Beglaubigte Abschrift

Landgericht Lüneburg
Geschäfts-Nr.:
3 O 92/23

Verkündet am:
14.02.2024

, Justizamtsinspektorin
als Urkundsbeamtin der Geschäftsstelle

Information zum Datenschutz unter www.landgericht-lueneburg.niedersachsen.de

Im Namen des Volkes!

Urteil

In dem Rechtsstreit

,

Kläger

Prozessbevollmächtigte: Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB, Eupener Straße 67, 50933 Köln,
Geschäftszeichen:

gegen

Meta Platforms Ireland Ltd., vertr. d. d. Mitglieder d. Board of Directors, Merrion Road, D04 X2K5, IRL Dublin 4,

Beklagte

Prozessbevollmächtigte: Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB, Josephsplatz 1, 90403 Nürnberg,
Geschäftszeichen:

hat die 3. Zivilkammer des Landgerichts Lüneburg auf die mündliche Verhandlung vom 15.01.2024 durch

den Vizepräsidenten des Landgerichts ,
die Richterin am Amtsgericht und
die Richterin am Landgericht

für **R e c h t** erkannt:

1. Die Beklagte wird verurteilt, an die klagende Partei immateriellen Schadensersatz in Höhe von 300,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 30. September 2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der klagenden Partei alle weiteren materiellen Schäden zu ersetzen, die dieser durch den unbefugten Zugriff Dritter, der nach Aussage der Beklagten im Jahr 2019 erfolgte, auf ihre bei der

Beklagten hinterlegte Telefonnummer und auf die auf ihrem Facebook-Profil öffentlich einsehbaren Daten, entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, an die klagende Partei vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 30. September 2023 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits tragen die klagende Partei 85 % und die Beklagte 15 %.

6. Das Urteil ist vorläufig vollstreckbar. Beide Parteien können die Vollstreckung gegen Sicherheitsleistung in Höhe von 120 % des jeweils auf Grund des Urteils vollstreckbaren Betrages abwenden, wenn nicht der andere vor der Vollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrages leistet.

Tatbestand

Die klagende Partei begehrt von der Beklagten Schadensersatz sowie Unterlassung und Auskunft hinsichtlich etwaiger Persönlichkeitsverletzungen und Verstößen gegen die Datenschutz-Grundverordnung (DS-GVO) im Zusammenhang mit einem sogenannten Scraping-Vorfall bei der Beklagten.

Die Beklagte ist Betreiberin der Social Media Plattform facebook.com. Die klagende Partei ist Nutzerin dieser Plattform. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile zu erstellen und diese mit Freunden zu teilen. Auf ihrem Profil können die Nutzer verschiedene Daten zu ihrer Person angeben. Bei den Angaben zu Name, Geschlecht und Nutzer-ID handelt es sich um immer öffentliche Nutzerinformationen, die für jeden sichtbar sind. Diese Daten sind auch auf dem Profil der klagenden Partei öffentlich einsehbar. Hinsichtlich der sonstigen Informationen bzw. Angaben können die Nutzer Privatsphäre-Einstellungen treffen und damit selbst darüber entscheiden, welche anderen Nutzer auf ihre Daten zugreifen können. Für das Verfahren relevant sind insbesondere die Zielgruppenauswahl und die Suchbarkeits-Einstellung. Im Rahmen der Zielgruppenauswahl kann der Nutzer festlegen, welche Personengruppe

einzelne Informationen wie Wohnort, Stadt, Beziehungsstatus, Geburtstag, E-Mail-Adresse etc. in seinem Facebook-Profil sehen kann. Mit der Suchbarkeits-Einstellung kann der Nutzer festlegen, wer sein Profil anhand der von ihm angegebenen Telefonnummer, unabhängig davon, ob die Telefonnummer auf dem Profil öffentlich einsehbar ist, finden kann. Bis zum 7. Februar 2018 hatte die klagende Partei die Suchbarkeit auf „Friends“ und danach bis zum 5. März 2019 entsprechend der von der Beklagten vorgenommenen Voreinstellung auf „alle“ („Everyone“) gestellt (Anlage B 17). Bei der Suchbarkeit für „alle“ blieb es, auch wenn der Nutzer im Rahmen der Zielgruppenauswahl die Sichtbarkeit der Telefonnummer in seinem Profil auf „privat“ einstellte. Die Suche nach Personen war mit der Facebook-Suchfunktion, welche sowohl ein Suchen anhand der Telefonnummer als auch anhand des Namens ermöglichte, wobei letztere üblicher war, als auch über das sog. Kontakt-Importer-Tool möglich. Eine Suche anhand der Telefonnummer erfolgte seitens der Facebook-Nutzer üblicherweise über die Kontakt-Importer-Funktion. Das Kontakt-Importer-Tool funktionierte dabei so, dass ein Nutzer eine Telefonnummer als Kontakt in seinem Smartphone abspeicherte und die Beklagte dem Nutzer über das Kontakt-Importer-Tool erlaubte, seine abgespeicherten Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die mit der Telefonnummer bei Facebook registrierte Person angezeigt zu bekommen und als Freund hinzufügen zu können.

Die Beklagte informierte ihre Nutzer auf verschiedenen Kanälen über die ihnen zur Verfügung stehenden Privatsphäre-Einstellungen und zwar im Hilfebereich, in Privatsphäre-Tools und in Datenrichtlinien.

Anfang April 2021 verbreiteten Dritte im sogenannten Darknet öffentlich Datensätze einer Vielzahl von Facebook-Nutzern. Davon betroffen ist auch die klagende Partei. Die Datensätze enthalten Daten wie Telefonnummer, FacebookID, Name und Vorname, Geschlecht und gegebenenfalls weitere korrelierende Daten. Die der Datenveröffentlichung vorausgegangene Datengewinnung beruht auf einer Nutzung des sogenannten Kontakt-Importer-Tools und des sogenannten „Scrapings“, d.h. eines automatisierten, massenhaften Sammelns öffentlich einsehbarer Daten. Die Parteien gehen davon aus, dass mithilfe des Kontakt-Importer-Tools und durch Generieren einer Vielzahl an Telefonnummern, eine Verknüpfung mit einem Facebook-Profil hergestellt wurde. Sodann wurden jedenfalls die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer den abgerufenen Daten hinzugefügt. So auch bei der klagenden Partei.

Die klagende Partei forderte die Beklagte mit vorgerichtlichem anwaltlichen Schreiben zur Zahlung von 500 € und Unterlassung zukünftiger Zugänglichmachung der Daten der klagenden Partei an unbefugte Dritte und zur Auskunft gemäß Art. 15 DS-GVO auf, insbesondere welche konkreten Daten von wem abgegriffen worden seien (vgl. Anlage K 1). Wegen der Antwort der Beklagten wird auf die vorgerichtlichen Schreiben, Anlagen K2 und B 16, Bezug genommen.

Am 25. November 2022 verhängte die irische Datenschutzbehörde (Data Protection Commission) gegen die Beklagte ein Bußgeld wegen Verstößen gegen die DS-GVO im Zusammenhang mit dem auch in dem hiesigen Verfahren unstreitig erfolgten Scraping-Vorfall. Die irische Datenschutzbehörde sah die von der Beklagten implementierten Maßnahmen zur Ratenbegrenzung und Bot-Erkennung im Sinne von Art. 25 Abs. 1 DS-GVO als nicht ausreichend an. Die Beklagte habe keine angemessenen technischen und organisatorischen Maßnahmen getroffen, die dafür ausgelegt seien, die Datenschutzgrundsätze, insbesondere die in Art. 5 Abs. 1 lit. b) und f) vorgesehenen Grundsätze, wirksam umzusetzen. Zudem nahm die irische Datenschutzbehörde einen Verstoß gegen Art. 25 Abs. 2 DS-GVO an, indem die Sucheinstellungen für Benutzer so voreingestellt worden seien, dass die Telefonnummer ohne Eingreifen des Einzelnen für eine unbestimmte Anzahl natürlicher Personen zugänglich gemacht worden sei. Diese Entscheidung ist noch nicht bestandskräftig.

Die klagende Partei behauptet, von ihr seien über die Telefonnummer hinaus weitere Daten abgegriffen worden. Es handele sich bei den „gescrapten“ Daten um nur zum Teil öffentlich zugängliche Daten. Es sei ein Programm verwendet worden, welches nach der Überprüfung und Verknüpfung unzähliger Telefonnummer-Kombinationen mit Facebook-Profilen sämtliche Daten des Nutzers habe abfragen und exportieren können. Der Datenabgriff durch Dritte sei aufgrund einer Sicherheitslücke möglich gewesen. Die Beklagte habe keine ausreichenden Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des bereitgestellten Kontakt-Importer-Tools zu verhindern. Die Beklagte habe keine Sicherheitscaptchas verwendet, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung der Kontakte um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handele. Die Beklagte habe keinen Mechanismus zur Überprüfung der Plausibilität der Anfragen verwendet, um ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal zu blocken oder Adressbücher mit auffälligen Telefonnummernabfolgen automatisch abzulehnen.

Die klagende Partei meint, die Einstellungen zur Sicherheit insbesondere der Telefonnummer auf Facebook seien so undurchsichtig und kompliziert dargestellt, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Sie ist der Ansicht, die Voreinstellungen seien nicht datenschutzfreundlich, weil z.B. die Voreinstellung hinsichtlich der Suchbarkeit „öffentlich“ sei. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit damit zu rechnen, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Bei der Registrierung werde der Nutzer nur auf die Datenschutzrichtlinie und Nutzungsbedingungen verwiesen, welche keine transparenten und konkreten Informationen über die Verarbeitungstätigkeiten, insbesondere über die Zwecke der Verarbeitung der Telefonnummer und die Funktionsweise der Kontakt-Importer-Funktion, über immer öffentliche Nutzerinformationen, Zielgruppenauswahl und Drittlandübermittlungen enthalte.

Die Beklagte habe ihre Nutzer nicht hinreichend über die ihr bekannten Gefahren informiert, insbesondere fehle der Hinweis, dass unberechtigte Dritte öffentlich zugängliche Daten leicht mit Hilfe von „Facebook-Tools“ anreichern, diese im Darknet veröffentlichen könnten und die Beklagte die betroffenen Personen nicht über solche Vorfälle informiere.

Die klagende Partei behauptet, die Veröffentlichung ihrer Daten habe weitreichende Folgen für sie. Sie habe einen erheblichen Kontrollverlust über ihre Daten erlitten, welcher großes Unwohlsein und große Sorge über einen möglichen Missbrauch der sie betreffenden Daten ausgelöst habe. Die klagende Partei habe ein verstärktes Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen entwickelt. Sie habe seit dem Vorfall unregelmäßig unbekannte Kontaktversuche per SMS oder E-Mail mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks erhalten. Sie könne nur noch mit äußerster Vorsicht auf E-Mails und Nachrichten reagieren.

Es könne zudem zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritte Zugriff auf die Daten der klagenden Partei erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden. Folgen von Datenschutzverletzungen würden sich ihrem Wesen nach erst spät zeigen und lange unerkannt bleiben. Es erscheine auf Grund der Veröffentlichung der Telefonnummern möglich, dass die klagende Partei durch eine Vielzahl betrügerischer Anrufe belästigt werde. Es sei

möglich, dass sich Anrufer als Bankmitarbeiter ausgeben, um an sensible Kontodaten zu gelangen.

Die klagende Partei ist der Ansicht, die Beklagte habe sie nicht rechtzeitig darüber informiert, dass ihre personenbezogenen Daten durch Dritte veröffentlich worden seien, so dass sie, die klagende Partei, auch nicht rechtzeitig Schutzmaßnahmen habe ergreifen können.

Die Beklagte trage die Darlegungs- und Beweislast, soweit die Einhaltung der DS-GVO in Streit stehe.

Die klagende Partei beantragt,

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

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

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

   a. bei Vorliegen einer Einwilligung des Klägers, die es der Beklagten erlaubt, Kontakte aufgrund eines Abgleichs mittels der Telefonnummer und des Facebookprofils vorzuschlagen, keine ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite durch Kontaktvorschläge für Dritte, welche diese Telefonnummer abfragen, mit dem Facebook Profil des Klägers zu verknüpfen, solange der Kläger hierzu nicht ausdrücklich einwilligt.

4. die Beklagte zu verurteilen, der klagenden Partei Auskunft über die klagende Partei betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten;

5. die Beklagte zu verurteilen, an die klagende Partei vorgerichtliche Rechtsanwaltskosten in Höhe von 800,39 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, es seien neben der Telefonnummer nur öffentlich auf dem Facebook-Profil der klagenden Partei einsehbare Informationen gesammelt worden, d.h. die immer öffentlichen Nutzerinformationen wie Vorname, Name, Geschlecht und die Nutzer-ID oder solche die aufgrund der Zielgruppenauswahl der klagenden Partei öffentlich einsehbar gewesen seien.

Die Beklagte behauptet, dass sie zur Bekämpfung von „Scraping“ Übertragungsbegrenzungen /-beschränkungen, sog. Captcha-Abfragen und Bot-Erkennung eingerichtet habe und diese auch fortlaufend weiterentwickle und ein Team von „Datenwissenschaftlern, -analysten und Softwareingenieuren beschäftige. Sie habe im April 2018 die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion deaktiviert. Zudem habe sie die Übertragungsbeschränkungen innerhalb der Kontakt-Importer-Funktion gesenkt, auch wenn sie zu diesem Zeitpunkt keine Scraping-Aktivität über diese Funktion festgestellt habe. Als weitere Schutzmaßnahme habe sie in einer nicht näher von ihr benannten Zeit zwischen Januar 2018 und September 2019 („Relevanter Zeitraum“) für den Kontakt-Import eine Funktion errichtet, die darauf abziele, einen übereinstimmenden Kontakt nur dann anzuzeigen, wenn die beiden Nutzer einander zu kennen schienen („Social Connection Check“). Wenn ein Nutzer seine Kontaktliste von seinem Mobiltelefon über das Kontakt-Importer-Tool auf die Plattform hochlade, werde der übereinstimmende Nutzer nur dann dem importieren

Nutzer angezeigt, wenn dieser zugleich einen Namen sowie die Telefonnummer für den hochgeladenen Kontakt importiere, der dem Namen des übereinstimmenden Nutzers ähnele oder der übereinstimmende Nutzer den importierenden Nutzer bereits in seinen Kontakten habe. Schließlich habe die Beklagte die Kontakt-Importer-Funktion in eine Liste mit Kontaktvorschlägen umgewandelt, die „Menschen, die du kennen könntest“ anzeige - „people you may know-Funktion“ (PYMK-Funktion).

Die Beklagte behauptet, die im Internet erfolgte Veröffentlichung von Daten der klagenden Partei habe sich nicht signifikant auf das ohnehin bestehende Risiko der Cyber-Kriminalität ausgewirkt. Es sei Teil des allgemeinen Lebensrisikos, Opfer von Internetkriminalität beziehungsweise Identitätsdiebstahl zu werden.

Wegen des weiteren Vorbringens der Parteien wird auf die zu den Akten gelangten Schriftsätze nebst Anlagen sowie das Protokoll zur mündlichen Verhandlung Bezug genommen.

Die Klageschrift ist der Beklagten am 29. September 2023 zugestellt worden (vgl. EB, Bl. 94, Bd. 1 d. A.).

Entscheidungsgründe

Die Klage ist zulässig (I.) und in dem aus dem Tenor ersichtlichen Umfang begründet, im Übrigen unbegründet (II.)

I. Die Klage ist zulässig.

1. Der Klageantrag zu Ziff. 1 ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Insbesondere liegt – entgegen der Auffassung der Beklagten – keine alternative Klagehäufung vor, bei der die klagende Partei ein einheitliches Klagebegehren aus mehreren prozessualen Ansprüchen (Streitgegenständen) herleiten und dem Gericht die Auswahl überlassen würde, auf welchen Klagegrund es die Verurteilung stützt. Zum Streitgegenstand sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden, den Sachverhalt „seinem Wesen nach“ erfassenden Betrachtungsweise zu dem zur Entscheidung gestellten Tatsachenkomplex gehören, den der Kläger zur Stützung seines Rechtsschutzbegehrens dem Gericht zu unterbreiten hat (vgl. BGH, Urteil vom 24.01.2008 – VII ZR 46/07). Die Klage bestimmt

den Streitgegenstand, wobei Klageantrag und Klagegrund gleichwertige Bestimmungsfaktoren sind (Zöller/Vollkommer, ZPO, 33. Auflage 2020, Einl. Rn. 63). Dies zugrunde gelegt, handelt es sich hier um einen einheitlichen Streitgegenstand. Aus der Klage, dort insbesondere der Klagebegründung, ergibt sich, dass sich die mit dem Klageantrag zu Ziff. 1 geltend gemachte Zahlungsforderung auf einen zusammenhängenden Lebenssachverhalt stützt. Dieser liegt darin, dass die klagende Partei zum Zeitpunkt des Scrapings auf der von der Beklagten betriebenen Plattform angemeldet war und betrifft die Frage, ob die Beklagte zu diesem Zeitpunkt hinreichende Datenschutzvorkehrungen getroffen hatte. Die von der klagenden Partei behaupteten Verstöße der Beklagten gegen die DS-GVO mündeten kumulativ in dem möglichen Schaden im Zusammenhang mit der Offenbarung der Telefonnummer der klagenden Partei. Auch etwaige nachträgliche Verstöße durch Verletzung von Informationspflichten können lediglich eine Vertiefung des möglichen Gesamtschadens darstellen.

2. Auch der Klageantrag zu Ziff. 2 ist zulässig.

a) Der Klageantrag zu Ziff. 2 ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Das festzustellende Rechtsverhältnis muss derart genau bezeichnet werden, dass über dessen Identität und damit über den Umfang der Rechtskraft der Feststellung keine Ungewissheit besteht (vgl. BGH, Urteil vom 22.11.2007 - I ZR 12/05, Rn. 22, beck-online). Hierbei sind die Klageanträge der Auslegung (§ 133 BGB) zugänglich (vgl. BGH, Urteil vom 24.04.2018 – XI ZR 207/17, Rn 10, beck-online mwN). Zwar genügt der Antrag zu Ziff. 2 auf Feststellung der Ersatzpflicht für *„alle künftigen Schäden“,* die *„entstanden sind“* für sich gesehen nicht dem Bestimmtheitsgebot des § 253 Abs. 2 Nr. 2 ZPO. Dieser ist ohne Hinzutreten weiterer Umstände widersprüchlich. Allerdings kann die Bestimmtheit des Antrages durch Auslegung des Prozessvortrages der klagenden Partei hinreichend hergestellt werden. Die klagende Partei hat in ihrer Klage vorgetragen, dass noch nicht absehbar sei, welche Schäden durch den Zugriff auf die Daten abschließend entstanden seien. Hieraus folgt, dass der Antrag zu Ziff. 2 dahingehend zu verstehen ist, dass es ihr auf die *„weiteren“* Schäden ankommt, die bereits entstanden sind oder noch entstehen werden.

b) Auch das für den Klageantrag zu Ziff. 2 erforderliche Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt vor. Voraussetzung hierfür ist es, dass dem Recht oder der Rechtslage der klagenden Partei eine gegenwärtige Gefahr oder Unsicherheit droht, die das erstrebte Urteil beseitigen kann (vgl. st. Rspr. BGH, Urteil vom 22.06.1977 – VIII ZR 5/76, Rn 11,

juris mwN). Eine Klage auf Feststellung der Verpflichtung zum Ersatz bereits eingetretener und künftiger Schäden, bei Verletzung absoluter Rechtsgüter, ist zulässig, wenn die Möglichkeit eines Schadenseintritts besteht. Das Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund gegeben ist, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. BGH, Urteil vom 20.03.2001 – VI ZR 325/99, Rn. 11, juris). Vorliegend ist möglicherweise das allgemeine Persönlichkeitsrecht der klagenden Partei betroffen. Die nicht von den Bestimmungen der DS-GVO gedeckte Übermittlung oder Verarbeitung personenbezogener Daten kann eine Verletzung des allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen (vgl. OLG Frankfurt, Urteil vom 14. April 2022 – 3 U 21/20 –, Rn. 29, juris mwN; Schleswig-Holsteinisches Oberlandesgericht, Urteil vom 2. Juli 2021 – 17 U 15/21 –, Rn. 70, juris). Diese Möglichkeit des Schadenseintritts hat die klagende Partei nach den allgemeinen zivilprozessualen Grundsätzen substantiiert darzutun. Gemessen an diesen Voraussetzungen wird die klagende Partei den Anforderungen an die Darlegung des Feststellungsinteresses gerecht. Hinsichtlich der weiteren materiellen Schäden hat diese zunächst ausgeführt, es könne noch nicht abgesehen werden, welche Dritte Zugriff auf die Daten erhalten hätten und für welche kriminellen Zwecke diese missbraucht würden. Die klagende Partei hat ihren Vortrag sodann dahingehend konkretisiert, dass es möglich erscheine, dass sie eine Vielzahl an betrügerischen Anrufen erhalte. Es sei nicht selten so, dass sich Anrufer als Bankmitarbeiter ausgeben würden, um an sensible Kontodaten zu gelangen. Gerade durch die Kenntnis der Daten bestehe die Möglichkeit, dass die Anrufer derart überzeugend aufträten, dass die Angerufenen auf die Betrugsmasche hereinfallen würden. Auf dieser Grundlage besteht zumindest die Möglichkeit, dass ein weiterer materieller Schaden hervorgerufen wird.

Soweit die Beklagte meint, es liege - hinsichtlich der immateriellen Schäden - ein Verstoß gegen den Grundsatz der Einheitlichkeit des Schmerzensgeldes vor, so verfängt dieser Einwand nicht. Unter Berücksichtigung des weiteren Prozessvorbringens der klagenden Partei ist der Antrag gem. § 133 BGB dahingehend auszulegen, dass diese ausschließlich den Ersatz künftiger materieller Schäden begehrt. Die klagende Partei hat ihren Vortrag nämlich dahingehend konkretisiert, dass diese lediglich die Feststellung materieller Schäden begehre. Zudem kann auch dem Wortlaut des Klageantrages nicht entnommen werden, dass die klagende Partei die Feststellung immaterieller Schäden

begehrt. Dieser spricht lediglich allgemein von „Schäden“, konkretisiert diese aber nicht weiter.

II. Die Klage ist jedoch nur teilweise begründet. Der klagenden Partei steht ein Anspruch gegen die Beklagte auf Ersatz ihres immateriellen Schadens, der außergerichtlichen Rechtsanwaltskosten jeweils nebst Zinsen in tenorierter Höhe sowie Ersatz weiterer materieller Schäden zu. Alle weiteren mit der Klage geltend gemachten Ansprüche stehen der klagenden Partei hingegen nicht zu.

1. Die klagende Partei hat gegen die Beklagte einen Anspruch auf Zahlung eines immateriellen Schadensersatzes in Höhe von 300,00 Euro gemäß § 82 Abs. 1 DS-GVO.

Der zeitliche Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) ist nach Art. 99 Abs. 2 DS-GVO eröffnet, weil sich nach dem unbestrittenen Vortrag der klagenden Partei der streitgegenständliche Vorfall im Jahre 2019 ereignete. Auch ist die DS-GVO räumlich (Art. 3 Abs. 1 DS-GVO) und sachlich anwendbar (Art. 2 Abs. 1 DS-GVO).

Art. 82 Abs. 1 DS-GVO legt fest, dass jeder Person, der wegen eines Verstoßes gegen die DS-GVO, der in einer Datenverarbeitung liegt, ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat. Diese Voraussetzungen sind vorliegend erfüllt. Die Beklagte hat gegen die DS-GVO verstoßen (dazu unter a.) und den ihr obliegenden Exkulpationsnachweis nicht geführt (dazu unter b.). Die klagende Partei hat einen ersatzfähigen Schaden erlitten (dazu unter c.), der kausal auf die Verstöße der Beklagten zurückzuführen ist (dazu unter d.) und den die Kammer auf 300,00 Euro beziffert (dazu unter e.).

a. Die Beklagte hat als Verantwortliche nach Art. 4 Nr. 7 DS-GVO gegen die Vorschriften der DS-GVO verstoßen. Die Beklagte hat keine geeigneten technischen und organisatorischen Maßnahmen auch im Hinblick auf Voreinstellungen getroffen, um die personenbezogenen Daten der klagenden Partei zu schützen (dazu unter aa. und bb.). Über das Vorliegen der weiteren von der klagenden Partei behaupteten Verstöße der Beklagten gegen die DS-GVO braucht die Kammer nicht zu entscheiden (dazu unter cc.).

aa) Die Beklagte hat gegen die ihr gemäß Art. 25 Abs. 1 DS-GVO auferlegte Obliegenheit verstoßen, geeignete Maßnahmen zu treffen, um die Rechte der klagenden Partei und ihre personenbezogenen Daten zu schützen.

Nach Art. 25 Abs. 1 DS-GVO hat der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Unter Verarbeitung fällt nach Art. 4 Nr. 2 DS-GVO u.a. die Offenlegung personenbezogener Daten durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Hiervon werden alle Vorgänge erfasst, durch die der Verantwortliche personenbezogene Daten anderen Stellen in der Weise zugänglich macht, dass diese Kenntnis vom Informationsgehalt der betreffenden Daten erlangen können (Kühling/Buchner/Herbst, DS-GVO BDSG, 3. Auflage 2020, DS-GVO Art. 4 Nr. 2 Rn. 29).

Es handelt sich vorliegend um personenbezogene Daten. Hierunter versteht man nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die durch das Scraping unstreitig abgegriffenen Daten der klagenden Partei betrafen jedenfalls die Telefonnummer und den Vor- und Nachnamen der betroffenen Person. Damit ist es möglich, die klagende Partei zu identifizieren. Es handelt sich mithin um personenbezogene Daten.

Eine Verarbeitung im vorgenannten Sinne liegt vor. Das von der Beklagten zur Verfügung gestellte Kontakt-Importer-Tool ermöglichte es unbekannten Dritten, mit den von den Dritten eingegebenen Telefonnummern Nutzerprofile aufzufinden und die darauf befindlichen öffentlich einsehbaren, personenbezogenen Daten der Nutzer abzugreifen und mit der eingegebenen Telefonnummer zu verknüpfen. Das Kontakt-Importer-Tool konnte von jedermann genutzt werden, mit der Folge, dass die Beklagte durch die Ausgestaltung dieses Tools die Daten ihrer Nutzer zum Abruf durch Dritte grundsätzlich ermöglichte und jedermann zugänglich machte.

Die von der Beklagten implementierten Sicherheitsmaßnahmen waren nicht ausreichend, um die Rechte der klagenden Partei und ihre personenbezogenen Daten insbesondere

vor unbefugter oder unrechtmäßiger Verarbeitung durch Dritte zu schützen. Dabei kann dahinstehen, ob die Beklagte die von ihr behaupteten Maßnahmen zur Bekämpfung von Scraping tatsächlich ergriffen hat, denn diese Maßnahmen waren jedenfalls für sich allein nicht geeignet, einen angemessenen Schutz der personenbezogenen Daten der klagenden Partei zu gewährleisten.

Die (angeblich) von der Beklagten implementierten Maßnahmen in Form von Ratenbegrenzung und Bot-Erkennungsmaßnahmen waren für die Zwecke des Art. 25 Abs. 1 DS-GVO nicht ausreichend, weshalb die Beklagte gegen Art. 25 Abs. 1 DS-GVO verstoßen hat. Insoweit befindet sich die Kammer im Einklang mit der irischen Datenschutzbehörde, die ebenfalls der Beklagten vorwirft, keine hinreichenden Sicherheitsmaßnahmen getroffen und damit gegen Art. 25 Abs. 1 DS-GVO verstoßen zu haben. Dabei berücksichtigt die Kammer, dass Scraping weit verbreitet und damit zum Zeitpunkt des Vorfalls unstreitig auch ein der Beklagten bekanntes Risiko gewesen ist. Hinsichtlich der von der Beklagten eingesetzten Übertragungsbeschränkungen war es nach dem eigenen Vortrag der Beklagten möglich, diese Beschränkungen zu umgehen. Trotz Kenntnis dieser Möglichkeit und auch des grundsätzlichen Risikos von „Scraping“ hat es die Beklagte indessen unterlassen, wirksame weitergehende Maßnahmen zu treffen, was hier nach Auffassung der Kammer jedoch notwendig gewesen wäre. Es wäre für die Beklagte beispielsweise möglich gewesen, das Kontakt-Importer-Tool derart auszugestalten, dass eine Suche nach Nutzerprofilen nicht nur anhand von Telefonnummern erfolgen kann. Das Tool hätte beispielsweise neben der Telefonnummer weitere Variablen, wie den von dem Nutzer in seinem Adressbuch hinterlegten Vor- oder Nachname berücksichtigen können. Dies vor allem deshalb, weil Nutzer die Telefonnummern häufig mit dem dazugehörigen Klarnamen ihres Kontakts abspeichern. Entsprechend hat die Beklagte die Funktionsweise des Tools nach Bekanntwerden des Vorfalls auch umgestaltet, was zeigt, dass die Nutzbarkeit der Plattform hierdurch nicht wesentlich beeinträchtigt wurde.

bb) Weiterhin hat die Beklagte gegen Art. 25 Abs. 2 DS-GVO verstoßen, indem sie keine geeigneten technischen und organisatorischen Maßnahmen getroffen hat, die sicherstellen würden, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Eine Verarbeitung im oben genannten Sinne liegt vor. Die Suchbarkeit umfasste automatisch die Telefonnummer der Nutzer. Die Suchbarkeits-Einstellungen hatte die Beklagte im hier relevanten Zeitraum auf „Alle“ voreingestellt, das heißt, dass jedermann mit der Telefonnummer nach einem Nutzerprofil suchen konnte und von jedermann auch über das Kontakt-Importer-Tool eine Verknüpfung zwischen Telefonnummer und dazugehörigem Nutzerprofil hergestellt werden konnte. Eine Ausnahme bestand nur dann, wenn der Nutzer nach seiner Registrierung die entsprechende Suchbarkeits-Einstellung in seinen Privatsphäre-Einstellungen aktiv änderte. Mit der Bereitstellung dieses Systems machte die Beklagte die personenbezogenen Daten der klagenden Partei ohne das Eingreifen der klagenden Partei einer unbestimmten Anzahl von Personen zugänglich. Entsprechend hat auch die irische Datenschutzbehörde einen Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO angenommen.

Im Hinblick auf die von der Beklagten behaupteten Sicherheitsmaßnahmen gilt das zuvor unter aa) Ausgeführte entsprechend.

cc) Es kommt an dieser Stelle nicht darauf an, ob die Beklagte zudem auch gegen Art. 13, 14, 33, 34 Abs. 1 und 2, Art. 15 DS-GVO verstoßen hat, indem sie (1) die klagende Partei nicht ausreichend im Sinne der DS-GVO über die Verarbeitung der personenbezogenen Daten informierte, weiterhin (2) die klagende Partei nach dem Scraping-Vorfall nicht von der Verletzung des Schutzes der personenbezogenen Daten der klagenden Partei und auch die zuständige Datenschutzbehörde nicht benachrichtigte und (3) der klagenden Partei in nicht ausreichendem Maße oder zu spät Auskunft erteilt hat.

(i) Nicht jeglicher Verstoß gegen die DS-GVO ist anspruchsbegründend im Sinne des Art. 82 Abs. 1 DS-GVO ist. Vielmehr ist erforderlich, dass der Verstoß im Rahmen einer Verarbeitung der personenbezogenen Daten begangen worden ist (vgl. EuGH, Urteil vom 04.05.23, Rs. C-300/21 = DB 2023, 1280, 1282; Ehmann/Selmayr/Nemitz, Datenschutz-Grundverordnung, 2. Auflage 2018; DS-GVO Art. 82 Haftung und Recht auf Schadenersatz, Rn. 8; Sydow/Marsch/Kreße, DS-GVO | BDSG, 3. Auflage 2022, DS GVO Art. 82 Haftung und Recht auf Schadensersatz, Rn. 7; Gola/Heckmann/Gola/Piltz, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, DS-GVO Art. 82 Haftung und Recht auf Schadenersatz Rn. 5; Schaffland/Wiltfang/Schaffland/Holthaus, Datenschutz-Grundverordnung/Bundesdaten schutzgesetz, Artikel 82 Haftung und Recht auf Schadenersatz, Rn. 5). Zwar ist Art. 82

Abs. 1 DS-GVO dem Wortlaut nach weit gefasst, wenn als Voraussetzung dort lediglich ein Verstoß gegen die DS-GVO verlangt wird. Art. 82 Abs. 1 DS-GVO ist jedoch unter Berücksichtigung des Art. 82 Abs. 2 DS-GVO und des Erwägungsgrunds 146 DS-GVO dahingehend auszulegen, dass von der Schadensersatzpflicht nur solche Schäden umfasst sind, die auf Grund einer Verarbeitung entstehen. Dies folgt zum einen aus dem Wortlaut des Absatzes 2 des Art. 82 DS-GVO, der die Anspruchsverpflichtung regelt, und explizit auf eine Verarbeitung Bezug nimmt. Anknüpfungspunkt für eine Haftung ist also eine der Verordnung nicht entsprechende Verarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO. Dies steht im Einklang mit dem Wortlaut des Erwägungsgrundes 146 DS-GVO, wonach der Verantwortliche oder der Auftragsverarbeiter Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit der DS-GVO nicht im Einklang stehen, ersetzen sollte. Daher kommt nur ein Verstoß durch die Verarbeitung selbst in Betracht, die verordnungswidrig sein muss, um einen Schadensersatzanspruch auszulösen (vgl. LG Düsseldorf, Urteil vom 28.10.2021 – 16 O 128/20, ZD 2022, 48; LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818; abweichend u.a. OLG Köln, Urteil vom 14. Juli 2022 – I-15 U 137/21 - juris).

Das Verhalten der Beklagten, durch welches sie möglicherweise ihre Auskunfts-, Informations- oder Benachrichtigungspflichten verletzt hat, stellt evident keine Verarbeitung im Sinne der oben genannten Legaldefinition dar und löst deshalb auch keinen Schadensersatzanspruch gemäß Art. 82 Abs. 1 DS-GVO aus, wie mit dem Klageantrag zu Ziffer 3 geltend gemacht.

(ii) Ferner begründet ein bloßer Verstoß des Verantwortlichen gegen die DS-GVO, ohne dass eine Schadenfolge eintritt, keine Haftung (vgl. EuGH aaO). Einen *konkreten* ersatzfähigen Schaden durch die (vermeintliche) Verletzung der Auskunfts-, der Informations- und der Benachrichtigungspflicht durch die Beklagte hat die klagende Partei nicht einmal behauptet. So hat sie weder vorgetragen, dass ihr inzwischen ein materieller Schaden entstanden ist, noch welche Sicherheitsmaßnahmen sie nach Kenntnis eingeleitet hat. Selbst eine hinreichende Substantiierung dieser (bestrittenen) Behauptung unterstellt, wäre die klagende Partei mangels eines entsprechenden Beweisangebotes jedenfalls diesbezüglich beweisfällig geblieben.

b. Die Beklagte hat sich nicht gemäß Art. 82 Abs. 3 DS-GVO von der vermuteten Haftung befreit. Die Verantwortung des Anspruchsverpflichteten wird zunächst grundsätzlich vermutet. Nach Art. 82 Abs. 3 DS-GVO wird der Anspruchsverpflichtete von der Haftung

befreit, wenn er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Der Begriff der Verantwortlichkeit wird nicht definiert. Es kann vorliegend dahingestellt bleiben, ob dieser Begriff mit dem Begriff des Verschuldens nach der deutschen Rechtsterminologie gleichzusetzen ist oder ob Art. 82 DS-GVO als Gefährdungshaftungstatbestand 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.

Die Haftungsbefreiung greift bei 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; Kühling/Buchner/Bergt, a.a.O., Rn. 54; Spindler/Schuster/Spindler/Horváth, Recht der elektronischen Medien, 4. Auflage 2019, DS-GVO Art. 82 Haftung und Recht auf Schadensersatz, Rn. 11; Sydow/Marsch/Kreße, a.a.O., Rn. 20 („Mitverschulden in Höhe von 100%“)).

Die Beklagte hat fahrlässig gehandelt. Der Beklagten war das Risiko von „Scraping“ bekannt. Weiterhin war ihr bekannt, dass Übertragungsbeschränkungen umgangen werden können wie ihr auch bekannt war, dass die Suchbarkeit der Telefonnummer der Nutzer auch dann aufgrund ihrer Voreinstellungen gegeben war, wenn der Nutzer die diesbezügliche Zielgruppenauswahl auf „privat“ einstellte. Die Beklagte hätte deshalb erkennen können, dass Dritte das Kontakt-Importer-Tool wie geschehen ausnutzen würden. Sie hätte die missbräuchliche Verwendung des Tools rechtzeitig bemerken und effektive Gegenmaßnahmen einleiten müssen.

Die Beklagte kann sich auch nicht unter Hinweis auf ein mögliches Mitverschulden seitens der klagenden Partei von ihrer Haftung befreien. Selbst wenn man der klagenden Partei ein Mitverschulden anlasten wollte, weil diese durch die Privatsphäre-Einstellungen selbst bestimmen konnte, inwieweit ihre Telefonnummer suchbar ist, erreicht das (mögliche) Mitverschulden jedoch nicht die 100%-Schwelle, wodurch die Haftung der Beklagten ausgeschlossen wäre. Das fahrlässige Verhalten der Beklagten tritt nicht vollständig hinter dem Verhalten der klagenden Partei zurück.

c. Die klagende Partei erlitt durch das Verhalten der Beklagten einen konkreten ersatzfähigen immateriellen Schaden.

Der Begriff des Schadens im Sinne des Art. 82 Abs. 1 DS-GVO ist nach dem Erwägungsgrund 146 Satz 3 DS-GVO weit auszulegen. Die Auslegung soll den Zielen der DS-GVO in vollem Umfang entsprechen, auch dem Ziel der Sanktion und Prävention (BeckOK Datenschutzrecht, Wolff/Brink/Quaas, 42. Edition, Stand: 01.08.2022, DS-GVO Art. 82 Haftung und Recht aus Schadenersatz, Rn. 25c). Ausreichend ist gemäß Art. 82 Abs. 1 DS-GVO auch ein immaterieller Schaden. Die Erwägungsgründe 75 und 85 DS-GVO zählen beispielhaft auf, welche konkreten Beeinträchtigungen einen immateriellen Schaden darstellen können, darunter der Verlust der Kontrolle über die eigenen Daten. Allein der Umstand, dass eine betroffene Person in Folge eines Verstoßes gegen die DS GVO befürchtet, dass Ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, kann einen „immateriellen Schaden“ im Sinne der DS GVO darstellen (vgl. EuGH, Urteil vom 14. Dezember 2023 (C-340/21) Rn. 86). Eine Erheblichkeitsschwelle muss nicht überschritten werden (vgl. EuGH, Urteil vom 04.05.23, Rs. C-300/21 = DB 2023, 1280, 1282).

Vorliegend erlitt die klagende Partei einen erheblichen Kontrollverlust über ihre personenbezogenen Daten durch die Offenbarung ihrer Telefonnummer, insbesondere auch, aber nicht nur durch die Verknüpfung dieser Telefonnummer mit weiteren personenbezogenen Daten wie Vor- und Nachname der klagenden Partei. Die abgegriffenen und veröffentlichen Daten bedeuten für die klagende Partei ein hohes Risiko, dass diese Daten unbefugt benutzt werden. Dies auch deshalb, weil die Daten im Darknet veröffentlicht wurden, welches bei entsprechender Kenntnis bekanntermaßen für jedermann zugänglich ist. 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 der klagenden Partei, sodass ein Schadensersatzanspruch gerechtfertigt ist.

d. Es liegt auch die erforderliche Kausalität zwischen dem Verstoß der Beklagten gegen § 25 Abs. 1 DS-GVO (vgl. oben unter II, 1. a, aa) und dem Schaden der klagenden Partei vor, nicht dagegen im Hinblick auf den Verstoß gegen § 25 Abs. 2 DS-GVO (vgl. oben unter II 1. a, bb), weil die klagende Partei die Voreinstellung der Suchbarkeit der Telefonnummer zunächst von „alle“ auf „Friends“ und dann erst am 6. Januar 2018 wieder auf „alle“ („Every“) umgestellt hatte. Die Voreinstellung hat sich daher auf den bei ihr entstanden Schaden nicht ausgewirkt. Der Schaden der klagenden Partei war für die Beklagte vorhersehbar. Ein völlig atypischer Verlauf, der die Kausalität ausschließen würde, liegt nicht vor.

e. Ein Schadensersatz in Höhe von 300,00 Euro ist vorliegend angemessen.

Art. 82 Abs. 1 DS-GVO macht bezüglich der Höhe des Schadensersatzanspruchs keine Vorgaben, sodass die Ermittlung gemäß § 287 ZPO dem Gericht obliegt. Für die Bemessung der Höhe des Schadensersatzes können die Kriterien des Art. 83 Abs. 2 DS-GVO herangezogen werden, wie etwa die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs und des Zwecks der betreffenden Verarbeitung, weiterhin das Ausmaß des von der klagenden Partei erlittenen Schadens sowie die betroffenen Kategorien personenbezogener Daten (vgl. LG München I, Urteil vom 09.12.2021 – 31 O 16606/20; BeckOK Datenschutzrecht, Wolff/Brink/Quaas, a.a.O., Rn. 31). Zudem ist das Ziel des Schadensersatzanspruchs nach Art. 82 Abs. 1 DS-GVO zu berücksichtigen, Verstöße gegen die DS-GVO effektiv und abschreckend zu sanktionieren. Wesentlich für die Bemessung der Höhe des Schadensersatzes sind die konkreten Umstände des Einzelfalls.

Vorliegend muss bei der Bemessung der Höhe des immateriellen Schadensersatzes der klagenden Partei zunächst berücksichtigt werden, dass der Kontrollverlust über die Daten hier zwar tatsächlich eingetreten ist und die oben beispielhaft dargestellten Risiken für die klagende Partei birgt. Allerdings ist auch zu berücksichtigen, dass die Gefahr von Spam- oder Phishing-SMS, sowie von mit krimineller Intention geführten Telefongesprächen auch zum allgemeinen Lebensrisiko gehört, mit welcher auch ohne den Verstoß gegen die DS-GVO gerechnet werden muss. Eine gesunde Skepsis gegenüber Anrufen oder SMS ist damit in gewisser Weise ohnehin angezeigt. In ganz erheblichem Maße wirkt sich vorliegend auch aus, dass die klagende Partei den Kontrollverlust ihrer Daten durch einen Wechsel ihrer Telefonnummer, die mit vergleichsweise wenig Umständen und Kosten verbunden ist, beseitigen kann. Aus diesem Grunde hatte die Kammer der Behauptung der klagenden Partei, wonach diese unter psychischen Beeinträchtigungen wie einem Unwohlsein leide, nicht weiter nachzugehen. Berücksichtigt werden muss daneben für die Bemessung der Schadensersatzhöhe auch die gesetzgeberisch beabsichtigte abschreckende Wirkung des Schadensersatzes, wobei die Kammer die hohe Abschreckungswirkung insbesondere in der Gesamtsumme aller immateriellen Schadensersatzansprüche gegen die Beklagte erblickt und berücksichtigt, dass das Allgemeininteresse im Schwerpunkt nach Art. 83 DS-GVO durch die Verhängung von Bußgeldern gewahrt wird. Die Höhe des von der Kammer angesetzten immateriellen Schadensersatzanspruchs berücksichtigt danach auch den Grundsatz der Verhältnismäßigkeit.

Dass sich der Verstoß der Beklagten gegen Art. 25 Abs. 2 DS-GVO vorliegend nicht ausgewirkt hat, schlägt sich nicht in der Höhe des zuzusprechenden Schadensersatzes nieder, weil der immaterielle Schaden, der empfundene Kontrollverlust über die Daten, gleich ist. Unter Abwägung dieser gesamten Gesichtspunkte erachtet die Kammer den ausgeurteilten (immateriellen) Schadensersatz für angemessen, aber auch ausreichend.

2. Die Entscheidung über die Zinsen folgt aus § 291, § 288 Abs. 1 BGB beginnend ab dem Tag nach Klagezustellung.

3. Der Feststellungsantrag zu Ziff. 2 ist im tenorierten Umfang begründet. Er war im Hinblick auf das feststehende Schadensereignis wie erfolgt zu präzisieren, weil er ansonsten zu weit gefasst gewesen wäre. Ein zulässiger Feststellungsantrag ist begründet, wenn die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vorliegen, also ein haftungsrechtlich relevanter Tatbestand gegeben ist, der zu möglichen künftigen Schäden führen kann (vgl. BGH, Beschluss vom 9. 1. 2007 - VI ZR 133/06, Rn. 6, beck-online). Es bedarf im Rahmen der Begründetheit - entgegen der Auffassung der Beklagten - keiner darüberhinausgehenden, gewissen Wahrscheinlichkeit des Schadenseintritts. An der Erforderlichkeit eines solchen zusätzlichen Begründungselements hat der BGH - jedenfalls für den Fall, dass Gegenstand der Feststellungsklage ein befürchteter Folgeschaden aus der Verletzung eines deliktsrechtlich geschützten absoluten Rechtsguts ist – Zweifel geäußert (vgl. BGH, Urteil vom 16.01.2001 – VI ZR 381/99). Streitgegenständlich sind die nicht von den Bestimmungen der DS-GVO gedeckten Übermittlungen oder Verarbeitungen personenbezogener Daten, welche eine Verletzung des allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen können (siehe dazu bereits unter I. 2. b). Die erkennende Kammer schließt sich diesbezüglich der vom Bundesgerichtshof vertretenen Ansicht ausdrücklich an. Demnach reicht vorliegend bereits die Möglichkeit eines Schadens aus. Es liegen, wie dargelegt, die Voraussetzungen des Schadensersatzanspruches aus Art. 82 Abs. 1 DS-GVO vor. Auch die Möglichkeit künftiger materieller Schäden ist zu bejahen. Diese Möglichkeit folgt – wie bereits angeführt – daraus, dass nicht absehbar ist, welche Dritte möglicherweise Zugriff auf die Daten erhalten haben und für welche kriminellen Zwecke diese möglicherweise missbraucht werden. Es erscheint eben nicht von vorneherein ausgeschlossen, dass die klagende Partei z.B. betrügerische Anrufe erhält, welche sich durch Ausgabe als Bankmitarbeiter Zugriff zu sensiblen Kontodaten der klagenden Partei erschleichen.

4. Der klagenden Partei stehen keine Unterlassungsansprüche gemäß den Klageanträgen zu 4 a) und b) aus § 1004 Abs. 1 S. 2, § 823 Abs. 1 BGB oder § 1004 Abs. 1 S. 2, § 823 Abs. 2 BGB iVm Art. 25 Abs. 1 u. 2 DS-GVO oder wegen Verletzung einer vertraglichen Nebenpflicht nach § 241 Abs. 2 BGB zu.

a. Ein Unterlassungsanspruch scheitert bereits an der Sperrwirkung der DS-GVO. Die DS-GVO sieht individualrechtliche Ansprüche in Art. 17 mit einem Löschungsanspruch und in Art. 82 mit einem Schadensersatzanspruch sowie in Art. 77 und 78 mit Ansprüchen gegen Aufsichtsbehörden vor, nicht aber einen Unterlassungsanspruch gegen den sog. Auftragsverarbeiter oder Verantwortlichen bei einem Datenschutzrechtsverstoß. Zugleich ist die DS-GVO angesichts des Anwendungsvorrangs des hierdurch unionsweit vereinheitlichten Datenschutzrechts als abschließend anzusehen (vgl. BGH, Urteil vom 3. Mai 2022 – VI ZR 832/20 –, Rn. 10, juris zum Auslistungsbegehren nach Art. 17 DS-GVO). Die klagende Partei kann ihren Anspruch nicht auf sonstige Vorschriften des nationalen deutschen Rechts stützen (vgl. aaO; LG Wiesbaden, Urteil vom 20. Januar 2022 – 10 O 14/21 –, Rn. 39, juris). Wie Art. 17 enthält auch Art. 32 DS-GVO, der die Sicherheit der Verarbeitung regelt, eine ausdifferenzierte Güterabwägung und unbestimmte Rechtsbegriffe wie „nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“ und „ein dem Risiko angemessenes Schutzniveau“, deren Prüfung nicht sinnvoll in das Vollstreckungsverfahren verlagert werden kann und nicht durch einen hiervon abweichenden Unterlassungsanspruch unterlaufen werden darf. Das Recht jeder betroffenen Person auf einen wirksamen gerichtlichen Rechtsbehelf nach Art. 79 Abs. 1 DS-GVO bezieht sich ausdrücklich nur auf die ihr aufgrund der DS-GVO zustehenden Rechte.

b. Selbst bei einer fehlenden Sperrwirkung der DS-GVO wären vorliegend die von der klagenden Partei begehrten, vorbeugenden Unterlassungsansprüche nicht gegeben.

Solche Ansprüche könnten nur auf § 1004 Abs. 1 S. 2 (analog) iVm § 823 Abs. 1 BGB und § 823 Abs. 2 BGB iVm Art. 25 Abs. 1 u. 2 DS-GVO gestützt werden, wobei die nicht von den Bestimmungen der DS-GVO gedeckte Übermittlung oder Verarbeitung personenbezogener Daten eine Verletzung des allgemeinen Persönlichkeitsrechts als sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen würde (vgl. OLG Frankfurt, Urteil vom 14. April 2022 – 3 U 21/20 –, Rn. 29, juris mwN; Schleswig-Holsteinisches Oberlandesgericht, Urteil vom 2. Juli 2021 – 17 U 15/21 –, Rn. 70, juris und vgl. oben unter I 2 b).

Voraussetzung eines jeden vorbeugenden Unterlassungsanspruch ist die Wiederholungsgefahr (vgl. BGH, Urteil vom 19. Oktober 2004 – VI ZR 292/03 –, Rn. 17, juris, mwN), an der es vorliegend fehlt. Zwar begründet eine vorausgegangene, rechtswidrige Beeinträchtigung (Erstbegehung) eine tatsächliche Vermutung für die Wiederholungsgefahr, an deren Widerlegung hohe Anforderungen zu stellen sind (vgl. BGH, Urteil vom 30. Oktober 1998 – V ZR 64/98 –, BGHZ 140, 1-11, Rn. 20). Vorliegend kann die Wiederholungsgefahr aber vollständig dadurch abgewendet werden, dass die klagende Partei die Suchbarkeit ihrer Telefonnummer auf der streitgegenständlichen Plattform der Beklagten auf „privat“ einstellt. Wie oben (unter 1.) ausgeführt, liegt der von der klagenden Partei gerügte und festgestellte Verstoß gegen die DS-GVO durch die Beklagte allein darin, dass es Dritten möglich war, die Telefonnummer der klagenden Partei mit den auf ihrem Profil ohnehin öffentlich zugänglichen Daten durch einen Missbrauch des Kontakt-Importer-Tools zu verknüpfen, weil die Suchbarkeit der Telefonnummer auf „für alle“ voreingestellt war bzw. die Beklagte hierüber nicht hinreichend informiert hat. Darin kann, wie die klagende Partei selbst vorträgt, nur dann ein Verstoß gegen die Datenschutzrechte gesehen werden, wenn die klagende Partei bei hinreichender Information bzw. anderer Voreinstellung ihre Telefonnummer (auch) hinsichtlich der Suchbarkeit auf „privat“ gestellt hätte bzw. nach Kenntnis von dem datenschutzrechtlichen Vorfall auf „privat“ stellt. Ob sie das vorliegend tatsächlich getan hat oder nicht, ist unerheblich, denn entweder hat sie damit die Wiederholungsgefahr ausgeräumt oder aber sie verstößt gegen den Grundsatz von Treu und Glauben nach § 242 BGB, indem sie sich selbst in einen unauflösbaren Selbstwiderspruch setzt. Eine Rechtsausübung kann dann unzulässig sein, wenn sich objektiv das Gesamtbild eines widersprüchlichen Verhaltens ergibt, weil das frühere Verhalten mit dem späteren sachlich unvereinbar ist und die Interessen der Gegenpartei im Hinblick hierauf vorrangig schutzwürdig erscheinen (vgl. BGH, Urteil vom 15. November 2012 – IX ZR 103/11 –, Rn. 12, juris). Diese engen Voraussetzungen sind vorliegend gegeben. Die klagende Partei kann nämlich nicht einerseits einen Verstoß gegen Art. 25 Abs. 1 u. 2 DS-GVO daraus herleiten, dass sie bei zutreffender Information bzw. richtiger Voreinstellung die Suchbarkeit der Telefonnummer auf „privat“ gestellt hätte, andererseits aber nach entsprechender Kenntnis hierüber die Suchbarkeit auf „für alle“ belassen, obwohl ihr die Umstellung aufgrund der entsprechenden Kenntnis hierüber unproblematisch möglich wäre, und dann darauf einen vorbeugenden Unterlassungsanspruch stützen.

Das Bestreiten der klagenden Partei, dass der Abgriff der Telefonnummer nur möglich gewesen sei, wenn deren Suchbarkeit auf „alle“ eingestellt gewesen sei, ist unbeachtlich, weil ohne greifbare Anhaltspunkte (vgl. zu diesem Kriterium BGH, Urteil vom 13. Juli 2021 – VI ZR 128/20 –, Rn. 22, juris). In den von ihr vorgetragenen, nicht streitgegenständlichen Fällen (vgl. Anlage K7) war die Suchbarkeit im Relevanten Zeitraum zumindest auch einmal für eine gewisse Zeit auf „alle“ gestellt, so dass diese Fälle als Anhaltspunkt für das Bestreiten der klägerischen Partei nicht herangezogen werden können.

Auch ist die klagende Partei den ausführlichen Darlegungen über die Maßnahmen, durch die die Beklagte ein Abgreifen der für alle suchbaren Telefonnummer mittlerweile verhindert hat, nicht substantiiert entgegengetreten. Ihr Bestreiten reicht hierfür nicht aus, weil die geänderte Funktionsweise des Kontakt-Importer-Tools auch für den Anwender ohne besondere Fachkunde überprüft werden kann. Nach dem Vortrag der Beklagten ist nämlich ein erneuter, gleicher Missbrauch des Kontakt-Importer-Tools durch dessen Neugestaltung erheblich erschwert bis unmöglich geworden. Im ersten Schritt habe die Beklagte das Kontakt-Importer-Tool derart geändert, dass wenn ein Nutzer seine Kontaktliste von seinem Mobiltelefon über das Kontakt-Importer-Tool auf die Plattform hochgeladen habe, der übereinstimmende Nutzer nur dann dem importierenden Nutzer angezeigt worden sei, wenn dieser zugleich einen Namen sowie die Telefonnummer für den hochgeladenen Kontakt importiert habe, der dem Namen des übereinstimmenden Nutzers geähnelt habe oder der übereinstimmende Nutzer den importierenden Nutzer bereits in seinen Kontakten gehabt habe (vgl. Duplik der Beklagten). Die Beklagte habe die Kontakt-Importer-Funktion schließlich dergestalt überarbeitet, dass nach dem Import der Kontakte nur noch eine Liste von Personen angezeigt werde, die die importierende Person kennen könnte, deren Telefonnummern aber nicht zwingend mit den importierten Kontakten übereinstimme („Menschen, die du kennen könntest“ - „people you may know-Funktion“, PYMK-Funktion; Duplik aaO). Diese Maßnahmen sind ohne Weiteres überprüfbar. Auch leuchtet unmittelbar ein, dass die Zuordnung eines Profils zu einer bestimmten Telefonnummer dadurch nicht mehr oder kaum noch möglich ist.

Soweit die Unterlassungsanträge über den oben unter 1. festgestellten, konkreten Verstoß gegen die DS-GVO hinausgehen, indem sie allgemeiner formuliert sind, fehlt es bereits an der Erstbegehung und damit an der tatsächlichen Vermutung der Wiederholungsgefahr. Insoweit besteht auch keine erstmalige konkret drohende Beeinträchtigung (vgl. zu diesem Erfordernis BGH, Urteil vom 5. Juli 2019 – V ZR 96/18 –,

Rn. 28, juris; Urteil vom 17. September 2004 – V ZR 230/03 –, BGHZ 160, 232-240, Rn. 11). Dies gilt etwa für: „die Telefonnummer auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Information darüber erlangt wurde“ gemäß dem Klageantrag zu 3 b).

Auch soweit der Antrag zu 3 a) über die Telefonnummer hinausgehende, personenbezogene Daten benennt, ist er jedenfalls deswegen unbegründet, weil keine Erstbegehung vorliegt. Dafür, dass über das Kontakt-Importer-Tool andere Daten als die jeweilige Telefonnummer abgegriffen wurden (und dadurch die Verbindung zu den ohnehin öffentlich einsehbaren Daten hergestellt wurde), ist die klagende Partei beweisfällig geblieben.

5. Auch der auf Auskunft gerichtete Klageantrag zu 5) hat keinen Erfolg.

Der allein in Betracht kommende datenschutzrechtliche Auskunftsanspruch der klagenden Partei nach Art. 15 DS-GVO ist durch Erfüllung nach § 361 BGB erloschen. Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Der klagenden Partei stand nach dieser Vorschrift grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortliche im Sinne des Art. 4 Nr. 7 HS. 1 DS-GVO verarbeiteten sie betreffenden personenbezogenen Daten zu. 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. Juni 2021 – VI ZR 576/19 –, Rn. 17 - 24, juris). Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen (aaO). Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen (aaO). Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (aaO). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll (aaO).

Vorliegend hat die Beklagte gemessen an diesen Grundsätzen, die Auskunft zum Teil vorgerichtlich und im Übrigen während des Rechtsstreits vollständig erfüllt. Das

Auskunftsverlangen der klagenden Partei gemäß dem Klageantrag zu 4) setzt sich aus zwei Teilen zusammen: einem allgemeinen, gerichtet auf die sie betreffenden personenbezogenen Daten und einem besonderen, gerichtet darauf, welche Daten durch welche Empfänger wann bei der Beklagten durch Scraping oder Anwendung des Kontakt-Importer-Tools erlangt werden konnten.

Das allgemeine Auskunftsverlangen hat die Beklagte mit ihren vorgerichtlichen Schreiben, inhaltsgleich zu den Anlagen K2 und Anlage B 16, erfüllt. Mit der Klagebegründung zeigt die klagende Partei nicht auf, welche Informationen ihr insoweit fehlen. Auch begegnet es keinen Bedenken, dass sich die klagende Partei die gewünschten Informationen mithilfe der ausführlichen Anleitung durch die Beklagte (vgl. Anlage K16) selbst von der Plattform herunterladen kann bzw. muss. Für die Auskunft und die Datenkopie ist keine bestimmte Form vorgeschrieben (BeckOK DatenschutzR/Schmidt-Wudy, 42. Ed. 1.11.2022, DS-GVO Art. 15 Rn. 83).

Was den besonderen Teil des Auskunftsverlangens angeht, kann die klagende Partei diesen – entgegen der Ansicht der Beklagten - auch auf Art. 15 DS-GVO stützen. Der Anspruch aus Art. 15 Abs. 1 Nr. 1 c DS-GVO umfasst die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden. Eine Offenlegung liegt schon dann vor, wenn Daten bloß zum Abruf bereitgehalten werden (Kühling/Buchner/Herbst DS-GVO Art. 4 Nr. 2 Rn 30). Der Ausdruck „andere Form der Bereitstellung“ in Art. 4 Nr. 2 DS-GVO verdeutlicht den Charakter der Offenlegung als „Zugänglichmachen“ (aaO, Rn. 33). Für die Auskunft über die Empfänger kommt es nicht darauf an, ob die Offenlegung rechtmäßig erfolgte (Gola/Heckmann/Franck DS-GVO Art. 15 Rn. 11). Auch entsprechende Schutzverletzungen sind insoweit mitzuteilen (aaO). Da somit ein Bereithalten der Daten zum Abruf für eine Offenlegung ausreichend ist, kann diese bereits in der Suchbarkeit der Telefonnummer des betroffenen Nutzers für alle sowie der Darstellung der öffentlich einsehbaren Daten in den jeweiligen Profilen gesehen werden. Der Begriff des Empfängers wird in Art. 4 Nr. 9 S. 1 DS-GVO als jede Stelle definiert, der personenbezogene Daten offengelegt wurden (Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 13 Rn. 28). Er muss kein Dritter iSv Art. 4 Nr. 10 DS-GVO sein (aaO).

Die Beklagte hat vorgetragen, dass unbekannte Dritte die auf dem Profil des jeweiligen Nutzers öffentlich einsehbaren Informationen abgegriffen und diese mit dessen Handynummer verknüpft haben. Damit hat sie sich darüber erklärt, welche Daten

betroffen waren. Sie hat im Termin zur mündlichen Verhandlung auf Nachfrage durch die Kammer zudem erklärt, ihr würden die entsprechenden Rohdaten aus den sich der Zeitpunkt des Abgriffes, der Umfang der Daten und auch die Person des Empfängers ergebe, die im Darknet veröffentlicht worden sein sollen, nicht vorliegen und sie habe sämtliche Auskünfte erteilt, die sie erteilen könne (vgl. Protokoll). Der Auskunftsanspruch erstreckt sich jedoch nur so weit, wie der Anspruchsgegner die Empfänger der Daten noch oder schon kennt (vgl. Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 15 Rn. 16). Soweit die Beklagte im Termin zur mündlichen Verhandlung mitgeteilt hat, dass ihr die Rohdaten für den damaligen Zeitraum nicht vorliegen, so löst auch dies keine Ergänzung des Auskunftsanspruchs aus, denn der Verantwortliche muss grundsätzlich keine Auskunft über Daten erteilen, die er in der Vergangenheit verarbeitet hat, über die er jedoch nicht mehr verfügt, wenn er sie nicht auf das Auskunftsersuchen hin gelöscht hat (vgl. Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 15 Rn. 8a). Letzteres ist vorliegend nicht ersichtlich. Ein Datenermittlungs- oder -beschaffungsanspruch ist, anders als die klagende Partei meint, mit dem Auskunftsrecht nach Art. 15 DS-GVO nicht verbunden.

Ob die klagende Partei darüber hinaus auch einen Anspruch auf Auskunft hat, wann genau ihre Daten abgegriffen wurden, kann dahinstehen, weil die Beklagte jedenfalls im Termin zur mündlichen Verhandlung angegeben hat, hierüber keine Kenntnis zu haben.

6. Als Teil des der klagenden Partei zustehenden Schadensersatzanspruchs hat sie gegen die Beklagte des Weiteren einen Anspruch auf Zahlung der außergerichtlichen Rechtsanwaltskosten, allerdings nur nach einem Gegenstandswert in Höhe von bis zu 800 €, so dass sich ein Anspruch in Höhe von 159,94 € (1,3 Geschäftsgebühr i. H. v. 114,40 € zzgl. Auslagenpauschale i. H. v. 20,00 € zzgl. Mwst.) ergibt. Vorgerichtlich sind als berechtigte Ansprüche nur der immaterielle Schaden (Wert: 300 €) und Auskunft (Wert: 500 €) verlangt worden (vgl. Anlage zur Klageschrift).

7. Die Entscheidung über die Zinsen betreffend den Anspruch gemäß oben unter 6 folgt ebenfalls aus § 291, § 288 Abs. 1 BGB beginnend ab dem Tag nach Klagezustellung.

III. Die Entscheidung über die Kosten beruht auf § 92 Abs. 1 Satz 1 ZPO, die Entscheidung zur vorläufigen Vollstreckbarkeit auf § 708 Nr. 11, § 711 S. 1 u. 2 ZPO.

Beglaubigt
Lüneburg, 19.02.2024

, Justizamtsinspektorin
als Urkundsbeamtin der Geschäftsstelle