Beglaubigte Abschrift

Landgericht München I

Az.: 37 O 9923/23

IM NAMEN DES VOLKES

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.LEGAL Wilde Beuger Solmecke**, Rechtsanwälte Partnerschaft mbB, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Limited, vertreten durch d. Direktor, 4 Grand Central Square, Dublin 2, Irland
- Beklagte -

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

wegen Forderung

erlässt das Landgericht München I - 37. Zivilkammer - durch den Richter am Landgericht Schmelcher als Einzelrichter aufgrund der mündlichen Verhandlung vom 09.02.2024 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an den Kläger 500,00 € nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 14.09.2023 zu zahlen.

2. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 90,96 € zuzüglich Zinsen seit 14.09.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

3. Im Übrigen wird die Klage abgewiesen.

4. Von den Kosten des Rechtsstreits haben der Kläger 90 % und die Beklagte 10 % zu tragen.

5. Das Urteil ist vorläufig vollstreckbar, für die Beklagte jedoch nur gegen Sicherheitsleistung in Höhe von 110 % des zu vollstreckenden Betrags. 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.

Tatbestand

Die Parteien streiten um Schadensersatzansprüche aus einem Fall des Daten-Scraping.

Der Kläger nutzte die von der Beklagten betriebene Social Media Plattform facebook.com mit der

Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Beim Anlegen eines Facebook-Accounts wird der künftige Nutzer auf Datenschutz- und Cookie-Richtlinien hingewiesen. Diese sind durch eine Verlinkung getrennt abrufbar. Nach der Anmeldung sind zunächst die Vor- bzw. Standardeinstellungen aktiviert. Demnach können „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse „finden“. Die Angabe der Mobilfunknummer ist nicht grundsätzlich zwingend. Wenn der Nutzer die Zweifaktor-Authentifizierung nutzen möchte, ist die Angabe einer Mobilfunknummer jedoch zwingend. Entscheidet sich ein Nutzer, diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Der Nutzer kann die Einstellungen individuell verändern und im Hilfebereich einlesen, wie die Beklagte insbesondere die Mobilfunknummer verwendet. Die Nutzer können angeben, ob es möglich sein soll, sie über ihre Telefonnummer zu finden („Suchbarkeits-Einstellungen“). Name, Geschlecht und Nutzer-ID sind dabei die immer öffentlichen Informationen. Bei anderen Informationen können die Nutzer bestimmen, wer diese einsehen und suchen kann. Die Voreinstellung der Suchbarkeits-Einstellungen bezüglich der Telefonnummer ist „Alle“. Der Kläger hatte bei Eröffnung seines Facebook-Accounts im Jahr 2013 seine Mobilfunknummer hinterlegt, die Such-

barkeitseinstellungen auf „Alle“ belassen (Anlage B22) und seitdem nicht mehr geändert.

Im April 2021 wurden Daten von 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet. Die veröffentlichten Daten waren im Jahr 2019 mittels des Facebook-Tools Kontakt-Importer aus öffentlich zugänglichen Daten ausgelesen worden. Die unbekannten Täter gingen hierbei so vor, dass sie Millionen von Telefonnummern generierten und diese über die zu Verfügung gestellten Software synchronisierten, sodass diese realen Facebook-Nutzern zugeordnet werden konnten. Sodann wurden die öffentlich zugänglichen Profilinformationen der Telefonnummer zugeordnet, ausgelesen und verbreitet. Dies betraf Nutzer, welche bei den Suchbarkeitseinstellungen ihre Telefonnummer auf „alle“ gestellt hatten. Ein Sicherungsmechanismus, welcher den vorgenannten massenhaften, automatisierten Datenabruf verhindert hätte, war nicht vorhanden.

Die irische Datenschutzbehörde hat aufgrund dieses Vorfalls eine Geldbuße in Höhe von 265 Millionen Euro verhängt.

Die Daten der Klagepartei wurden bei dem dargestellten Scraping-Vorfall abgegriffen.

Mittlerweile hat der Kläger seinen Account bei der Beklagten gelöscht.

Mit E-Mail vom 07.06.2023 (Anlage K1) begehrte die Klagepartei von der Beklagten Auskunft und Schadensersatz. Hierauf sandte die Beklagte an den Kläger ein Schreiben, in welchem dem Kläger mitgeteilt wurde, welche seiner Daten vom fraglichen Vorfall betroffen worden sind. Dieses enthielt einen Link zur Seite der Beklagten, auf der die bei der Beklagten gespeicherten Daten des Nutzers eingesehen werden können. Hinsichtlich der weiteren Einzelheiten wird auf die Anlage B 17 verwiesen.

Die Klagepartei begehrt Schadensersatz, Unterlassung und Auskunft.

Die Klagepartei trägt vor, die Einstellung zur Sicherheit der Telefonnummer seien so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Hinsichtlich der Einzelheiten wird auf S. 7 ff. der Klageschrift verwiesen. Entgegen den Grundsätzen der DSGVO seien die Voreinstellungen der Beklagten nicht datenschutzfreundlich. Insbesondere werde der Nutzer nicht ausreichend darüber informiert, dass die Beklagte die Telefonnummer der Nutzer verwende um den Account zu identifizieren. Die Standard-Einstellung sei, dass sämtliche Daten öffentlich einsehbar seien.

Die Beklagte verhindere einen effektiven Datenschutz zur Gewinnmaximierung.

Die veröffentlichten Daten könnten und würden zu gezielten Phishing-Attacken genutzt.

Von der Klagepartei sind folgende Daten im Darknet veröffentlicht worden:

Dabei handele es sich um die Telefonnummer, die Facebook-ID, den Namen und das Geschlecht des Klägers.

Diese Daten seien für jedermann im Internet einsehbar.

Die Klagepartei habe durch die Betroffenheit in dem vorliegenden Fall einen Kontrollverlust erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über den möglichen Missbrauch ihrer Daten verblieben. Dies habe sich unter anderem in einem verstärkten Misstrauen bezüglich Emails und Anrufen von unbekannten Nummern und Adressen manifestiert.

Darüber hinaus erhalte die Klagepartei seit dem Vorfall unregelmäßig unbekannte Kontaktversuche. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen. Es würden auch bekannte Plattformen wie Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Dies habe dazu geführt, dass die Klagepartei nur noch mit äußerster Vorsicht auf jegliche Nachrichten reagieren kann und jedes Mal einen Betrug fürchtet und Unsicherheit verspüre.

Wäre der Klägerseite aber bewusst gewesen, dass die Beklagte unzureichende Sicherheitsmaßnahmen hinsichtlich der Verknüpfbarkeit der Telefonnummer und der übrigen Daten ergriffen hätte, so hätte sie diese Option zu keinem Zeitpunkt aktiviert.

Der Schutz der personenbezogenen Daten der Beklagten sei zum Zeitpunkt des Daten-Scraping nach dem Stand der Technik nicht ausreichend im Sinne des Art. 5 Abs. 1 f. DSGVO gewesen.

Über ihre eigenen Verarbeitungstätigkeiten, insbesondere über die Zwecke der Verarbeitung der Telefonnummer und die Funktionsweise der Kontact-Importer-Funktion, über immer öffentliche Nutzerinformationen, Zielgruppenauswahl und Drittlandübermittlungen stelle die Beklagte keine transparenten und konkreten Informationen nach Vorgabe der Art. 13, 14 DSGVO — insbesondere bei Registrierung — zu Verfügung.

Dem Auskunftsersuchen der Klagepartei sei die Beklagte nicht ausreichend nachgekommen.

Die Datenschutzverstöße seien kausal für den eingetretenen Schaden.

Es werde bestritten, dass ein Umstellen der Suchbarkeitseinstellungen der Telefonnummer den Scraping-Vorfall verhindert hätte.

Die Klagepartei meint ihr stünde ein Schadensersatzanspruch nach Art. 82 Abs. 1 DGVSO zu.

Die Klagepartei meint, es liege ein Verstoß gegen die DSGVO vor, da die Beklagte als Verantwortlicher im Jahr 2019 die Klägerseite betreffende Daten ohne Rechtsgrundlage verarbeitet, sie unbefugten Dritten zugänglich machte und hierbei die Pflichten aus Art 5, 25, 32 und 34 DSGVO sowie die Betroffenenrechte des Klägers nach Art. 15, 17 und 18 DSGVO verletzte. Das Schutzniveau von Scrapingangriffen sei zu niedrig. Die Voreinstellung zur Suchbarkeit der Telefonnummern verstoße gegen Art. 25 Abs. 2 S. 3 DSGVO.

Die Klagepartei meint, die Auskunft mittels Link sei unzureichend, da offen bleibe, welche Daten der Klägerseite abgegriffen worden sei und wieviele Beteiligte diese Funktion hinsichtlich der Daten des Klägers ausgenutzt hätten.

Die Beklagte habe die Klagepartei nicht in ausreichendem Maße über die Verarbeitung der sie betreffenden personenbezogenen Daten aufgeklärt. Die Art der Belehrung über die Verwendung und Geheimhaltung der Telefonnummer stelle einen Verstoß gegen die DSGVO dar. Die Beklagte unterrichte die Nutzer unzureichend über die Nutzung der Telefonnummer. Eine Folgenabschätzung des Nutzers zur Übermittlung seiner Telefonnummer sei so nicht möglich. Die Tatsache, dass die Nutzer nur per Unterverlinkung darüber unterrichtet würden, dass andere Nutzer sie mit der Telefonnummer finden könnten, sei nicht ausreichend.

Der Schadensersatz müsse eine abschreckende Präventionsfunktion haben. Eine Erheblichkeit sei nicht erforderlich.

Der Unterlassungsanspruch bestehe aus §§ 1004 analog, 823 Abs. 1 und aus Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO.

Die Beklagte trage die vollständig Darlegungs- und Beweislast hinsichtlich der Einhaltung der DSGVO. Selbst wenn man davon ausgehen würde, dass der Eintritt eines konkreten Schadens auf Seiten des Betroffenen notwendig sei, würde Art. 82 DSGVO eine Beweislastumkehr enthalten. Eine Kausalität und ein Verschulden sei für den Schadensersatzanspruch nach Art. 82 DSGVO nicht erforderlich.

Die Klagepartei beantragt:

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

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

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

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 713,76 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte trägt vor, die Beklagte habe umfassend und transparent über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl informiert. Die Privatsphäre-Einstellungen seien leicht zugänglich. Zur Ergänzung wird auf Seite 26 ff. des Schriftsatzes vom 01.12.2024 verwiesen.

Die Beklagte habe Maßnahmen getroffen, das Risiko von Scraping zu unterbinden. Hinsichtlich der Einzelheiten wird auf Seite 35 ff. der Klageerwiderung vom 13.10.2023 verwiesen. Von dem

Schadenseintritt könne nicht rückgeschlossen werden, dass die von der Klagepartei veranlassten Maßnahmen unzureichend gewesen seien; dies sei vielmehr ex ante zu betrachten. Die Beklagte habe die Nutzer auch ausreichend über das Scraping informiert.

Ein immaterieller Schaden sei nicht vorhanden, insbesondere läge keine spürbare Beeinträchtigung der Klagepartei vor. Ein Gefühl des Kontrollverlustes sei bereits deshalb ausgeschlossen, weil die abgegriffenen Daten öffentlich einsehbar gewesen seien. Gegen den Eintritt eines Schadens spreche auch, dass die Klagepartei die Suchbarkeitseinstellungen ihrer Telefonnummer auf „Alle“ belassen habe.

Der Scraping-Vorfall erhöhe nicht die Gefahr Opfer von Betrug oder anderen schweren Internetverbrechen zu werden.

Die Beklagte meint, der Klageantrag unter Ziffer 1 sei nicht hinreichend bestimmt, da die Klagepartei den Anspruch auf zwei zeitlich auseinanderfallende angebliche Verstöße stütze. Auch die Klageanträge unter Ziffer 2 und 3 seien zu unbestimmt. Zudem fehle ein Feststellungsinteresse.

Der Vortrag der Klagepartei sei hinsichtlich angeblich abgerufener Daten nicht konkret genug.

Ein Verstoß scheide aus, da die durch Scraping abgerufene Daten nach den Einstellungen der Klagepartei öffentlich einsehbar gewesen seien. Die Beklagte müsse die Vertraulichkeit öffentlich einsehbarer Daten nicht gewährleisten. Die Voreinstellungen ergäben sich aus dem Wesen des sozialen Netzwerks und dienten dazu, dass Freunde sich gegenseitig finden.

Eine Melde- und Benachrichtigungspflicht habe nicht bestanden, da es an einer Verletzung der Sicherheit gefehlt habe.

Ein Verstoß gegen die DSGVO liege nicht vor. Bei dem streitgegenständlichen Vorfall seien lediglich öffentlich einsehbare Daten abgerufen und an anderer Stelle erneut zugänglich gemacht worden. Dies sei im Internet allgegenwärtig. Scraping könnte nicht vollständig verhindert werden.

Der Schutzbereich des Art. 82 DSGVO umfasse keine Verstöße gegen Art. 13, 14, 15, 24, 25 und 34 DSGVO.

Ein Verstoß der Beklagten gegen die DSGVO sei nicht ausreichend substantiiert dargelegt. Die Beklagte müsse keine Informationen zu hypothetischen Datenverarbeitungen Dritter erteilen.

Ein etwaiger Schaden wäre der Klagepartei selbst zuzurechnen gewesen, da die Einsehbarkeit der Daten den Privatsphäre-Einstellungen der Klagepartei entsprochen hätten.

Eine Anspruchsgrundlage für den Unterlassungsanspruch bestehe nicht. Der geltend gemachte Anspruch stelle keinen Unterlassungsanspruch dar, vielmehr verlange die Klagepartei ein aktives Tun. Zudem fehle es an einer Erstbegehungs- und Wiederholungsgefahr.

Der Auskunftsanspruch sei in erster Linie auf die Datenverarbeitung durch Dritte gerichtet. Soweit er die Beklagte betreffe, sei der Anspruch bereits erfüllt.

Es fehle an einem Verschulden der Beklagten.

Eine Abschreckungswirkung sei bei einem etwaigen Schadensersatzanspruch nicht zu berücksichtigen.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze und die zu den Akten gereichten Unterlagen sowie das Protokoll der mündlichen Verhandlung vom 09.02.2024 Bezug genommen.

Entscheidungsgründe

A. Die Klage ist zulässig und teilweise begründet.

I. Die Zulässigkeit der Klage ergibt sich aufgrund folgenden Ausführungen:

1. Der Klageantrag zu Ziff. 1 ist zulässig. Dieser ist entgegen der Auffassung der Beklagten insbesondere hinreichend bestimmt. 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 Zusammenwir-

kens 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.)

2. Es liegt auch das für den Klageantrag in Ziff. 2 erforderliche Feststellungsinteresse im Sinne des § 256 ZPO vor. Der Kläger behauptet die Möglichkeit weiterer Schäden. Dies erscheint - nach dem im Rahmen der Zulässigkeitsprüfung eingeschränkten Prüfungsmaßstab - nicht ausgeschlossen. Durch den Scraping-Vorfall sollen nach Auffassung des Klägers schützenswerte Daten von ihm über das Internet einer Vielzahl an Personen zugänglich gemacht worden sein. Es besteht danach die abstrakte Möglichkeit, dass seine veröffentlichen Daten missbräuchlich verwendet werden.

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

a) Der Klageantrag zu Ziff. 3 a) ist hinreichend bestimmt. Daneben liegt auch das erforderliche Rechtsschutzbedürfnis vor. Soweit die Beklagte rügt, dass die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ im Klageantrag zu Ziff. 3 a) zu unbestimmt sei, führt dieses nicht zur Unzulässigkeit des Antrags.

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 (LG Paderborn, Urteil vom 19.12.2022, Az: 3 O 99/22, GRUR-RS 2022, 39349).

Die Beklagte als Betreiberin einer Kommunikationsplattform mit großer Entwicklungsabteilung kann nicht von einem einzelnen Kläger verlangen, dass dieser genau angibt, welche konkreten Sicherheitsmaßnahmen erforderlich sind. Diese sind zudem in Fluss. Würde die Beklagte auf bestimmte - ggf. sogar noch zu veröffentlichende - Sicherheitsmaßnahmen festgelegt, könnte dies zudem die Sicherheitsbemühungen konterkarieren, da dann unter Umstände verstärkte Bemühungen ergriffen würden, genau diese Maßnahmen zu umgehen.

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 der Kläger durch die Anpassung der Privacy-Einstellungen die Suchbarkeit über die Telefonnummer deaktivieren. Dieses genügt aber nicht, um zukünftige unrechtmäßige Datenverarbeitung zu verhindern, da der Kläger keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat (LG Paderborn a.a.O.).

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

II. Zur Begründetheit ist Folgendes auszuführen:

1. 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 ange-

messenes 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.

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.

Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklagte zumindest nicht ausreichend nachgekommen.

Als Indiz kann hierbei bereits der ergangene Bußgeldbescheid der irischen Datenschutzbehörde herangezogen werden. Im Übrigen ist von Folgendem auszugehen:

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, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum 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 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.

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.

2. Der Kläger hat daher einen Anspruch auf immateriellen Schadensersatz, dies allerdings nur in Höhe von 500,00 €.

a) Entgegen der Auffassung der Klägerseite begründet allein das Vorliegen eines Verstoßes gegen Vorschriften der DSGVO nicht automatisch einen Schaden im Sinne von Art. 82 Abs. 1 DSGVO. Es bedarf vielmehr des Nachweises eines konkreten (auch immateriellen) Schadens (s. auch OLG Frankfurt a. M., Urt. v. 02.03.2022, 13 U 206/20; EuGH, Urt. v. 15.01.2024, Az. C-687/21).

Bereits aus dem Wortlaut des Art. 82 Abs. 1 DSGVO ergibt sich, dass ein Schadensersatzanspruch nur besteht, wenn einer Person wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist. Es handelt sich bei dem Erfordernis des Vorliegens eines Verstoßes gegen die DSGVO und dem daraus entstandenen Schaden um zwei unterschiedliche Tatbestandsmerkmale; der Schaden ist dabei nicht mit der zugrundeliegenden Rechtsgutsverletzung gleichzusetzen. Insofern führt auch nicht jeder Verstoß gegen die DSGVO automatisch zu einem Anspruch auf Schadensersatz.

Auch wenn der Begriff des Schadens grundsätzlich weit zu verstehen und eine schwere Verletzung des Persönlichkeitsrechts nicht erforderlich ist, muss er jedoch auch wirklich „erlitten“ sein (Erwägungsgrund Nr. 146 S. 6), das heißt die Verletzungshandlung muss zu einem konkreten, spürbaren, nicht nur völlig unbedeutenden oder nur individuell empfundenen Nachteil bei dem Betroffenen geführt haben (vgl. LG Landshut, Urteil vom 06.11.2020 – 51 O 513/20; LG Hamburg, Urteil vom 04.09.2020 – 324 S 9/19), wobei eine Erheblichkeitsschwelle für das Vorliegen eines solchen Schadens sich gerade nicht aus der DSGVO ergibt. Als mögliche Schäden werden in

den Erwägungsgründen Nr. 75 und 85 Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, der Verlust der Kontrolle über die eigenen Daten, die Erstellung unzulässiger Persönlichkeitsprofile sowie die bloße Verarbeitung einer großen Menge personenbezogener Daten einer großen Anzahl von Personen genannt. Auch Ängste, Stress sowie Komfort- und Zeiteinbußen zählen dazu (OLG Frankfurt a. M., Urt. v. 02.03.2022, 13 U 206/20 mit Verweis auf Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18 b).

b) Diesen Maßstab zugrunde gelegt - gerade auch unter Berücksichtigung eines weiten Verständnisses des immateriellen Schadens, das ausdrücklich auch Bagatellschäden einschließt - hat der Kläger zur Überzeugung des Gerichts dargelegt, dass bei ihm aufgrund eines Datenschutzverstoßes der Beklagten tatsächlich ein immaterieller Schaden in Form von berechtigter Sorge vor Missbrauch eingetreten ist, wie in der Klageschrift vorgetragen.

a) Hinsichtlich des Vortrags der Klageseite, dass durch den Scraping-Vorfall an sich der Klägerin ein Sorgegefühl bzw. Gefühl des Kontrollverlustes entstanden war, schilderte der Kläger in der mündlichen Verhandlung bei seiner persönlichen Anhörung glaubhaft, und ohne hierbei zu übertreiben, Folgendes:

> *Als ich davon erfahren habe, hat sich das schlecht angefühlt im ersten Moment, weil ich auch nicht wusste, welche Daten betroffen waren. Ich habe auf Facebook viele persönliche Daten unter anderem Bilder, Chats oder Gruppen in denen ich bin die nur für Freunde bestimmt sind. Da wollte ich nicht das die öffentlich zugänglich werden. Auch wenn ich jetzt darüber informiert wurde, dass grundsätzlich erstmal nur die Handynummer veröffentlicht wurde, bleibt unter anderem natürlich die Unsicherheit, insbesondere wie der Rest der dortigen Daten gesichert ist. Auch hin-sichtlich der Veröffentlichung meiner Handynummer fühlt sich das natürlich nicht gut an. Ich will eigentlich nicht, dass diese im Netz kursiert. Außerdem kann jetzt meine Handynummer natürlich meiner Person zugeordnet werden, wodurch weiteres Missbrauchsrisiko besteht und auch dadurch auf Freundesnetzwerke von mir geschlossen werden kann.*

b) Die Forderung des immateriellen Schadensersatzes ist auch nicht deswegen ausgeschlossen, weil der Kläger damals seine Suchbarkeitseinstellungen nicht einschränkte. Der Kläger gab glaubhaft an, dass er bereits vor dem Scraping-Vorfall bemüht war, seine Datenschutzeinstellungen bei Facebook möglichst einschränkend vorzunehmen. Dass dennoch die Suchbarkeitseinstellungen auf der Voreinstellung „Alle“ vorgenommen gewesen war, ist mit den tatsächlich nicht

ohne Weiteres übersichtlichen Einstellungsansichten der Beklagten zu erklären.

b) Soweit der Kläger vorgetragen hat, dass er Adressat von Spam-Mails Dritter geworden sei, ist davon auszugehen, dass diese auf den vorliegenden Datenschutzverstoß zurückzuführen sind. Der Kläger hat glaubhaft vorgetragen, seine Handynummer nicht im Internet veröffentlicht zu haben und bei sozialen Netzwerken auf sensible Datenschutzeinstellungen (nur für Freunde) geachtet zu haben. Anhaltspunkte für Daten-Scraping bei anderen großen Plattformen, bei denen der Kläger aktiv ist oder war, bestehen aufgrund des Parteivortrags nicht.

d) Hinsichtlich der Anspruchshöhe war das verzögerte und nicht eigeninitiativ erfolgte Schreiben der Beklagten mit der Auskunft zu dem Scraping-Vorfall nicht zu berücksichtigen. Unabhängig von der Frage, ob auch in Scraping-Fällen eine Pflicht der Beklagten zur unverzüglichen Benachrichtigung der Klägerin über den Datenvorfall gem. Art. 34 DSGVO bestand oder nicht - ist unklar, warum die nicht erteilte Auskunft kausal für den seitens der Klägerin behaupteten Schaden sein soll (s. im Übrigen auch LG Paderborn, Urteil vom 19.12.2022, Az: 3 O 99/22, GRUR-RS 2022, 39349, wonach ein etwaiger Verstoß gegen die Auskunftspflicht nach Art. 15 DSGVO keinen Schadensersatzanspruch nach Art. 82 DSGVO auslöst). Der Kläger hat sich nach seinen Angaben schon gar nicht mit im späteren Auskunftsschreiben befasst. Dieser klägerseits vorgetragene Punkt war daher bei der Bemessung der Anspruchshöhe nicht zu berücksichtigen.

e) Nach alledem war eine Bemessung des immateriellen Schadensersatzes gemäß § 287 ZPO unter Berücksichtigung aller Umstände mit 500,00 € angezeigt, aber auch ausreichend.

3. Der Kläger hat dagegen die Beklagte keinen Feststellungsanspruch hinsichtlich etwaig zukünftiger Schäden.

Angesichts des Scraping-Vorfalls 2018/2019 und des Zeitablaufs von nunmehr über vier Jahren seit dem Vorfall ist nicht zu erkennen, wie der Kläger noch Schäden aus dem Scraping-Vorfall erleiden können soll, die dann auch mit dem Beweismaß zumindest des § 287 ZPO diesem Scraping-Vorfall zugeordnet werden könnten. Es fehlt mithin an der Schadenswahrscheinlichkeit.

4. Hinsichtlich der Unterlassungsanträge fehlt es derweil an einer Wiederholungsgefahr. Nachdem der Kläger seinen Account bereits vor längerer Zeit gelöscht hatte, ist eine Wiederholung des beanstandeten Verhaltens nicht zu befürchten. Der Datenverstoß der Beklagten führte zur Veröffentlichung der Daten aktiver Nutzer. Eine mögliche Wiederholung eines solchen Vorfalls, der ihn betreffen könnte, hat der Kläger selbst durch Löschung seines Accounts verhindert.

5. Der Kläger hat gegenüber der Beklagten keinen Auskunftsanspruch (Ziff. 4 des Klageantrags)

mehr, da dieser bereits erfüllt worden ist:

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. Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23).

Unter Berücksichtigung des Vorstehenden ist daher Erfüllung eingetreten. Die Beklagte hat in dem Schreiben der Anlage B17 den Ablauf des Vorfalls erläutert, die Daten aufgezählt, welche entwendet sein könnten und einen Link zur Verfügung gestellt, wie die gespeicherten Informationen überprüft werden können. Der Vortrag der Klagepartei im vorliegenden Prozess zeigt, dass die Klagepartei weiß, welche Informationen bei dem Scraping-Vorfall abgegriffen wurden und wie dies geschehen ist. Der Auskunftsanspruch der Klagepartei ist daher erfüllt.

6. Die Rechtsanwaltskosten, welche nach § 286 BGB geschuldet werden, waren daher lediglich aus einem Gegenstandswert von 500,00 € geschuldet.

B. Die Kostenentscheidung folgt aus § 92 Abs. 1 S. 1.

Der bezifferte Klageantrag wurde hierbei mit 1.000,00 € berücksichtigt, der Feststellungsantrag mit 500,00 € bemessen. Die als Unterlassungsanträge formulierten Klageanträge Ziffer 3 a und b wurden mit jeweils 1.600,00 € bewertet. Der Auskunftsanspruch wurde mit 500,00 € bewertet.

C. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt für den Kläger aus §§ 708 Nr. 11, 711 ZPO, für die Beklagte aus § 709 ZPO.

gez.

Richter am Landgericht

Verkündet am 15.03.2024

gez.
, JAng
Urkundsbeamtin der Geschäftsstelle

Für die Richtigkeit der Abschrift
München, 15.03.2024

, JAng
Urkundsbeamtin der Geschäftsstelle