Beglaubigte Abschrift

Aktenzeichen:
**2 O 116/22**

# Landgericht Trier

## IM NAMEN DES VOLKES

# Urteil

In dem Rechtsstreit

[redacted]

**- Kläger -**

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

gegen

Meta Platforms Ireland LimitedFacebook Ireland Ltd., vertreten durch den Director Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland

**- Beklagte -**

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

wegen Persönlichkeitsrechtsverletzung

hat die 2. Zivilkammer des Landgerichts Trier durch den Vorsitzenden Richter am Landgericht [redacted], den Richter am Landgericht [redacted] und den Richter [redacted] auf Grund der mündlichen Verhandlung vom 03.02.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 500,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 14.06.2022 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle weiteren materiellen

Schäden zu ersetzen, die diesem 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, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 90,96 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 14.06.2022 zu zahlen.

   Im Übrigen wird die Klage abgewiesen.

4. Von den Kosten des Rechtsstreits hat der Kläger 64 % und die Beklagte 36 % zu tragen.

5. Das Urteil ist vorläufig vollstreckbar. Beide Parteien können die Vollstreckung des jeweils anderen durch Sicherheitsleistung in Höhe von 110 % des gegen sie insgesamt vollstreckbaren Betrages abwenden, wenn nicht der jeweils andere vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

6. Der Streitwert wird auf 5.500 € festgesetzt.

# Tatbestand

Die Parteien streiten darum, ob die Beklagte bei dem Betrieb eines sozialen Netzwerks gegen Datenschutzbestimmungen verstoßen hat.

Der Kläger nutzt das von der Beklagten betriebene soziale Netzwerk facebook.com, um mit Freunden zu kommunizieren, private Fotos zu teilen und mit anderen Nutzern im Internet zu diskutieren. Die Dienste der Beklagten ermöglichen es ihren Nutzern, persönliche Profile für sich zu erstellen und mit Freunden zu teilen.

Damit Nutzer leichter mit anderen Nutzern in Kontakt treten können, müssen sie bestimmte Informationen bei der Registrierung angeben, die als Teil des Nutzerprofils für jeden jederzeit öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und die sog. Nutzer-ID. Hinsichtlich der weiteren Angaben, die der Nutzer auf sein Profil eintragen kann, gibt es im Rahmen der Privatsphäre-Einstellungen verschiedene Wahlmöglichkeiten, das heißt jeder Nutzer kann selbst darüber entscheiden, welche anderen Nutzer auf seine Daten zugreifen können. Jedenfalls bis September 2019 wies das soziale Netzwerk hierzu folgende Funktionen auf: Die Nutzer konnten zwischen der sog. Zielgruppenauswahl und der sog. Suchbarkeitseinstellung zu differenzieren. Bei

der Zielgruppenauswahl legte der Nutzer fest, wer einzelne Informationen auf seinem Facebook-Profil, wie etwa Telefonnummer, Wohnort, Stadt, den sog. Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen konnte. So konnte der Nutzer anstelle der standardmäßigen Voreinstellung „öffentlich“ auswählen, dass nur „Freunde“ auf der Facebook-Plattform, oder „Freunde von Freunden“ die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wurde insoweit gesondert behandelt, dass diese nach der Grundeinstellung nicht öffentlich einsehbar war.

Mit der Suchbarkeitseinstellung konnte der Nutzer festlegen, wer sein Profil anhand seiner freiwillig angegebenen Telefonnummer finden konnte, und dies unabhängig davon, ob die Mobilfunknummer auf dem Profil öffentlich einsehbar war oder nicht. Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange die Suchbarkeitseinstellung für Telefonnummern auf der Standard-Voreinstellung „Alle“ eingestellt war. Daneben waren die Einstellungen nur „Freunde von Freunden“ oder „Freunde“ auswählbar. Ab Mai 2019 stand Nutzern auch die Option „Nur ich“ zur Verfügung. Der Kläger hatte seine Mobilfunknummer eingetragen. Seine Suchbarkeiteinstellung war ab dem 9.12.2013 auf „alle“ eingestellt (Anlage B 17).

Die Suche nach Personen war mit der Facebook-Suchfunktion und über das sog. Contact-Importer-Tool (im folgenden CIT) möglich. Letzteres funktionierte so, dass ein Nutzer eine Telefonnummer als Kontakt in seinem Smartphone abspeicherte und die Beklagte dem Nutzer über das CIT erlaubte, seine abgespeicherten Kontakte mit den bei Facebook hinterlegten – auch nicht öffentlich einsehbaren – Telefonnummern abzugleichen, um die mit der Telefonnummer bei Facebook registrierte Person angezeigt zu bekommen und diese als Freund hinzufügen zu können.

Mit der Registrierung im sozialen Netzwerk stimmte der Kläger den Nutzungsbedingungen zu, in denen unter anderem auf die sog. Datenrichtlinie Bezug genommen wurde. Die Datenrichtlinie beinhaltete Informationen dazu, welche der vom Nutzer gemachten Angaben immer öffentlich sichtbar waren und so von jedermann – also auch von Personen außerhalb der Plattform – eingesehen werden konnten. Bezüglich weiterer Ausführungen in der Datenrichtlinie wird auf Anlage B 9 verwiesen. Den Nutzern wurden zudem im sog. Hilfebereich Erläuterungen zur Öffentlichkeit seiner jeweiligen Informationen zur Verfügung gestellt. Hier wurde den Nutzern auch der Unterschied zwischen der Zielgruppenauswahl und den Suchbarkeitseinstellungen erläutert und mitgeteilt, wie sie ihre Einstellungen ändern konnten.

In einem Zeitraum, der mehrmonatig war und sich jedenfalls bis September 2019 erstreckte, lasen unbefugte Dritte Telefonnummern, Facebook-IDs, Namen, Vornamen, Geschlecht und weite-

re Daten bei der Beklagten aus (im folgenden: Der Scraping-Vorfall). Dieses sog. Scraping ist eine weitverbreitete Methode, um Daten, die typischerweise öffentlich einsehbar sind, von Internetseiten durch automatisierte Computer-Programme abzurufen. Ein solches methodisches und automatisiertes Sammeln von Daten war nach den Nutzungsbedingungen der Beklagten untersagt.

Die Parteien gehen übereinstimmend davon aus, dass mithilfe des CIT durch eine Vielzahl von automatisch generierten Telefonnummern Verknüpfungen mit Facebook-Profilen hergestellt wurden. Sodann wurden die öffentlich einsehbaren Informationen aus den betreffenden Nutzerprofilen kopiert und die Telefonnummer dem Datensatz hinzugefügt. Anfang April 2021 verbreiteten Dritte im sog. Darknet öffentlich diese Datensätze von ca. 533 Millionen Nutzern des sozialen Netzwerks. Davon betroffen ist auch der Kläger. Von ihm wurden konkret veröffentlicht: „[redacted],,"

Mit außergerichtlichem Schreiben forderte er die Beklagte vergeblich zur Zahlung von 500,- € und Unterlassung künftiger Zugänglichmachung der Daten sowie Erteilung einer Auskunft auf, welche konkreten Daten im Einzelnen „abgegriffen“ worden seien (vgl. Anlage K 1). Wegen der Antwort der Beklagten wird auf die vorgerichtlichen Schreiben in Anlage K 2 und Anlage B 16 Bezug genommen.

Die irische Datenschutzbehörde DPC verhängte am 25. November 2022 gegen die Beklagte im Hinblick auf den streitgegenständlichen Scraping-Vorfall wegen Verstößen gegen die Datenschutzgrundverordnung (im folgenden: DSGVO) eine Geldbuße in Höhe von 265 Mio. €. Die Behörde sah die von der Beklagten implementierten technischen Schutzmaßnahmen zur sog. Ratenbegrenzung und sog. Bot-Erkennung nicht als ausreichend an. Wegen der Einzelheiten wird auf Anlage K3 verwiesen.

Der Kläger ist der Ansicht, die Beklagte habe gegen die Artt. 5, 13, 14 DSGVO, Artt. 24, 25 DSGVO, Art. 32, 34, 35 DSGVO und Art. 15 DSGVO verstoßen, sodass ihr ein Schadensersatzanspruch aus Art. 82 DSGVO zustehe.

Er behauptet, bei dem Scraping-Vorfall seien Daten wie Telefonnummer, Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere „korrelierende“ Daten veröffentlicht worden. Da auch er betroffen sei, habe er einen erheblichen Kontrollverlust über seine Daten erlitten. Er leide unter großem Unwohlsein und Sorgen, da er einen Missbrauch seiner Daten befürchte. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen, aber auch in der ständigen Sorge, dass die veröffentlichen Daten von Kriminellen für unlautere Zwecke verwendet wer-

den könnten. Hierzu behauptet der Kläger zudem, die betreffenden personenbezogenen Daten seien im Internet auf Seiten veröffentlicht worden, die illegale Aktivitäten begünstigen sollen, zum Beispiel auf der Seite raidforums.com, einem „Hacker-Forum“. Zum jetzigen Zeitpunkt könne noch nicht abgesehen werden, welche Dritten Zugriff auf seine Daten erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden.

Der Kläger ist der Auffassung, dass es sich bei seiner Telefonnummer um nicht öffentliche Daten handele. Der Datenabgriff durch Dritte sei aufgrund einer Sicherheitslücke möglich gewesen. Die Beklagte habe keine ausreichenden Sicherheitsmaßnahmen vorgehalten, um einen Missbrauch des CIT zu verhindern. So habe die Beklagte keine Sicherheitscaptchas (Abkürzung für automatisierte Programme, um Computer von Menschen zu unterscheiden) verwendet, um sicherzustellen, dass es sich bei den massenhaft eingespeisten Telefonnummern um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handele. Auch habe die Beklagte keinen Mechanismus verwendet, um ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal zu blockieren oder Adressbücher mit auffälligen Telefonnummernabfolgen automatisch abzulehnen. Eine Kombination mehrerer solcher Sicherheitsmaßnahmen sei erforderlich, angemessen und üblich gewesen. Die Einführung einer Begrenzung der abgleichbaren Rufnummern oder einer Nutzung des CIT nur für „Freunde von Freunden“ sei möglich gewesen. Mindestens aber habe ein expliziter Hinweis auf die Standard-Einstellungen für die uneingeschränkte Suchbarkeit per Telefonnummer gefehlt, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers sei auch eine Information über etwaige Risiken im Hinblick auf Missbrauchsmöglichkeiten durch Dritte oder über die Verwendung der Telefonnummer im Allgemeinen nicht erfolgt. Wären derartigen Sicherheitsmaßnahmen ergriffen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht zu dem Scraping-Vorfall gekommen.

Darüber hinaus meint der Kläger, die Beklagte habe durch die vielschichtigen Einstellungsmöglichkeiten ein oberflächliches Gefühl der Sicherheit hinsichtlich der Datensicherheit und konkret der Telefonnummer der Nutzer erzeugt. Die intransparenten Sicherheitskonfigurationen der Telefonnummer ließen einen tiefgreifenden Überblick über deren tatsächlichen Sicherheitsstatus nicht zu. Er - der Kläger - sei um die Geheimhaltung der Telefonnummer bemüht gewesen, jedoch sei die Option in der Suchbarkeitseinstellung zur Identifizierung über die Telefonnummer versteckt gewesen.

Schließlich meint der Kläger, dass die seitens der Beklagten erteilte Auskunft auf sein außergerichtliches Schreiben unzureichend gewesen sei. Das Antwortschreiben habe lediglich allgemein gehaltene Informationen zu den im Netzwerk verarbeiteten Daten enthalten. Diese pauschale In-

formation habe zu einer Intensivierung des Schadens geführt, weil sie die Ungewissheit und Sorge um einen unbemerkten Missbrauch der Daten durch Dritte noch gesteigert habe. Bei angemessener Benachrichtigung hätte er zeitnah Schritte zur Risikominimierung und Absicherung der Daten eingeleitet.

Der Kläger 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 354,62 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, der Vortrag des Klägers hinsichtlich der ausgelesenen und veröffentlichten Daten sei mangels hinreichender Substantiierung bereits unzulässig, da unklar bleibe, welche konkreten Daten von ihm überhaupt betroffen seien. Auch sei der Unterlassungsantrag nicht hinreichend bestimmt und ein Feststellungsinteresse nicht dargelegt.

Im Übrigen ist die Beklagte der Auffassung, dass die von dem Kläger geltend gemachten, vermeintlichen Verstöße nicht vom Anwendungsbereich des Schadensersatzanspruches nach Art. 82 DSGVO erfasst seien. Vor allem liege auch gar kein Datenschutzverstoß vor. Eine Beeinträchtigung der Informationssicherheit habe nicht stattgefunden, da die ausgelesenen Daten des Klägers öffentlich einsehbar gewesen seien. Der Beklagten sei keine Sicherheitslücke anzulasten, die zu schließen gewesen wäre, da die Verknüpfung zwischen der Telefonnummer des Klägers und seinem Nutzerprofil auf seine Suchbarkeitseinstellung zurückzuführen gewesen sei. Lediglich öffentlich einsehbare Daten seien durch Dritte in Form des Scraping abgerufen worden. Die Telefonnummer des Klägers sei nicht „gescraped“ worden.

Es sei Hauptzweck ihres sozialen Netzwerks andere Nutzer zu finden und mit diesen in Kontakt zu treten, woran sich auch die Standard-Voreinstellungen orientierten. Die unbekannten „Scraper“ hätten mit dem CIT lediglich eine diesem Zweck dienende Funktion ausgenutzt. Es sei grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung ihrer Funktionen zu unterlaufen. Da die Funktionen, die Scraper ausnutzen würden, rechtmäßige, gewöhnliche Nutzerfunktionen darstellten, würden zur Begrenzung von Scraping regelmäßig nicht die gesamten zugrunde liegenden Funktionen beseitigt. Vielmehr würden in der Regel lediglich die Methoden beschränkt, mit denen auf diese Funktionen zugegriffen werden könne. Deshalb habe sie - die Beklagte - zur Bekämpfung von „Scraping“ Übertra-

gungsbegrenzungen und -beschränkungen sowie eine Bot-Erkennung eingerichtet. Diese habe sie auch fortlaufend weiterentwickelt und außerdem ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren beschäftigt. Nach dem streitgegenständlichen Vorfall habe sie als weitere Schutzmaßnahme im CIT eine Funktion errichtet, die darauf abziele, einen übereinstimmenden Kontakt nur dann anzuzeigen, wenn die beiden Nutzer einander zu kennen scheinen (sog. „Social Connection Check“).

Die Beklagte meint weiter, dass ein kompensationsgeeigneter und messbarer Schaden nicht durch den Kläger dargelegt sei. Selbst bei einem unterstellten vorübergehenden Kontrollverlust über personenbezogene Daten des Klägers wäre dies nicht der Beklagten zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe.

Im Übrigen habe sie umfassend und transparent über die Möglichkeit der Anpassung der Suchbarkeitseinstellungen und Zielgruppenauswahl informiert. Die entsprechenden Einstellungen habe der Kläger jederzeit anpassen können.

Zu dem geltend gemachten Auskunftsanspruch meint die Beklagte, dass sie über die Verarbeitungstätigkeit durch Dritte weder Erkenntnisse habe, über die sie Auskunft erteilen könne, noch dass sie nach Art. 15 DSGVO hierzu rechtlich verpflichtet sei.

Wegen der weiteren Einzelheiten des Parteivorbringens wird auf die gewechselten Schriftsätze nebst Anlagen und auf das Protokoll der mündlichen Verhandlung vom 03.02.2023 Bezug genommen.

# Entscheidungsgründe

Die Klage ist teilweise zulässig (dazu unter A.) und im tenorierten Umfang begründet (dazu unter B.).

A. Die Klage ist, mit Ausnahme des Klageantrags zu 3), zulässig.

I. Das Landgericht Trier ist international, örtlich und sachlich zuständig. Hierbei folgt die internationale Zuständigkeit deutscher Gerichte sowie die örtliche Zuständigkeit des Landgerichts Trier aus Art. 6 Abs. 1, Art. 18 Abs. 1 EuGVVO sowie Art. 79 Abs. 2 DSGVO, da der Kläger seinen Wohnsitz und gewöhnlichen Aufenthaltsort im Landgerichtsbezirk Trier und damit in der Bundesrepublik Deutschland hat. Die sachliche Zuständigkeit ergibt sich aus §§ 23, 71 GVG, nachdem der Streit-

wert mehr als 5.000 € beträgt (vgl. unten VI.).

II. Im Übrigen begegnen die Klageanträge 1, 2, und 4 keinen durchgreifenden Bedenken hinsichtlich ihrer Zulässigkeit.

1. Entgegen der Auffassung der Beklagten ist der Klageantrag zu 1) hinreichend bestimmt. Gemäß § 253 Abs. 2 Nr. 2 ZPO ist ein Klageantrag hinreichend bestimmt, wenn er den erhobenen Antrag konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis absteckt, Inhalt und Umfang der begehrten Entscheidung erkennen lässt, das Risiko eines Unterliegens der klagenden Partei nicht durch vermeidbare Ungenauigkeiten auf den Beklagten abwälzt und schließlich eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (*Becker-Eberhard*, in: MüKo, ZPO, 6. Aufl., § 253 Rn. 88). Dabei sind alternative Klageanträge grundsätzlich unzulässig (*Becker-Eberhard*, a.a.O., § 260 Rn. 22). Die Kammer verkennt nicht, dass der Kläger sein Begehren auf einen Tatsachenstoff stützt, der sinnvoll auf mindestens zwei verschiedene eigenständige, den Sachverhalt in seinem Kerngehalt nicht verändernde Geschehensabläufe aufgeteilt werden kann (vgl. BGH GRUR 2013, 401, Rn. 18, 19), nämlich einerseits eine unzureichende Aufklärung seiner Person und ein zu niedriges technisches Sicherungsniveau des sozialen Netzwerks der Beklagten und den aus beidem resultierenden Datenverlust im Rahmen des Scraping-Vorfalls sowie andererseits eine sich hieran anschließende unterbliebene Information, dass er von dem Scraping-Vorfall betroffen gewesen ist. Allerdings liegt keine unzulässige Alternativklage vor, da sich aus der Klagebegründung ergibt, dass das im Klageantrag mit mindestens 1.000,00 € bemessene Schmerzensgeld nicht für den einen oder den anderen der beiden Lebenssachverhalte geltend gemacht wird, sondern für beide in Kumulation. Das ist gemäß § 260 ZPO zulässig (*Foerste*, in: Musielak/Voit, ZPO, 19. Aufl., § 260 Rn. 2; so auch Landgericht Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 35, juris; LG Bielefeld GRUR-RS 2022, 38375, Rn. 16 ff.; LG Essen GRUR-RS 2022, 34818, Rn. 38).

2. Auch der Klageantrag zu 2) ist einerseits hinreichend bestimmt (dazu unter a.), andererseits hat der Kläger ein Interesse an der begehrten Feststellung (dazu unter b.).

a. Ein Feststellungsantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn das Recht oder das Rechtsverhältnis, dessen Bestehen oder Nichtbestehen festgestellt werden soll, so genau beschrieben wird, dass über dessen Identität und damit über den Umfang der Rechtskraft des Urteils keinerlei Ungewissheit herrschen kann (*Becker-Eberhard*, a.a.O., § 253 Rn. 154). Vorliegend geht es dem Kläger um die Feststellung des Ersatzes zukünftiger materieller Schäden, die aus dem Scraping-Vorfall resultieren. Wenngleich die Kammer nicht verkennt, dass die

Formulierung „[...] alle künftigen Schäden, die [...] entstanden sind [...]“ missverständlich sein kann, lässt sich der Antrag unter Berücksichtigung der Schriftsätze des Klägers, insbesondere der Replik, so auslegen, dass dieser die „weiteren“ Schäden ersetzt haben möchte, die bereits entstanden sind oder noch entstehen werden (so auch: LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 11).

b. Der Kläger hat sein gemäß § 256 ZPO erforderliches Feststellungsinteresse auch hinreichend dargelegt. Das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts - wie hier dem Recht auf informationelle Selbstbestimmung - bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (*Bacher*, in: BeckOK, ZPO, Bearbeitungsstand 01.09.2022, § 256 Rn. 24, Rn. 34). Bei verständiger Würdigung, dass die im Wege des Scrapings erlangten personenbezogenen Daten im Internet veröffentlicht worden sind, erscheint es zumindest nicht ausgeschlossen, dass dem Kläger deswegen noch ein irgendwie gearteter materieller Schaden entsteht (ebenso LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 42 ff., juris; LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 11; LG Essen GRUR-RS 2022, 34818, Rn. 39; offenlassend: LG Bielefeld GRUR-RS 2022, 38375, Rn. 16 ff.).

Darüber hinaus ist der Antrag des Klägers gem. §§ 133, 157 BGB auszulegen, dass dieser ausschließlich den Ersatz materieller Schäden begehrt. Denn er hat seinen Vortrag dahingehend konkretisiert, tatsächlich nur diese Feststellung zu begehren (so auch LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 11).

lll. Der Unterlassungsantrag (Klageanträge zu 3) ist hingegen unzulässig. Ob der Antrag den Bestimmtheitsanforderungen genügt, kann dahinstehen. Jedenfalls fehlt dem Kläger ein schutzwürdiges Interesse an der gerichtlichen Geltendmachung. Zwingende Prozessvoraussetzung für jede Klage ist ein Rechtsschutzbedürfnis. Dieses kann fehlen, wenn das verfolgte Begehren auf einem einfacheren Weg zu erlangen ist (BGH NJW-RR 2010, 19 Rn. 20). Dabei ist zu berücksichtigen, dass ein schnelleres und billigeres Mittel ein berechtigtes Interesse nur entfallen lässt, wenn es wenigstens vergleichbar sicher oder wirkungsvoll alle erforderlichen Rechtsschutzziele herbeiführen kann (BGH NJW-RR 2009, 1148 Rn. 6). Das ist hier der Fall. Hinsichtlich des Klageantrags 3a. folgt das daraus, dass der Kläger die Funktionsweise des CIT beeinflussen kann. Denn er kann nach dem unstreitigen Vortrag durch Vornahme der Einstellungen selbst darüber entscheiden, dass seine Telefonnummer nicht mehr mittels des CIT gefunden werden kann. Hier-

für muss der Kläger lediglich seine Suchbarkeitseinstellungen ändern (i. E. so auch LG Hildesheim, Hinweisbeschluss vom 22.12.2022, 3 O 99/22). Aus demselben Grund fehlt auch das Rechtsschutzbedürfnis hinsichtlich des Klageantrags 3b. Denn der Kläger hat es auch hier selbst in der Hand hat, die Verarbeitung seiner Telefonnummer durch die entsprechenden Einstellungen zu ändern (vgl. hierzu auch LG Stade, Hinweisbeschluss vom 14.12.2022, 1 O 36/22).

B. In der Sache ist die Klage im tenorierten Umfang begründet. Während dem Kläger das Schmerzensgeld (dazu unter I.) teilweise zusteht und der Feststellungsantrag (dazu unter II.) vollumfänglich begründet ist, ist der Antrag zu 4) unbegründet (dazu unter III.). Aufgrund dessen steht dem Kläger die Erstattung außergerichtlich angefallener Rechtsanwaltskosten lediglich in der tenorierten Höhe zu (dazu unter IV.).

I. Der Kläger hat gegen die Beklagte einen Anspruch auf immateriellen Schadensersatz in Höhe von 500,00 € aus Art. 82 Abs. 1 DSGVO.

Nach dieser Norm hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den sog. Auftragsverarbeiter. Diese Voraussetzungen sind vorliegend erfüllt. Die Beklagte hat gegen DSGVO-Vorschriften verstoßen, indem sie nicht dieser Verordnung entsprechend Daten verarbeitete (dazu unter 1. und 2.); den ihr obliegenden Exkulpationsnachweis hat sie nicht geführt (dazu unter 3.). Der Kläger hat einen ersatzfähigen Schaden erlitten (dazu unter 4.), der kausal auf die Verstöße der Beklagten zurückzuführen ist (dazu unter 5.) und den die Kammer mit 500,00 € beziffert (dazu unter 6.).

1. Die Kammer ist der Auffassung, dass der Anwendungsbereich des Art. 82 Abs. 1 DSGVO nur eröffnet ist, wenn bei einer Verarbeitung von Daten gegen die DSGVO verstoßen wurde. Nicht jeglicher Verstoß gegen Normen der DSGVO begründet einen Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO. Es ist vielmehr erforderlich, dass der Verstoß im Rahmen einer Verarbeitung personenbezogener Daten begangen wird. Der Begriff der Verarbeitung ist ausweislich der Legaldefinition des Art. 4 Nr. 2 DSGVO weit gefasst und schließt jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten ein.

Hierbei verkennt die Kammer nicht, dass Teile der Literatur und der Rechtsprechung unter Bezugnahme auf den weiten Wortlaut des Art. 82 Abs. 1 DSGVO davon ausgehen, dass jeder materielle und formelle Verstoß gegen die Verordnung genügt, um eine Haftung nach dieser Norm auszulösen (vgl. *Quaas*, in: BeckOK Datenschutzrecht, Bearbeitungsstand 01.08.2022, Art. 82 Rn.

14; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl., Art. 82 Rn. 8; *Bergt*, in: Kühling/Buch, DS-GVO BDSG, 3. Aufl., Art. 82 Rn. 23; LG Stuttgart, Urteil vom 26.01.2023, 53 O 95/22; wohl auch: LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 55, juris). Diese Auffassung verkennt aber, dass der sachliche Anwendungsbereich der Verordnung gem. Art. 2 DSGVO auf die „Verarbeitung personenbezogener Daten“ beschränkt wird. Diese Auslegung steht in Einklang zu Art. 82 Abs. 2 DSGVO und zu dem Erwägungsgrund 146 S. 1 der DSGVO, aus der die eigentliche Zielsetzung des europäischen Gesetzgebers ersichtlich wird: Der Verantwortliche oder der Auftragsverarbeiter soll Schäden ersetzen, die einer Person aufgrund einer Verarbeitung entstehen, die mit der DSGVO nicht in Einklang zu bringen sind. Vor diesem Hintergrund ist auch Art. 82 Abs. 1 DSGVO in diesem Sinne auszulegen (*Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl., Art. 82 Rn. 8; LG Bonn ZD 2021, 586 Rn. 33; LG Düsseldorf ZD 2022, 48 Rn. 27; zum vorliegenden Scraping-Vorfall: LG Essen GRUR-RS 2022, 34818 Rn. 44; LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 15; LG Heilbronn, Urteil vom 13.01.2023, Bu 8 O 131/22, S. 7; AG Strausberg BeckRS 2022, 27811 Rn. 17).

2. Unter Berücksichtigung dessen ist die Kammer zu der Überzeugung gelangt, dass die Beklagte als Verantwortliche nach Art. 4 Nr. 7 DSGVO keine geeigneten organisatorischen Maßnahmen getroffen hat, um die personenbezogenen Daten des Klägers zu schützen (dazu unter a.). Über das Vorliegen der weiteren von dem Kläger behaupteten Verstöße der Beklagten gegen die DS-GVO brauchte die Kammer nicht mehr zu entscheiden (dazu unter b.)

a. Aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des CIT verstieß die Beklagte gegen Artt. 32, 24, 5 Abs. 1 f) DSGVO.

Gemäß Art. 32 Abs. 1 Hs. 1 DSGVO haben Verantwortliche und Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierbei konkretisiert Art. 32 DSGVO die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient damit unter anderem der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DSGVO. Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen sind die in Art. 32 Abs. 1 DSGVO genannten Faktoren in die Verhältnismäßigkeitsprüfung einzubeziehen, jedoch nicht notwendigerweise absolut zu befolgen (*Piltz*, in: Gola/Heckmann, 3. Aufl., DS-GVO Art. 32 Rn. 14).

Dabei ist zu berücksichtigen, dass ein absolutes Schutzniveau nicht erreicht werden kann und damit ein etwaiges Risiko nicht gänzlich ausgeschlossen werden kann. Letztlich kommt es bei der Bemessung des Schutzniveaus 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 (*Hladjk,* in: Ehmann/Selmayr, 2. Aufl., DS-GVO Art. 32 Rn. 4; *Laue*, in: Spindler/Schuster, 4. Aufl., DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (*Piltz*, a. a. O., Art. 32 Rn. 41).

Zur Bestimmung des angemessenen Schutzniveaus ist Art. 32 Abs. 2 DSGVO in die Betrachtung einzubeziehen. Danach sind in der Beurteilung 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 zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden (*Laue*, a. a. O., Art. 32 Rn. 5).

Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklagte nicht ausreichend nachgekommen. Denn die von ihr behaupteten „Anti-Scraping-Maßnahmen“ sind selbst, wenn der Beweis geführt würde, dass die von ihr behaupteten Sicherheitsmaßnahmen schon vor dem Scraping-Vorfall ergriffen waren, für sich allein nicht geeignet, um ein dem Risiko für Nutzerdaten angemessenes Schutzniveau zu gewährleisten.

Das CIT ermöglichte 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 zum Beispiel durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank erfolgen, auf die auch Dritte zugreifen können (*Jandt,* in: Kühling/Buchner, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34).

So liegt der Fall hier, da das CIT zweckwidrig nicht nur zum Auffinden von realen persönlichen Kontakten auf Facebook, sondern entgegen der Nutzungsbedingungen der Beklagten auch zu Missbrauchszwecken im Wege eines großangelegten, automatisierten Datenausleseprozesses genutzt werden konnte und wurde. Konkret wurde Dritten eine Zuordnung von Telefonnummern zu Facebook-Profilen, bei denen diese hinterlegt war, ermöglicht. Dementsprechend konnte in Er-

fahrung gebracht werden, welche Person hinter der Telefonnummer stand. Hierbei konnten durch den Rückgriff auf das Facebook-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies barg für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiterem Missbrauch der Daten und damit dem Eintritt von materiellen und immateriellen Schäden (so zutreffend LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 88 ff., juris).

Dieses erhebliche Risiko bedingt bereits, dass der Maßstab für die Bestimmung des angemessenen Schutzniveaus entsprechend hoch anzusetzen ist. Auch ist das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagte, mithin ein Datenverarbeitungsvorgang in deren geschützter interner Sphäre. Des Weiteren handelt es sich bei den Daten - entgegen der Auffassung der Beklagten - nicht nur um ohnehin öffentlich einsehbare Daten. Vielmehr wurde Dritten ein Zugang zu der Telefonnummer des Nutzers gewährt. Denn es erfolgte eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren öffentlichen Daten des Nutzers auf der Facebook-Plattform. Soweit es den Stand der Technik und die Implementierungskosten betrifft, ist nach Auffassung der Kammer maßgeblich, dass es sich bei der Beklagten um eines der größten und erfolgreichsten Unternehmen der IT-Branche weltweit handelt, das sowohl in personeller als auch finanzieller Hinsicht über außerordentliche Ressourcen verfügt und damit in der Lage sein muss, die weltweit höchsten Standards an Datensicherheit zu gewährleisten. Hinzu kommt, dass das Betreiben sozialer Netzwerke, und hier insbesondere „Facebook“, gerade das Geschäftsmodell der Beklagten ist. Vor diesem Hintergrund besteht eine berechtigte Erwartung der Nutzer, dass wesentliche Teile des Konzernbudgets in die Fortentwicklung der sozialen Netzwerke fließen und hier insbesondere in deren Sicherheitsmechanismen.

Die Kammer verkennt nicht, dass die Verknüpfung zwischen der Telefonnummer des Klägers und dessen Daten auf dem Facebook-Profil nur dadurch ermöglicht wurde, dass dieser seine Suchbarkeitseinstellung, also die Suchbarkeit seiner Telefonnummer, auf „alle“ stehen hatte. Doch auch dies ändert nichts daran, dass die Beklagte aufgrund der Sensibilität der Daten ein höheres technisches Schutzniveau hätte bereitstellen müssen (a. A. LG Essen GRUR-RS 2022, 34818, Rn. 54). Hier ist nach diesseitiger Auffassung insbesondere zu berücksichtigen, dass der Scraping-Vorfall mittels einer vergleichsweise primitiv anmutenden Methode erfolgte und dabei sogar offenkundig über einen mehrmonatigen Zeitraum unbemerkt bleiben konnte. „Scraping“ war bereits zuvor weit verbreitet und entsprechende Versuche waren bei dem weltweit stark nachgefragten sozialen Netzwerk der Beklagten auch aus einer ex-ante-Sicht zu erwarten gewesen. Dem war sich auch die Beklagte nach ihrem Vortrag bewusst. Die behauptete teilweise Einschränkung des CIT ist nach ihrem Vorbringen aber erst nach dem streitgegenständlichen Vorfall eingeführt worden. Auch die behauptete Beschäftigung eines Teams von Datenwissenschaftlern,

-analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie Captcha-Abfragen genügte den Anforderungen des Art. 32 DSGVO im vorliegenden Fall offenkundig nicht. Denn die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den – aus ihrer Sicht im hiesigen Verfahren ausreichenden – Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Datenscraping kommen konnte (so zutreffend LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 93, juris)

Welche konkreten Sicherheitsmaßnahmen es bedurft hätte, lässt die Kammer offen. Bekanntlich werden „Scraper“ vor ein Problem gestellt, wenn neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren zum Auslesen von Daten und würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Entsprechende Schutzmaßnahmen, wie den sog. „Social Connection Check“ implementierte die Beklagte erst nach dem Scraping Vorfall.

b. Nach der von der Kammer vertretenen Rechtsauffassung (vgl. oben S. 11 f.) konnte offengelassen werden, ob die Beklagte gegen die von dem Kläger vorgetragenen weiteren Pflichten verstoßen hat (Artt. 13, 15, 25, 33, 34 DSGVO), da selbst bei einem Verstoß der Anwendungsbereich des Art. 82 Abs. 1 DSGVO nicht eröffnet wäre. Dem steht auch nicht entgegen, dass die irische Datenschutzbehörde unter Rückgriff auf Art. 25 DSGVO ein Bußgeld gegen die Beklagte verhängt hat, da im hiesigen Verfahren der Individualanspruch eines Facebook-Nutzers gegen die Beklagte im Raum steht.

3. Die Beklagte hat sich nicht von der Haftung exkulpiert (Art. 82 Abs. 3 DSGVO). Nach dieser Norm wird der Anspruchsverpflichtete von der Haftung befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Dabei wird die Verantwortlichkeit der Beklagten vermutet (*Quaas*, a. a. O., Art. 82 Rn. 17).

Der Begriff der Verantwortlichkeit wird nicht definiert. Es kann vorliegend dahinstehen, ob dieser Begriff mit dem Begriff des Verschuldens nach der deutschen Rechtsterminologie gleichzusetzen oder ob Art. 82 DSGVO als Tatbestand der Gefährdungshaftung zu verstehen ist, mit der Folge, dass eine Haftung des Verantwortlichen nur bei atypischen Kausalverläufen oder bei höherer Gewalt entfiele. Der Beklagten gelingt vorliegend nämlich weder der Nachweis fehlenden Verschuldens noch des Vorliegens eines solchen Ausnahmefalls (so auch: LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 132 ff., juris; LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 16; LG Stuttgart, Urteil vom 26.01.2023, 53 O 95/22, S. 17 f.)

Die Haftungsbefreiung greift bei der Annahme, dass ein Verschulden vorauszusetzen ist, nur dann ein, wenn der Verantwortliche sämtliche Sorgfaltsanforderungen erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist (vgl. AG Hildesheim, Urteil vom 5. Oktober 2020 – 43 C 145/19, ZD 2021, 384; *Spindler/Horváth* , in: Spindler/Schuster, DS-GVO, 4. Auflage 2019, Art. 82, Rn. 11).

Die Beklagte hat aber fahrlässig gehandelt. Das Risiko von „Scraping“ war ihr bekannt. Die Beklagte hätte bei Anwendung der gebotenen Sorgfalt erkennen müssen, dass das CIT ein Einfallstor für eine Missbrauchsmöglichkeit ist. Hinzu kommt, dass der Scraping-Vorfall sich über mehrere Monate erstreckte. Ein so lange dauernder automatisierter Zugriff auf das CIT hätte der Beklagten auffallen müssen.

Die Beklagte kann sich auch nicht unter Hinweis auf ein mögliches Mitverschulden seitens des Klägers von ihrer Haftung befreien. Die Beklagte hat den Kläger nicht über das bestehende erhebliche Missbrauchsrisiko informiert, dass sich aus der Preisgabe seiner Telefonnummer und der Funktionsweise des CIT ergibt. Auch wenn der Nutzer durch seine Einstellungen die Möglichkeit des Datenabgleichs eröffnet, heißt das noch nicht, dass er damit auch sein Einverständnis erklärt, dass Dritte Daten „abgreifen“ dürfen (*Grimm,* GRUR-Prax 2023, 108). Entgegen dem Landgericht Heilbronn (Urteil vom 13.01.2023, Bu 8 O 131/22, S. 15 f.) ist die Kammer auch nicht der Auffassung, dass sich hier ein allgemeines Lebensrisiko realisiert hat, dass jeder Nutzer des Internets bei der Preisgabe seiner Daten in Kauf nimmt. Im Übrigen behauptet die Beklagte das Vorliegen ganz ungewöhnlicher Kausalverläufe, einen Fall höherer Gewalt oder ein weit überwiegendes eigenes Fehlverhalten der klagenden Partei auch nicht.

4. Dem Kläger ist ein immaterieller Schaden entstanden.

Aus dem Wortlaut des Art. 82 DSGVO folgt, dass der europäische Gesetzgeber nicht davon ausgeht, schon allein die Pflichtverletzung begründe den Schaden. Denn ein Anspruch besteht nur, wenn ein materieller oder immaterieller Schaden „entstanden“ ist. Dieser Unterscheidung hätte es nicht bedürft, wenn ein bloßer Pflichtenverstoß konstitutiv für den Anspruch wäre (OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 77, juris; zu vorliegendem Scraping-Vorfall: LG Bielefeld GRUR-RS 2022, 38375 Rn. 27 m. w. N.). Dies entspricht auch der Auffassung des Generalanwalts beim Europäischen Gerichtshof, der in seinen Schlussanträgen im Rahmen des Vorabentscheidungsersuchens des österreichischen Obersten Gerichtshofs vom 12.05.2021 auf das Erfordernis eines konkreten Schadens abstellt (Generalanwalt beim EuGH, Schlussantrag v. 06.10.2022, BeckRS 2022, 26562).

Das Merkmal des immateriellen Schadens ist europarechtlich autonom auszulegen. Der Begriff des Schadens soll nach dem Erwägungsgrund 146 S. 3 DSGVO „im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht." Daraus kann abgeleitet werden, dass der nach Abs. 1 bereits weite – weil Ansprüche aus § 253 BGB umfassende – Schadensbegriff im Zweifel nicht begrenzend auszulegen ist (vgl. *Frenzel,* a. a. O., Art. 82 Rn. 10; OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 81, juris). Die Erwägungsgründe 75 und 85 DSGVO konkretisieren dieses weite Verständnis dahingehend, indem sie beispielhaft aufzählen, welche konkreten Beeinträchtigungen einen immateriellen Schaden darstellen können. Hierunter fallen neben Identitätsdiebstahl oder Identitätsbetrug auch der Verlust der Kontrolle über die personenbezogenen Daten. Aufgrund dessen stellt bereits das ungute Gefühl der Ungewissheit, ob personenbezogene Daten Unbefugten bekannt geworden sind, einen immateriellen Schaden dar (OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 85, juris). Dieser immaterielle Schaden ist, mag er auch niederschwellig sein, auszugleichen.

Darüber hinaus sieht Art. 82 DSGVO eine etwaige Bagatellgrenze nicht vor. Zwar hatte § 8 Abs. 2 BDSG a. F. einen Ersatz immaterieller Schäden von einer schweren Verletzung des Persönlichkeitsrechts abhängig gemacht. Die dazu ergangene Rechtsprechung ist aber nicht auf die neue Rechtslage übertragbar, da nach dem Wortlaut des Art. 82 DSGVO gerade keine Bagatellgrenze mehr zu berücksichtigen ist (so auch OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 78, juris).

Diese Grundsätze berücksichtigend hat der Kläger in ausreichendem Maße dargelegt, dass er einen erheblichen Kontrollverlust über seine Daten erlitten hat. Soweit die Beklagte meint, der Kläger könne einen Kontrollverlust nicht erlitten haben, da sowieso nur öffentlich zugängliche Daten „gescraped" worden seien, dringt sie mit dieser Auffassung nicht durch. Sie verkennt, dass die Telefonnummer des Klägers nicht öffentlich zur Verfügung gestellt wurde. Es ist gerade die Offenbarung der Telefonnummer in Verknüpfung mit weiteren personenbezogenen Daten wie dem Vor- und Nachnamen des Klägers, der zu einem erheblichen Kontrollverlust geführt hat. Denn die Veröffentlichung dieser Daten im öffentlich zugänglichen Darknet bedeuten für den Kläger ein hohes Risiko, dass jene zu irgendeinem Zeitpunkt in unbefugter Weise genutzt werden. Die negativen Folgen können dabei vielfältig sein und schwere Nachteile mit sich bringen, wie zum Beispiel die Belästigung durch Spam- und Werbenachrichten, die Zusendung von Viren oder vermögenswirksame Handlungen zu Lasten des Klägers, sodass ein immaterieller Schadensersatzanspruch gerechtfertigt ist (so bereits: LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 18).

Dabei ist auch zu berücksichtigen, dass es nicht darauf ankommen kann, ob der Kläger Spam- oder Werbenachrichten oder etwaige Ping-Anrufe bereits erhalten hat. Denn aus teleologischen Gesichtspunkten kann es keine Rolle spielen, ob der Kläger bereits solche Anrufe/Nachrichten erhalten hat oder diese möglicherweise erst in Zukunft erhalten wird. Spätestens durch die Veröffentlichung der Daten im Darknet ist er einer dauerhaften konkreten Gefahrenlage ausgesetzt worden.

5. Der Verstoß der Beklagten gegen die DSGVO ist auch kausal für den Schaden des Klägers. Es besteht kein Zweifel daran, dass der Kontrollverlust über die eigenen Daten, die der Kläger erlitten hat, auf das unzureichende technische Schutzniveau des sozialen Netzwerks zurückzuführen ist. Soweit verschiedentlich die Auffassung vertreten wird, dass unklar sei, ob etwaige Spam-Nachrichten oder Anrufe auf den „Scraping-Vorfall“ zurückgehen würden und deshalb die Kausalität zwischen Pflichtverletzung und Schaden verneint wird (so LG Bielefeld GRUR-RS 2022, 38375 Rn. 33; LG Essen GRUR-RS 2022, 34818, Rn. 84, LG Coburg, Urteil vom 25.01.2023, 14 O 224/22, S. 15; LG Ellwangen (Jagst), Urteil vom 25.01.2023, 2 O 198/22, S. 25; Amtsgericht München, Urteil vom 01.02.2023, 178 C 13527/22, S. 7), wird verkannt, dass bei einem so engen Verständnis des Schadensbegriffs ein Kausalitätsnachweis faktisch nie zu führen wäre und damit der Schadensersatzanspruch des Art. 82 DSGVO entgegen der gesetzgeberischen Konzeption entwertet würde. Der Schaden des Klägers war für die Beklagte auch vorhersehbar. Denn ein völlig atypischer Verlauf, der die Kausalität ausschließen würde, liegt nicht vor und wurde auch nicht vorgetragen.

6. Die Kammer erachtet ein Schmerzensgeld in Höhe von 500,00 € für angemessen. Art. 82 DSGVO enthält keine Kriterien zur Bestimmung der Höhe des Anspruchs auf immateriellen Schadensersatz. Ausgangspunkt für dessen Bewertung ist der weit auszulegende europarechtliche Schadensbegriff, wobei die Ermittlung gemäß § 287 ZPO der Kammer obliegt. Zu berücksichtigen sind neben der inhaltlichen Schwere des Verstoßes, seiner Dauer und dem Kontext, in dem der Verstoß erfolgte, auch die Ausgleichs-, Genugtuungs- und Vorbeugefunktion des Schadensersatzanspruchs (vgl. *Frenzel,* a. a. O., DSGVO Art. 82 Rn. 12a) sowie drohende Folgen (*Bergt,* a. a. O., Art. 82 Rn. 18d). Maßgeblich sind stets die konkreten Umstände des Einzelfalles (so auch BAG v. 26.08.2021, 8 AZR 253/20; OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 100, juris; LG Lüneburg, Urteil vom 13.12.2022, 3 O 83/22, S. 18). Um den verschiedenen Funktionen des Schadensersatzanspruches Rechnung zu tragen ist es dabei nicht erforderlich, die Beträge hoch anzusetzen, um die geforderte Wirksamkeit und abschreckende Wirkung zu erzielen (OLG Koblenz, Urteil vom 18.05.2022 - 5 U 2141/21, Rn. 101, juris).

Insoweit muss hier bei Bemessung der Höhe gesehen werden, dass der Kontrollverlust über eigene Daten erhebliche Risiken für den Kläger birgt künftig mit Missbräuchen seiner Telefonnummer überzogen zu werden. Einschränkend muss aber gesehen werden, dass Spam-Nachrichten und Ping-Anrufe mittlerweile weit verbreitet und für regelmäßige Nutzer des Internets allgemeines Lebensrisiko geworden sind. Soweit der Kläger vorträgt, dass sich sein Unwohlsein auch aus dem Erhalt von E-Mails resultiert, ist dieser Vortrag nicht nachvollziehbar, weil die E-Mail gerade nicht zu den abgeschöpften Daten gehört.

Auf den Anspruch wirkt sich zudem aus, dass der Kläger den Kontrollverlust der Daten durch einen Wechsel der Telefonnummer einfach und ohne großen Kostenaufwand selbst beseitigen kann. Zwar ist das Ändern der Telefonnummer lästig, aufgrund dieser grundsätzlichen Möglichkeit hat die Kammer aber der Behauptung des Klägers, dass er wegen des Scraping-Vorfalls unter psychischen Beeinträchtigungen bzw. einem Unwohlsein leide, nicht weiter nachgehen müssen; diese wären nämlich vermeidbar.

Die Höhe des von der Kammer angesetzten immateriellen Schadensersatzanspruchs berücksichtigt den Grundsatz der Verhältnismäßigkeit. Unter Abwägung der genannten Gesichtspunkte erachtet die Kammer einen immateriellen Schadensersatzanspruch in Höhe von 500,00 € für angemessen aber auch ausreichend.

7. Die Entscheidung über die Zinsen folgt aus den §§ 291, 288 Abs. 1 BGB.

II. Der mit dem Antrag zu 2) geltend gemacht Feststellungsantrag ist begründet. Nach den Ausführungen unter B. I. steht dem Kläger ein Schadensersatzanspruch aus Art. 82 DSGVO zu, der ein feststellungsfähiges Rechtsverhältnis darstellt. Da die Möglichkeit noch unbekannter materieller Schäden nicht auszuschließen ist, ist der Feststellungsantrag begründet (BGH NJW-RR 2007, 601 Rn. 6, beck-online).

III. Dem Kläger steht allerdings unter keinen rechtlichen Gesichtspunkten ein Auskunftsanspruch zu. Insbesondere folgt ein solcher Anspruch nicht aus Art. 15 Abs. 1 Hs. 1, 2 DSGVO. Nach dieser Norm hat die betroffene Person zunächst einen Anspruch gegen den Verantwortlichen, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so hat die betroffene Person ein Recht auf Auskunft über diese personenbezogenen Daten (vgl. BGH NJW 2021, 1381). Im Ausgangspunkt steht dem Kläger nach dieser Vorschrift grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortlicher im Sinne des Art. 4 Nr. 7 Hs. 1 DSGVO verarbeiteten, ihn betreffenden personenbezogenen Daten zu. Dieser Anspruch ist jedoch durch Erfüllung

untergegangen, § 362 Abs. 1 BGB (i. E. ebenfalls den Auskunftsanspruch verneinend: LG Essen GRUR-RS 2022, 34818; LG Gießen GRUR 2022, 30480; LG Bielefeld GRUR-RS 2022, 38375, LG Paderborn, Urteil vom 13.12.2022, 2 O 212/22, Rn. 180 ff., juris; LG Lüneburg Urteil vom 13.12.2022, 3 O 83/22, S. 23; LG Stuttgart, Urteil vom 26.01.2023, 53 O 95/22, S. 17 f.).

Erfüllt ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen (BGH, Urteil vom 15.06.2021, VI ZR 576/19, Rn. 17 - 24, juris). 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. Die Beklagte hat dem Kläger mit außergerichtlichem Schreiben mitgeteilt, welche personenbezogenen Daten verarbeitet werden. Soweit der Kläger Auskunft darüber begehrt, welche Daten Dritte beim Scraping-Vorfall erlangen konnten, besteht der Anspruch nicht, da die Beklagte nachvollziehbarerweise keine Angaben zu Verarbeitungstätigkeiten Dritter machen kann. Weitere Anspruchsgrundlagen sind nicht ersichtlich und werden auch nicht vorgetragen.

IV. Der Kläger hat gegen die Beklagte einen Anspruch auf Zahlung der außergerichtlichen Rechtsanwaltskosten, allerdings nur unter Berücksichtigung eines Gegenstandswerts in Höhe von 500,00 €. Bei einem teilweisen Obsiegen kann der Kläger grundsätzlich die Rechtsanwaltskosten nur einfordern, soweit er mit dem vorgerichtlich geltend gemachten Anspruch später vor Gericht durchdringt (BGH NJW 2008, 1888 Rn. 13). Vorliegend dringt er mit dem Klageantrag zu 1) teilweise (Gegenstandswert: 500 €) durch. Zwar obsiegt er außerdem mit dem Klageantrag zu 2), allerdings wurde die Beklagte vorgerichtlich nicht aufgefordert, ihre Einstandspflicht für materielle Schäden anzuerkennen, so dass insoweit keine vergütungspflichtige Tätigkeit entfaltet wurde. Der Anspruch auf Zahlung der außergerichtlichen Rechtsanwaltskosten beläuft sich damit auf 90,96 € (1,3 Geschäftsgebühr i. H. v. 63,70 €; Auslagenpauschale 12,74 €; Umsatzsteuer: 14,53 €). Die Hinzuziehung eines Rechtsanwalts war zur effektiven Durchsetzung der Ansprüche aufgrund der Schwierigkeit der Sach- und Rechtslage geboten. Der Zinsanspruch folgt auch hier aus §§ 288, 291 BGB.

V. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit hat für beide Parteien ihre Rechtsgrundlage in den §§ 708 Nr. 11, 711 ZPO.

VI. Der Streitwert wird auf 5.500,00 € festgesetzt. In nicht-vermögensrechtlichen Streitigkeiten wie der vorliegenden bestimmt sich der Streitwert nach § 3 ZPO, wobei alle Umstände des Einzelfalles, insbesondere der Umfang der Sache und ihre Bedeutung für den Kläger zu berücksichtigen sind. Danach hält die Kammer die folgenden Einzelstreitwerte für angemessen:

Antrag zu 1): 1.000,00 €

Antrag zu 2): 1.500,00 €

Antrag zu 3): 2.000,00 €

Antrag zu 4): 1.000,00 €

[redacted]
Vorsitzender Richter
am Landgericht

[redacted]
Richter
am Landgericht

[redacted]
Richter

Verkündet am 17.03.2023

[redacted], Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle

Beglaubigt:

(Dienstsiegel)

([redacted]), Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle