, die Telefonnummer zu hinterlegen um die Sicherheit des Accounts zu erhöhen (Zwei Faktor-Authentifizierung). Hierbei werde nicht erwähnt, dass die Nummer verwendet werden könne, um das Profil des Nutzers zu identifizieren. Nutzer hätten deshalb ihre Nummer preisgegeben, um mehr persönliche Sicherheit zu erreichen.

Die Klagepartei trägt vor, die beklagte Partei habe keine zureichenden Sicherheitsmaßnahmen ergriffen, um ein Ausnutzen des Kontakt-Import-Tools zu verhindern. Insbesondere habe die Beklagte keine Sicherheitscaptchas bei der Verwendung des Kontakt-Import-Tools eingesetzt sowie keinen Mechanismus zur Prüfung der Plausibilität von Anfragen. Dies, obwohl Scraping als Methode der Informationsgewinnung bekannt und weit verbreitet sei. Zudem lägen datenschutzunfreundliche Voreinstellungen vor, da durch die technische Gestaltung wesentliche Informationen des Nutzers als „öffentlich“ voreingestellt seien. Das Resultat seien die Veröffentlichung von Datensätzen auf Internetseiten, die illegale Aktivitäten begünstigten, bspw. der Seite „raidforums.com“, Namen und Rufnummern von Nutzern würden für gezielte Phishing-Attacken genutzt.

Die Klagepartei bringt in der Klageschrift vor, die Klägerseite habe deswegen einen erheblichen Kontrollverlust über ihre Daten erlitten und sei in einem Zustand großen Unwohlseins und großer

Sorge über möglichen Missbrauch ihrer sie betreffenden Daten verblieben. Dies manifestiere sich in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Die Klägerseite erhalte seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks.
Mit Schriftsatz vom 31.01.2023 trägt die Klagepartei vor, die Klägerseite habe regelmäßig Anrufe von unbekannten Telefonnummern erhalten. Zudem habe sie SMS-Benachrichtigungen mit dubiosen Aufforderungen zum Anklicken von unbekannten Links erhalten (Bl. 238/239 d. A.).

Die Klagepartei ist der Auffassung, durch die Verwendung des Kontakt-Import-Tools und durch die Gestaltung ihres Plattform- Angebots habe die beklagte Partei gegen zahlreiche Bestimmungen der DSGVO verstoßen. Insbesondere liege ein Verstoß gegen Art. 25 DSGVO vor, den auch die irische Datenschutzbehörde in ihrer Entscheidung vom 28.11.2022 festgestellt und bzgl. dessen sie ein Bußgeld gegen die Beklagte verhängt habe.

Es lägen datenschutzunfreundliche Einstellungen vor. An drei unterschiedlichen Orten bestünden Einstellmöglichkeiten, die zudem unübersichtlich seien. Sie befänden sich in verschiedenen Apps teilweise räumlich getrennt, ein Abweichen von aufgedrängten Einstellungen sei erforderlich, um zu verhindern, dass die Telefonnummer mit sonstigen Daten verknüpft werden können - wie geschehen.

Der Klagepartei stehe ein Schadensersatzanspruch nach Art. 82 DSGVO zu.

Zudem, bestehe ein Unterlassungsanspruch nach Art. 17 DSGVO. Durch die Rechtsverletzung werde die Wiederholungsgefahr indiziert. Das Auskunftsbegehren der Klagepartei sei nicht im erforderlichen Umfang erfüllt, so dass der geltend gemachte weitere Auskunftsanspruch bestehe. Es fehlten Angaben zu den konkreten Empfängern der personenbezogenen Daten (Bl. 41/42 d. A.).

Die Klagepartei beantragt:

> I. 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.

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

Die beklagte Partei beantragt:

Klageabweisung.

Die beklagte Partei trägt vor, die Klagepartei zähle Datenpunkte auf, bei denen unklar sei, ob sie Gegenstand des Scraping-Sachverhalts sein sollen. Teilweise würden auch Datenpunkte genannte, die keinen Profilfeldern bei Facebook entsprächen (Bundesland, Geburtsort).

Sie bestreite, dass Dritte einen bestimmten Nutzer über das Kontakt-Import-Tool hätten finden können unter Bezugnahme auf eine Telefonnummer, die ausschließlich für die Zwei-Faktor-Authentifizierung hinterlegt worden sei.
Einstellungen in der Messenger-App entsprächen den Einstellungen im Facebook-Konto. Änderungen bei Privatsphäre- Einstellungen auf der Facebook-Plattform würden automatisch auch im Messenger angewandt. Eigene Einstellungsmöglichkeiten unabhängig von der Facebook-Plattform bestünden nicht.

Die Beklagte bringt vor, sie habe bereits zum Zeitpunkt des hier gegenständlichen Scraping-Falles Sicherheitsmaßnahmen implementiert gehabt, mit denen die Ausnutzung des CIT habe verhindert werden sollen (Übertragungsbegrenzungen, Bot-Erkennung). Sie habe keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten.

Sie ist der Auffassung, sie hab eine ausführliche Unterrichtung der Klagepartei vorgenommen. Die Möglichkeit, Einstellungen vorzunehmen sei im Privatsphärebereich des Haupteinstellungsmenüs leicht zu finden. Insbesondere im Hilfebereich würden umfassend und verständlich erklärt, zu welchen Zwecken die Telefonnummer verwendet werde.

Die Beklagte ist der Rechtsauffassung, die Klage sei weitgehend unzulässig. Der Klageantrag zu Ziffer 1) sei nicht hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Die Klagepartei mache einen Zahlungsantrag geltend, stütze das Begehren jedoch auf zwei zeitlich auseinanderfallende angebliche Verstöße und damit auf unterschiedliche Lebenssachverhalte. Auch der Klageantrag zu Ziffer 2) sei zu unbestimmt, zudem habe die Klagepartei kein Feststellungsinteresse gem. § 256 Abs. 2 ZPO dargelegt. Zuletzt sei auch der Klageantrag zu Ziffer 3) zu unbestimmt.

Die Beklagte meint weiter, es bestünden keine Ansprüche der Klagepartei, weil nur ohnehin öffentlich einsehbare Daten der Klagepartei „gescraped“ worden seien. Verstöße gegen die Art. 13, 14, 24, 25 und 34 DSGVO könnten ohnehin keinen Schadensersatzanspruch nach Art. 82 DSGVO auslösen. Eine Benachrichtigungspflicht in Scraping-Fällen bestehe nach der Kommentarliteratur nicht. Im Hinblick auf Art. 82 DSGVO fehle es zudem an einem der Beklagten zurechenba-

ren ersatzfähigen immateriellen Schaden im Sinne des Art. 82 DSGVO. Die Kausalität des Sraping Vorgangs bzw. der Ausnutzung des Kontakt-Import-Tools für etwaige SMS, die die Klagepartei erhalten zu haben behaupte, werde bestritten. Auch treffe die Beklagte kein Verschulden.
Für einen Unterlassungsanspruch gebe es keine Anspruchsgrundlage. Der geltend gemachte Anspruch stelle tatsächlich keinen Unterlassungsanspruch dar. Die Klagepartei verlange von der Beklagten ein aktives Tun, nämlich die Implementierung von (nicht näher definierten) Sicherheitsmaßnahmen und die Erteilung von (nicht näher definierten) Informationen bzgl. der Erteilung ihrer Telefonnummer. Ein Anspruch auf Implementierung von „nach dem Stand der Technik möglichen“ Sicherheitsmaßnahmen bestehe schon deshalb nicht, weil dieser Anspruch nicht hinreichend bestimmt sei. Zudem finde sich in der DSGVO keine Anspruchsgrundlage für einen Unterlassungsanspruch, andere Anspruchsgrundlagen wie § 1004 BGB seien nicht anwendbar. Überdies beruhe der Unterlassungsanspruch auf der unzutreffenden Annahme, dass die Beklagte unbefugten Dritten Zugriff auf Nutzerdaten gewährt habe. Vor diesem Hintergrund mangle es sowohl an einer Erstbegehungs- als auch an einer Wiederholungsgefahr.
Der Auskunftsanspruch sei erfüllt, ein Anspruch über die erteilte Auskunft hinaus bestehe nicht. Die Beklagte habe das klägerische Auskunftsersuchen ordnungsgemäß beantwortet und den Auskunftsanspruch vollumfänglich erfüllt (Rn. 237 der Klageerwiderung). Die von der Klagepartei begehrte Auskunft, welche Daten durch welche Empfänger durch Scraping erlangt werden konnten, sei nicht von Art. 15 DSGVO erfasst. Es handle sich um Verarbeitungstätigkeiten Dritter und nicht um eigene Verarbeitungstätigkeiten der Beklagten. Die Beklagte sei zur Beantwortung der Fragen bzgl. Verarbeitungstätigkeiten Dritter weder imstande noch rechtlich verpflichtet. Die Klagepartei begehre zudem Auskunft bzgl. potenzieller Verarbeitungstätigkeiten und nicht bzgl. tatsächlich erfolgter Verarbeitungen. Soweit die Klagepartei allgemeine Informationen nach Art. 15 DSGVO begehre, welche Daten die beklagte Partei verarbeite (über das Schreiben vom 11.06.2021 hinausgehend), verweise die Beklagte darauf, dass die Auskunft bereits durch den Verweis auf das Selbstbedienungstool der Beklagten mit Hinweis im Schreiben vom 09.09.2021 erteilt sei (Rn. 239 der Klageerwiderung).

Die Beklagte verweist zudem darauf, dass die Entscheidung der irischen Datenschutzbehörde vom 25.11.2022 bzgl. des streitgegenständlichen Scraping-Vorfalls nicht rechtskräftig sei, die Beklagte habe Berufung eingelegt.
Im Hinblick auf den Schadensbegriff sprächen u. a. die Ausführungen des Generalanwalts Campos Sanchez Bordona im Verfahren C 300/12 dafür, dass pauschale, nicht nachprüfbare Behauptungen wie es läge ein „Gefühl der Hilflosigkeit infolge eines Kontrollverlusts über die personenbezogenen Daten“ vor, nicht ausreichten, um einen Schaden nach Art. 82 DSGVO zu begründen.

Das Gericht hat in Bezug auf die sachliche Zuständigkeit mit Verfügung vom 08.12.2022 Hinweise erteilt. Die beklagte Partei hat die sachliche Zuständigkeit des Landgerichts München I nicht gerügt.

In der mündlichen Verhandlung vom 10.02.2023 hat das Gericht die Klagepartei informatorisch angehört.

Zur Ergänzung des Sachverhalts wird Bezug genommen auf die gewechselten Schriftsätze der Parteien nebst Anlagen sowie das Protokoll über die mündliche Verhandlung vom 10.02.2023.

Entscheidungsgründe

A.

Die zulässige Klage erweist sich teilweise als begründet.

I.

Die Klage ist zulässig.

1. Das Landgericht München I ist gemäß §§ 39 ZPO sachlich und gemäß Art. 17, 18 EuGVVO bzw. Art. 7 Nr. 2 EuGVVO örtlich für die Entscheidung zuständig.

2. Die Klageanträge sind hinreichend bestimmt.

a) der Klageantrag in Ziff. 1. ist entgegen der Auffassung der Beklagten hinreichend bestimmt.

Insoweit hat das LG München I im Urteil vom 02.03.2023, Az. 4 O 4944/22 in Verfahren mit gleichgelagerten Anträgen zutreffend ausgeführt:
„Eine hinreichende Bestimmtheit des Antrags im Sinne des § 253 Abs. 2 Nr. 2 ZPO kann grundsätzlich angenommen werden, wenn er den Anspruch konkret bezeichnet, den Rahmen der gerichtlichen Entscheidungsbefugnis erkennbar abgrenzt, den Inhalt und Umfang der materiellen Rechtskraft erkennen lässt, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und wenn er die Zwangsvollstreckung aus dem beantragten Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21. November 2017 - II ZR 180/15 -, juris, Rn. 8 m.w.N.).

Aus der Klageschrift ergibt sich, dass dem Klageantrag zu Ziff. 1 ein zusammenhängender, sich zwar auf einen längeren Zeitraum erstreckender, aber in sich abgeschlossener Lebenssachverhalt zu Grunde liegt. Der Schadensersatzanspruch bezieht sich nach dem Vortrag des Klägers auf die Vorgänge ab der Anmeldung des Klägers auf der Plattform Facebook über das „Scraping" seiner Daten bis hin zu einer angeblich unzureichenden Information von ihm. Der Klageschrift lässt sich überdies entnehmen, dass der Schaden aufgrund eines kumulativen Zusammenwirkens der gerügten Datenschutzverstöße geltend gemacht wird, die Bezifferung des Schadens dabei indes in zulässiger Weise in das Ermessen des Gerichts gestellt wird (Urteil des LG Paderborn vom 19.12.2022, Az.: 3 O 99/22, GRUR-RS 2022, 39349.

Gleiches gilt im vorliegenden Fall mit gleichlautenden Anträgen.

b) Auch die Klageanträge zu Ziff. 3 a) und b) sind hinreichend bestimmt.

Soweit die Beklagte rügt, dass die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen" im Klageantrag zu Ziff. 3 a) zu unbestimmt sei, führt dies nicht zur Unzulässigkeit des Antrags. Denn dieser unbestimmte Begriff ist der DSGVO immanent und eine weitere Konkretisierung im Klageantrag auch angesichts des sich ständig wandelnden Stands der Technik nicht möglich.

Hierzu hat das LG Paderborn in seinem Urteil vom 19.12.2022 (siehe oben) ausgeführt:

„*Nach der ständigen höchstrichterlichen Rechtsprechung darf ein Verbotsantrag im Hinblick auf § 253 Abs. 2 Nr. 2 ZPO nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 ZPO) 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. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen. Etwas anderes kann dann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete*

Verhalten das fragliche Tatbestandsmerkmal erfüllt.

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, Urt. v. 26.1.2017 - I ZR 207/14 = GRUR 2017, 422 m.w.N.). Unzulässigkeit liegt hingegen vor, wenn die Klägerseite seinen Antrag ohne weiteres konkreter fassen kann (vgl. BGH, Urteil vom 11.6.2015 - I ZR 226/13 = GRUR 2016, 88).

Daran gemessen weist der Klageantrag zu 3) a.) eine ausreichende Bestimmtheit auf. Selbst bei einer Benennung derzeitiger möglicher Sicherheitsmaßnahmen würde dies in Anbetracht der technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping - Angriffen vorbeugen. Die gesetzlich vorgeschrieben Sicherheitsstandards einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen.“

Den überzeugenden Ausführungen wird beigetreten, insbesondere vor dem Hintergrund, dass die DSGVO selbst entsprechende unbestimmte Rechtsbegriffe vorsieht (Art. 25, 32 DSGVO).

c) Dass mit dem Klageantrag zu Ziff. 3 b) begehrte Anspruchsziel ist ebenfalls hinreichend bestimmt. Das Anspruchsziel wird jedenfalls durch die Klagebegründung hinreichend konkretisiert.

3. Dem Klageantrag zu Ziff. 3 a) fehlt auch nicht das Rechtsschutzbedürfnis.

Das Rechtschutzbedürfnis ist gegeben, wenn der Rechtssuchende ein berechtigtes Interesse daran hat, gerichtliche Hilfe in Anspruch zu nehmen, d. h. sein Ziel nicht auf einem einfacheren, billigeren Weg erreichen kann.
Zwar kann die Klagepartei durch die Anpassung der Privacy-Einstellungen die Suchbarkeit über die Telefonnummer deaktivieren. Dieses genügt aber nicht, um zukünftige unrechtmäßige Datenverarbeitung zu verhindern, da die Klagepartei keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat (vgl. LG Paderborn a.a.O.).

4. Im Hinblick auf den Klageantrag in Ziff. 2 liegt das erforderliche Feststellungsinteresse im Sinne des § 256 ZPO vor.

Die Klagepartei behauptet die Möglichkeit weiterer Schäden. Dies erscheint - nach dem im Rahmen der Zulässigkeitsprüfung eingeschränkten Prüfungsmaßstab - nicht ausgeschlossen. Durch den Scraping-Vorfall sollen nach Auffassung der Klagepartei schützenswerte Daten über das Internet einer Vielzahl an Personen zugänglich gemacht worden sein. Es besteht danach die abstrakte Möglichkeit, dass seine veröffentlichen Daten missbräuchlich verwendet werden.

II.

Die Klage ist teilweise begründet.

1. Die Klagepartei hat gegen die Beklagte einen Schadensersatzanspruch nach Art. 82 DSGVO im Hinblick auf erlittene immaterielle Schäden in Höhe von 700,00 EUR. (Ziff. 1 der Klageanträge).

a. Das Gericht geht von einem Verstoß der Beklagten gegen Art. 25 abs. 1 DSGVO hinsichtlich der nötigen technischen und organisatorischen Maßnahmen aus, welcher den Scraping-Vorfall erst ermöglicht hat.

aa. Nach Art. 25 Abs 1 DSGVO hat der Verantwortliche 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen – wie z.B. Pseudonymisierung – zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Dies gilt sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung. Bei dem Begriff „geeignete technische und organisatorische Maßnahmen“ handelt es sich um einen unbestimmten Rechtsbegriff. Konkretisiert werden die Anforderungen durch die in die Überlegung einzustellenden Umstände (Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken).

bb. Die irische Datenschutzbehörde CDC hat in ihrem Bescheid vom 25.11.2022 (Anlage K3) umfassend dargelegt, dass die Beklage hinsichtlich des Kontakt-Importer-Tools nicht den Anforderungen der DSGVO gerecht wurde und ein Verstoß gegen Art. 25 Abs. 1 DSGVO gegeben ist. Berücksichtigt wurde dabei insbesondere, dass angesichts der enormen Datenmengen, die die Beklagte in ihren Datenbanken vorhält, ein erhebliches Angriffsrisiko und eine Anfälligkeit für Scra-

ping-Angriffe besteht. In Rn. 141 der Entscheidung wird ausgeführt, dass die Beklagte weitere technische Schutzmaßnahmen hätte ergreifen können, beispielsweise, indem keine exakten Profile durch Einsatz des Kontakt-Importer-Tool Telefonnummern zugeordnet würden, sondern mehrere verwandte Profilvorschläge. Rn. 142 der Entscheidung stellt die Bedeutung von quantitativen Beschränkungen (“rate limiting“) heraus. Rn. 143 verweist auf die Möglichkeit technischer Maßnahmen wie „Captchas“ (dazu und zu den Einwänden der Beklagten insoweit auch Rn. 165 f.) oder Veränderungen in der Benutzeroberfläche. Als organisatorische Maßnahme wird beispielsweise der Einsatz eines „red team“ genannt, um Scraping-Aktivitäten zu erkennen und das Risiko eines Datenscraping zu mindern.

cc. Die Ausführungen der Fachbehörde sind überzeugend, auch unter Berücksichtigung des Umstandes, dass die Beklagte in Reaktion auf den Vorfall nach eigenem Vorbringen ihre Sicherheitsvorkehrungen angepasst hat. Vor diesem Hintergrund steht - entsprechend der Entscheidung der irischen Datenschutzbehörde vom 25.11.2022 (K3) - zur Überzeugung des Gerichts fest, dass ein Verstoß gegen Art. 25 Abs. 1 DSGVO gegeben ist.

b. Der Klagepartei ist im vorliegenden Fall durch den Verstoß auch ein Schaden entstanden.

aa. Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Zum hier gegenständlichen Begriff des Schadens hat das Landgericht Bielefeld in seinem Urteil vom 19.12.2022 – Az. 8 O 182/22 (zitiert nach juris) ausgeführt was folgt (Rn. 27):

„Das Merkmal des immateriellen Schadens ist autonom auszulegen (für alle: Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 82 Rn. 17 ff.). Erwägungsgrund 146 (und in diesem S. 3) zur DSGVO sieht vor, dass der Begriff des Schadens im Lichte der Rechtsprechung des Gerichtshof weit auf eine Art und Weise ausgelegt werden soll, die den Zielen dieser Verordnung in vollem Umfang entspricht. Erwägungsgrund 75 zur DSGVO nennt etwa Identitätsdiebstahl, finanzielle Verluste, Rufschädigung oder den Verlust der Kontrolle personenbezogener Daten. Ein deutsches Verständnis zum Begriff des Schadens - etwa eine enge Auslegung - ist mithin nicht angezeigt (vgl. dazu BVerfG 14.1.2021, 1 BvR 2853/19, NJW 2021, 1005, 1007). Eine Erheblichkeitsschwelle für das Vorliegen eines solchen Schadens ergibt sich gerade nicht aus der DSGVO. Bagatellschäden sind nicht auszuschließen. Zu verlangen ist aber jedenfalls, dass ein konkreter immaterieller Schaden auch tatsächlich eingetreten („entstanden“) ist (OLG Frankfurt

a.M. 2.3.2022, 13 U 206/20, GRUR-RS 2022, 4491 Rn. 61 ff.; LG Essen 10.11.2022, 6 O 111/22, GRUR-RS 2022, 34818 Rn. 75; LG Gießen 3.11.2022, 5 O 195/22, GRUR-RS 2022, 30480 Rn. 18). Diesen muss der Kläger darlegen und ggf. beweisen (s. OLG Frankfurt a.M. 2.3.2022, 13 U 206/20, GRURRS 2022, 4491 Rn. 57, 65; Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 82 Rn. 20 mwN).“

Diesen zutreffenden Ausführungen des Landgerichts Bielefeld wird beigetreten. Unter Zugrundelegung dieser Maßstäbe konnte im vorliegende Fall zur Überzeugung des Gerichts festgestellt werden, dass der Klagepartei ein Schaden entstanden ist, § 287 ZPO. Eine Aussetzung im Hinblick auf das Verfahren des EuGH im Verfahren C 300/12 „Österreichische Post“ war nicht erforderlich. Denn das Gericht geht vorliegend davon aus, dass ein immaterieller Schaden entstanden ist, der auch über einen Bagatellschaden hinausgeht.

bb. Schriftsätzlich hat die Klagepartei zwar lediglich Formulierungen wiederholt, die gerichtsbekannt in zahlreichen gleichgelagerten Klagen aufgrund des streitgegenständlichen Scraping-Vorfalls Verwendung finden (die Klägerseite habe deswegen einen „erheblichen Kontrollverlust über ihre Daten erlitten“ und sei in einem „Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffenden Daten verblieben“). Aufgrund der informatorischen Anhörung und der dort geschilderten konkreten Auswirkungen konnte indes ein immaterieller Schaden der Klägerseite festgestellt werden, § 287 ZPO.
Der Kläger hat in der informatorischen Anhörung geschildert, dass der Vorfall erhebliche Auswirkungen auf sein Privatleben und auch auf sein Berufsleben gehabt habe. Er hat geschildert, dass er ab dem Jahr 2019 bis in das Jahr 2022 hinein Anrufe von unbekannten Nummern aus dem Ausland (Italien und Großbritannien) auf seinem Handy erhalten habe. Die Hoch-Zeit sei im Jahr 2020 gewesen, der letzte Anruf erinnerlich im Mai 2022. Es habe sich um Anrufe von unbekannten Nummern gehandelt, bei denen niemand in der Leitung gewesen sei, wenn er ans Telefon gegangen sei. Im Jahr 2020 (in der Hoch-Zeit der Anrufe) habe er begonnen, Anrufe bestimmter Nummer zu blockieren, er habe sogar mitten in der Nacht derartige Anrufe erhalten und sich gedacht das sei wieder so ein „bot-Anruf“. Das Blockieren habe letztlich nicht geholfen, da er sodann von anderen Rufnummern aus Anrufe erhalten habe.

Er habe im privaten und beruflichen Bereich, Maßnahmen aufgrund der Störungen durch Anrufe ergriffen. Im beruflichen Bereich habe er die Anrufe bei der IT seiner Firma gemeldet, die Sicherheitsmaßnahmen seien hochgefahren worden (bzgl. Firewall, Authentifizierung bzw. Verifizierungsmethoden, Einführung eines anderen Identifizierungssystems). Zudem habe er erstmals neben seinem privaten Telefon aus Sicherheitsgründen ein dienstliches erhalten, dessen Nummer

nur dem Arbeitgeber bekannt sei. Privat habe er sein Speichermedium für Fotos verändert und sein privates NAS derart umgebaut, dass er es nur noch als lokales NAS nutze, so dass ein Zugriff von außen ausgeschlossen sei. Er habe die Anrufe „bedrohlich“ gefunden, weil niemand dran gegangen sei. Er habe nicht den Hintergrund gewusst und sei verunsichert gewesen. Er habe nicht gewusst, ob auch eine Software überspielt werde oder sonst eine Gefahr bestehe, auch wenn er sich gesagt habe, dass dies bei Apple-Telefonen keine große Gefahr sei.

Die Angaben des Klägers in der informatorischen Anhörung sind glaubhaft. Er hat sie belegt durch Screenshots bzgl der blockierten Nummern (Anlage zum Protokoll vom 10.02.2023). Zudem hat er anschaulich anhand konkreter Ereignisse geschildert, warum er eingrenzen könne, dass sich die Anrufe 2020 gehäuft haben. Er konnte sich nachvollziehbar deshalb an die gehäuften Anrufe erinnern, da diese in die Zeit fielen, in der er sich aufgrund der Lockdown- Situation (1. Lockdown) im Homeoffice befunden habe. Er hat auch differenzierende Angaben gemacht. So hat er klar eingeräumt, dass er keinen SPAM über SMS erhalten habe. Lediglich das SPAM-Aufkommen über E-Mail habe zugenommen. Dies zeigt, dass der Kläger nicht pauschalisierte mögliche Auswirkungen für sich reklamierte, sondern differenzierend berichtete. Aufgrund des persönlich Eindrucks in der Verhandlung und des besonnenen, differenzierenden Aussageverhaltens erschien der Kläger glaubwürdig.
Vor diesem Hintergrund konnte festgestellt werden, dass erhebliche Auswirkungen auf Klägerseite bestanden, die - auch unter Berücksichtigung der zeitlichen Nähe der Vorfälle zu dem Datenabgriff 2018/2019 bzw. der Veröffentlichung 2021 - kausal auf den Scraping-Vorfall zurückgeführt werden können, § 287 ZPO. Bei der Höhe des immateriellen Schadens waren insbesondere die Intensität der Beeinträchtigung (stark zunehmende Anrufe, auch nachts), die Dauer der Beeinträchtigung über mehrere Jahre mit einer Hoch-Zeit im Jahr 2020, die Auswirkung auf verschiedene Lebensbereiche (privat, beruflich), der vom Kläger geschilderte Grad der gefühlsmäßigen Beeinträchtigung („bedrohlich“, „verunsichert“) sowie der Umstand berücksichtigt, dass lediglich die Verknüpfung der Telefonnummer mit weiteren Daten des Klägers aufgrund des streitgegenständlichen Vorfalls ermöglicht wurde, während einige der Daten, deren Abgriff der Kläger rügt, ohnehin öffentlich waren (Name, Facebook ID, Geschlecht).

2. Die Klagepartei hat gegen die Beklagte keinen Feststellungsanspruch hinsichtlich etwaiger zukünftiger Schäden.

Angesichts des Scraping-Vorfalls 2018/2019 und des Zeitablaufs von nunmehr über vier Jahren

seit dem Vorfall bzw. zwei Jahren seit der Veröffentlichung der Daten ist nicht zu erkennen, wie der Klagepartei noch Schäden aus dem Scraping-Vorfall entstehen sollen, die dann auch mit dem Beweismaß zumindest des § 287 ZPO diesem Scraping-Vorfall zugeordnet werden könnten. Dies gilt insbesondere, wenn man berücksichtigt, dass nach den eigenen Angaben des Klägers die Anrufe von unbekannten Nummern im Mai 2022 endeten und er seitdem keine weiteren Auffälligkeiten registriert habe.

3. Der Klagepartei steht der geltend gemachte Unterlassungsanspruch nur teilweise zu.

a. Ein Anspruch besteht, soweit die Klagepartei geltend macht, ihre im Antrag 3.a aufgelisteten personenbezogenen Daten dürfe nicht über das Kontakt-Importer-Tool Dritten zugänglich gemacht werden.

Insoweit kann auf die zutreffenden Ausführungen des LG München I im Urteil vom 02.03.2023, Az. 4 O 4944/22 Bezug genommen werden, welches seinerseits auf die Entscheidung des LG Paderborn vom 19.12.2022 verweist:

Der Unterlassungsanspruch folgt aus § 1004 Abs. 1 S. 2 BGB i.V.m. Art. 17, 18 DSGVO.

„1. (...) Entgegen der Rechtsauffassung der Beklagten sind Unterlassungsansprüche nach nationalem Recht nicht durch die DSGVO gesperrt (vgl. Bundesgerichtshof, Urteil vom 12.10.2021, Az.: VI ZR 488/19). Zutreffend ist, dass die DSGVO selber keine Anspruchsgrundlage für einen Unterlassungsanspruch gibt. Allerdings gewährt die DSGVO dem Betroffenen in Art. 17 einen Löschungsanspruch und in Art. 18 einen Anspruch auf Einschränkung der Verarbeitung. Art. 79 DSGVO bestimmt das Recht eines Betroffenen auf einen „wirksamen gerichtlichen Rechtsbehelf“ unbeschadet von außergerichtlichen und verwaltungsrechtlichen Rechtsbehelfen oder Beschwerdemöglichkeiten. Dieser Bestimmung ist zu entnehmen, dass der Rechtsschutz des Betroffenen gerade nicht eingeschränkt werden soll, sondern dem Betroffenen wirksamer Rechtsschutz zur Verfügung stehen soll. Wäre der Kläger aber auf einen reinen Löschungsanspruch verwiesen, so würde seiner Zielsetzung, die Facebook-Plattform weiter zu nutzen, jedoch ohne Inkaufnahme der von ihm gesehenen rechtswidrigen Gestaltungen hinsichtlich der Datenverarbeitung nicht gerecht. Der Kläger wäre dann faktisch nur vor die Möglichkeit gestellt, seinen Account abzumelden und ggf. seine Daten löschen zu lassen oder aber ohne weitere Möglichkeiten die Face-

book-Plattform weiter zu nutzen trotz gerichtlich festgestellter Datenschutzverstöße. Eine derartige Einschränkung entspricht nicht dem Telos von Art. 79 DSGVO.

2. Die Gestaltung des Kontakt-Importer-Tools in den Jahren 2018 und 2019 entsprach auf der Basis der Darstellungen der Parteien nicht Art. 32 DSGVO. Nach dieser Bestimmung muss der Verantwortliche „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“, treffen. Nach Art. 32 Abs. 2 DSGVO muss bei der Beurteilung des angemessenen Schutzniveaus insbesondere berücksichtigt werden, welches Risiko verbunden sein können mit „[...] unbefugte[r] Offenlegung von beziehungsweise unbefugte[m] Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden“. Dem genügten die seitens der Beklagten behaupteten (und seitens des Klägers bestrittenen) Schutzmaßnahmen - diese für einmal unterstellt - nicht.

Das Landgericht Paderborn hat hierzu in seiner grundlegenden Entscheidung vom 19.12.2022 ausgeführt:

„Art. 32 DSGVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Er konkretisiert die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DSGVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 1).

Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Paal/Pauly/Martini, 3. Aufl. 2021, DSGVO Art. 32 Rn. 2; vgl auch Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DSGVO Art. 32 Rn. 2).

Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO sind dabei der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Perso-

nen als Faktoren zu berücksichtigen. Dies bedeutet allerdings nur, dass sie in die Verhältnismäßigkeitsprüfung einzustellen, jedoch nicht notwendigerweise absolut zu befolgen sind (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 14).

Die DSGVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere weiter fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten müssen. Dabei kommt es letztlich darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 41).

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen und Auftragsverarbeiter aber nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 3).

Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zupersonenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Diese sind zwingend in die Risikobetrachtung einzubeziehen (Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 5).

Ausweislich des Erwägungsgrunds 76 zur DSGVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten des betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

cc) Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklag-

te zumindest nicht ausreichend nachgekommen. Denn die von ihr behaupteten „Anti-Scraping-Maßnahmen“ sind selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO. Beim Zugang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34). So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf G sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum G-Profil, bei dem diese angegeben wurde, ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das G-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden. [...]

Daher wären weitergehende Maßnahmen notwendig gewesen. Diese hätten beispielsweise so ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind. Es kann ein Missbrauch des CIT in Form von Datenscraping dann zumindest erschwert werden, so z.B. durch die weitere Angabe eines Vornamens, der sich neben der Telefonnummer ebenfalls hochladen ließe. So würden weitere Variablen hinzutreten, die auf eine den Nutzungsbedingungen entsprechende Nutzung des CIT hindeuten. Datenscraper hingegen werden vor das Problem gestellt, das neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren. Zudem wäre ein höherer Datenverkehr erforderlich, der ggf. den bereits behaupteten Maßnahmen der Übertragungsbeschränkungen und der Arbeit des EDM-Teams einen größeren Nutzen verleiht. Dies würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen. Denn laut der Beklagten sei es Hauptzweck der G-Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Das CIT ermöglicht dementsprechend Nutzer ihre Kontakte ihrer Mobilgeräte auf G hochzuladen und anhand der Telefonnummern die G-Profile ihrer Kontakte zu finden. Wei-

tergehende Angaben laufen diesen Absichten nicht zuwider, zumal diese ggf. ebenfalls über das CIT automatisch über die Kontaktliste des Mobilgeräts des Nutzers in Erfahrung gebracht werden könnte.

Diese oder andere Schutzmaßnahmen, wie die klägerseits angeführten Begrenzungen der abgleichbaren Rufnummern oder Nutzung nur für Freunde von Freunden, implementierte die Beklagte jedoch vor oder während des streitgegenständlichen Datenscrapings nicht. Erst im Nachgang implementierte die Beklagte eine vergleichbare Sicherheitsmaßnahme, der sog. „Social Connection Check". Die Beklagte nahm damit vielmehr erst den Vorfall zum Anlass ihre Schutzmaßnahmen zu evaluieren und traf ausweislich ihres als Anlage B11 vorgelegten Artikel „Scraping nach Zahlen" vom 19.05.2021 „eine Reihe von Verbesserungen" im September 2019."

Den überzeugenden Ausführungen wird beigetreten. Ergänzend wird darauf verwiesen, dass auch ein Verstoß gegen Art. 25 Abs. 1 DSGVO aufgrund unzureichender technischer und organisatorischer Maßnahmen vorliegt, siehe oben.
Vor diesem Hintergrund besteht bzgl. des Zugänglichmachens der genannten Daten ein Anspruch auf Unterlassung im Hinblick auf das Zugänglichmachen durch das Kontakt-Importer-Tool. Der Verstoß gegen Art. 25 DSGVO und damit verbundene Rechtsgutseingriff indiziert eine Wiederholungsgefahr.
Diese ist durch zwischenzeitlich getroffene Maßnahmen der Beklagten nicht entfallen, zumal die Maßnahmen fortlaufend an den Stand der Technik anzupassen sind. Die Beklagte hat insbesondere keine strafbewehrte Unterlassungsverpflichtung abgegeben, welche die Annahme einer Wiederholungsgefahr ausräumen könnte.

Etwas anderes ergibt sich auch nicht daraus, dass Teile der Daten ohnehin öffentlich einsehbar waren. Denn der Unterlassungsanspruch bezieht sich gerade auf das Zugänglichmachen durch das Kontakt-Importer-Tool und die damit verbundene Erstellung einer Verbindung zwischen den genannten Daten und einer Telefonnummer.

b. Die unter Ziffer 3b) des Klageantrags geltend gemachten Unterlassungsansprüche bestehen nicht.

Angesichts der Anforderungen der DSGVO sind mittlerweile Informationen zum Datenschutz regelmäßig verhältnismäßig lang. Ob dies tatsächlich geeignet ist, dem Nutzer einen besseren

Überblick zum Datenschutz zu geben, kann dahinstehen. Selbst wenn unterstellt würde, die Informationen der Beklagten zur Datenverarbeitung wären tatsächlich „unübersichtlich und unvollständig“ gewesen, so hätte die Klagepartei durch den vorliegenden Prozess alle nötigen Informationen bekommen. Speziell für die Klagepartei fehlt es deshalb an der Wiederholungsgefahr. Eine allgemeine Prüfung, ob für irgendwelche Dritte in der Zukunft Probleme entstehen, ist nicht Gegenstand des vorliegenden Individualklageverfahrens.

4. Der Klagepartei steht der mit der Klageforderung geltend gemachte Auskunftsanspruch nicht zu, da bereits Erfüllung eingetreten ist.

Zwar besteht gemäß Art. 15 DSGVO ein Auskunftsrecht der Klagepartei gegen die Beklagte, insbesondere auch bzgl. der Empfänger bzw. Kategorien von Empfängern personenbezogener Daten. Jedoch hat die Beklagte der Klagepartei unstreitig bereits mit Schreiben vom 23.08.21 und 09.09.21 Auskunft erteilt. Nach Darstellung der Klagepartei ist insoweit noch keine Auskunft erteilt worden, weil nicht mitgeteilt wurde welchen konkreten Empfängern Daten zugänglich gemacht wurden (S. 41/42 der Klageschrift). Jedoch hat die Beklagte insoweit dargelegt, sie habe dazu keine Kopie der Rohdaten und könne daher nichts sagen. Damit ist der Auskunftsanspruch aber gemäß § 362 BGB erfüllt. Wenn die Klagepartei diese Auskunft für unzutreffend halten sollte, müsste sie die nach dem Bürgerlichen Gesetzbuch bestehenden Möglichkeiten (Antrag auf Abgabe der eidesstattlichen Versicherung) ergreifen.

5. Der Klagepartei steht teilweise ein Schadensersatzanspruch zu, soweit sie Zahlung von Rechtsanwaltsgebühren fordert.

Ein Anspruch besteht, soweit eine Rechtsanwaltsgebühr in Höhe von 280,60 € verlangt wird (1,3-facher Satz aus einem Gegenstandswert von 1.600 EUR zzgl. Auslagenpauschale und Mehrwertsteuer).

Der Klagepartei standen Ansprüche bzgl. der unter Ziffer 1.), 3.a) und 4.) geltend gemachten Forderungen zu. Rechtsanwaltskosten kann die Klagepartei jedoch lediglich aus Schadensersatzgesichtspunkten bzw. bzgl. des Unterlassungsanspruchs (Abwehranspruch nach Rechtsguteingriff) verlangen, § 280 Abs. 1 BGB. Soweit die Klagepartei vorgerichtlich Auskunft begehrte, besteht keine Anspruchsgrundlage für den Ersatz dieser Kosten. Insbesondere befand sich die Beklagte bzgl. der begehrten Auskunft im Zeitpunkt des anwaltlichen Schreibens nicht im Verzug.

Der Gegenstandswert war vorliegend nach § 23 Abs. 3 S. 1 RVG, § 48 GKG durch Addition vorgerichtlich berechtigter Ansprüche (Schadensersatz, Abwehr bzw. Unterlassung) zu bestimmen. Der Wert eines Unterlassungsanspruchs bestimmt sich nach dem Interesse des Anspruchstellers an der Unterbindung weiterer gleichartiger Verstöße. Dieses Interesse ist pauschalierend unter Berücksichtigung der Umstände des Einzelfalls zu bewerten und wird maßgeblich durch die Art des Verstoßes, insbesondere seine Gefährlichkeit und Schädlichkeit für den Inhaber des verletzten Schutzrechts bestimmt. Vorliegend ist zu beachten, dass personenbezogene Daten betroffen waren, die nicht der Intimsphäre der Klagepartei zuzuordnen sind oder unter die „besondere Kategorien von Daten“ nach Art. 9 DSGVO fällt. Die Daten der Klagepartei waren teilweise bereits unstreitig öffentlich bekannt. Auch unter Berücksichtigung des mit der DSGVO gewollten effektiven Schutzes personenbezogener Daten ist der Wert des zugesprochenen Unterlassungsanspruchs angesichts der Art des Verstoßes und der Bedeutung der geschützten Daten mit 1.000 EUR anzusetzen.

Nicht werterhöhend sind vorliegend die Einkommens- und Vermögensverhältnisse der beteiligten Parteien. Insoweit führt Toussaint in: BeckOK Kostenrecht, Dörndorfer/Wendtland/Gerlach/Diehn 40. Edition Stand: 01.01.2023 zutreffend aus:
„Anders als bei den beiden vorgenannten Kriterien geht es bei den Vermögens- und Einkommensverhältnisse (Einzelheiten → Rn. 44.1 f.) der Parteien nicht um die Streitigkeit, sondern um die davon unabhängigen Verhältnisse der Parteien. Sie sind zu berücksichtigen, damit Umfang und Bedeutung der Sache in ein angemessenes Verhältnis zur wirtschaftlichen Leistungskraft der Parteien gesetzt werden. Maßgeblich sind dabei nicht nur die Verhältnisse des „Angreifers“, sondern – im Hinblick auf eine mögliche Kostentragungspflicht auch dessen Gegners – stets die beider Parteien (Meyer Rn. 17). Während sie in Familiensachen seit jeher eine zentrale Rolle bei der Bewertung haben (vgl. § 48 Abs. 3 aF bzw. jetzt § 43 Abs. 2 FamGKG), dürften sie bei allen übrigen nichtvermögensrechtlichen Streitigkeiten eher die Bedeutung eines Korrektivs haben.“

Ein derartiges Korrektiv könnte allenfalls in die Richtung erfolgen, dass wegen des Kostenrisikos für beide Parteien der Gegenstandswert auch bei vermögenden Anspruchsgegnern des Unterlassungsanspruchs nicht zu hoch anzusetzen ist.

B.

Die Kostenentscheidung folgt aus § 92 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit ergeht nach §§ 708 Nr. 11, 711, 709 S. 1 ZPO.

C.

Die Streitwertfestsetzung richtet sich nach §§ 63, 48, 39 GKG. Auf die Ausführungen im Beschluss vom 21.10.2022 (Bl. 155/156 d. A.) wird Bezug genommen.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht München I
Prielmayerstraße 7
80335 München

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem dritten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als **elektronisches Dokument** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen
- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:
- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das be-

sondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

[redacted]
Richterin am Landgericht

Verkündet am 20.04.2023

gez.
[redacted], JAng
Urkundsbeamtin der Geschäftsstelle

Für die Richtigkeit der Abschrift
München, 21.04.2023

[redacted], JAng
Urkundsbeamtin der Geschäftsstelle