
Datum: 22.05.2023
Gericht: Landgericht Dortmund
Spruchkörper: 24. Zivilkammer
Entscheidungsart: Urteil
Aktenzeichen: 24 O 20/23
ECLI: ECLI:DE:LGDO:2023:0522.24O20.23.00

Tenor:

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits werden dem Kläger auferlegt.

Das Urteil ist vorläufig vollstreckbar. Dem Kläger bleibt nachgelassen, die Vollstreckung der Beklagten wegen ihrer Kosten durch Sicherheitsleistung in Höhe von 110 % des jeweils zur Vollstreckung gestellten Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in gleicher Art und Höhe leistet.

Der Streitwert wird auf 4.500,00 € festgesetzt:

(immaterieller Schadensersatz zu 1.): 2.000,00 €

(immaterieller Schadensersatz zu 2.): 1.000,00 €

(Auskunft zu 3.):
0.500,00 €

(Unterlassungsanspruch zu 4.): 1.000,00
€

(vorgerichtliche Anwaltskosten):
0.000,00 €

Der Kläger macht Ansprüche auf Schadensersatz, Unterlassung, Auskunft und Kostenerstattung wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (DS-GVO) geltend.

Die Beklagte ist Betreiberin der Social Media-Plattform Facebook, die über die Website www.facebook.com sowie Apps abrufbar ist, und Anbieterin der Dienste auf dieser Plattform auf dem Gebiet der Europäischen Union. Der Kläger ist Nutzer von Facebook und unterhält dort ein Benutzerprofil. 3

Das von der Beklagten auf dieser Seite angebotene soziale Netzwerk ermöglicht es den Nutzern, persönliche Profile zu erstellen und in dem Umfang ihrer so erstellten Präsenz in diesem Netzwerk mit anderen Nutzern in Kontakt zu treten. 4

Bei der für den Zugang zu der Plattform erforderlichen Registrierung werden zur Erstellung eines Nutzerprofils verschiedene Daten abgefragt. Der Nutzer wird aufgefordert, seinen Vor- und Nachnamen, sein Geburtsdatum, sein Geschlecht und entweder seine Email-Adresse oder seine Handynummer anzugeben sowie ein entsprechendes Passwort zu erstellen. In dem sich unter den genannten Angaben befindlichen Informationssegment heißt es sodann: „Indem du auf ‘Registrieren‘ klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen (...)“. Die Datenrichtlinie enthält u.a. Angaben dazu, welche der vom Nutzer erteilten Informationen immer öffentlich zugänglich sind – nämlich Name, Profil- und Titelbilder, Netzwerke, Geschlecht, Nutzernamen und Nutzer-ID – und die Angabe, dass öffentlich zugängliche Informationen jeder, also auch Personen außerhalb von der Plattform der Beklagten, sehen kann. 5

Darüber hinaus steht es dem Nutzer frei, weitere Angaben, z.B. zu seinem Beziehungsstatus, seinem Geburtstag oder seiner Telefonnummer, zu machen. Die Beklagte stellt Erklärungen zur Verfügung, wie der Nutzer festlegen kann, wer diese weiteren Informationen sehen kann (sog. Zielgruppenauswahl) und wer ihn anhand seiner E-Mail-Adresse oder seiner Telefonnummer, sofern er E-Mail-Adresse bzw. Telefonnummer auf der Plattform bereitgestellt hat, finden kann (sog. Suchbarkeits-Einstellungen). Trifft der Nutzer keine Zielgruppenauswahl, richtet sich die Zugänglichkeit seiner über die öffentlichen Informationen hinausgehenden Informationen nach der Standardeinstellung, wonach „alle“ die weitergehenden Informationen einsehen können mit Ausnahme der Telefonnummer, die standardmäßig nur vom Nutzer selbst eingesehen werden kann. Passt der Nutzer die Suchbarkeits-Einstellungen nicht an, sieht die Standardeinstellung vor, dass alle Personen, die über die E-Mail-Adresse oder die Telefonnummer des Nutzers verfügen, das Profil des Nutzers, sofern dieser E-Mail-Adresse bzw. Telefonnummer bereitgestellt hat, finden. 6

Im Rahmen der Registrierung gab der Kläger seinen Vornamen, Nachnamen, sein Geburtsdatum und Geschlecht an. Ferner gab er seine Telefonnummer ein. Die Suchbarkeitseinstellung war, jedenfalls bis September 2019, auf „alle“ eingestellt. 7

In der Zeit von Januar 2018 bis September 2019 sammelten Dritte unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. „Scraping“ von scrapen, zu Deutsch „kratzen“, sinngemäß hier „abgreifen“). Es handelte sich dabei um Profilinformatoren, die entweder „immer öffentlich“ oder aber zu diesem Zeitpunkt aufgrund der Privatsphäreinstellungen der Nutzer öffentlich einsehbar waren. Zudem nutzten sie eine „Telefonnummernaufzählung“, um über die Kontakt-Importer-Funktion (das Contact Importer Tool) festzustellen, ob die hochgeladenen Telefonnummern mit dem Konto eines Nutzers verbunden waren. Soweit dies 8

der Fall war, wurde die Telefonnummer den gescrapten Daten des entsprechenden Nutzerprofils hinzugefügt.

Anfang April 2021 wurden die so erstellten Datensätze von über 500 Mio. Facebook-Nutzern im Internet veröffentlicht und frei zum Download bereitgestellt. Hierzu gehörten auch die immer öffentlich zugänglichen Informationen vom Profil des Klägers und die mit seinem Konto verknüpfte Telefonnummer. 9

Mit vorgerichtlichem Anwaltsschreiben vom 19.08.2022 machte der Kläger wegen datenschutzrechtlicher Verstöße Schadensersatz, Feststellung, Ersatz vorgerichtlicher Anwaltskosten sowie Unterlassungs- und Auskunftsansprüche gegenüber der Beklagten geltend (Anlage K4). Mit vorgerichtlichem Anwaltsschreiben vom 29.08.2022 übermittelte die Beklagte – unter Zurückweisung der Ansprüche – eine dezidierte Anleitung nebst Links zur Einsichtnahme in die bei der Plattform hinterlegten Informationen sowie Angaben zu deren Verwendung (Anlage K5). 10

Der Kläger behauptet, die Beklagte habe seine personenbezogenen Daten ohne Gewährleistung der Sicherheit gem. Art. 32 DS-GVO verarbeitet und unbefugten Dritten zugänglich gemacht, weder ihn noch die zuständige Behörde (die Irish Data Protection Commission) über die Datenschutzverletzungen gem. Art. 33, 34 DS-GVO informiert, ihn über die Datenverarbeitungen i.S.d. Art. 13 DS-GVO nicht vollständig informiert und sein Auskunftsrecht aus Art. 15 DS-GVO verletzt. Sämtliche dieser Verstöße würden von Art. 82 DS-GVO erfasst und begründeten Schadensersatz. 11

Der Kläger behauptet, die Beklagte sei auch nicht vorrangig ein soziales Netzwerk zur Kontaktpflege und deshalb zur Erfüllung ihres Unternehmenszwecks auf die Nutzerdaten angewiesen. Vielmehr diene die beispiellose Verarbeitung personenbezogener Daten von Milliarden Menschen ihren eigenen - vorrangigen - kommerziellen Interessen und Marketingzwecken. Die Plattform der Beklagten sei gerade darauf ausgelegt, dass Nutzer so viele personenbezogene Daten wie möglich preisgäben, um ihr Werbenetzwerk zu befeuern. 12

Der Kläger behauptet, die Beklagte habe seine Daten nicht ausreichend geschützt und gegen das bekannte Phänomen des „Scraping“ die zumutbaren Sicherheitsvorkehrungen nicht getroffen, insbesondere weder Sicherheitscapchas gegen automatisch generierte Informationseingaben noch einen Mechanismus zu Überprüfung der Plausibilität der Anfragen bereitgehalten. Dabei sei ersichtlich, dass die Scraper das Tool mit randomisierten Nummernfolgen befüttert haben müssten, um echte Telefonnummern als Zufallstreffer abzufischen und mit den zugehörigen Facebook-Profilen verknüpfen zu können; dies folge aus der Häufigkeit elfstelliger Telefonnummern, die Ende der 90er Jahre „aufgebraucht“, also mit höherer Wahrscheinlichkeit auch tatsächlich vergeben und damit für die Scraper erfolgversprechender gewesen seien. Dadurch, dass die Beklagte die Daten ihrer Nutzer für das Kontakt-Import-Tool zugänglich gemacht habe, seien diese für Unbefugte offengelegt worden, ohne dass der Kläger auf die Möglichkeit eines solchen Missbrauchs des Tools vorab hingewiesen worden sei und darin eingewilligt habe; die unmissverständliche Einwilligung sei aber Voraussetzung für den Erlaubnisvorbehalt bei der grundsätzlich verbotenen Verarbeitung personenbezogener Daten. Hierdurch sei auch das informationelle Selbstbestimmungsrecht des Klägers verletzt. 13

Der Kläger meint, ein Verstoß der Beklagten gegen Art. 25 Abs. 1 und 2 DS-GVO stehe fest, weil die irische Datenschutzbehörde DPC ihn erkannt und gegen die Beklagte eine Geldbuße von 265 Mio. € verhängt habe. Jedenfalls sei die Beklagte der ihr obliegenden Darlegungs- und Beweislast für die Einhaltung dieser Vorschrift nicht nachgekommen. 14

Der Kläger behauptet, die „gescrapten“ Daten seien im Internet in einem bekannten „Hacker-Forum“ zum Download eingestellt und damit öffentlich verbreitet worden. Dadurch sei böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie bspw. Identitätsdiebstahl, die Übernahme von Accounts oder gezieltes Phishing eröffnet worden.	15
Der Kläger behauptet, er sei nach dem erlittenen Kontrollverlust über seine Daten in einem Zustand von gehörigem Unwohlsein und großer Sorge über möglichen Missbrauch verblieben und habe das Gefühl des Beobachtetwerdens und der Hilflosigkeit. Seit über einem Jahr erhalte er Mails in erheblichem Umfang. Der Kläger meint auch, bereits die Verletzung der DS-GVO als solche führe zu einem auszugleichenden immateriellen Schaden, jedenfalls reiche bereits die Ungewissheit, ob personenbezogene Daten an Unbefugte gelangt seien. Außerdem müsse der Schadensersatz abschreckenden Charakter haben.	16
Der Kläger behauptet, es ziehe sich eine künstliche und verwirrende Aufspaltung und Verästelung durch sämtliche Datenschutzeinstellungen mit einer Fülle von Untereinstellungen, die über verschiedene Links zu erreichen seien, was letztlich dazu führe, dass die meisten Nutzer zum größten Teil die vorbestimmten Standardeinstellungen beibehielten. Es werde durch oberflächlich sichere Einstellungen ein Gefühl der Sicherheit vermittelt, während für tatsächlich wirksamen Datenschutz viele Einstellungen gleichzeitig hätten geändert werden müssen. Die Suchbarkeit nach Rufnummer hätte dabei per default auf „Freunde-Freunde“ stehen müssen. Ihrer Informationspflicht über die Erhebung der personenbezogenen Daten werde die Beklagte durch die gewählte Darstellung ebenfalls in keiner Weise gerecht.	17
Der Kläger meint, die Beklagte habe nicht ausreichend konkret auf seine vorgerichtliche Auskunftsanfrage reagiert, sondern ihm nur allgemeine Informationen zukommen lassen. Insbesondere enthalte die Auskunft keine konkreten Aussagen dazu, welche Daten des Klägers von den Scrapern erlangt worden seien.	18
Der Kläger beantragt,	19
<ul style="list-style-type: none"> • 1. die Beklagte zu verurteilen, 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 € nebst Zinsen ab Rechtshängigkeit i.H.v. 5 Prozentpunkten über dem Basiszinssatz, 	20
<ul style="list-style-type: none"> • 2. festzustellen, 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, 	22
die Beklagte weiter zu verurteilen,	23
<ul style="list-style-type: none"> • 3. es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes von bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft von bis zu sechs Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, 	25

a)	personenbezogene Daten der Klägerseite, namentlich Telefonnummer, Facebook-IF, 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,	27
	<ul style="list-style-type: none"> • 4. 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. 	28
	Die Klageschrift ist der Beklagten am 23.03.2023 zugestellt worden (Bl. 99 d.A.).	30
	Die Beklagte beantragt,	31
	die Klage abzuweisen.	32
	Die Beklagte meint, die Klage sei bereits unzulässig. Der Klageantrag zu 1) sei nicht hinreichend bestimmt, denn der Schadensersatz werde für mehrere, zeitlich auseinanderfallende angebliche Verstöße geltend gemacht. Für den Feststellungsantrag zu 2) sei weder das festzustellende Rechtsverhältnis hinreichend genau bezeichnet noch ein Feststellungsinteresse dargelegt. Der Klageantrag zu 3) a) und b) sei deshalb unzulässig, weil sie die immer öffentlichen Nutzerinformationen nicht ausnehme und die zu unterlassenden Verhaltensweisen zu ungenau beschreibe; bezüglich der Telefonnummer fehle es überdies am Rechtsschutzbedürfnis, denn hier könne der Kläger das gewünschte Ergebnis durch eine Änderung seiner Profileinstellungen selbst erreichen.	33
	Die Beklagte hält die Klage auch für unbegründet, da keine Verstöße gegen die DS-GVO vorlägen.	34
	Die Beklagte meint, das erfolgte „Scraping“ stelle keinen Datenschutzverstoß dar, da lediglich öffentlich zugängliche Profilinformatoren des Klägers abgerufen und auch keine spezifischen Sicherheitsmaßnahmen oder Zugriffsberechtigungen dafür umgangen oder überwunden worden seien (wie beim „Hacking“). Es habe insoweit weder eine Sicherheitsverletzung noch eine unbefugte Offenlegung von personenbezogenen Daten gegeben. Vielmehr sei die hergestellte Verknüpfung zwischen der Telefonnummer des Klägers und seinem Nutzerkonto auf die seinerzeit von ihm selbst gewählte Suchbarkeitseinstellung zurückzuführen. Zu den wählbaren Profileinstellungen stelle die Beklagte ihren Nutzern alle in Art. 13 DS-GVO festgelegten Informationen zur Verfügung, insbesondere informiere sie umfassend und transparent über die Möglichkeiten zur Einstellung der Suchbarkeit und Zielgruppenauswahl; die gewünschten Informationen seien durch entsprechende Überschriften leicht zu finden und einfach aufzurufen.	35

Die Beklagte behauptet, sie verwende sowohl Captchas als auch geänderte Einstellungen, die ein automatisches Verknüpfen über das Kontakt-Importer-Tool nicht mehr ermöglichen, obwohl dadurch eine legitime und nützliche Funktion für ihre Nutzer entfallen sei. Die Beklagte meint, sie sei nicht verpflichtet, darüber hinaus weitergehende Schutzvorkehrungen gegen eine Erhebung der immer öffentlich zugänglichen Informationen eines Nutzerprofils durch Dritte zu ergreifen. Soweit es dazu komme, gehe sie mit Unterlassungs- und Beseitigungsaufforderungen sowie Kontosperrungen gegen die Scraper vor.	36
Die Beklagte meint, ein kompensationsgeeigneter und messbarer Schaden sei nicht dargelegt, da selbst ein angenommener vorübergehender Kontrollverlust über personenbezogene Daten des Klägers nicht der Beklagten zuzurechnen sei, weil die öffentliche Einsehbarkeit seinen Privatsphäre-Einstellungen entsprochen habe. Mindestens fehle es an der Kausalität und an einem Verschulden der Beklagten.	37
Die Beklagte meint, eine Melde- oder Benachrichtigungspflicht habe schon mangels einer Verletzung von Vorschriften der DS-GVO nicht bestanden. Für einen Unterlassungsanspruch sei keine Anspruchsgrundlage ersichtlich; die insoweit abschließenden Regelungen der DS-GVO sähen gerade keinen Unterlassungsanspruch vor.	38
Die Beklagte behauptet, es sei unzutreffend, dass sie auf den Scraping-Vorfall nicht reagiert habe. Über die technischen Anpassungen hinaus widme sie in ihrem Hilfebereich einen eigenen Abschnitt der Information, wie der Nutzer sich vor nicht autorisiertem Scraping schützen könne.	39
Bezüglich des geltend gemachten Auskunftsanspruches meint die Beklagte, dass sie zur Erteilung weitergehender Auskünfte, insbesondere über eine etwaige Datenverarbeitung durch Dritte, weder imstande noch nach Art. 15 DS-GVO rechtlich verpflichtet sei.	40
Wegen der weiteren, von beiden Seiten noch umfangreich vorgetragenen Rechtsausführungen, die mangels Darstellung entscheidungserheblicher Tatsachen keiner Wiedergabe im Tatbestand bedurften, wird auf die zwischen den Parteien gewechselten Schriftsätze und deren sämtliche Anlagen Bezug genommen.	41
Entscheidungsgründe	42
Die Klage ist zulässig, aber unbegründet.	43
I.	44
Die Klage ist zulässig.	45
1.	46
Das Landgericht Dortmund ist sachlich sowie international und örtlich zuständig.	47
a)	48
Die sachliche Zuständigkeit des Landgerichts folgt ungeachtet des Streitwertes unter 5.000,00 € vorliegend aus § 39 S. 1 ZPO. Nach dieser Vorschrift wird die Zuständigkeit eines Gerichts des ersten Rechtszuges dadurch begründet, dass der Beklagte, ohne die Unzuständigkeit geltend zu machen, zur Hauptsache mündlich verhandelt.	49

Die Beklagte hat sich vorliegend mit dem Stellen ihrer Anträge in der mündlichen Verhandlung (§ 137 Abs. 1 ZPO) rügelos zur Hauptsache eingelassen.

b) 51

Die internationale Zuständigkeit des Landgerichts Dortmund folgt aus Art. 79 Abs. 2 DS-GVO sowie aus Art. 18 Abs. 1 Alt. 2 i.V.m. Art. 17 Abs. 1 lit. c) EuGVVO (so auch LG Kiel, GRUR-RS 2023, 328). 52

Hiernach kann der Verbraucher seinen Vertragspartner wegen Streitigkeiten aus einem Vertrag an seinem Wohnsitz verklagen, wenn der Vertragspartner in dem Mitgliedstaat, in dessen Hoheitsgebiet der Verbraucher seinen Wohnsitz hat, eine berufliche oder gewerbliche Tätigkeit ausübt oder eine solche auf irgendeinem Wege auf diesen Mitgliedstaat oder auf mehrere Staaten, einschließlich dieses Mitgliedstaats, ausrichtet und der Vertrag in den Bereich dieser Tätigkeit fällt. 53

So verhält es sich hier. 54

Durch die Nutzung der Plattform ist der Kläger mit der Beklagten vertraglich verbunden (Brandenburgisches OLG, Urteil vom 25.01.2022, 3 U 119/20, juris). Der Kläger ist dabei Verbraucher im Sinne des Art. 17 Abs. 1 lit. c) EuGVVO, weil er die Plattform der Beklagten lediglich für private Zwecke nutzt. Das Anbieten des sozialen Netzwerks stellt für die Beklagte wiederum eine berufliche Tätigkeit auf dem Gebiet der Europäischen Union dar. Auch wenn das Netzwerk als solches zur kostenfreien Nutzung zur Verfügung gestellt ist, so dient die Plattform dennoch auch einer gewerblichen Tätigkeit der Beklagten (EuGH, Urteil vom 05.06.2018, Az. C-210/16, juris). 55

c) 56

Die örtliche Zuständigkeit des Landgerichts Dortmund folgt ebenfalls aus Art. 18 Abs. 1 Alt. 2 EuGVVO. Der Kläger hat seinen Wohnsitz im hiesigen Landgerichtsbezirk. 57

2. 58

Die Klageanträge sind auch gemäß § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt. 59

Grundsätzlich ist ein Klageantrag hinreichend bestimmt, wenn er den erhobenen Anspruch durch Bezifferung oder gegenständliche Beschreibung so konkret bezeichnet, dass der Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) klar abgegrenzt ist, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennbar sind, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abgewälzt und eine etwaige Zwangsvollstreckung nicht mit einer Fortsetzung des Streits im Vollstreckungsverfahren belastet wird (Zöller/Greger, ZPO, 34. Aufl. 2022, § 253 Rdnr. 13). Diesen Anforderungen werden die beklagtenseits beanstandeten Anträge zu Ziffer 1) und Ziffer 3) gerecht. 60

Die Auslegung des Antrags zu Ziffer 1) ergibt, dass dieser dahingehend zu verstehen ist, dass dem Kläger aufgrund des kumulativen Zusammenwirkens der etwaigen Verstöße gegen die DS-GVO vor und nach dem Vorfall des Scrapings ein größerer Schaden entstanden sei. Nach dem Verständnis des Gerichts liegen diesem Antrag nicht etwa mehrere Streitgegenstände, sondern lediglich ein sich über einen längeren Zeitraum abspielender Sachverhalt zu Grunde, sodass sich der Zahlungsantrag des Klägers auf diesen länger andauernden, aber zusammenhängenden Sachverhalt stützt. Zudem ist der Klageschrift auch 61

zu entnehmen, dass die potentiellen Verstöße gegen die Datenschutzgrundverordnung nicht etwa in einem Alternativverhältnis zueinander stehen, sondern gerade in ihrer Zusammenschau betrachtet werden müssen (so auch LG Kiel, GRUR-RS 2023, 328).

Auch der Antrag zu Ziffer 3) a) und b) ist hinreichend bestimmt. Dabei sind Anträge insbesondere der Auslegung zugänglich, die unter gewissen Umständen auch hingenommen werden muss (Zöller, a.a.O., Rdnr. 13b). Eine auslegungsbedürftige Antragsformulierung ist dann hinzunehmen, wenn dies zur Gewährleistung eines effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) erforderlich ist und die Klägerseite ihren Antrag nicht konkreter fasst (LG Gießen, GRUR-RS 2022, 30480). So liegt es hier. Die streitgegenständlichen technischen Vorkehrungen unterliegen einem ständigen Wandel. So wären selbst bei Angabe der konkreten aktuellen Sicherheitsmaßnahmen diese alsbald überholt, sodass der Kläger erneut klagen müsste. 62

Der Schmerzensgeldantrag verstößt der Höhe nach nicht gegen den Bestimmtheitsgrundsatz des § 253 Abs. 2 Nr. 2 ZPO, da der Kläger sowohl in der Klagebegründung als auch im Klageantrag zu Ziffer 1) einen Mindestbetrag von 1.000,00 € angegeben hat. 63

3. 64

Der Feststellungsantrag zu Ziffer 2) ist – jedenfalls in der im Termin zur mündlichen Verhandlung vom 22.05.2023 klargestellten Beschränkung auf künftig noch entstehen werdende Schäden – gem. § 256 ZPO ebenfalls zulässig. Das ist dann der Fall, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann (OLG Hamm, Urteil vom 21.05.2019, 9 U 56/18, juris). Ausgehend vom Klägervorbringen war nicht völlig ausgeschlossen, dass er infolge der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Namen und weiteren persönlichen Daten einen irgendwie gearteten Schaden hätte erleiden können. 65

4. 66

Gem. § 260 ZPO war schließlich die Verbindung mehrerer Anträge zulässig. 67

II. 68

Die Klage ist jedoch unbegründet. 69

Dem Kläger stehen die geltend gemachten Ansprüche unter keinem rechtlichen Gesichtspunkt zu. 70

1. 71

Dem Kläger steht gegen die Beklagte kein Anspruch auf Zahlung eines immateriellen Schadensersatzes zu. 72

a) 73

Ein Anspruch des Klägers auf Zahlung eines immateriellen Schadensersatzes ergibt sich nicht aus Art. 82 Abs. 1 DS-GVO. Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die Datenschutzgrundverordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Verantwortlicher in diesem Sinne ist gemäß Art. 4 Nr. 7 DS-GVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die 74

allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden.

Zwar ergibt sich aus dem Vortrag der Beklagten, dass sich diese als Verantwortliche im Sinne dieser Norm ansieht. 75

Ein Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung liegt hingegen nicht vor, sodass auch offenbleiben kann, ob die Art. 13, 14, 15, 24, 25, 32, 34 DS-GVO in den Schutzbereich des Art. 82 DS-GVO fallen. 76

(1) 77

Ein Verstoß gegen die Transparenzpflichten aus Art. 5 Abs. 1 a), 13, 14 DS-GVO fällt der Beklagten nicht zur Last. Nach dem Grundsatz des Art. 5 Abs. 1 a) DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Das Erfordernis der Transparenz führt Art. 13 DS-GVO dann in Form von Informations- und Aufklärungspflichten fort. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. Ähnliche Vorgaben sieht auch Art. 14 DS-GVO für den Fall vor, dass der Verantwortliche die Daten nicht direkt bei der betroffenen Person erhebt. Auch Art. 12 DS-GVO sieht eine Information in präziser, transparenter und leicht zugänglicher Form vor. 78

Diesem Maßstab wurde die Beklagte gerecht. Sie hat ihren Nutzern – und damit auch dem Kläger – im streitgegenständlichen Zeitraum im Rahmen ihrer Datenrichtlinie und dem Hilfebereich in Bezug auf die Verwendung der Daten und insbesondere der Verwendung der Telefonnummer sowie die Funktion des Contact-Import-Tools klare Informationen zur Verfügung gestellt. Dabei fand die Aufklärung über die Verwendung der Daten in verständlicher Sprache statt, wie es nach Inaugenscheinnahme der streitgegenständlichen Bestimmungen der Datenrichtlinie und des Hilfebereiches zur Überzeugung des Gerichts feststeht. Zudem ist sie auch in für den Nutzer zugänglicher Art und Weise erfolgt. Dies gilt vor allem im Hinblick darauf, dass die Beklagte eine sog. Mehrebenen-Datenschutzerklärung verwendet, bei der der Nutzer auf der ersten Ebene einen Überblick über die ihm hinsichtlich der Verarbeitung seiner personenbezogenen Daten zur Verfügung stehenden Informationen erhält und auf der zweiten Ebene die detaillierten Auskünfte durch das Anklicken eines qualifizierten Abschnitts einsehen kann. Dies dient letztlich der Vermeidung einer Überforderung des Nutzers mit einer blockartigen und überfrachteten Datenschutzzinformation. Zwar trifft es zu, dass die Einstellungsmöglichkeiten über mehrere Links erreichbar sind. Die Beklagte informiert den Nutzer jedoch über sämtliche Nutzungs- und Suchbarkeitsoptionen, wie bereits aus den durch den Kläger selbst vorgelegten Screenshots hervorgeht. Der Leser kann dabei auch gleich zu Beginn der Datenschutzerklärung feststellen, dass seitens der Beklagten auf die individuelle Anpassung der Privatsphäre-Einstellungen aufmerksam gemacht wird. 79

Auch aus dem Umfang dieser Datenschutzzinformation kann nicht auf eine Unübersichtlichkeit geschlossen werden. In Anbetracht der Vorgaben der DS-GVO und der damit verbundenen vielseitigen Informationsverpflichtungen liegt es in der Natur der Sache, dass eine Datenschutzzinformation umfangreich ausfällt (LG Essen, GRUR-RS 2022, 34818). Diesem Umstand begegnet die Beklagte aber gerade mit einer Erklärung, die es dem Nutzer ermöglicht, die für ihn interessanten Bereiche anzusteuern, auch wenn das Durchlesen der verschiedenen Hinweise einen gewissen zeitlichen Aufwand erfordert. Soweit der Kläger darüber hinaus den Umfang der Aufklärung der Datenschutzerklärung in Bezug auf die 80

Telefonnummer für unzureichend hält, so setzt er sich mit der Vorlage von Screenshots von den einschlägigen Seiten der Beklagten, die genau diese Hinweise erteilen, selbst in Widerspruch. Diese Screenshots bilden die tatsächlichen Inhalte der Information ab. Die Inhalte auf dieser Website sind offenkundige Tatsachen gemäß § 291 ZPO, die jedem Nutzer zugänglich sind, und enthalten sämtliche Informationen zum Umfang der Verarbeitung und Hinweise zu den Möglichkeiten der Konfiguration der Privatsphäre des Accounts.

Entgegen der Auffassung des Klägers war die Beklagte auch nicht dazu verpflichtet, über die Verarbeitungstätigkeit unbefugter Dritter zu informieren. Denn der Kläger ist seitens der Beklagten über den Umstand der Öffentlichkeit seiner Daten informiert worden. So durfte und musste die Beklagte aufgrund ihrer erteilten Information davon ausgehen, dass dem Kläger bekannt gewesen ist, dass sein Name, sein Geschlecht und sein Benutzername für jedermann abrufbar sind. Das ist auch gerade Sinn und Zweck der Einrichtung eines Profils in einem sozialen Netzwerk, das – für den Nutzer – der Selbstdarstellung in diesem gewählten Rahmen und der Kontaktaufnahme und dem Austausch mit anderen dienen soll. Damit liegt der Fall bereits grundsätzlich anders als in Konstellationen, in denen es z.B. um Daten geht, die notwendigerweise und mit einem ganz anderen Hauptzweck z.B. bei einer Krankenkasse mitgeteilt werden müssen und auch aus Sicht des Kunden/Nutzers definitiv vertraulich sein sollen. In diesem Zusammenhang musste sich der Kläger auch über den Umstand bewusst gewesen sein, dass der – bewusst und gezielt gewährte – offene Zugang zu bestimmten Daten eine potentielle Missbrauchsmöglichkeit durch Dritte eröffnen kann. Hierbei handelt es sich nämlich um ein allgemeines Lebensrisiko, das jedem Internetnutzer in der heutigen Zeit bewusst sein muss. Eine Verpflichtung zur Information über ein derartiges – wenn auch im Zusammenhang mit der Nutzung des sozialen Netzwerks stehendes – allgemeines Lebensrisiko trifft die Beklagte jedoch nicht. Hieran ändert es auch nichts, dass der Kläger unterstellt, Unternehmenszweck der Beklagten sei überhaupt nicht das Anbieten einer gemeinschaftsbildenden Plattform, sondern ihr eigenes kommerzielles Interesse, denn gerade durch letzteres finanziert die Beklagte überhaupt erst das kostenlose Angebot, das sie den Nutzern zur Verfügung stellt.

Eine Intransparenz resultiert schließlich auch nicht etwa aus dem Umstand, dass die Verwendung der Telefonnummer nur möglicherweise erfolgt. Im Hinblick auf die potentiellen Verwendungszwecke, über die die Beklagte informiert, erschließt sich dem Leser unmittelbar, dass nicht alle Verwendungszwecke für alle Nutzer gelten können. So etwa, wenn ein Nutzer die Zwei-Faktor-Authentifizierung zur Sicherheit seines Kontos nicht nutzt (s. auch insg. LG Gießen, GRUR-RS 2022, 30480; LG Bielefeld, GRUR-RS 2022, 38375; LG Kiel, GRUR-RS 2023, 328).

(2) 83

Es liegt auch kein Verstoß gegen Art. 24 Abs. 1, 32 Abs. 1 DS-GVO durch die Beklagte vor. 84

Nach diesen Vorschriften hat der Verantwortliche bei der Verarbeitung personenbezogener Daten geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Anknüpfend an den Gedanken der Schaffung eines Schutzniveaus kann sich eine derartige Verpflichtung in Anbetracht des Wortlautes des Art. 32 Abs. 1 b) DS-GVO allerdings nur auf solche Datensätze beziehen, die nicht gerade einem Schutz der Vertraulichkeit entzogen werden sollen. Bei den Daten, die im Wege des Scrapings durch Dritte erlangt worden sind, handelt es sich aber gerade um Datensätze, für die der Kläger von vornherein keine Vertraulichkeit vorgesehen hat. Denn diese Daten des Klägers, nämlich sein Name, sein Geschlecht und sein Benutzername, sind Daten, die für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen

wie Logins oder ähnlichen Sicherheitsvorkehrungen abrufbar sind (AG Strausberg, Urteil vom 13.10.2022, 25 C 95/21, ZD 2023, 109). Dass andere als die vorgenannten Daten – insbesondere die Telefonnummer des Klägers – seitens Dritter erlangt worden sind, kann das Gericht nicht feststellen. Insoweit tritt der Kläger keinen konkreten Beweis an. Vielmehr beschränkt er sich auf teilweise divergierende Aufzählungen, ohne dabei genau zu benennen, welche Daten konkret bei ihm abgegriffen worden sein sollen. Insoweit steht nach dem Dafürhalten des Gerichts fest, dass Dritte bereits über diese Daten verfügt haben. Dass eine Verknüpfung der Telefonnummer mit dem Account des Klägers stattfinden konnte, beruht demnach dann aber nicht auf einem Mangel an technischen Vorkehrungen der Beklagten, sondern ist auf den Umstand der eingestellten Suchbarkeit des Profils des Klägers zurückzuführen, die er jederzeit hätte ändern können. Wenn der Nutzer es aber selbst in der Hand hat, über die einschlägigen Einstellungen selbst festzulegen, für wen er bei einer Suche auffindbar ist, so kann von der Beklagten darüber hinaus – ungeachtet der Klärung der Frage, ob sie derartige Maßnahmen vorgehalten hat – nicht erwartet werden, dass diese noch weitere technische Maßnahmen implementiert. Gegenteiliges stünde auch im konträrem Verhältnis zu der Tatsache, dass sich der Nutzer freiwillig bei einem sozialen Netzwerk registriert, das dazu dient, ihren Nutzern eine Kontaktaufnahme untereinander zu ermöglichen, aber dann Sicherheitsmaßnahmen fordert, die diesen Zweck vereiteln, obwohl der Nutzer bei dem Registrierungsvorgang der Datenrichtlinie zustimmt, die ihn über die Verwendung seiner Daten aufklärt. Darüber hinaus gewährleistet die Beklagte einen Schutz sensiblerer Daten – wie etwa der Telefonnummer –, indem sie deren Verwendung beziehungsweise die Auffindbarkeit des Nutzers über diese für ihn nur optional zur Verfügung stellt. Überdies wird er auf die Möglichkeit der Ein- oder Umstellung dieser und anderer Auffindbarkeitsfunktionen gerade – wie bereits dargestellt – über Hinweise und Hilfestellungen auf die jeweiligen Schutzmöglichkeiten aufmerksam gemacht (s. auch insg. LG Gießen, GRUR-RS 2022, 30480; LG Bielefeld, GRUR-RS 2022, 38375; LG Kiel, GRUR-RS 2023, 328).

- (3) 86
- Die Beklagte hat ferner nicht gegen Art. 25 Abs. 1 und Abs. 2 DS-GVO verstoßen. 87
- Der Umstand, dass die irische Datenschutzbehörde im Rahmen der ihr übertragenen Aufgaben hierauf erkannt und gegen die Beklagte ein Bußgeld verhängt haben soll, ist für das vorliegende Verfahren nicht bindend, zumal es dort ganz allgemein um die ungefragte Nutzung personenbezogener Daten für die Personalisierung der Werbung und nicht um den hier streitgegenständlichen Scraping-Vorfall ging, auf den allein der Kläger aber seine Klageansprüche stützt. 88
- Nach Art. 25 Abs. 2 DS-GVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden. Sinn und Zweck der Vorschrift ist es, einem Zielkonflikt zu begegnen, der darin besteht, dass der Betroffene einen Dienst der Informationsgesellschaft nutzen möchte und im Rahmen der erstmaligen Eingabe möglichst viele Daten angeben muss, auf die sich die Voreinstellungen beziehen, obwohl diese Daten für die Nutzung nicht erforderlich sind. Vor diesem Hintergrund soll der Betroffene davor geschützt werden, dass er unbeabsichtigt seine Daten einer unbestimmten Anzahl von Personen zugänglich macht (vgl. LG Kiel, a.a.O., m.w.N.). Die initiale Einstellung der Suchbeziehungsweise Auffindbarkeit für alle Nutzer dient aber gerade dem Sozialaspekt und damit dem Verarbeitungszweck der Plattform. Auch wenn die Beklagte mit ihrer Plattform 89

Marketingzwecke verfolgen mag, so ist für den Nutzer aber in der Regel nicht etwa der kommerzielle Aspekt, wie es der Kläger in seiner Replik ausführt, sondern gerade die soziale Komponente des Netzwerks von Bedeutung. Diese besteht darin, den jeweiligen Nutzern die Möglichkeit zu eröffnen, mit anderen in Kontakt zu treten oder zu bleiben, sich an öffentlichen Diskussionen zu beteiligen oder Inhalte aller Art mit der Öffentlichkeit zu teilen. Wünscht es sich der Nutzer nicht, Mitglied des soeben dargestellten Publikums zu sein, steht es ihm offen, sich mit Vornahme der entsprechenden Einstellungen „in ein privateres Profil zurückzuziehen“. Sowohl der kommunikative Zweck des Netzwerks als auch die Möglichkeit der Anpassung der Privatsphäre-Einstellungen war dem Kläger bekannt. Überdies war es ihm ohne Weiteres möglich, bei entsprechendem Interesse den Hilfebereich aufzusuchen, wo er über den Reiter „Privatsphäre-Check“ so-dann unmittelbar zu den einschlägigen Einstellungen gelangen konnte.

Soweit der Kläger hierzu behauptet, dass der kommunikative Zweck ebenso erreicht werden könne, wenn die entsprechenden Voreinstellungen für die Telefonnummern der Nutzer von Anfang an auf „nicht-öffentlich“ beziehungsweise „nicht sichtbar“ gestellt seien, weil die Nutzer der Plattform sich lediglich über ihre Namen und nicht über ihre Telefonnummer suchen, trifft dies nicht zu. Auch wenn es in der Tat unwahrscheinlich erscheint, dass sich Freunde oder Familienmitglieder über ihre Nummern suchen, so ist dies in Bezug auf Externe nicht unbedingt der Fall. Gerade in Anbetracht der Vielzahl an aktiven Nutzern der Plattform können sich die Namen wiederholen, sodass ein einfaches Auffinden des angesteuerten Kontakts nicht immer möglich ist. Vor diesem Hintergrund kann aber gerade die Auffindbarkeit durch die Telefonnummer oder E-Mail-Adresse Abhilfe schaffen, um so eine schnellere und bequemere Kontaktaufnahme zu ermöglichen (so die überzeugende Argumentation des LG Kiel, a.a.O.).

Zwar sehen die Voreinstellungen der Zielgruppenauswahl sowie der Suchbarkeit bei erstmaliger Nutzung der Plattform eine Zugänglichkeit in Form der Ansteuerung und der Einsichtnahme in das Profil des Betroffenen durch einen unbestimmt weit gefassten Personenkreis vor. Dem Betroffenen ist es jedoch gleich nach der Anmeldung möglich, eine Änderung dieser Konfiguration vorzunehmen, um so sein Vertraulichkeitsinteresse in Bezug auf seine Daten zu wahren. Durch diese Möglichkeit, auf die der Nutzer nach seiner Anmeldung durch die Beklagte hingewiesen wird, wird so letztlich dem Zweck der unkontrollierten Weitergabe der Daten des Betroffenen entsprochen.

(4) 92

Eine Verletzung der Pflicht gemäß Art. 33 DS-GVO, der zuständigen Aufsichtsbehörde den Datenschutzverstoß zu melden, liegt seitens der Beklagten ebenfalls nicht vor. Gemäß Art. 33 DS-GVO hat der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Eine Verletzung des Schutzes personenbezogener Daten liegt aber – wie dargestellt – nicht vor, so dass die Beklagte auch nicht in der Pflicht gestanden hat, diese der zuständigen Behörde, der „Irish Data Commission“, zu melden.

(5) 94

Schließlich hat die Beklagte auch nicht gegen ihre Verpflichtung aus Art. 15 Abs. 1 a) und c) DS-GVO verstoßen. 95

Hiernach hat der Betroffene das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob ihn betreffende personenbezogene Daten verarbeitet worden sind; ist dies der Fall, so hat der Betroffene ein Recht auf Auskunft über diese personenbezogenen Daten, über die Verarbeitungszwecke und über die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen. Das klägerische Auskunftersuchen hat die Beklagte unter Angabe der Nutzer ID, des Vor- und Nachnamens, des Landes sowie des Geschlechts des Klägers beantwortet. Lediglich in diesem Rahmen bestand der Auskunftsanspruch des Klägers. Denn eine weitere Auskunft – insbesondere, wie vom Auskunftsbegehren des Klägers gefordert, welchen Empfängern die Daten des Klägers durch das Scraping bekannt geworden sind – war der Beklagten weder möglich noch war sie hierzu verpflichtet. Im Hinblick darauf, dass aufgrund des nahezu unendlichen Spektrums der möglichen Empfänger sowie des Umstandes, dass das Scraping als plattform-externer Vorgang stattgefunden hat, ist es für die Beklagte unmöglich, den Informationsfluss zurückzuverfolgen, zumal der Kläger nicht dargelegt hat, in welcher Form eine derartige Information erfolgen könnte. Nichts anderes ergibt sich hinsichtlich des Zeitraumes, in welchem die Daten gescraped worden sind. Die bloße Angabe des Zeitraumes durch den Kläger von dem Jahr 2019 bis zur Veröffentlichung im April 2021 vermag die zeitliche Angabe nicht zu präzisieren (s. auch insg. LG Gießen, GRUR-RS 2022, 30480; LG Bielefeld, GRUR-RS 2022, 38375; LG Kiel, GRUR-RS 2023, 328).

b) 97

Im Übrigen mangelt es an einem ersatzfähigen Schaden des Klägers i.S.d. Art. 82 Abs. 1 DS-GVO. Der Eintritt des Schadens muss dabei im Sinne des § 287 ZPO als überwiegend wahrscheinlich dargetan werden (Musielak/Voit/Foerste, ZPO, 19. Aufl. 2022, § 287 Rdnr. 7).

Dabei kann dahinstehen, wie der Schadensbegriff des Art. 82 Abs. 1 DS-GVO konkret zu verstehen ist (vgl. BAG NZA 2021, 1713; ÖOGH, ZD 2021, 631; AG München, GRUR 2022, 1772). Denn es ist es dem Kläger bereits nicht gelungen, jedweden Ansatzpunkt für einen ersatzfähigen Schaden hinreichend konkret darzulegen. 99

Gerichtsbekannt aus der Vielzahl nahezu identischer Verfahren wird in sämtlichen Klageschriften dieselbe Floskel vom erlittenen Kontrollverlust „der Klägerseite“ über die Daten und dem Zustand des Unwohlseins und der Sorge über möglichen Missbrauch ihrer Daten, in dem sie seitdem verblieben sei, wiederholt. Es ist deshalb schon nicht davon auszugehen, dass diese Formulierung überhaupt auf persönlichen Angaben des hiesigen Klägers beruht, mithin auch nicht seine konkret-individuelle Situation beschreibt. Es ist außerdem völlig lebensfremd, dass sämtliche vom „Scraping-Vorfall“ betroffenen Facebook-Nutzer unterschiedslos dieselbe emotionale Reaktion gezeigt und dieselbe Besorgnis entwickelt haben sollten. 100

Angesichts des nicht ansatzweise substantiierten Vorbringens hätte auch keine Veranlassung bestanden, den Kläger gerichtlicherseits ergänzend persönlich anzuhören, um seine Befindlichkeiten näher zu beleuchten. Nicht nur wäre eine solche – wohl erstmalige – konkrete Sachverhaltsaufklärung ohne substantiierten Klagevortrag hierzu auf eine verbotene Ausforschung hinausgelaufen und einseitig von dem prozessualen Grundsatz abgewichen, dass zunächst jede Streitpartei im Zivilprozess die ihr günstigen Tatsachen eigenverantwortlich zusammenstellen und vortragen muss. 101

Gegen das tatsächliche Vorliegen der floskelhaft behaupteten Ängste, Sorgen und Unwohlseinsempfindungen der Kläger spricht ohnehin entscheidend, dass es sich bei den gescrapten Daten um solche handelt, die immer öffentlich sichtbar sind. Es ist diesen Daten gerade immanent, dass sie jedem jederzeit zugänglich sind. Hierauf wird der Nutzer auch durch die Beklagte hingewiesen, sodass nicht nachvollziehbar ist, weshalb eine „weitere Veröffentlichung“ dieser Daten bei den Klägern zu einem unguuten Gefühl geführt haben sollte. In diesem Sinne kann schon nicht von einer Veröffentlichung der Daten durch Dritte gesprochen werden, die die Nutzer selbst öffentlich zugänglich gemacht haben. Allenfalls entspricht die Zuordnung der öffentlich einsehbaren Daten mit der Telefonnummer und das anschließende Publizieren eines derartig erstellten „Profils“ durch Dritte einem derartigen Verständnis. Die Ermöglichung eines derartigen Umstandes beruht aber wiederum gerade nicht auf einem Vorgehen, das der Beklagten zuzurechnen ist, sondern vielmehr auf den Suchbarkeitseinstellungen der Nutzer selbst, die sie jederzeit hätten ändern können. Weiterhin ist die Eingabe der Telefonnummer freiwillig und wäre für die Registrierung nicht erforderlich gewesen. Trotzdem hat auch der hiesige Kläger seine Telefonnummer eingegeben. Wäre ihm an der größtmöglichen Geheimhaltung seiner Telefonnummer gelegen gewesen, so hätte er sich darauf beschränken können, nur die notwendigen Informationen, also die für die Registrierung erforderliche E-Mail, preiszugeben.

2. 103
- Für einen immateriellen Schadensersatzanspruch ist auch keine andere Anspruchsgrundlage dargetan oder ersichtlich. 104
- a) 105
- Ein solcher Schadensersatz folgt nicht aus den §§ 280 Abs. 1, 3, 281, 327, 327e, 327i BGB. Sowohl das Scrapen von Daten im Jahre 2019 als auch deren Veröffentlichung durch Dritte April 2021 lagen vor dem Inkrafttreten der §§ 327 ff. BGB am 01.01.2022 (vgl. Art. 229 § 57 Abs. 2 EGBGB). 106
- b) 107
- Ein immaterieller Schadensersatzanspruch ergibt sich ferner nicht aus § 823 Abs. 2 BGB i.V.m. dem Recht auf informationelle Selbstbestimmung, da dem Kläger kein ersatzfähiger Schaden entstanden ist. Deshalb besteht auch kein entsprechender Anspruch gemäß §§ 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 13, 14 DS-GVO. 108
- c) 109
- Aus denselben Gründen scheidet ein immaterieller Schadensersatzanspruch des Klägers aus §§ 823 Abs. 1, 253 Abs. 2 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG. Vor diesem Hintergrund kann die Anwendbarkeit des nationalen Rechts neben der DS-GVO dahingestellt bleiben. 110
3. 111
- Dem Kläger steht gegen die Beklagte auch kein Anspruch aus §§ 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 6 Abs. 1, 17 DS-GVO und Art. 13, 14 DS-GVO auf Unterlassung zu, seine personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen. Ungeachtet der Einordnung des Art. 6 Abs. 1 DS-GVO als Schutzgesetz fehlt es schon an 112

einem Verstoß der Beklagten, der zu einem Unterlassungsanspruch führt. Insbesondere hat die Beklagte den Kläger über die Zwecke und den Umfang der Verarbeitung seiner Daten ausreichend, insbesondere gemäß Art. 13 Abs. 1 DS-GVO in verständlicher Weise, aufgeklärt (s.o.).

Ein Auskunftsanspruch des Klägers nach Art. 15 Abs. 1 DS-GVO besteht ebenfalls nicht. Soweit dem Kläger hier ein Auskunftsanspruch zustand, ist dieser durch die Erteilung der Information seitens der Beklagten untergegangen (§ 362 Abs. 1 BGB). Denn der Umfang der Auskunft hat dabei lediglich die eigene Datenverarbeitung betroffen. Vor diesem Hintergrund kann eine Auskunftspflicht im Hinblick darauf, inwieweit die durch das Scraping erlangten öffentlich einsehbaren Daten von Dritten etwaig verarbeitet wurden, für die Beklagte hingegen nicht bestehen.	113
4.	114
Der Feststellungsantrag ist aus denselben Erwägungen unbegründet.	115
5.	116
Weiterhin hat der Kläger keinen Anspruch auf Erstattung vorgerichtlicher Rechtsanwaltskosten aus § 280 Abs. 1 BGB oder aus Art. 82 Abs. 1 DS-GVO, da es in der Hauptsache bereits an einem Anspruch mangelt.	117
Aus demselben Grund scheidet auch ein Zinsanspruch des Klägers aus § 291 BGB.	118
III.	119
Die prozessualen Nebenentscheidungen beruhen auf den §§ 91 Abs. 1 ZPO, 708 Nr. 11, 711 ZPO.	120