Beglaubigte Abschrift

Landgericht Nürnberg-Fürth

Az.: 10 O 5189/23

IM NAMEN DES VOLKES

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.LEGAL Rechtsanwalts GmbH & Co. KG**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

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

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

wegen Persönlichkeitsrechtsverletzung

erlässt das Landgericht Nürnberg-Fürth - 10. Zivilkammer - durch den Richter am Landgericht als Einzelrichter aufgrund der mündlichen Verhandlung vom 12.08.2024 folgendes

Endurteil

I. Die Beklagte wird verurteilt, an die Klägerseite 250,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 19.10.2023 zu zahlen.

II. 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.

III. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 19.10.2023 zu zahlen.

IV. Im Übrigen wird die Klage abgewiesen.

V. Von den Kosten des Rechtsstreits hat der Kläger 75 %, die Beklagte 25 % zu tragen.

VI. Das Urteil ist vorläufig vollstreckbar. Beiden Parteien wird nachgelassen, die Vollstreckung durch die jeweils andere Partei gegen Sicherheitsleistung in Höhe von 110 % des jeweils vollstreckbaren Betrages abzuwenden, wenn nicht die jeweils andere Partei vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten über Ansprüche wegen eines Datenschutzvorfalls im Jahr 2019 bei der von der Beklagten betriebenen Plattform Facebook. Dabei fordert die Klagepartei wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016) Schadensersatz, Unterlassung, Auskunft, sowie Ersatz vorgerichtlicher Rechtsanwaltskosten.

Die Beklagte betreibt die Plattform Facebook unter der Domain www.facebook.com auf dem Gebiet der europäischen Union. Die Beklagte hatte im Jahr 2021 einen weltweiten Gesamtumsatz von 118 Milliarden €. Die Klagepartei nutzt die Plattform in Deutschland. Facebook ist eine Social-Media-Plattform, die unter anderem der sozialen Verknüpfung von Menschen dienen soll. Ein Nutzer kann hierbei ein Profil erstellen, über welches er persönliche Informationen einstellen kann.

Die Beklagte stellt dabei Einstellungsmöglichkeiten und Informationen zur Verfügung, damit Nutzer ihre Privatsphäre auf der Facebook-Plattform verwalten können. Zur leichteren Verbindung mit anderen Nutzern müssen die Nutzer bestimmte Informationen bei der Registrierung angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name und Geschlecht.

Bei Facebook gibt es verschiedene Einstellungsmöglichkeiten für die Einsehbarkeit der personenbezogenen Daten des jeweiligen Nutzers. Dabei wird zwischen der Zielgruppenauswahl und den Suchbarkeits-Einstellungen unterschieden.

Bei der Zielgruppenauswahl legt der Nutzer fest, welche anderen Nutzer einzelne Informationen auf seinem Facebook-Profil einsehen können. Dabei konnte ein Nutzer zwischen „öffentlich“ und „Freunde von Freunden“ als Personenkreis auswählen. Die Einstellung der Zielgruppenauswahl war standardgemäß auf „Freunde“ voreingestellt.

Die Suchbarkeits-Einstellungen legen fest, wer das Profil eines Nutzers anhand seiner Telefonnummer finden kann. Der Nutzer hatte die Möglichkeit diese Suchbarkeitseinstellung auf „Alle“, „Freunde von Freunden“ oder „Freunde“ einzustellen. Die Suchbarkeit für „Alle“ war voreingestellt. Ab Mai 2019 stand Nutzern die Option „Nur ich“ zur Verfügung. Im relevanten Zeitraum waren die Suchbarkeitseinstellungen der Klagepartei so voreingestellt, dass alle anderen Nutzer ihr Profil mithilfe der Telefonnummer finden konnten. Im vorliegenden Fall gab die Klagepartei auch die Telefonnummer bei Facebook an.

Über das „Contact-Import-Tool“ (im Folgenden: CIT) können andere Nutzer nur anhand der Eingabe der Telefonnummer gefunden werden. Dabei ist das automatisierte Sammeln von Daten (Scraping) ohne Erlaubnis durch die Nutzungsbedingungen der Beklagten verboten.

Bei Facebook gab es mehrschichtige Datenschutzinformationen. In den Einstellungen des jeweiligen Nutzerkontos wurden unter verschiedenen Menüpunkten Informationen zur Verarbeitung der personenbezogenen Daten des Nutzers und Einstellungsmöglichkeiten von Facebook angeboten. In der Datenrichtlinie von Facebook (Anlage B9) sind die meisten Informationen über die Verarbeitung personenbezogener Daten der Nutzer zusammengefasst. Ebenso waren im Hilfebereich und den Privatsphäre-Einstellungen Informationen zur Verwendung der personenbezogenen Daten der Nutzer vorhanden.

Unter „Kontoeinstellungen“ konnte ein Nutzer seine Telefonnummer hinterlegen und ändern. Unter dem Unter-Menüpunkt „Benachrichtigungen – Handy“ war die Information enthalten, dass standardmäßig nur der jeweilige Nutzer die Telefonnummer sehen kann. Über das CIT wurde an dieser Stelle nicht informiert. Durch einen weiterführenden Link „Mehr dazu“ gelangte man zu weiteren Informationen, die auch keine weiteren Informationen über das CIT enthielten. Im Hilfebereich bei Facebook informierte die Beklagte über potenzielle Verwendungszwecke der Mobilnummer (Anlage B6). Ein potenzieller Verwendungszweck war, interessante Menschen und Themen auf Facebook vorzustellen. In den Einstellungen, unter „Deine Privatsphäre“ und dort unter „Bestimme, wer dich finden kann“ konnten die Nutzer einstellen, dass sie nicht anhand der Mobilfunknummer gefunden werden wollten. Dort wurde weiter darüber informiert, dass „finden“ abhängig von den Einstellungen des Nutzers auch bedeuten kann, dass bei Eingabe der Telefonnummer in die Suchzeile der Website das zugehörige Nutzerprofil angezeigt werden kann. Eine weitere Information, dass das CIT auf das jeweilige Profil verweist und zu dessen konkreter Funktionsweise, ist nicht enthalten. Eine weitergehende Beschreibung der Verarbeitung der Telefonnummer seitens der Beklagten war nicht vorhanden. Wegen der relevanten Informationen im Hilfebereich, dem Privatsphäre-Tool und den Einstellungen wird auf die Abbildungen in der Klageschrift Bezug genommen.

Im Jahr 2019 erstellten unbekannte Dritte (Scraper) Telefonnummern und glichen diese über das CIT mit Profilen von Nutzern ab. Die Nutzerdaten im Profil wurden in der Folge abgeschöpft und mit der Handynummer zusammengeführt (Anlage B 11).

Am 03.04.2021 veröffentlichte der Business Insider einen Artikel, wonach Informationen einer Vielzahl von Facebook-Nutzern von Dritten im Internet zugänglich gemacht worden seien. Die Be-

klagte wandte sich mit einem am 06.04.2021 in Facebook zugänglichen Artikel an ihre Nutzer (Anlage B 10). Eine Benachrichtigung seitens der Beklagten hinsichtlich der Verletzung des Scraping-Vorfalls an die zuständige Aufsichtsbehörde oder die Klagepartei persönlich erfolgte nicht.

Mit Anwaltsschreiben (Anlage K1) forderte die Klagepartei die Beklagte zur Zahlung von 500,00 € immateriellen Schadensersatzes und zur Unterlassung zukünftiger Zugänglichmachung der klägerischen personenbezogenen Daten an unbefugte Dritte auf. Zudem verlangte sie Auskunft im Rahmen des Art. 15 DSGVO über den Scraping-Vorfall. Wegen der Einzelheiten des Auskunftsbegehrens wird Bezug genommen auf die Anlage K1. Die Beklagte wies die Ansprüche auf immateriellen Schadensersatz und auf Unterlassung zurück und erteilte Auskünfte gegenüber der Klagepartei. Wegen der Einzelheiten wird Bezug genommen auf die Anlage B16.

Die Klagepartei behauptet, es seien Telefonnummern von den Facebook-Profilen der Facebook-Nutzer gescrapt worden. Mithilfe des CIT sei es möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren. Die Einstellungen zur Datensicherheit seien nur als Teil einer Masse an schwer verständlichen Informationen und unklaren Angaben für Nutzer auffindbar. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalten und nicht selbstständig ändern würde. Ein Nutzer könne keine sicheren Einstellungen erreichen, weil diese undurchsichtig und kompliziert seien.

Die Klagepartei trägt weiter vor, in der Messenger-App habe es separate Privatsphäre-Einstellungen mit mindestens drei unterschiedlichen Einstellungsmöglichkeiten für die Verwendung der Telefonnummer gegeben.

Die Klagepartei behauptet, die Scraper hätten eine Sicherheitslücke bei der Beklagten ausgenutzt. Es sei denkbar einfach gewesen, das CIT für kriminelle Zwecke zu missbrauchen. Die Beklagte habe keinerlei Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des CIT zu verhindern. So sei kein Mechanismus zur Überprüfung der Plausibilität der Anfragen der Scraper durch Blockieren ungewöhnlich vieler Anfragen derselben IP-Adresse bereitgehalten worden. Ebenso seien keine Sicherheits-Captchas durch die Beklagte verwendet worden. Die Scraper hätten lediglich fortlaufende Zahlenfolgen wie 000001, 000002 wahllos in das CIT importiert. Es seien vermutlich allein für die Rufnummer eines deutschen Mobilfunkanbieters, ca. 10.000.000 Anfragen gestellt worden. Mit dem Programm der Scraper sei es möglich, sämtliche Daten des Nutzers zu exportieren. Bei den öffentlich verbreiteten Daten handele es sich um Telefonnummer,

E-Mail-Adresse, Land, Wohnort, Geburtsdatum, Stadt und Beziehungsstatus und weitere korrelierende Daten der Klagepartei.

Die Klägerseite trägt vor, sie habe einen erheblichen Kontrollverlust über ihre Daten erlitten. Es bestünde bei der Klagepartei durch den erheblichen Kontrollverlust über ihre personenbezogenen Daten ein Zustand großen Unwohlseins und große Sorge über einen möglichen Missbrauch ihrer sie betreffenden Daten. Die Zuordnung von Telefonnummern zu weiteren Daten wie Mail-Adresse oder Anschrift würde böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie beispielsweise Identitätsdiebstahl, die Übernahme von Accounts oder gezielte Phishing-Nachrichten eröffnen. Die Klagepartei erhalte infolge des Scraping-Vorfalls unregelmäßig Kontaktversuche via SMS und E-Mail mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks.

Die Klagepartei behauptet weiter, wenn die Klägerseite angemessen zügig benachrichtigt worden wäre, so hätten zeitnah Schritte zur Risikominimierung und Absicherung eingeleitet werden können, um einen weiteren Schaden zu vermeiden.

Die Klägerseite meint im Wesentlichen, die Beklagte habe für die Verarbeitung der Telefonnummer der Klagepartei keine Rechtsgrundlage gemäß Art. 6 Abs. 1 Unterabsatz 1 DSGVO. Insbesondere läge keine wirksame Einwilligung der Klagepartei vor. Zudem habe die Beklagte nicht hinreichend über die Verarbeitung und die Zwecke der Verarbeitung informiert. Die Beklagte habe auch keine geeignete technische und organisatorische Maßnahme, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Außerdem seien die Konfiguration der Seiten und die Voreinstellungen von Facebook von der Beklagten nicht datenschutzfreundlich gestaltet. Des Weiteren habe es die Beklagte versäumt die Aufsichtsbehörden und die Klagepartei als Betroffene über den Scraping-Vorfall zu informieren. Die Klägerseite meint, ihr sei ein immaterieller Schaden entstanden. Die Beklagte sei im Wege ihrer Rechenschaftspflicht darlegungs- und beweisbelastet. Die Klägerseite ist zudem der Ansicht, die Klageanträge zu 1) bis 3) seien hinreichend bestimmt. Insbesondere bestünde auch ein Feststellungsinteresse bzgl. des Klageantrags zu 2). Zudem meint die Klagepartei, ein Unterlassungsanspruch sei auch im Anwendungsbereich der DSGVO gegeben.

Die Klagepartei **beantragt,**

1. **Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz**

in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

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

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

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

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

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

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 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, sämtliche datenschutzrechtliche relevante Themen seien über eine entsprechende Suche (z.B. nach dem Begriff „Handynummer“) leicht zu finden. Auch die Standard-Einstellung der Suchbarkeit auf „Alle“ entspräche dem Hauptzweck der Facebook-Plattform.

Es sei für Dritte nicht möglich gewesen, während des relevanten Zeitraums einen bestimmten Nutzer über das CIT unter Bezugnahme auf seine Telefonnummer zu identifizieren, die ausschließlich für die Zwei-Faktor-Authentifizierung hinterlegt war. So seien auch keine Daten abgerufen worden, die nur zum Teil öffentlich gewesen seien. Die personenbezogenen Daten „Land“ und „Telefonnummer“ seien vom Facebook-Nutzerprofil der Klagepartei nicht abgerufen worden. Vielmehr sei die Telefonnummer von den Scrapern generiert und bereitgestellt worden.

Die Beklagte behauptet weiter, sie habe hinreichende Sicherheitsmaßnahmen bezüglich der Datenverarbeitungen getroffen. So habe sie Übertragungsbegrenzungen und -beschränkungen sowie eine Bot-Erkennung implementiert. Dabei werde diese auch fortlaufend weiterentwickelt. Zudem sei ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping beschäftigt. Die Beklagte habe ihre Systeme insofern an sich entwickelnde Scraping- Taktiken angepasst, um sicherzustellen, dass das Verknüpfen von Telefonnummern mit bestimmten Facebook-Nutzern durch das CIT nicht mehr möglich sei. Durch eine automatisierte Zurückweisung von vermeintlich auffälligen Telefonnummern hätten Scraping-Aktivitäten nicht verhindert werden können.

Die Beklagte trägt weiter vor, der Zugriff auf die Telefonnummer einer Person, selbst in Kombination mit den Profildaten in den durch Scraping abgerufenen Daten, erhöhe nicht das Risiko, dass diese Person Opfer von Betrug oder anderen schweren Internetverbrechen werde, da diese Informationen häufig weitergegeben würden.

Die Beklagte ist im Wesentlichen der Ansicht, die Klage sei hinsichtlich der Klageanträge zu 1)

bis 3) unzulässig, da die Klageanträge zu unbestimmt seien und dem Klageantrag zu 2) das Feststellungsinteresse fehle. Die Voraussetzungen des Art. 82 DSGVO lägen nicht vor, da kein Verstoß seitens der Beklagten gegen die DSGVO gegeben sei, die personenbezogenen Daten der Klagepartei immer öffentlich seien, kein kausaler Schaden gegeben sei und die Beklagte von der Haftung mangels Verschulden gemäß Art. 82 Abs. 3 DSGVO befreit sei. Die Klägerseite träfe bezüglich der anspruchsbegründenden Tatsachen die Darlegungs- und Beweislast. Des Weiteren sei das im Klageantrag zu 4) enthaltene Auskunftsbegehren am Maßstab des Art. 15 DSGVO bereits gemäß § 362 Abs. 1 BGB erfüllt.

Das Gericht hat die Klagepartei in der mündlichen Verhandlung informatorisch angehört.

Wegen der weiteren Einzelheiten wird auf die gewechselten Schriftsätze nebst Anlagen sowie das Protokoll der mündlichen Verhandlung Bezug genommen.

Entscheidungsgründe

Die Klage hat teilweise Erfolg.

A.

Die Klage ist teilweise zulässig. Hinsichtlich des Klageantrags zu 3a) ist die Klage unzulässig.

I.

Das Landgericht Nürnberg-Fürth ist international, sachlich und örtlich zuständig.

1.

Die internationale Zuständigkeit der deutschen Gerichte folgt aus Art. 79 Abs. 2 S. 2 DSGVO, da die Klägerseite ihren gewöhnlichen Aufenthalt in Deutschland hat.

Nach Art. 79 Abs. 2 S. 2 DSGVO können solche Klagen wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

Vorliegend hat die Klagepartei als betroffene Person (Art. 4 Nr. 1 DSGVO) ihren gewöhnlichen

Aufenthalt in Deutschland, weil sie ihren Wohnsitz in Deutschland hat. Die Beklagte ist Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO, da sie allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten der Klagepartei als Betreiberin der Plattform Facebook in Bezug auf deren Nutzung von Facebook entscheidet (Vgl. EuGH, Urteil vom 5. Juni 2018 – C-210/16 –, Rn. 30, juris; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 45, juris; LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 40, juris).

Auch verarbeitet die Beklagte bereits durch das Erheben personenbezogener Daten im Registrierungsprozess auf der Plattform Facebook. Die personenbezogenen Daten werden sodann für verschiedene Zwecke, wie aus der Datenrichtlinie (Anlage B9) oder der Unterseite „Wozu verwendet Facebook meine Mobilnummer“ (Anlage B6) zum Teil ersichtlich wird, weiterverarbeitet. Die Beklagte bestimmt als Betreiberin über die Zwecke der Verarbeitung. Die Beklagte ist vorliegend auch keine Behörde eines Mitgliedstaates, sondern ein Unternehmen in der Rechtsform der Limited.

Es kann vorliegend offenbleiben, ob Art. 79 Abs. 2 DSGVO die Zuständigkeitsvorschriften der EuGVVO verdrängen oder diese daneben anwendbar bleiben, da jedenfalls keine ausschließliche Zuständigkeit nach Art. 24 EuGVVO und eine Zuständigkeit nach Art. 18 Abs. 1 Alt. 2, Art. 17 Abs. 1 lit. c) EuGVVO gegeben ist (vgl. BGH, Urteil vom 29. Juli 2021 – III ZR 179/20 –, BGHZ 230, 347-389, Rn. 24; LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 41, juris). Die Klagepartei nutzt als Privatperson die auch in Deutschland durch die Beklagte gewerblich betriebene Plattform Facebook.

2.

Das Landgericht Nürnberg-Fürth ist jedenfalls in Folge des rügelosen Einlassens der Beklagten sachlich zuständig (§ 39 S.1 ZPO). Die örtliche Zuständigkeit folgt aus § 44 Abs. 1 S. 2 BDSG.

II.

Der Klageantrag zu 1) ist zulässig. Insbesondere ist er hinreichend bestimmt gemäß § 253 Abs. 2 Nr. 2 ZPO.

Grundsätzlich ist ein Klageantrag hinreichend bestimmt, wenn er den erhobenen Anspruch durch Bezifferung oder gegenständliche Beschreibung so konkret bezeichnet, dass der Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) klar abgegrenzt ist, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennbar sind, das Risiko des Unterliegens der Klagepartei nicht durch vermeidbare Ungenauigkeit auf den Beklagten abgewälzt

und eine etwaige Zwangsvollstreckung nicht mit einer Fortsetzung des Streits im Vollstreckungsverfahren belastet wird. Der Klageantrag ist der Auslegung zugänglich, wobei dafür auch die Klagebegründung heranzuziehen ist (vgl. Zöller/Greger, ZPO, 34. Auflage, § 253 Rn. 13 m.w.N.)

Nach Auslegung des Klageantrags zu 1) ist dieser dahingehend zu verstehen, dass die Klagepartei für mehrerer Verstöße der Beklagten gegen die DSGVO Schadensersatz verlangt. Es liegt dem Klageantrag zu 1) ein einzelner Streitgegenstand zugrunde, da ein einheitlicher Lebenssachverhalt und ein einzelner Antrag vorliegt. Wegen der von der Klagepartei vorgetragenen Verstöße der DSGVO soll das Scrapen der Daten durch Dritte erst möglich geworden sein und der Schaden resultieren. Der Klage ist zu entnehmen, dass die vorgetragenen Verstöße gegen die DSGVO nicht in einem Alternativverhältnis stehen sollen, sondern diese zusammenhängend betrachtet werden müssen. Nach dem Klagevortrag ist von einem einheitlich geltend gemachten Schaden durch den Scraping-Vorfall auszugehen, der sich im Nachgang an den Scraping-Vorfall durch weitergehende mögliche DSGVO-Verstöße der Beklagten potenziert oder verschlimmert hat (Vgl. So auch OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23, Rn. 51, juris; LG Kiel Urt. v. 12.1.2023 – 6 O 154/22, GRUR-RS 2023, 328).

lll.

Der Klageantrag zu 2) ist zulässig.

1.

Der Klageantrag zu 2) ist hinreichend bestimmt gemäß § 253 Abs. 2 Nr. 2 ZPO.

Eine Unbestimmtheit des Klageantrags zu 2) folgt insbesondere nicht daraus, dass der Antrag mit „alle materiellen künftigen Schäden […], die der Klägerseite […] entstanden sind und/oder noch entstehen werden“ formuliert ist. Nach Auslegung des Antrags unter Heranziehung der Schriftsätze der Klagepartei wird deutlich, dass die Klagepartei den Ersatz von zukünftig entstehenden materiellen Schäden mit dem Klageantrag zu 2) geltend macht, soweit diese nicht vom Klageantrag zu 1) umfasst sind (vgl. LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621; LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 55, juris).

2.

Die Klagepartei hat hinsichtlich des Klageantrags zu 2) ein Feststellungsinteresse gemäß § 256 Abs. 1 ZPO.

Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abge-

schlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss vom 9. 1. 2007 – VI ZR 133/06, NJW-RR 2007, 601).

Es ist vorliegend nicht auszuschließen, dass der Klagepartei bei den behaupteten Verstößen gegen die DSGVO und der Veröffentlichung ihrer personenbezogenen Daten ein Schaden auch künftig entstehen könnte (vgl. LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818, Rn. 39; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 37). Deswegen muss man bei verständiger Würdigung damit rechnen, dass zumindest eine gewisse Wahrscheinlichkeit für das Eintreten eines künftigen Schadens nicht auszuschließen ist.

IV.

Der Klageantrag zu 3a) ist unzulässig. Der Klageantrag zu 3b) ist zulässig.

1.

Der Klageantrag zu 3a) ist nicht hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Auch nach Auslegung des Klageantrags zu 3a) ist dieser zu unbestimmt.

Nach § 253 Abs. 2 Nr. 2 ZPO darf ein Unterlassungsantrag - und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung - nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen. Abweichendes kann gelten, wenn der gesetzliche Verbotstatbestand eindeutig und konkret gefasst ist, sein Anwendungsbereich durch eine gefestigte Auslegung geklärt ist oder der Kläger hinreichend deutlich macht, dass er kein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bestimmtheit des Unterlassungsantrags setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Die Wiedergabe des gesetzlichen Verbotstatbestands in der Antragsformulierung ist auch unschädlich, wenn sich das mit dem nicht hinreichend klaren Antrag begehrte durch Auslegung unter Heranziehung des Sachvortrags des Klä-

gers eindeutig ergibt und die betreffende tatsächliche Gestaltung zwischen den Parteien nicht in Frage steht, sondern sich deren Streit auf die rechtliche Qualifizierung der angegriffenen Verhaltensweise beschränkt. Eine auslegungsbedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (BGH, Urteil vom 26. Januar 2017 – I ZR 207/14 –, Rn. 18, juris m.w.N.).

Nach diesen Kriterien weist der Klageantrag zu 3a) keine hinreichende Bestimmtheit auf.

Das Gericht schließt sich insoweit den Ausführungen des LG Lübeck im Urteil vom 25. Mai 2023 (Aktenzeichen: 15 O 74/22) zu dem gleichlautenden Klageantrag 3a) an:

„Der Antrag beschränkt sich bereits im Ausgangspunkt nicht auf die Wiedergabe des – überdies nicht eindeutig und konkret gefassten - gesetzlichen Verbotstatbestandes des Art. 32 Abs. 1 DSGVO, sondern greift aus den dort genannten, zur Gewährleistung eines angemessenen Schutzniveaus zu berücksichtigenden Umständen (Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen) isoliert den Stand der Technik heraus. Unabhängig davon, dass damit mit Blick auf die Begründetheit des Antrages bereits der Maßstab des Art. 32 Abs. 1 DSGVO verkürzt wiedergegeben wird, ist aus dem Antrag bei dieser Fassung nicht hinreichend ersichtlich, welche Maßnahmen die Beklagte konkret zur Erfüllung ihrer Pflicht zu ergreifen hat. Ohne eine solche Konkretisierung ist für die Beklagte aber nicht klar, wann sie ihrer Pflicht Genüge getan hat und wann sie sich einer Haftung bzw. einer Vollstreckung aussetzen würde. Darüber hinaus wäre für das Vollstreckungsgericht - auch und insbesondere angesichts des unbestimmten Standes der Technik - nicht hinreichend deutlich, welche Maßnahmen zu welchem Zeitpunkt von der Beklagten veranlasst werden müssten. Dies gilt vorliegend umso mehr, als Gegenstand des Unterlassungsantrages nicht lediglich die Unterlassung der Gewährleistung desjenigen Schutzniveaus zum Zeitpunkt des streitgegenständlichen sogenannten „Scraping“ Vorfalles ist, sondern darüber hinausgehend und mit Blick auf etwaige zukünftige Entwicklungen und Verstöße die Unterlassung der Zugänglichmachung von personenbezogenen Daten über eine Software zum Importieren von Kontakten ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen. In der Sache beansprucht die Klägerseite damit aber lediglich ein Verbot im Umfang des - zudem nur unvollständig berücksichtigten - Gesetzeswortlaut des Art 32 Abs. 1 DSGVO. Die auslegungsbedürftige Antragsformulierung lässt sich auch durch Auslegung unter Heranziehung des Sachvortrags der Klägerseite nicht eindeutig präzisieren, da insoweit kein Vortrag erfolgt ist. Sie ist entgegen der Auffassung der Klägerseite auch nicht unter dem

Gesichtspunkt der Gewährung effektiven Rechtsschutzes ausnahmsweise hinzunehmen. Es steht der Klägerseite frei, eine hinreichende Konkretisierung zu erreichen, indem sie ihr Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert, was sie vorliegend nicht getan hat“ (LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 59 - 60, juris).

2.

Der Klageantrag zu 3b) ist zulässig. Insbesondere genügt er den Bestimmtheitsanforderungen gemäß § 253 Abs. 2 S. 2 ZPO.

Nach Auslegung des Klageantrags zu 3b) unter Heranziehung des gesamten Vortrags der Klägerseite ist deutlich, dass die Klagepartei eine Verarbeitung ihrer Telefonnummer erst nach einer hinreichend transparenten Information und übersichtlichen Gestaltung durch die Beklagte und ohne eine Solche ein Unterlassen der Verarbeitung ihrer Telefonnummer begehrt. Eine übersichtliche Gestaltung liegt nach Auslegung des Vortrags der Klagepartei erst vor, wenn explizit über die Verwendung der Telefonnummer in den hierauf gerichteten Einstellungsmöglichkeiten informiert wird (so auch LG Kiel Urt. v. 12.1.2023 – 6 O 154/22, GRUR-RS 2023, 328; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023).

B.

Die Klage ist, soweit sie zulässig ist, teilweise begründet. Die Klageanträge zu 1), 2) und 5) sind in dem aus dem Tenor ersichtlichen Umfang begründet. Im Übrigen ist die Klage unbegründet.

I.

Der Klageantrag zu 1) ist teilweise begründet. Der Klagepartei hat gegen die Beklagte einen Schadensersatzanspruch in Höhe von 250 € gemäß Art. 82 DSGVO.

1.

Der Anwendungsbereich der DSGVO ist eröffnet. Der sachliche Anwendungsbereich der DSGVO ist vorliegend gemäß Art. 2 DSGVO gegeben, da die Beklagte unstreitig personenbezogene Daten der Klagepartei über die Plattform Facebook verarbeitet und kein Ausschlussgrund des Art. 2 Abs. 2, 3 DSGVO vorliegt. Auch der räumliche Anwendungsbereich nach Art. 3 Abs. 1 DSGVO ist eröffnet. Die Beklagte ist als Betreiberin der Plattform Facebook unstreitig Verantwortliche i.S.d. Art. 82, Art. 4 Nr. 7 DSGVO (Siehe auch A.I. m. w. N.). Sie hat ihren Sitz in Irland und damit eine Niederlassung innerhalb der europäischen Union.

2.

Die Beklagte hat gegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 Unterabsatz 1 DSGVO verstoßen, da sie vorliegend nicht den Nachweis einer rechtmäßigen Verarbeitung der Telefonnummer der Klagepartei gemäß Art. 6 Abs. 1 Unterabsatz 1 DSGVO erbringt.

Die DSGVO enthält in Art. 5 Abs. 2 DSGVO eine spezifische Beweislastregelung. Danach ist der für die Datenverarbeitung Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO enthaltenen Grundsätze der Datenverarbeitung verantwortlich und muss deren Einhaltung nachweisen ("Rechenschaftspflicht"). Der Verantwortliche muss dies auch im zivilprozessualen Verfahren im Rahmen der Rechenschaftspflicht nachweisen können (vgl. EuGH Urt. v. 4.7.2023 - C-252/21, GRUR 2023, 1131 Rn. 95, 152, 154; EuGH Urt. v. 4.5.2023 - C-60/22, BeckRS 2023, 8967 Rn. 53; EuGH Urt. v. 24.2.2022 - C-175/20, BeckRS 2022, 2616 Rn. 77 f.; EuGH Urt. v. 24.2.2024 - C-175/20, EuZW 2022, 527 Rn. 77 f., 81; auch BVerwG Urt. v. 1.3.2022 - 6 C 7 /20, BVerwGE 175, 76 Rn. 49 f.; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 87 f., juris).

Soweit es deshalb um die materielle Rechtmäßigkeit der Verarbeitung geht, ist zu beachten, dass eine Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn mindestens einer der in Art. 6 Abs. 1 Unterabsatz 1 DSGVO genannten Tatbestände erfüllt ist (sog. Verbot mit Erlaubnisvorbehalt). Hierbei handelt es sich um einen für den Verantwortlichen bzw. Auftragsverarbeiter günstigen Umstand, den dieser bereits nach allgemeinen Grundsätzen beweisen muss (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 46). Zudem ergibt sich die Nachweispflicht für die Rechtmäßigkeit der Verarbeitung aus der in Art. 5 Abs. 2 DSGVO verankerten Rechenschaftspflicht (BeckOK DatenschutzR/Quaas, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 53; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 46).

Ein Verstoß gegen Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 DSGVO kann Schadensersatzansprüche nach Art. 82 DSGVO begründen (Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 164; BeckOK DatenschutzR/Albers/Veit, 44. Ed. 1.5.2023, DS-GVO Art. 6 Rn. 115).

Die Beklagte hat vorliegend die Telefonnummer unstreitig auf ihrer Plattform Facebook verarbeitet (Vgl. Anlage B16).

a.

Die Verarbeitung der Telefonnummer der Klagepartei im Hinblick auf die Suchbarkeit eines Facebook-Profils über die Telefonnummer durch das Contact-Import-Tool (im Folgenden: "CIT“) ist nicht zur Vertragserfüllung erforderlich i.S.d. Art. 6 Abs. 1 Unterabsatz 1 lit. b DSGVO. Die Be-

klagte kann hierfür nicht den erforderlichen Nachweis erbringen (So auch OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 94 ff., juris).

Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne des Art. 6 Abs. 1 Unterabsatz 1 1 lit. b DSGVO angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil, der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte. Der Umstand, dass eine solche Verarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist, ist insoweit für sich genommen unerheblich. Entscheidend für die Anwendung des in Art. 6 Abs. 1 Unterabsatz 1 lit. b DSGVO genannten Rechtfertigungsgrundes ist nämlich, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen (EuGH Urt. v. 4.7.2023 – C-252/21, GRUR-RS 2023, 15772 Rn. 98 f.).

Vorliegend ist es nicht der Fall, dass die Auffindbarkeit des Profils mittels der Telefonnummer zwingend unerlässlich ist, um den Hauptzweck des Vertrags zwischen den Parteien, das Anbieten und Nutzen eines Social-Media-Profils, zu erfüllen.

Durch das CIT ermöglicht die Beklagte einem Nutzer einen Abgleich der in seinem Smartphone gespeicherten Kontakte mit auf Facebook registrierten Nutzerprofilen, die ihr Profil mit einer Mobilfunknummer verknüpft haben. So können diese Kontakte auf der Facebook-Plattform gefunden und mit den dahinterstehenden Nutzern in Verbindung getreten werden.

Eine Notwendigkeit oder Erforderlichkeit einen Nutzer mittels seiner Telefonnummer zu finden, ist nicht gegeben. Dies ergibt sich auch nicht aus dem sozialen Zweck der Vernetzung von Menschen auf Social-Media-Plattformen. Die Nutzer können sich gegenseitig ebenfalls anhand ihres Namens finden. Es bestünde auch die Möglichkeit eine zufällig generierte Zahlenfolge den Nutzern als Nutzer-ID zur Verfügung zu stellen, anhand welcher sie sodann, wenn es im Interesse des Nutzers ist, diesen auf Facebook finden können. Dies gilt insbesondere im Hinblick auf den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO.

Überdies wird aus den nachträglich etablierten Suchbarkeitseinstellungen ersichtlich, dass der Klagepartei als Nutzer eine freie Wahl bleiben kann, ob sie mittels ihrer Telefonnummer gefunden werden möchte. Somit ist es keine zwingende Notwendigkeit die Facebook-Plattform nur mittels

öffentlich auffindbarer Telefonnummer zu nutzen. Die Funktion ist nützlich, um die im Mobiltelefon hinterlegten Kontakte auf Facebook zu finden, jedoch nicht zwingend erforderlich zur Vertragserfüllung. Eine Beeinträchtigung des gesamten Vertrages zwischen den Parteien und eine zwingende Notwendigkeit einer öffentlich Suchbarkeit des Nutzerprofils anhand der Telefonnummer sind nicht gegeben, weswegen nicht von einer erforderlichen Verarbeitung der Telefonnummer zur Erfüllung des Vertrages auszugehen ist.

b.

Die Beklagte hat kein überwiegendes berechtigtes Interesse an der öffentlichen Auffindbarkeit der Telefonnummer der Klagepartei. Jedenfalls kann sie den Nachweis hierfür nicht erbringen.

Verarbeitungen personenbezogener Daten sind nach Art. 6 Abs. 1 Unterabsatz 1 lit. f DSGVO unter drei kumulativen Voraussetzungen rechtmäßig. Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (EuGH Urt. v. 4.7.2023 – C-252/21, GRUR-RS 2023, 15772 Rn. 106).

Das Gericht kann vorliegend kein berechtigtes Interesse der Beklagten an der öffentlichen Auffindbarkeit der Telefonnummer der Klagepartei feststellen. Die Beklagte bleibt hierfür den Nachweis schuldig. Allein aus dem von der Beklagten vorgetragenen sozialen Zweckgedanken von Facebook als Social-Media Plattform lässt sich ein berechtigtes Interesse an der öffentlichen Auffindbarkeit eines Nutzerprofils anhand der Telefonnummer nicht begründen. Die soziale Interaktion bleibt auch ohne die Suchbarkeitsfunktion für jedermann anhand der Telefonnummer uneingeschränkt, da das Nutzerprofil auch anhand des Namens gefunden werden und so den gewünschten Interessen der Beklagten an der sozialen Verbindung von Menschen hinreichend Rechnung getragen werden kann.

Es fehlt jedenfalls an der Erforderlichkeit der Verarbeitung der Telefonnummer zur Verwirklichung eines berechtigten Interesses der Beklagten. Insoweit gelten die obigen Ausführungen auch für Art. 6 Abs. 1 Unterabsatz 1 lit. f DSGVO (Vgl. C.I.2.a.).

c.

Eine wirksame Einwilligung der Klagepartei gemäß Art. 6 Abs. 1 Unterabsatz 1 lit. a, Art. 7 DS-

GVO liegt nicht vor.

Nach Art. 6 Abs. 1 Unterabsatz 1 lit. a DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung für einen oder mehrere bestimmte Zwecke freiwillig in informierter Weise und unmissverständlich im Sinne von Art. 4 Nr. 11 DSGVO erteilt hat (EuGH Urt. v. 4.7.2023 - C-252/21, GRUR-RS 2023, 15772 Rn. 91 f.; EuGH Urt. v. 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f., OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 113, juris). Eine wirksame Einwilligung erfordert ein aktives Verhalten des Einwilligenden. Entsprechend Erwägungsgrund 32 Satz 3 folgt aus Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit der betroffenen Person keine wirksame Einwilligung des Betroffenen (vgl. EuGH Urt. v. 11.11.2020 - C-61/19, NJW 2021, 841 Rn. 35 f.; EuGH Urt. v. 1.10.2019 - C-673/17, NJW 2019, 3433 Rn. 51 ff., OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 115, juris).

Anhand dessen lässt sich vorliegend keine wirksame Einwilligung der Klagepartei in die Verarbeitung ihrer Telefonnummer zum Zweck der öffentlichen Suchbarkeit feststellen.

Eine wirksame Einwilligung liegt nicht in der Voreinstellung der Suchbarkeit der Telefonnummer auf „Alle“. Nach der Rechtsprechung ist ein aktives Tun des Nutzers erforderlich. Vorliegend hätte die Beklagte die Möglichkeit zur Einwilligung ähnlich eines „Opt-In“ und nicht eines „Opt-Out“ der Klagepartei anbieten müssen, damit ein aktives Tun gerichtet auf eine Einwilligung der Klagepartei vorliegt.

Im Abschluss der Registrierung mit dem Klick auf den Button „Registrieren“ ist ebenfalls keine Einwilligung nach den vorangestellten Kriterien zu sehen. Eine Einwilligung hätte insbesondere im Hinblick auf den Transparenzgrundsatz (Art. 5 Abs. 1 lit. a DSGVO) abgesondert vom Registrierungsvorgang oder besonders hervorgehoben abgegeben werden müssen (Vgl. Kühling/Buchner/Buchner/Kühling, 3. Aufl. 2020, DS-GVO Art. 7 Rn. 25; BeckOK DatenschutzR/Albers/Veit, 44. Ed. 1.5.2023, DS-GVO Art. 6 Rn. 38).

Die Klagepartei hätte eine Einwilligung überdies auch nicht in informierter Art und Weise abgegeben. Die Beklagte hätte unbeschadet der weiteren Anforderungen der Art. 13, 14 DSGVO darüber informieren müssen, welche Daten zu welchem Zweck und von wem verarbeitet werden (Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DS-GVO Art. 6 Rn. 8; ähnlich: BeckOK DatenschutzR/Albers/Veit, 44. Ed. 1.5.2023, DS-GVO Art. 6 Rn. 36). Dafür reicht es vorliegend nicht aus, dass der Klagepartei beim Registrierungsvorgang ein Hinweis auf die jeweils verlinkten Nutzungsbedingungen, die Datenrichtlinie und die Cookie-Richtlinie gegeben wird. Es werden kei-

ne Informationen über die Nutzung der Telefonnummer dergestalt zur Verfügung gestellt, dass ein Nutzer vor Abgabe seiner Einwilligung weiß, zu welchem Zweck, in welcher Art und Weise und von wem seine Telefonnummer verarbeitet wird. Insbesondere findet sich weder in der Datenrichtlinie, in den Nutzungsbedingungen, dem Hilfebereich noch in der Cookie-Richtlinie ein Hinweis auf die Verarbeitung der Telefonnummer zur öffentlichen Suchbarkeit des Profils der Klagepartei mittels des CIT. Ein Hinweis in den Privatsphäre-Einstellungen und dort unter „Bestimme wer dich finden kann“ zur Suchbarkeit der Telefonnummer und was „Finden“ bedeutet, reicht für eine informierte Einwilligung vorliegend nicht. Dabei muss der Nutzer unter Privatsphäre-Einstellungen einen weiteren Untermenüpunkt anklicken. Dieser Menüpunkt ist erst nach Registrierung für den Nutzer auffindbar und nicht hinreichend transparent erreichbar, da der Nutzer nicht an dieser Stelle mit Informationen zur Verarbeitung seiner Telefonnummer rechnen muss und diese erst über mehrere Klicks in einem Untermenüpunkt zu finden ist.

Die Beklagte führt in der Klageerwiderung überdies selbst aus, dass eine Einwilligung des Nutzers i.S.v. Art. 6 Abs. 1 Unterabsatz 1 lit. a DSGVO im gegenständlichen Kontext nicht erforderlich war (Rn. 243 d. Klageerwiderung).

3.

Die Beklagte ist ihrer Verpflichtung zur Information über die Verarbeitung der Telefonnummer der Klagepartei gemäß Art. 5 Abs. 1, Art. 13 DSGVO nicht hinreichend nachgekommen.

Eine Verletzung von den gemäß Art. 13 DSGVO bestehenden Informations- und Aufklärungspflichten ist vom Anwendungsbereich des Art. 82 DSGVO erfasst (LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, GRUR-RS 2023, 1098 Rn. 64; LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 47; BeckOK DatenschutzR/Schmidt-Wudy, 44. Ed. 1.5.2023, DS-GVO Art. 13 Rn. 18; Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 64).

Gemäß Art. 13 Abs. 1 lit. c DSGVO hat der Verantwortliche die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung mitzuteilen. Die Mitteilung über die Zwecke der Verarbeitung ist für die Transparenz der Datenverarbeitung aus Sicht der betroffenen Person von entscheidender Bedeutung und steht im Zusammenhang mit dem Grundsatz der Zweckbindung, wonach personenbezogene Daten grundsätzlich nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Die Angaben müssen vollständig und so detailliert sein, dass die betroffene Person sich ein Bild davon machen kann, mit welchen Datenverarbeitungen sie zu rechnen hat (Paal/Pauly/Paal/Hennemann, 3. Aufl. 2021, DS-GVO Art. 13 Rn. 16; Kühling/Buchner/Bäcker, 3. Aufl. 2020, DS-GVO Art. 13 Rn. 25;

Gola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 12 f.).

Die Beklagte hat die Klagepartei bei Datenerhebung hinreichend darüber aufgeklärt, dass deren Mobilfunknummer zum Zweck der Hilfe bei der Anmeldung, zur „Zwei-Faktor-Authentifizierung“, zu Werbezwecken, zum Zweck des Vorschlagens potenzieller Bekanntschaften sowie zur Kommunikation mit Facebook verwendet wird (Anlagen B6, B9).

Die Beklagte hat die Klagepartei jedoch unzureichend über den Zweck der Verwendung der Telefonnummer für das seitens der Beklagten verwendete CIT aufgeklärt (so auch: LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 55; LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, GRUR-RS 2023, 1098 Rn. 60 ff.).

Die Beklagte hat in den mehrschichtigen Datenschutzinformationen keinen Hinweis über die Verarbeitung der Telefonnummer der Klagepartei, um diese öffentlich über das CIT zu finden, platziert. In der Datenrichtlinie (Anlage B9) findet sich kein Hinweis auf die Verarbeitung der Telefonnummer mittels des CIT.

Es genügt der Hinweis im Hilfebereich von Facebook „Wozu verwendet Facebook meine Mobilnummer […] um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst“ (Anlage B6) nicht, da gerade nicht auf die öffentliche Auffindbarkeit der Telefonnummer der Klagepartei hingewiesen wird. Vielmehr wird nur darüber informiert, dass Personen, die die Klägerseite kennen könnte, ihr über eine Verknüpfung zur Telefonnummer vorgeschlagen werden. Es lässt sich allenfalls der gedankliche Rückschluss ziehen, dass anderen Nutzern das Profil der Klagepartei anhand ihrer Mobilfunknummer ebenfalls vorgeschlagen wird. Damit unterlässt die Beklagte aber gerade die Information auf die öffentliche Suchbarkeit der Mobilfunknummer über das CIT.

Ein Hinweis in den Privatsphäre-Einstellungen und dort unter „Bestimme wer dich finden kann“ zur Suchbarkeit der Telefonnummer und was „Finden“ bedeutet, genügt den Anforderungen des Art. 13 DSGVO nicht. Dabei muss der Nutzer unter Privatsphäre-Einstellungen einen weiteren Untermenüpunkt anklicken. Der Zugang zu diesem Menüpunkt ist erst nach Registrierung für den Nutzer möglich und nicht hinreichend transparent erreichbar, da der Nutzer nicht an dieser Stelle mit Informationen zur Verarbeitung seiner Telefonnummer rechnen muss und diese erst über mehrere Klicks in einem Untermenüpunkt zu finden ist. Überdies wird über die Funktionsweise des CIT und den Verwendungszweck der Telefonnummer dort nicht hinreichend aufgeklärt.

4.

Die Beklagte hat gegen Art. 32. Abs. 1, Art. 24, Art. 5 Abs. 1 lit. f DSGVO verstoßen, da sie keine hinreichenden technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten der Klagepartei getroffen hat. Bezüglich der Einhaltung der technischen und organisatorischen Maßnahmen ist die Beklagte im Zuge ihrer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO darlegungs- und beweisbelastet (Generalanwalt beim EuGH Schlussantrag v. 27.4.2023 – C-340/21, GRUR-RS 2023, 8707 Rn. 42; OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23 –, Rn. 88, juris).

Eine Verletzung von Art. 32 DSGVO ist dabei generell vom Schutzbereich des Art. 82 DSGVO umfasst. (LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 81, juris; Kühling/Buchner/Jandt DS-GVO Art. 32 Rn. 40a; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 31).

Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko der Datenverarbeitung angemessenes Schutzniveau zu gewährleisten. Die Geeignetheit bezieht sich demnach auf das Ziel der Risikovermeidung (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 5). Dabei kommt es darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 41). Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen nicht zu einem absoluten Schutz der Daten (vgl. LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 72Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 3).

Der Begriff "geeignet" setzt voraus, dass die zur Sicherung der Informationssysteme gewählten Maßnahmen sowohl in technischer (Angemessenheit der Maßnahmen) als auch in qualitativer Hinsicht (Wirksamkeit des Schutzes) ein akzeptables Niveau erreichen. Um die Einhaltung der Grundsätze der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit zu gewährleisten, muss die Verarbeitung nicht nur geeignet sein, sondern auch den Zwecken entsprechen, denen sie dienen soll. Dabei spielt der Grundsatz der Minimierung eine entscheidende Rolle, wonach auf allen Stufen der Datenverarbeitung stets darauf geachtet werden muss, dass Sicherheitsrisiken minimiert werden (GA Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, BeckRS 2023, 8707 Rn. 26).

Es ist eine Frage des konkreten Einzelfalls, ob die vom Verantwortlichen darzulegenden und zu beweisenden Maßnahmen das Risiko einer Datenverletzung Dritter - aus ex-ante-Sicht - hinreichend zu verhindern geeignet waren, wobei dem Verantwortlichen bei der Auswahl und Umsetzung der Maßnahmen ein gewisser subjektiver Beurteilungsspielraum zuzugestehen ist (vgl. GA Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, BeckRS 2023, 8707 Rn. 40; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 140, juris).

Gemäß Art. 32 Abs. 3 DSGVO hat der Verantwortliche die Möglichkeit, die Anforderungen an die geeigneten technischen und organisatorischen Maßnahmen durch Einhaltung genehmigter Verhaltensregeln (Art. 40 Abs. 2 lit. h DSGVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DSGVO) nachzuweisen (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 12). Der für die betreffende Verarbeitung Verantwortliche trägt die Beweislast dafür, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 dieser Verordnung geeignet waren (EuGH Urt. v. 14.12.2023 – C-340/21, BeckRS 2023, 35786).

Die Beklagte hat vorliegend aus einer ex-ante Sicht keine hinreichenden technischen und organisatorischen Maßnahmen angemessen zum Risiko während des Zeitraums des Scraping-Vorfalls dargelegt und nachgewiesen. Die von der Beklagten vorgetragenen „Anti-Scraping-Maßnahmen“ wären selbst im Falle deren Nachweises nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Vgl. so auch OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 138 ff. juris; LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 76).

Es besteht vorliegend ein hohes Risiko für die Rechte und Freiheiten der Klagepartei i.S.d. Art. 32 DSGVO.

Die Verarbeitung der personenbezogenen Daten durch die Offenlegung und Übermittlung an andere Nutzer geht über das bloße Speichern oder Erheben hinaus. Es handelt sich auch nicht um öffentlich einsehbare Daten, da Dritten Zugang über Facebook gewährt wird (LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 77). Nur weil die Daten „öffentlich“ auf der Plattform Facebook einsehbar sind, befreit dies die Beklagte nicht von der Pflicht, geeignete organisatorische und technische Maßnahmen i.S.d. Art. 32 DSGVO zu treffen. Die personenbezogenen Daten der Nutzer sind eben nicht überall „öffentlich einsehbar“, sondern nur auf Facebook. Zudem werden eine Vielzahl der von der Beklagten verarbeitenden Daten (u.a. Telefonnummer, Nachname, Vorname, Land, Geschlecht) in einem Nutzerprofil zusammengefasst. So ist ein ge-

bündeltes „Datenpaket“ über die angegebenen Daten der Klagepartei auf Facebook vorhanden. Diese Verknüpfung personenbezogener Daten lässt weitere Rückschlüsse auf die Klagepartei zu, als wenn z.B. die Telefonnummer ausschließlich einzeln auffindbar wäre. Außerdem war das Nutzerprofil der Klagepartei im Zeitpunkt des Scraping-Vorfalls über das CIT suchbar und auffindbar. Die Einstellung der Suchbarkeit auf „Alle“ war voreingestellt, sodass die Telefonnummer der Klagepartei nie ausschließlich für die Zwei-Faktor-Authentifizierung von der Beklagten verarbeitet wurde, sondern auch für die Nutzung des CIT.

Mit der öffentlichen Einsehbarkeit des Nutzerprofils auf Facebook besteht, wie der vorliegende Fall zeigt, ein hohes Missbrauchsrisiko der personenbezogenen Daten durch Dritte. Durch den Rückgriff auf das Nutzerprofil und die Telefonnummer besteht die Gefahr von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren rechtswidrigen Verarbeitungen durch Dritte (Vgl. LG Paderborn Urt. v. 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 76). Scraping stellte im Jahr 2019 nach Angaben der Beklagten bereits eine weit verbreitete Technik zum unbefugten Abgriff personenbezogener Daten dar. Die Beklagte war sich des „Scraping als gängige Taktik“ von „böswilligen Akteuren“ in diesem Zeitraum bewusst (Vgl. Anlagen B10, B11).

Aufgrund des hohen Risikos für die personenbezogenen Daten ist im vorliegenden Fall ein hoher Maßstab an ein angemessenes Schutzniveau zu stellen. Die Beklagte hat dieses Schutzniveau nicht eingehalten.

Der Vortrag der Beklagten dahingehend, dass eine Beschäftigung eines „External Data Misuse Team“ von Datenwissenschaftlern, -analysten und Software-Ingenieuren, Übertragungsbeschränkungen zur Reduzierung der Anzahl von Anfragen, ein Vorgehen gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren und Bestrebungen gegen Hosting-Anbieter stattfände, reicht nicht für ein angemessenes Schutzniveau der personenbezogenen Daten der Klagepartei aus. Wie die Beklagte selbst einräumt, sind die Maßnahmen, die Onlineplattformen zur Verringerung von Scraping einsetzen, in der Regel Übertragungsbegrenzungen und Bot-Erkennungen. Diese Maßnahmen hätten vorliegend das Scraping mittels Telefonnummeraufzählung verhindert oder zumindest erheblich erschwert. Die konkret aufgeführten Maßnahmen der Begrenzung des Rufnummernabgleichs und der eingeschränkten Auffindbarkeit von Nutzerprofilen über das CIT führte die Beklagte nach ihren eigenen Schilderungen erst im Nachgang des Scraping-Vorfalls ein („Vor einer Reihe von Verbesserungen, die wir im September 2019 vorgenommen haben“ Anlage B11). Soweit die Beklagte außerdem vorträgt, sie gehe mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor, greifen diese (nicht technischen) Maßnahmen erst, wenn Scraping tatsächlich eingetreten ist.

Hinsichtlich der Beschäftigung eines „External Data Misuse Team“ von Datenwissenschaftlern, -analysten und Software-Ingenieuren bleibt die Beklagte im Zuge ihrer Darlegungslast insoweit fällig, was genau dieses Team an Beschäftigten gegen Scraping vor dem September 2019 unternommen hat. Der Hinweis auf die Identifizierung von „Aktivitätsmustern und Verhaltensweisen, die typischerweise mit automatisierten Computeraktivitäten in Zusammenhang stehen“ durch das „External Data Misuse Team“ reicht zwar für die Erkennung von Scraping aus. Jedoch bleibt offen, welche konkreten Gegen- und Schutzmaßnahmen sodann durch das „External Data Misuse Team“ oder die Beklagte ergriffen worden sind. Ebenfalls bleibt unklar, wie diese Schutzmaßnahmen funktionieren sollten. Insbesondere erschließt sich für das Gericht nicht, dass die Beschäftigung dieses Teams ausreichend für die Erkennung von Scraping war, wenn im Zuge des Scraping-Vorfalls circa 533 Millionen Datensätze von Nutzern der Plattform Facebook im Internet veröffentlicht worden sind. Überdies wird das „External Data Misuse Team“ erst dann tätig, wenn bereits Scraping auftritt. Die Beklagte hätte vorliegend Systeme zur Erkennung von massenhaften Abfragen vor September 2019 vorhalten und die Suchbarkeit der Nutzerprofile über die Telefonnummer (z.B. „Nur für Freunde von Freunden“) einschränken müssen, um ein angemessenes Schutzniveau im Hinblick auf das hohe Risiko zu gewährleisten. Die Beklagte hätte zudem für die Suche eines Nutzerprofils über das CIT weitergehende Informationen, wie z.B. den Vor- und Nachnamen, abfragen können. Diese Maßnahmen hätten zumindest die Suchbarkeit über die wahllose Eingabe von Telefonnummern erheblich eingeschränkt. Da die Beklagte schon nicht hinreichend substantiiert zu den getroffenen technischen und organisatorischen Maßnahmen vorträgt, worauf die Klagepartei bereits hingewiesen hat (A.I.5. der Replik), wäre im Übrigen eine Vernehmung des als Zeugen angebotenen Geschäftsführers der Beklagten nicht erforderlich.

5.

Ob ein Verstoß gegen Art. 25 DSGVO vorliegt, kann vorliegend wegen seines organisatorischen Charakters und der Unanwendbarkeit des Art. 82 DSGVO auf organisatorische Normen der DS-GVO offenbleiben (Vgl. LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 98, juris).

Allein aus einem Verstoß gegen Art. 25 DSGVO kann wegen seines organisatorischen Charakters ein Anspruch nach Art. 82 Abs. 1 DSGVO nicht begründet werden (vgl. LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22; Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31). Die Vorschrift entfaltet bereits vor dem eigentlichen Beginn der Datenverarbeitung ihren Regelungscharakter. Zu diesem, einer tatsächlichen Datenverarbeitung vorgelagerten Zeitpunkt, entfaltet die DSGVO jedoch nach Art. 2 Abs. 1 DSGVO noch keine Wirkung. Die Anwendbarkeit der DSGVO setzt viel-

mehr eine tatsächliche Verarbeitung personenbezogener Daten voraus (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DSGVO setzt daher darüber hinaus voraus, dass weitere Verstöße gegen die DSGVO vorliegen (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3, 34; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 120, juris).

6.

Die Klagepartei ist der ihr obliegenden Darlegungslast bezüglich eines Schadens hinsichtlich etwaiger Verstöße gegen Art. 33 DSGVO und Art. 34 DSGVO nicht nachgekommen. Deshalb kann es vorliegend offenbleiben, ob ein Verstoß gegen Art. 33 DSGVO und Art 34 DSGVO vorliegt und dieser vom Anwendungsbereich des Art. 82 DSGVO umfasst ist. Hinsichtlich etwaiger Verstöße gegen Art. 33, 34 DSGVO schließt sich das Gericht den Ausführungen des Oberlandesgericht Hamm an (OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 147 - 149, juris):

„Ob die Beklagte ihrer Darlegungslast mit Blick auf mögliche weitere Verstöße gegen die DSGVO zeitlich nach dem Scraping-Vorfall und der Veröffentlichung im Darknet nachgekommen ist, kann dahinstehen; denn hinsichtlich der seitens der Klägerin gerügten Verstöße gegen die Meldepflicht nach Art. 33 DSGVO, die Benachrichtigungspflicht nach Art. 34 DSGVO […] hat die Klägerin keinen konkreten auf die fehlenden Informationen zurückzuführenden Schaden dargelegt noch ist ein solcher sonst ersichtlich. Dass das Scrapen aufgrund einer rechtzeitigen Information noch konkret bezüglich der Klägerin hätte verhindert oder die Veröffentlichung des Leak-Datensatzes mitsamt den Daten der Klägerin hätte verhindert werden können, ist schon nicht ersichtlich, hätte aber auch allenfalls zum Entfallen des aus Sicht der Klägerin erst auf Grund der Veröffentlichung entstandenen Schadens und gerade nicht zu einer Vertiefung oder Begründung desselben geführt.“

7.

Die Klagepartei hat einen kausalen Schaden durch den Kontrollverlust über ihre gescrapten personenbezogenen Daten erlitten. Für einen weitergehenden Schaden bleibt die Klägerseite darlegungs- und beweisfällig.

a.

Die Darlegungs- und Beweislast für einen kausalen Schaden nach Art. 82 DSGVO trägt nach allgemeinen zivilprozessualen Grundsätzen der Anspruchsberechtigte. Eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, muss nachwei-

sen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (EuGH Urt. v. 14.12.2023 – C-340/21, BeckRS 2023, 35786 Rn. 83; EuGH Urt. v. 4.5.2023 – C-300/21, GRUR-RS 2023, 8972 Rn. 50). Eine Beweislastumkehr ist in Art. 82 Abs. 3 DSGVO dem Wortlaut nach ausdrücklich nur bezüglich des Tatbestandsmerkmals des Verschuldens vorgesehen.

b.

Der Klagepartei ist ein kausaler Schaden durch das Scrapen ihrer personenbezogenen Daten durch unbefugte Dritte und den damit einhergehenden Kontrollverlust über ihre personenbezogenen Daten entstanden. Den Kontrollverlust hat die Klägerseite hinreichend substantiiert dargelegt.

aa.

Der Schadensbegriff des Art. 82 DSGVO ist unionsrechtlich auszulegen und setzt nach dem Wortlaut der Norm, der Systematik und Telos des Art. 82 Abs. 2, Abs. 1 DSGVO sowie der Art. 77 ff. DSGVO und den Erwägungsgründen 75, 85 und 146 DSGVO einen über den schlichten Verstoß gegen die DSGVO hinausgehenden Schaden voraus (so EuGH Urt. v. 4.5.2023 - C-300/21, GRUR-RS 2023, 8972 Rn. 29-42; GA Campos Sánchez-Bordona Schlussantr. v. 6.10.2022 - C-300/21, GRUR-RS 2022, 26562 Rn. 117; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 152, juris). Ein Schaden i.S.d. Art. 82 DSGVO kann nach dem Wortlaut materieller oder immaterieller Art sein. Ein immaterieller Schaden liegt dabei jedoch noch nicht in der bloßen Verletzung einer Norm der DSGVO (EuGH, Urteil vom 4. Mai 2023 - C-300/21; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23).

Ein solcher Schaden setzt nach Wortlaut, Erwägungsgründen 10, 146 DSGVO und dem Telos nicht voraus, dass der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (so EuGH Urt. v. 4.5.2023 - C-300/21, GRUR-RS 2023, 8972 Rn. 44-51; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 154, juris).

Hierbei ist zu beachten, dass nach Erwägungsgrund 146 der DSGVO der Schadensbegriff weit und den Zielen der DSGVO entsprechend ausgelegt werden soll. So wird aus Erwägungsgrund 7 der DSGVO das Ziel ersichtlich, dass natürliche Personen die Kontrolle über ihre eigenen Daten besitzen sollten. Insoweit soll der Schadensersatzanspruch auch abschreckende Wirkung entfalten und eine wirksame Sanktionierung sein (OLG Frankfurt a. M. Urteil vom 14.4.2022 – 3 U 21/20 = NJW-RR 2022, 1608 Rn. 50; LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 114, juris; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 65). Der Zweck der Abschreckung

kann nur durch die Ausurteilung ausreichend hoher immaterieller Schadensersatzansprüche erfüllt werden (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18). Einen Schaden erst dann anzunehmen, wenn es etwa zu einer mit einer unrechtmäßigen Zugänglichmachung von Daten liegenden (öffentlichen) „Bloßstellung“, einem Identitätsdiebstahl, einer Weitergabe intimer Informationen oder einer anderen „ernsthaften Beeinträchtigung für das Selbstbild oder Ansehen einer Person“ kommt, und ein „besonderes immaterielles Interesse“ zu verlangen, das über den allein durch die Verletzung an sich hervorgerufenen Ärger oder sonstige Gefühlsschäden hinausgeht, verkennt den autonom und nach Erwägungsgrund 146 ausdrücklich weit auszulegenden Begriff des Schadens (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18a).

So sieht Erwägungsgrund 75 der DSGVO, dass eine Verarbeitung „zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere […] wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren.“

Mit dem Wort „insbesondere“ bringt der europäische Gesetzgeber zum Ausdruck, dass er eine nicht abschließende Aufzählung von für ihn möglich gehaltenen Schadensereignissen im Erwägungsgrund 75 getroffen hat und bereits in einem Kontrollverlust den eingetretenen Schaden sieht (Ähnlich: Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 18b). Dies wird an den anderen aufgezählten Fallgruppen deutlich. So sind eine Diskriminierung, ein Identitätsdiebstahl oder -betrug, ein finanzieller Verlust, eine Rufschädigung, ein Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, die unbefugten Aufhebung der Pseudonymisierung oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile bereits ein materieller oder immaterieller Schaden. Es erschließt sich sodann nicht, warum sich bei einem Kontrollverlust ein (immaterieller) Schaden erst bei der betroffenen Person in Form einer emotionalen Betroffenheit zeigen muss.

Ebenso ist Erwägungsgrund 85 der DSGVO zu beachten, der einen Kontrollverlust als Schaden bezeichnet. Danach kann eine Verletzung des Schutzes personenbezogener Daten „einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte […]“ nach sich ziehen (Vgl. hierzu Gola/Heckmann/Gola, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 112).

Allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, kann einen „immateriellen Schaden“ im Sinne des Art. 82 DSGVO darstellen (EuGH Urt.

v. 14.12.2023 – C-340/21, BeckRS 2023, 35786 Rn. 86).

Die Kontrolle über die eigenen Daten findet im deutschen Zivilrecht Ausdruck über das Recht auf informationelle Selbstbestimmung (verankert in Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG), welches als Ausprägung des allgemeinen Persönlichkeitsrechts gewährleistet wird (Grüneberg, BGB, 82. Auflage 2023, §823, Rn. 132; BeckOGK/Specht-Riemenschneider, 1.8.2023, BGB § 823 Rn. 1373 ff.). Das im Zivilrecht deliktrechtlich über § 823 BGB und im Datenschutzrecht durch Art. 82 DSGVO geschützte Recht auf informationelle Selbstbestimmung enthält die „Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ (vgl. hierzu im Einzelnen BeckOGK/Specht-Riemenschneider, 1.2.2023, BGB § 823 Rn. 1365-1383).

Eine Kontrolle über die gescrapten personenbezogenen Daten besitzt die Klagepartei nach Überzeugung des Gerichts nicht mehr, da diese zumindest öffentlich im Internet angeboten werden. Vorliegend sind nach den Angaben der Beklagten im Informationsschreiben an die Klagepartei (Anlage B16) Nutzer-ID, Vorname, Nachname, Land, Geschlecht und die Telefonnummer durch die Scraper abgegriffen worden.

Der Kontrollverlust tritt mit dem Abscrapen der personenbezogenen Daten durch unbefugte Dritte ein und nicht mit der unrechtmäßigen Verarbeitung und den weiteren Verstößen gegen die DSGVO. Die personenbezogenen Daten der Klagepartei, insbesondere die Telefonnummer, werden nicht mehr ausschließlich bei der Beklagten verarbeitet, sondern sind einem unbegrenzten Personenkreis zugänglich. Erst durch die Verstöße gegen die DSGVO hat es die Beklagte ermöglicht, dass unbefugte Dritte das Contact-Import-Tool für einen Datenabgriff ausnutzen konnten. Die personenbezogenen Daten der Klagepartei befinden sich öffentlich im Internet und werden dort zur Weitergabe und Verkauf angeboten. Dadurch hat die Klagepartei keine Kontrolle mehr, wer, wann und wie mit den gescrapten personenbezogenen Daten der Klagepartei umgeht. In dieser Ungewissheit, was mit den eigenen Daten passiert, liegt der Schaden der Klagepartei. Der (immaterielle) Schaden realisiert sich vorliegend nicht durch die Datenschutzverstöße als solche realisiert, sondern erst durch das Abgreifen der Daten, das weitere Vorgehen der Scraper und der Veröffentlichung der personenbezogenen Daten der Klagepartei (ähnlich LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 106 - 107, juris). Folglich findet der Schaden seine Ursache in den DSGVO-Verstößen durch die Beklagte, begründet sich aber erst durch den objektiven Kontrollverlust.

Eine weitergehende subjektive Beeinträchtigung in Form von starkem Unwohlsein über den Kon-

trollverlust ist nach Überzeugung des Gerichts nicht erforderlich. Vielmehr kann sich der eingetretene immaterielle Schaden durch eine weitergehende subjektive Beeinträchtigung der Klagepartei intensivieren.

Eine solche weitergehende subjektive Beeinträchtigung kann das Gericht vorliegend nach der informatorischen Anhörung des Klägers jedoch nicht feststellen. Insbesondere hat der Kläger kein weitergehendes Unwohlsein oder weitere Beeinträchtigung in Form einer Verhaltensänderung nach Bekanntwerden des Scrapingvorfalls aufgrund des Kontrollverlusts über seine personenbezogenen Daten angegeben.

Die Klagepartei hat insoweit nur Auswirkungen auf ihr Verhalten hinsichtlich der vorgetragenen Belästigungsanrufe und -SMS und nicht über den Kontrollverlust in der informatorischen Anhörung bestätigt.

Der Vortrag in der Klageschrift zum großen Unwohlsein und zur großen Sorge über möglichen Missbrauch der betreffenden Daten ist für eine weitere Beeinträchtigung zu pauschal. Insbesondere wird diese Formulierung in zahlreichen Schriftsätzen der Prozessbevollmächtigten der Klagepartei verwendet. Eine Konkretisierung und objektive Nachvollziehbarkeit dieses Unwohlseins in Form einer Verhaltensänderung der Klagepartei lässt sich so vorliegend nicht feststellen.

bb.

Der Schaden ist vorliegend auch kausal auf die Datenschutzverletzungen der Beklagten zurückzuführen.

Der Verantwortliche haftet lediglich für kausal durch die rechtswidrige Verarbeitung verursachte Schäden (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 41; LG Paderborn Urteil vom 19.12.2022 – 3 O 99/22, GRUR-RS 2022, 39349 Rn. 128). Eine Mitursächlichkeit des Verstoßes gegen die DSGVO genügt (OLG Stuttgart ZD 2021, 375; LG Köln ZD 2022, 52 Rn. 21).

Möglich wurde das Scraping durch die rechtswidrige Verarbeitung der Telefonnummer der Beklagten mittels des CIT ohne Einwilligung der Klagepartei. Denn hätte die Klagepartei erst eine Einwilligung für die Verarbeitung der Telefonnummer abgeben müssen, wäre diese grundsätzlich ohne Einwilligung nicht öffentlich über das CIT suchbar gewesen und die Klagepartei hätte keinen Kontrollverlust erlitten. Gleiches gilt für die mangelnde hinreichende und transparente Information durch die Beklagte. Denn hätte die Klagepartei von der öffentlichen Suchbarkeit durch andere und die Funktionsweise des CIT hinreichende Informationen zur Verfügung gehabt, hätte sie ihre Einstellungen auf dieser Grundlage ändern können oder hinreichend bewusst öffentlich lassen kön-

nen. Im Sinne einer conditio-sine-qua-non wäre der Kontrollverlust ebenfalls nicht eingetreten, wenn die Beklagte hinreichende technische und organisatorische Maßnahmen getroffen hätte. Es wäre den Scraper technisch nicht möglich gewesen, den Datensatz der Klagepartei abzugreifen.

c.

Es liegt kein kausaler Schaden vor, soweit die Klagepartei vorträgt, sie erhalte regelmäßig Spam-Nachrichten, Spam-Mails und Belästigungsanrufe.

Grundsätzlich können in einem Datenverlust durch das Scrapen und Veröffentlichen von personenbezogenen Daten (immaterielle) Schäden in Form von Spam oder Belästigungsanrufe eintreten. Ob solche Schäden vorliegend substantiiert durch die Klägerseite vorgetragen sind, kann offenbleiben, da jedenfalls keine Kausalität zwischen den Verstößen der Beklagten gegen die DS-GVO und den Spam-Nachrichten und Belästigungsanrufen hinreichend darlegt ist.

Die Klagepartei trägt die Darlegungs- und Beweislast für die Kausalität nach allgemeinen zivilprozessualen Grundsätzen (Vgl. C.I.7.a). Für die Frage der haftungsbegründenden Kausalität gilt § 286 ZPO. § 286 ZPO erfordert keine absolute oder unumstößliche Gewissheit und auch keine an Sicherheit grenzende Wahrscheinlichkeit, sondern nur einen für das praktische Leben brauchbaren Grad von Gewissheit, der Zweifeln Schweigen gebietet (BGH Urt. v. 23.6.2020 - VI ZR 435/19, VersR 2021, 1497 Rn. 13; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 196, juris).

Die Klägerseite trägt nicht hinreichend vor, dass der Scraping-Vorfall ursächlich für die Spam-Nachrichten, -SMS und Belästigungsanrufe ist. Es steht nicht fest, dass die Belästigungsanrufe und -SMS ihre Ursache im Scraping-Vorfall finden. Es besteht zwar die Möglichkeit, dass die personenbezogenen Daten für die Belästigungsanrufe und -SMS verwendet werden. Jedoch ist ein konkreter Ursachenzusammenhang nicht hinreichend von der Klagepartei dargelegt.

Dem Gericht ist es aus eigener Wahrnehmung bekannt, dass auch Personen, die keinen Facebook-Account haben, Spamnachrichten und -anrufe erhalten. Es kann vorliegend viele Ursachen für solche Belästigungen geben, die jedoch nicht zwingend aus dem Scraping-Vorfall resultieren. Es besteht die Möglichkeit, dass die Klagepartei ihre personenbezogenen Daten an anderer Stelle weitergegeben hat und diese von dort sodann für die Spam-Nachrichten und -anrufe genutzt werden oder an unbefugte Dritte gelangt sind. Allein aus einer Zunahme der Spamnachrichten und Belästigungsanrufe nach dem Jahr 2019 lässt sich nicht die Schlussfolgerung ziehen, dass die Absender der Nachrichten oder die Anrufer die entsprechenden personenbezogenen Daten der Klagepartei aus dem gescrapten Datensatz haben. Aufgrund der Alternativmöglichkeit der Ursa-

chen ist keine hinreichende Kausalität gegeben (Vgl. auch OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 200, juris; LG Münster Urt. v. 7.3.2023 – 02 O 54/22, GRUR-RS 2023, 4183 Rn. 57; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 80; LG Itzehoe Urt. v. 9.3.2023 – 10 O 87/22, GRUR-RS 2023, 3825 Rn. 75; LG Regensburg Endurteil v. 11.5.2023 – 72 O 1413/22, GRUR-RS 2023, 13826 Rn. 68).

8.

Die Beklagte kann sich vorliegend auch nicht gemäß Art. 82 Abs. 3 DSGVO exkulpieren.

Nach Art. 82 Abs. 3 DSGVO wird die Beklagte von der Haftung nur frei, wenn sie nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Dadurch wird die Verantwortlichkeit der Beklagten für den Schaden widerleglich vermutet. Zum Begriff der Verantwortlichkeit führt das Landgericht Paderborn (Urteil vom 19. Dezember 2022 – 3 O 99/22 –, Rn. 125, juris) zutreffend aus:

„Zwar ist der Begriff der Verantwortlichkeit im Sinne des § 82 Abs. 3 DSGVO nicht näher definiert. So wird dieser vorwiegend mit dem Begriff des Verschuldens gleichgesetzt (vgl. OLG Stuttgart 31.3.2021 - 9 U 34/21; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 24; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 49). Teilweise wird dies hingegen nicht angenommen mit der Folge, dass Art. 82 DSGVO möglicherweise als Gefährdungshaftungstatbestand zu begreifen sei, sodass dem Verantwortlichen oder Auftragsverarbeiter unabhängig von jedwedem Verschulden lediglich ganz ungewöhnliche Kausalverläufe, die jeder Lebenserfahrung widersprechen, sowie Fälle höherer Gewalt und weit überwiegenden eigenen Fehlverhaltens der betroffenen Person nicht anzulasten seien (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 18).“

Vorliegend kommt es hierauf jedoch nicht entscheidend an, da die Beklagte ein fehlendes Verschulden ihrerseits nicht nachweisen kann und kein Fall eines ungewöhnlichen Kausalverlaufs, noch höherer Gewalt oder weit überwiegenden eigenen Fehlverhaltens der Klagepartei gegeben ist. Die Beklagte hat vorliegend mehrere ihr obliegenden Pflichten aus DSGVO verletzt. Dadurch kann sich die Beklagte von fahrlässigem Handeln nicht entlasten. Vielmehr wäre bei normgemäßen Verhalten der Beklagten ein Abscrapen der personenbezogenen Daten der Klagepartei ihres Facebook-Profil nicht oder nur erschwert möglich gewesen und kein Kontrollverlust der Klagepartei über ihre personenbezogenen Daten entstanden.

9.

Die Höhe des Schadens beziffert das Gericht mit 250,00 €.

Dabei hält es diesen Betrag für angemessen und ausreichend, um den immateriellen Schaden auszugleichen. Gleichzeitig trägt es der Abschreckungswirkung des Schadensersatzes nach Art. 82 DSGVO und den besonderen Umständen des Falles Rechnung. Dem Gericht steht insoweit ein Ermessen zu (§ 287 ZPO).

Bei der Bemessung der Höhe des Schadensersatzes kann § 253 BGB herangezogen werden, sofern die unionsrechtlichen Grundsätze der Äquivalenz und Effektivität beachtet werden (EuGH Urteil vom 04.05.2023 – C-300/21 = GRUR-RS 2023, 8972 Rn. 59; BeckOK DatenschutzR/Quaas, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 31). Dabei können die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden. Dazu zählen die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des entstandenen Schadens, frühere Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten, die betroffenen Kategorien personenbezogener Daten zur Ermittlung (BeckOK DatenschutzR/Quaas, 44. Ed. 1.5.2023, DS-GVO Art. 82 Rn. 31; so auch LG Essen, Urteil vom 23.9.2021 – 6 O 190/21 = ZD 2022, 50 (Rn. 48); LG Lübeck, Urteil vom 25. Mai 2023 – 15 O 74/22 –, Rn. 115, juris).

Vorliegend war einerseits zu berücksichtigen, dass die Beklagte mehrfach gegen die DSGVO verstoßen hat und die Veröffentlichung der personenbezogenen Daten der Klagepartei erst aufgrund dieser Verstöße möglich war. Zudem beläuft sich der weltweite Jahresumsatz der Beklagten im Jahr 2021 auf 118 Milliarden €.

Andererseits ist in die Bewertung der Höhe des Schadensersatzanspruches einzufließen, dass die Beklagte im Nachgang weitere Sicherheitsmaßnahmen gegen Scraping getroffen hat, keine besonders sensiblen Daten i.S.d. Art. 9 Abs. 1 DSGVO gescrapt wurden und es vorliegend zu keiner Vermögensgefährdung oder einem Vermögensschaden gekommen ist. Des Weiteren ist zu berücksichtigen, dass die Beklagte die Daten nicht selbst veröffentlicht hat, sondern dies durch unbefugte Dritte geschehen ist und sie nur eine Mitursächlichkeit trifft. Außerdem hat die Klagepartei im Anspruchsschreiben an die Beklagte selbst einen Betrag von 500 € als ausreichende Kompensation für die Datenschutzverstöße und die Veröffentlichung angesehen.

Da nur der Kontrollverlust als Schaden vorliegend gegeben und keine weitere subjektive Beeinträchtigung durch die Klagepartei dargelegt ist, reduziert das Gericht diesen Betrag unter Berücksichtigung der Gesamtumstände um 50 %. Das Gericht hält wegen der ausgeführten Erwägungen einen Betrag von 250,00 € zum Ausgleich des eingetretenen immateriellen Schadens für an-

gemessen.

Auf eine vergleichbare Entscheidung des OLG Frankfurt vom 14.04.2022, Az. 3 U 21/20 zum Verlust sensibler Daten hinsichtlich der Schadenshöhe kann verwiesen werden. Das OLG Frankfurt sah einen angemessenen Schadensersatz in Höhe von 500 € für eine Beeinträchtigung wegen eines versehentlichen Versendens von Kontodaten einer Bank als angemessen an (OLG Frankfurt am Main, Urteil vom 14.04.2022, 3 U 21/20 = ZD 2022, 621). Da es sich vorliegend nicht um ähnlich sensible personenbezogene Daten (Bankdaten), sondern um die Telefonnummer der Klagepartei handelt, ist ein Abschlag von 50 % zu 500 € unter Berücksichtigung des Einzelfalls angemessen. Insoweit die Klägerseite einwendet, andere Gerichte hätten für weniger gravierende Verstöße 5000 € (ArbG Düsseldorf Urteil vom 06.02.2020 - 3 SaGa 7 öD/19 = NZA-RR 2020, 409 Rn. 85) oder 1500 € (ArbG Neumünster Urteil vom 11.8.2020 – 1 Ca 247 c/20 = ZD 2021, 171 Rn. 37) zugesprochen, ist dies auf den vorliegenden Fall nicht übertragbar. So wurde wegen mangelhafter Auskunft in den benannten Verfahren ein Schaden festgestellt und nicht wegen eines Kontrollverlusts. Überdies ging es im dortigen Sachverhalt jeweils um ein nicht erfülltes Auskunftsverlangen sowie um ein Verfahren in der Zuständigkeit der Arbeitsgerichtsbarkeit, welche für das vorliegend entscheidende Gericht nicht bindend ist.

II.

Der Klageantrag zu 2) ist begründet. Die Klagepartei hat einen Anspruch auf Feststellung künftiger materieller Schäden aus den konkret vorliegenden Verletzungen der DSGVO durch die Beklagte.

Nach dem BGH ist ein Feststellungsantrag begründet, wenn die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs vorliegen, also ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann. Von einer Wahrscheinlichkeit des Schadenseintritts hängt die Entstehung des Anspruchs nicht ab. Da der Feststellungsausspruch nichts darüber aussagt, ob ein künftiger Schaden eintreten wird, ist es unbedenklich, die Ersatzpflicht des Schädigers für den Fall, dass der Schaden eintreten sollte, bereits jetzt festzustellen (BGH, Urteil vom 17. Oktober 2017 – VI ZR 423/16 –, BGHZ 216, 149-174, Rn. 49; ähnlich MüKoZPO/Becker-Eberhard, 5. Aufl., § 256 Rn. 32).

Dies ist auf den vorliegenden Fall übertragbar. Da jedenfalls die Voraussetzungen eines immateriellen Schadensersatzanspruch der Klagepartei bestehen (Vgl. C.I.), ist der Klageantrag zu 2) nach den Vorgaben des BGH begründet. Es wird vorliegend nur festgestellt, dass die Verletzungen der DSGVO durch die Beklagte bei einem potenziell künftigen und festzustellenden Schaden

Grundlage sind. Dies ist nach dem BGH auch unbedenklich, da der Feststellungsausspruch keine Aussage darüber trifft, ob ein möglicher zukünftiger Schaden auch tatsächlich gegeben ist.

lll.

Der Klageanspruch zu 3b) ist unbegründet.

Es kann vorliegend dahinstehen, ob ein Unterlassungsanspruch im Anwendungsbereich der DS-GVO in Betracht kommt und auf welche Rechtsgrundlage dieser zu stützen wäre (Art. 17, Art. 21 DSGVO; §§823, 1004 BGB), da ein Anspruch auf Unterlassung eine Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise des CIT und der Verwendung von Telefonnummern mangels Wiederholungsgefahr nicht gegeben ist.

Die Beklagte hat vorliegend gegen die DSGVO verstoßen, indem sie nicht hinreichend und transparent über die Verarbeitung der personenbezogenen Daten der Klagepartei informiert und die Daten der Klagepartei unrechtmäßig verarbeitet hat (Vgl. C.I.3.).

Eine Wiederholungsgefahr durch die Beklagte ist vorliegend jedoch nicht gegeben.

Die mangelnde hinreichende und transparente Information der Beklagten löst für die Zukunft keine nachteiligen Folgen mehr für die Klagepartei aus. Die Klägerseite ist im Rahmen des Rechtsstreits hinreichend über die Datenverarbeitung durch die Beklagte aufgeklärt worden (vgl. LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22; LG Ulm, Urteil vom 16.02.2023 – 4 86/22). Die Kenntnis von dem die Klagepartei eine weitere Verarbeitung der Telefonnummer im Zusammenhang mit dem CIT abhängig macht, hat sie bereits erlangt. Zudem ist es der Klagepartei mittlerweile zumindest möglich, die „Suchbarkeits-Einstellung“ entsprechend des gewünschten Datenschutzniveaus anzupassen.

lV.

Der Klageantrag zu 4) ist ebenfalls unbegründet. Der Klagepartei steht kein Anspruch gemäß Art. 15 Abs. 1 DSGVO gegenüber der Beklagten zu, da die Beklagte den Auskunftsanspruch, soweit er bestand, bereits gemäß § 362 Abs. 1 BGB erfüllt hat.

1.

Grundsätzlich besteht nach Art. 15 Abs. 1 DSGVO ein Anspruch auf Auskunft der betroffenen Person gegen den Verantwortlichen in dem in Art. 15 Abs. 1 lit. a) – lit. h) bezeichneten Umfang, wenn der Verantwortliche personenbezogene Daten verarbeitet (vgl. BGH, Urteil vom 15.06.2021

- VI ZR 576/19 = NJW 2021, 1381).

Der Anspruch erstreckt sich jedoch nicht auf eine Verarbeitung personenbezogener Daten durch Dritte. Soweit durch den Scraping-Vorgang personenbezogene Daten von unbefugten Dritten verarbeitet wurden, ist jedenfalls nicht die Beklagte auskunftspflichtig (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 96-98; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 101; LG Regensburg Endurteil v. 11.5.2023 – 72 O 1413/22, GRUR-RS 2023, 13826 Rn. 82).

Hinsichtlich der Auskunft über die Empfänger, die personenbezogene Daten durch den Scraping-Vorfall erlangen konnten, stellt das Abgreifen der personenbezogenen Daten keine Verarbeitung durch die Beklagte als Verantwortliche dar. Vielmehr sind die Personen, die die Daten scrapen, selbst Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO, da die Beklagte bei diesem Datenverarbeitungsvorgang eben nicht über die Zwecke und Mittel der Verarbeitung entscheidet. So sieht es vorliegend auch die Klagepartei in der Replik, die Scraper als „selbstverständlich ebenfalls datenschutzrechtlich Verantwortliche“ bezeichnet.

2.

Der Anspruch ist, soweit er bestand, wegen Erfüllung nach § 362 Abs. 1 BGB erloschen.

Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (BGH, Urteil vom 15. Juni 2021 – VI ZR 576/19, Rn. 19 m.w.N.) Überdies muss der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, dem Betroffenen zur Verfügung stellen (vgl. EuGH Urt. v. 22.6.2023 - C-579/21, BeckRS 2023, 14515 Rn. 37 ff; OLG Hamm, Urteil vom 15. August 2023 – 7 U 19/23 –, Rn. 246, juris).

Die Beklagte hat unstreitig personenbezogene Daten der Klagepartei verarbeitet. Die Beklagte hat durch das außergerichtliche Schreiben (Anlage B 16) hinreichend Auskunft über die Verarbeitung der personenbezogenen Daten von Nutzer-ID, Vorname, Nachname, Land, Geschlecht und der Telefonnummer der Klagepartei gegeben. Die konkreten Rohdaten in Form von Logdaten der Kla-

gepartei oder eine Kopie hiervon hat die Beklagte nach ihren Angaben nicht mehr.

Soweit die Klagepartei ein neues Auskunftsbegehren mit dem Klageantrag zu 4) an die Beklagte stellt, hat die Beklagte die Klägerseite mit der Klageerwiderung und dem Verweis auf das Schreiben der Beklagten (Anlage B16) bereits auf ihre Selbstbedienungstools („Access Your Information“ und „Download Your Information“) verwiesen. Dort kann die Klägerseite jederzeit die von der Beklagten verarbeitenden Daten abrufen und einsehen.

V.

Der Klageantrag zu 5) ist teilweise begründet. Der Klägerseite steht ein Anspruch auf Ersatz vorgerichtlicher Rechtsanwaltsgebühren in Höhe von 159,94 € zu.

Der Ersatz vorgerichtlicher Rechtsanwaltskosten ist von Art. 82 Abs. 1 DSGVO umfasst. Kostenerstattung aufgrund des materiell-rechtlichen Kostenerstattungsanspruchs kann der Geschädigte vom Schädiger dagegen grundsätzlich nur insoweit verlangen, als seine Forderung diesem gegenüber auch objektiv berechtigt ist (BGH Urt. v. 5.12.2017 – VI ZR 24/17, BeckRS 2017, 138416 Rn. 6 m. w. N.). Zur effektiven Durchsetzung der klägerischen Ansprüche war aufgrund der Schwierigkeit der Sach- und Rechtslage die Hinzuziehung eines Rechtsbeistandes erforderlich und notwendig. Ausgehend von einem Wert des berechtigten Verlangens der Klägerseite von 750 € (Klageantrag zu 1) 250€; Klageantrag zu 2) 500 €) zum Zeitpunkt der außergerichtlichen Tätigkeit ergibt dies Kosten in Höhe von 159,94 € (1,3 Geschäftsgebühr Nr. 2300, 1008 VV RVG: 114,40 € Auslagen Nr. 7001 u. 7002 VV RVG: 20,00 €; 19% MwSt: 25,54 €).

VI.

Der Zinsanspruch folgt aus §§ 288 Abs. 1, 291 BGB.

Die Klage ist der zustellungsbevollmächtigten Kanzlei der Beklagten am 18.10.2023 zugestellt worden. Ab dem Folgetag sind Rechtshängigkeitszinsen zu gewähren.

VII.

Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO. Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus § 708 Nr. 11, § 711, § 709 ZPO.

C.

Der Streitwert ist auf 7.000 € festzusetzen.

1.

Der Streitwert für den Klageantrag zu 1) ist wegen der Angabe eines Mindestbetrags (Vgl. Zöller, ZPO, 34. Auflage 2022, §3 Rn. 16.171) auf 1000 € festzusetzen.

2.

Der Streitwert für den Klageantrag zu 2) ist gemäß § 3 ZPO nach Schätzung des Klägerinteresses auf 500,00 € festzusetzen. Das Gericht schätzt dieses Interesse unter Berücksichtigung der hinsichtlich etwaiger künftiger Schäden ersichtlich schwierig nachzuweisenden Kausalität auf 500,00 € (Vgl. OLG Hamm, Urteil vom 15. August 2023 – I-7 U 19/23 –, Rn. 279, juris; OLG Frankfurt, Beschluss vom 18. Juli 2023 – 6 W 40/23 –, Rn. 11, juris; OLG Karlsruhe, Beschluss vom 5. Juli 2023 – 10 W 5/23 –, Rn. 15, juris).

3.

Gemäß § 3 ZPO wird der Wert von dem Gericht nach freiem Ermessen festgesetzt. Für den nichtvermögensrechtlichen Anspruch im Klagantrag Ziff. 3 wird der Streitwert gem. § 48 Abs. 2 GKG unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache und der Vermögens- und Einkommensverhältnisse der Parteien, nach Ermessen bestimmt. Der in 23 Abs. 3 S. 2 RVG genannten Ausgangswert von 5.000,00 € gibt zwar einen ersten Anhalt (BGH, Beschluss vom 28. Januar 2021 - III ZR 162/20-, juris Rn. 9), ausreichende Anhaltspunkte, die vorliegend eine Abweichung von diesem Ausgangspunkt rechtfertigen könnten, sind jedoch auch unter Berücksichtigung sämtlicher Umstände des Einzelfalls, insbesondere des Umfangs des Datenverstoßes, der wirtschaftlichen Beeinträchtigung des Klägers, der Bedeutung der Sache für die Parteien und ihrer Vermögensverhältnisse, nicht gegeben (so auch OLG Celle, Beschluss vom 04.08.2023, Az. 5 W 40/23, Anlagenkonvolut SW2 im Verfahren 15 W 2331/23; OLG Bamberg, Beschluss vom 23.05.2023, Az. 8 UH 5/23, Anlagenkonvolut Sw2 im Verfahren 15 W 2331/23; OLG Bamberg, Beschluss vom 13.07.2023, AZ. 1 W 26/23e, Anlagenkonvolut SW2 im Verfahren 15 W 2331/23; OLG Oldenburg, Anlagenkonvolut SW2 im Verfahren 15 W 2331/23, Datum und Az. geschwärzt; OLG Stuttgart, Beschluss vom 06.02.2023, Az. 4 W 103/22, Anlagenkonvolut SW2 im Verfahren 15 W 2331/23).

Ausgehend von diesen Maßstäben hält das Gericht für die Klageanträge zu 3) einen Streitwert

von 5.000,00 € für angemessen.

4.

Der Streitwert für den Klageantrag zu 4) ist auf 500 € festzusetzen.

5.

Der Klageantrag zu 5) ist als Nebenforderung nicht streitwerterhöhend.

Rechtsbehelfsbelehrung:

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

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

Landgericht Nürnberg-Fürth
Fürther Str. 110
90429 Nürnberg

einzulegen.

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

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

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

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

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

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

tungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

Richter am Landgericht

Verkündet am 19.08.2024

gez.
, JAng
Urkundsbeamtin der Geschäftsstelle

Für die Richtigkeit der Abschrift
Nürnberg, 20.08.2024

, JAng
Urkundsbeamtin der Geschäftsstelle