Oberlandesgericht Dresden

Zivilsenat

Aktenzeichen: **4 U 480/24**
Landgericht Leipzig, 08 O 643/22

IM NAMEN DES VOLKES

URTEIL

In dem Rechtsstreit

- Kläger und Berufungskläger -

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

gegen

Meta Platforms Ireland Ltd., Merrion Road, Dublin 4, D04 X2K5, Irland
vertreten durch d. Director

- Beklagte und Berufungsbeklagte -

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

wegen Schadensersatz, Feststellung, Unterlassung und Auskunft

hat der 4. Zivilsenat des Oberlandesgerichts Dresden durch

Vorsitzenden Richter am Oberlandesgericht
Richterin am Oberlandesgericht und
Richter am Landgericht

aufgrund der mündlichen Verhandlung vom 27.08.2024 am 03.09.2024

für Recht erkannt:

1.
Auf die Berufung des Klägers wird das Urteil des Landgerichtes Leipzig vom 08.03.2024 - 8 O 643/22 - unter Zurückweisung der Berufung im Übrigen wie folgt abgeändert:

Die Beklagte wird verurteilt, an den Kläger 100 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 22.07.2022 zu zahlen. Im Übrigen wird die Klage abgewiesen.

2.
Die Kosten des Berufungsverfahrens trägt der Kläger.

3.
Das Urteil ist wegen der Kosten gegen Sicherheitsleistung in Höhe von 110% vorläufig vollstreckbar.

4.
Die Revision wird zugelassen.

Beschluss:

Der Streitwert wird auf 5.500 EUR festgesetzt.

Gründe

I.

Die Klagepartei nimmt die Beklagte als Betreiberin des sozialen Netzwerkes Facebook wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung in der Zeit von 2018 bis 2019 in Zusammenhang mit einem „Scraping Vorfall“ auf immaterielle Entschädigung, Feststellung, Unterlassung und Auskunft in Anspruch.

Die Beklagte betreibt in der Europäischen Union das soziale Online-Netzwerk Facebook und bietet Dienste an, die für private Nutzer kostenlos sind. Das Geschäftsmodell der Beklagten basiert auf der Finanzierung durch Online-Werbung, die auf den individuellen Nutzer des sozialen Netzwerks insbesondere nach Maßgabe seines Konsumverhaltens, seiner Interessen, seiner Kaufkraft und seiner Lebenssituation zugeschnitten ist. Die Facebook-Plattform ermöglicht es Nutzern, persönliche Profile zu erstellen und diese mit Freunden oder der Öffentlichkeit zu teilen und sich auszutauschen. Die Klagepartei ist Nutzerin des von der Beklagten betriebenen sozialen Netzwerkes Facebook, auf das sie nach Registrierung auf der Website oder über Apps für Mobiltelefone und Tablets zugreifen kann. Mit der Registrierung wird ein Nutzungsvertrag abgeschlossen und eine Nutzer ID generiert. Hierbei muss den Nutzungsbedingungen zugestimmt werden und der Nutzer wird auf die Datenschutz- und Cookierichtlinien der Beklagten hingewiesen. Die Angabe des Vor- und Nachnamens und des Geschlechtes sind bei der Registrierung zwingend. Diese Daten sind stets öffentlich. Bei der Angabe von weiteren fakultativen Daten (z. B. Geburtsdatum, Wohnort, E-Mail-Adresse und Telefonnummer) können in der Privatsphäreneinstellung unterschiedliche Einstellungen gewählt werden. Der Nutzer kann entscheiden, ob diese Daten für alle, also „öffentlich“ oder für „Freunde“ oder „Freunde von Freunden“ einsehbar sind. Bei der Zielgruppenauswahl wird festgelegt, wer einzelne Informationen im Facebook-Profil des Nutzers sehen, bei der Suchbarkeitseinstellung, wer das Profil eines Nutzers z. B. anhand einer Telefonnummer finden kann. Die Standardeinstellung für die Suchbarkeit nach der Telefonnummer war während des relevanten Zeitraumes „alle“. Das Auffinden eines Nutzerprofils auf der Facebook-Plattform mittels einer Telefonnummer fand u. a. mit dem von der Beklagten angebotenen Contact Import Tool (CIT) statt. Das CIT ermöglichte es Nutzern, ihre Kontakte von ihren Mobilgeräten auf der Facebook - Plattform zu finden und mit ihnen in Verbindung zu treten.

Die Klagepartei ist bei Facebook registriert. Die Suchbarkeitseinstellung bezüglich der Telefonnummer war auf „alle“ gestellt und wurde am 01.02.2020 auf „only me“ geändert (Anlage B 17). Die Telefonnummer war auf dem Facebook-Profil nicht öffentlich einsehbar.

Zu einem unbekannten Zeitpunkt im Zeitraum bis September 2019 kam es auf der Facebook-Plattform zu einem sogenannten Scraping, also dem massenhaften, automatisierten Sammeln persönlicher Daten von Facebook-Nutzern. Dritte nutzten hierfür das Contact Import Tool und luden einen großen Satz von Telefonnummern bzw. Ziffernkombinationen hoch, um festzustellen, ob diese mit Facebook-Nutzern übereinstimmen. Sie konnten so den generierten Telefonnummern ein bestimmtes Nutzerprofil zuordnen und die öffentlich einsehbaren Daten - das heißt die stets zwingend öffentlichen Daten und die vom Nutzer öffentlich eingestell-

ten Daten - einsehen. Dies bemerkte die Beklagte für die Facebook Plattform und deaktivierte das CIT. Als es auch bei dem Messenger zum Scraping kam, wurde es auch dort deaktiviert. Anfang April 2021 wurden in einem Hackerforum die Namen und teilweise weitere Daten, wie z. B. Telefonnummer und Wohnort, von 533 Mio Nutzern veröffentlicht. Am 06.04.2021 veröffentlichte die Beklagte eine Information über das Scraping (Anlage B10). Die Klagepartei ist von dem Datenschutzvorfall betroffen. Nach ihrem Vorbringen sind Name, Telefonnummer, Facebook-ID, Geschlecht, Wohnort und Land veröffentlicht.

Die irische Datenschutzbehörde (DPC) hat gegen die Beklagte wegen dieses Scraping-Vorfalls am 25.11.2022 eine Geldbuße in Höhe von 265 Mio EUR verhängt und der Beklagten unzureichende Sicherheitsmaßnahmen vorgeworfen. Der Bescheid wurde von der Beklagten angefochten.

Die Klagepartei hat im Juni 2021 die Beklagte zur Zahlung von Schadensersatz und zur Unterlassung der zukünftigen Zugänglichmachung von Daten aufgefordert und Auskunft darüber begehrt, welche konkreten Daten vom Scraping betroffen waren. Die Beklagte hat auf das Auskunftsersuchen am 09.09.2021 geantwortet (Anlage B 16).

Die Klagepartei hat behauptet, dass die Beklagte keine ausreichenden Vorkehrungen zum Schutz der Daten ergriffen habe. Es seien keine branchenüblichen Sicherheitsmaßnahmen, wie Captchas oder eine Plausibilitätsüberprüfung der Anfragen im CIT eingerichtet worden. Die Einstellungen und Hinweise zur Privatsphäre bei der Registrierung seien undurchsichtig und verwirrend gestaltet. Eine Information über etwaige Risiken sei nicht erfolgt. Die Voreinstellungen seien nicht datenschutzfreundlich und würden daher dem Prinzip der Datenminimierung widersprechen. Durch die Pflichtverletzungen der Beklagten, sei es zu einer Veröffentlichung ihrer Daten im Darknet gekommen. Der Beklagten sei zudem vorzuwerfen, dass sie ihren Informationspflichten nicht nachgekommen sei. Sie habe über den Datenschutzvorfall weder die Klagepartei noch die zuständige Behörde informiert. Die Daten könnten zu kriminellen Zwecken missbraucht werden. Die Klagepartei habe wegen des Scraping in erheblichem Ausmaß die Kontrolle über ihre abgegriffenen Daten verloren und sei vermehrt von Unbekannten via E-Mail und SMS kontaktiert worden. Dies führe zu großen Sorgen über einen möglichen Missbrauch der Daten und stelle einen immaterieller Schaden dar. Ein materieller Schaden sei zu befürchten. Die Beklagte sei zur Unterlassung ihrer rechtwidrigen Datenverarbeitung verpflichtet. Die vorgerichtlichen Auskünfte seien unzureichend.

Die Beklagte hat behauptet, die Daten seien nicht durch mangelhafte Sicherheitssysteme in

die Hände Dritter gefallen. Es liege nur ein automatisiertes massenhaftes Sammeln ohnehin öffentlicher und damit nicht vertraulicher Daten vor. Daten wie z. B. „Bundesland“ seien nicht durch Scraping erlangt worden, da sie nicht den Profilfeldern der Plattform entsprächen. Sie habe ausreichende technische und organisatorische Vorkehrungen gegen das Scraping getroffen. So habe sie Übertragungsbeschränkungen eingesetzt, die die Anzahl der konkreten Datenabfragen, die pro Nutzung der IP-Adresse in einem bestimmten Zeitraum gestellt werden können, reduziere. Sie beschäftige ein Team von Mitarbeitern, um Scrapingaktivitäten zu erkennen und zu verhindern. Sie habe auch Captcha-Abfragen (automatisierter Turing Test, um Computer von Menschen zu unterscheiden) genutzt. Dies sei eine Möglichkeit herauszufinden, ob hinter einer Anfrage ein menschlicher Nutzer stehe. Gänzlich verhindern lasse sich das Scraping öffentlich einsehbarer Daten nicht. Des Weiteren habe die Beklagte die CIT-Funktion nach dem Vorfall dergestalt geändert, dass sie die Anzeige direkter Kontaktübereinstimmungen durch eine Liste mit Kontaktvorschlägen, der „Menschen, die Du kennen könntest“- Funktion ersetzt habe. Die Datenrichtlinien und die Hinweise zur Privatspähreneinstellung seien hinreichend klar. Die Beklagte habe z. B. einen Privatssphärencheck angeboten, in dem die Nutzer ihre Einstellungen überprüfen konnten. Der Klageantrag Ziffer 1 auf Zahlung sei unzulässig, weil er nicht ausreichend bestimmt sei. Es werde eine Vielzahl vermeintlicher Verstöße gerügt, diese stellten unterschiedliche Streitgegenstände dar. Es sei nicht ersichtlich, womit der immaterielle Schaden begründet werde. Ein erstattungsfähiger immaterieller Schaden sei nicht entstanden. Soweit ein Kontrollverlust und Sorgen vor einer Weiterverbreitung der Daten beklagt würden, finde sich der identische Vortrag auch in den weiteren ca. 6.000 Klagen gegen die Beklagte. Der Kontrollverlust sei kein erstattungsfähiger Schaden. Für den Feststellungsantrag Ziffer 2 fehle es an einem Feststellungsinteresse, denn es sei fernliegend, dass mit den gescrapten Daten ein Vermögensschaden der Klagepartei noch herbeigeführt werden könne. Jedenfalls fehle eine hinreichende Wahrscheinlichkeit des Schadenseintritts. Die abgegriffenen Daten erhöhten nicht die Gefahr schwerwiegender Internetverbrechen, denn die Daten seien ohnehin öffentlich einsehbar gewesen. Der Klageantrag Ziffer 3 sei unzulässig, da er nicht hinreichend bestimmt sei. Der Auskunftsanspruch bestehe schon deshalb nicht, weil die Auskunft erteilt worden sei.

Das Landgericht Leipzig hat die Klage mit Urteil vom 08.03.2024 - auf das wegen der Einzelheiten Bezug genommen wird - abgewiesen.

Hiergegen richtet sich die Berufung des Klägers. Er meint, er sei nicht ausreichend über die Art und Weise der Verarbeitung der sie betreffenden Daten aufgeklärt worden. Die Transparenz sei bei den verschachtelten Informationen nicht gewahrt. Die Verarbeitung sei rechtswid-

rig gewesen, weil es an einem Rechtfertigungsgrund gefehlt habe. Zudem habe die Beklagte keine ausreichenden Sicherheitsvorkehrungen gegen das Scraping getroffen. Dies belege schon das Einschreiten der irischen Datenschutzaufsichtsbehörde. Darüber hinaus habe die Beklagte ihre Melde- und Benachrichtigungspflichten sowie die Pflicht zur Datenschutz-Folgenabschätzung verletzt. Die Beklagte trage die Beweislast dafür, dass sie die Voraussetzungen der DSGVO erfülle. Allein der Kontrollverlust über die Daten sowie auch Sorgen und Ängste im Hinblick auf die Spam sms und Anrufe seien ein zu ersetzender immaterieller Schaden. Ein Mitverschulden liege nicht vor. Die Kausalität sei zu bejahen, denn die Zahl der Anrufe und Nachrichten sei im Zeitraum des Scrapings und der Veröffentlichung schlagartig angestiegen. Es sei ein Schadensersatzbetrag von mindestens 1.000 EUR anzusetzen. Bei der Bemessung sei zu berücksichtigen, dass die Zuwiderhandlung schwer wiege. Der Feststellungsanspruch bestehe, denn die Möglichkeit des Eintritts eines Schadens sei gegeben. Zu Unrecht habe das Landgericht die Unterlassungsanträge abgewiesen. Der Anspruch ergebe sich aus Vertrag und Gesetz. Es bestehe eine Wiederholungsgefahr. Schließlich sei die Beklagte ihrer Verpflichtung zur Auskunft nicht nachgekommen. Das Landgericht habe den Auskunftsanspruch zu Unrecht abgewiesen. Das Verfahren sei auszusetzen und dem Europäischen Gerichtshof vorzulegen.

Der Kläger beantragt:

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

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

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,
a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die

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

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

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

Die Beklagte beantragt, die Berufung zurückzuweisen.

Sie verteidigt das landgerichtliche Urteil.

Wegen der Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen sowie die Protokolle der mündlichen Verhandlungen Bezug genommen.

II.

Die zulässige Berufung der Klagepartei ist zum Teil begründet.

A

Die internationale Zuständigkeit deutscher Gerichte ist gemäß Art. 18 Abs. 1 EuGVVO sowie gemäß Art. 79 Abs. 2, Satz 2 DSGVO gegeben, denn die Klagepartei hat ihren gewöhnlichen Aufenthalt in Deutschland. Der sachliche, räumliche und zeitliche Anwendungsbereich der am 25.05.2018 in Kraft getretenen Datenschutzgrundverordnung ist eröffnet.

B

Die Berufung der Klagepartei ist zum Teil begründet.

1.

Der Klagepartei steht lediglich ein Anspruch auf Ersatz eines immateriellen Schadens aus Art. 82 DSGVO in Höhe von 100 EUR zu. Die weitergehende Berufung war zurückzuweisen.

1.1

Der Zahlungsantrag ist hinreichend bestimmt gemäß § 253 ZPO.

Dem steht nicht entgegen, dass der geltend gemachte Schadensersatzanspruch auf mehrere behauptete Verstöße gestützt wird. Entgegen der Ansicht der Beklagten liegt keine Häufung unzulässiger alternativer Klagegründe bzw. Streitgegenstände vor. Der Streitgegenstand wird durch den Klageantrag, in dem sich die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt bestimmt, aus dem der Kläger die begehrte Rechtsfolge herleitet (§ 253 Abs. 2 Nr. 2 ZPO). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören, den der Kläger zur Stützung seines Rechtsschutzbegehrens dem Gericht vorträgt (vgl. BGH, Urteil vom 22.10.2013 – XI ZR 42/12, Rn 15 – juris).

Die Klagepartei begehrt mit dem Klageantrag zu 1) eine Entschädigungsleistung, die sich auf behauptete Verstöße gegen die DSGVO gründet – vor und nach deren Inkrafttreten - infolge der Veröffentlichung ihrer Daten und des Scraping-Vorfalls, damit auf einem einheitlichen Lebenssachverhalt und einen dadurch näher bestimmten Streitgegenstand (vgl. OLG Oldenburg, Urteil vom 21.05.2024 - 13 U 100/23, Rn 21 - juris; vgl. OLG Köln, Urteil vom 07.12.2023 - 15 U 33/23, Rn 26 - juris; vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 51 - juris). Dieser ist dadurch gekennzeichnet, dass die Klagepartei zum Zeitpunkt des Scrapings auf der von der Beklagten betriebenen Facebook-Plattform angemeldet war. Maßgeblich ist, ob die Beklagte zu diesem Zeitpunkt hinreichende Datenschutzvorkehrungen getroffen hatte, mit denen sie das Abgreifen der Daten hätte verhindern können, und wie sie im Nachhinein mit dem Vorfall umgegangen ist. Miteinander verknüpft sind sämtliche Einzelaspekte dieses Vorgangs durch die Daten, welche die Klagepartei bei der Registrierung hinterlegt hat. Dies stellt bei natürlicher Betrachtung einen einheitlichen Sachverhalt dar.

1.2.

Der Klagepartei steht ein Anspruch auf immateriellen Schadensersatz gemäß Art. 82 DSGVO zu. Die Beklagte hat bei der Verarbeitung der Daten gegen die Bestimmungen der DSGVO verstoßen (a), der Klagepartei daraus ein kausaler Schaden entstanden (b).

a)

Die Beklagte hat in mehrfacher Hinsicht bei der Datenverarbeitung gegen die DSGVO verstoßen. Sie hat gegen das Gebot der datenschutzfreundlichen Voreinstellung nach Art. 25 Abs. 2 DSGVO verstoßen (aa). Die Handynummer wurde ohne rechtfertigenden Grund nach Art. 6 DSGVO verarbeitet (bb). Offenbleiben kann, ob sie ausreichende technische und organisatorische Maßnahmen nach Art. 24, 32 DSGVO ergriffen hat (cc) und ob sie ihrer Benachrichtigungspflicht aus Art. 34, 25 DSGVO und ihrer Auskunftspflicht aus Art. 15 DSGVO nachgekommen ist (dd).

Verstöße im Rahmen des Anmeldeprozesses fallen aus dem zeitlichen Anwendungsbereich der DSGVO heraus, da die Datenerhebung vor dem 25.05.2018 abgeschlossen war.

Allerdings unterfällt die zeitlich nach dem 25.05.2018 liegende Weiterverarbeitung der Daten den Anforderungen der DSGVO, denn aus Erwägungsgrund 171 Satz 2 DSGVO sowie aus Art. 4 Nr. 2 DSGVO und Art. 24 Abs. 1 DSGVO ergibt sich die Pflicht, die Datenverarbeitungen, die zum Zeitpunkt der Anwendung der DSGVO bereits begonnen hatten, bis zum 25.05.2018 in Einklang mit der Verordnung zu bringen (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 72 - juris; vgl. auch Generalanwalt Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, Rn. 43 - juris). Zudem folgt aus Erwägungsgrund 171 Satz 3 DSGVO, dass die Beklagte zum 25.05.2018 zur Einholung neuer Einwilligungen verpflichtet gewesen ist, soweit bereits bestehende Einwilligungen nicht den Anforderungen an diese Verordnung entsprachen.

Es ist davon auszugehen, dass das Scraping nach dem 24.05.2018 erfolgte, da die Beklagte im Rahmen ihrer sekundären Darlegungslast nicht vorgetragen hat, dass sich der Vorfall vor dem Inkrafttreten der DSGVO ereignet hat

aa)

Die Beklagte hat gegen Art. 25 Abs. 2 DSGVO verstoßen, denn in dem relevanten Zeitraum war die Standardeinstellung für die Suchbarkeit nach der Telefonnummer auf „alle“ und damit nicht datenschutzfreundlich (data protection by default) auf „nur ich“ eingestellt. Dies hat die Beklagte eingeräumt. Nach Art. 25 Abs. 2 DSGVO muss die Beklagte geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch die Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der

Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Bei der Registrierung soll dem Betroffenen nämlich gewährleistet werden, dass er nur in eine solche Verarbeitung einwilligt, die die Veröffentlichung seiner Daten ohne sein Eingreifen kategorisch ausschließt (vgl. LG Freiburg (Breisgau), Urteil vom 15.09.2023 - 8 O 21/23, Rn 122 - juris). Der Betreiber eines sozialen Netzwerks soll damit verpflichtet werden, die Default-Einstellungen so zu treffen, dass Inhalte der Nutzer nicht standardmäßig mit anderen Nutzern oder Dritten geteilt werden (vgl. LG Freiburg a.a.O.). Als Voreinstellung ist daher der kleinstmögliche Empfängerkreis vorzusehen (vgl. LG Freiburg (Breisgau), Urteil vom 15.09.2023 - 8 O 21/23, Rn 122 - juris). Da der Kläger sich bereits vor dem 25.05.2018 registriert hat, hatte die Beklagte sicherzustellen, dass die datenschutzunfreundliche Voreinstellung zum 25.05.2018 unter Abkehr des „opt-out“ Systems geändert wird (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 128 - juris). Hierfür ist nichts ersichtlich. Die gewählte Voreinstellung war zur Erfüllung des Vertragszweckes nicht erforderlich, denn der Nutzer konnte auch ohne die Einstellung der Suchbarkeit auf „alle“ nach der Telefonnummer mit anderen in Kontakt treten und sich austauschen. Personen, die bereits über die Telefonnummer eines anderen Nutzers verfügen, können ohne weiteres mit ihm in Kontakt treten und sich auf facebook vernetzen. Es ist auch nicht ersichtlich, dass für den Geschäftszweck des Netzwerkes, personalisierte online Werbung zu platzieren, eine solche Sucheinstellung erforderlich war, zumal der Nutzer die Einstellung auch auf „nur ich“ setzen und die Plattform gleichwohl nutzen konnte.

Die Verletzung dieser Regelung hat auch dazu geführt, dass die Klagepartei es bei der Voreinstellung belassen hat und ihre Telefonnummer von den Scrapern ihrem Profil zugeordnet werden konnte.

bb)
Die Beklagte hat die Handynummer der Klagepartei mit der ab dem 25.05.2018 fortgesetzten Verarbeitung in der Suchbarkeitsfunktion ohne ausreichenden Rechtfertigungsgrund gemäß Art. 6 DSGVO verarbeitet. Die weitere Datenverarbeitung ist nur dann rechtmäßig, wenn ab diesem Zeitpunkt mindestens einer der Bedingungen des Art. 6 DSGVO vorliegt. Dies ist nicht der Fall.

(a) Die Verarbeitung war zur Erfüllung des Vertragszweckes nicht erforderlich i.S.d. Art. 6 Abs.1 b) DSGVO. Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne von Art. 6 Abs.1 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 so-

mit nachweisen können, dass der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (vgl. EuGH, Urteil vom 04.07.2023 - C - 252/21, Rn 98 - juris; vgl. OLG Oldenburg, Urteil vom 21.05.2024 - 13 U 100/23, Rn 29 - juris; vgl. OLG Hamm Urteil vom 15.08.2023 - 7 U 19/23, Rn 97 - juris). Dafür ist nichts ersichtlich. Der Contact Import Tool mag zwar für den Nutzer praktisch sein, aber zur Nutzung der Plattform ist die Funktion nicht notwendig. Der Nutzer kann facebook auch nutzen, ohne seine Telefonnummer in der Suchbarkeitsfunktion auf „alle“ zu setzen. Die Beklagte hat jedenfalls nicht dargetan, dass die Funktion unerlässlich für die Vertragsdurchführung gewesen ist. Die fehlende Erforderlichkeit der Auffindbarkeit über das CIT Tool ergibt sich schon daraus, dass die Angabe der Telefonnummer bei der Anmeldung bei Facebook nicht zwingend ist und das CIT im Jahr 2018 für den PC und 2019 für den Messenger Dienst ausgeschaltet wurde, ohne dass die Nutzbarkeit der Plattform wesentlich gelitten hätte. Auf die Ausführungen unter aa) wird im Übrigen Bezug genommen.

(b) Die Beklagte konnte sich ab dem 25.05.2018 nicht auf eine wirksame Zustimmung der Klagepartei stützen, Art. 6 Abs.1 a), Art. 5 Abs.1 a), Art. 13 Abs.1 DSGVO, da sie diese über die Zwecke der Verarbeitung der Telefonnummer nicht transparent informiert hat. Die Beklagte kann sich insoweit nicht auf die vor dem 25.05.2018 erklärte Einwilligung stützen, denn diese konnte unter der Geltung der DSGVO keine rechtfertigende Wirkung mehr entfalten (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 114 - juris). Nach Erwägungsgrund Nr. 171 DSGVO musste eine vorab erteilte Einwilligung bereits den Bedingungen der DSGVO entsprechen, um fortzugelten. Daran fehlt es. Denn auch die im April 2018 von der Beklagten zur Verfügung gestellten Bedingungen genügen den Anforderungen der DSGVO nicht (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 114 - juris). Auf eine wirksame Zustimmung beruft sich die Beklagte letztendlich nicht, sie liegt auch nicht vor.

Die wirksame Zustimmung setzt die Information des Nutzers nach Art. 5 Abs.1 a) DSGVO und Art. 13 Abs. 1 DSGVO voraus. Es ist bei der Einwilligung eine Voraussetzung ihrer Wirksamkeit, dass über die Datenverarbeitungsvorgänge Transparenz hergestellt wird, bevor die betreffende Person die Einwilligung erteilt (vgl. Taeger in Taeger/Gabel (Hrsg.) DSGVO, 2022, Art. 6 Rn 37; vgl. OLG Hamm, Urteil vom 25.08.2023 - 7 U 19/23, Rn 113 - juris).

Art. 13 Abs. 1 c) DSGVO verlangt bei der Erhebung personenbezogener Daten bei der betroffenen Person, dass der Verantwortliche der Person zum Zeitpunkt der Erhebung der Daten die Zwecke mitteilt, für die die personenbezogenen Daten verarbeitet werden sollen. Dabei sind alle Zwecke anzugeben, die die verantwortliche Stelle im Zeitpunkt der Erhebung verfolgt

(vgl. LG Freiburg, Urteil vom 15.09.2023 - 8 O 21/23, Rn 88 - juris). Die Informationspflicht aus Art. 13 DSGVO soll die betroffenen Personen von Beginn an in die Lage versetzen, bestimmen und einschätzen zu können, wer was wann über sie weiß (vgl. LG Freiburg, Urteil vom 15.09.2023 - 8 O 21/23, Rn 88 - juris). Nach ihrem Zweck müssen die Informationspflichten (ggf. unmittelbar) vor Beginn der Datenerhebung erfüllt werden. Denn die Informationen sollen der betroffenen Person auch ermöglichen, darüber zu entscheiden, ob sie in die Verarbeitung ihrer Daten einwilligt bzw. ob sie hiergegen Einwände erhebt. Dieser Zweck würde bei einer Information nach Beginn der Datenerhebung verfehlt oder zumindest beeinträchtigt (LG Freiburg a.a.O.).

Aus der von der Beklagten vorgelegten Anlage B 5 (Wie kann ich festlegen, wer mich über meine e-mail Adresse oder Handynummer auf Facebook finden kann) wird nicht hinreichend klar, dass der Nutzer auch ohne seine Telefonnummer in der Zielgruppenauswahl auf „öffentlich“ zu stellen über seine Handynummer gefunden werden kann. Vielmehr erweckt der folgende Hinweis den Eindruck, dass der Nutzer nur dann anhand der Telefonnummer gefunden werden kann, wenn er festlegt, wer seine Telefonnummer sehen kann:

„Beachte bitte, dass du separat festlegen kannst, wer deine Telefonnummer und deine E-Mail-Adresse in deinem Profil sehen kann. Wenn du deine Telefonnummer oder deine E-Mail-Adresse in deinem Profil mit jemandem teilst, kann diese Person dich anhand dieser Informationen finden...“

Die von der Beklagten vorgelegte Anlage B 6 (Wozu verwendet Facebook meine Mobilnummer) enthält keinen Hinweis darauf, dass die Klagepartei allein anhand der angegebenen Telefonnummer, die nicht „öffentlich“ sichtbar ist, gefunden werden kann. Wörtlich weist die Beklagte zur Verwendung der Handynummer auf folgendes hin: „Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst.“ Damit ist die Suchbarkeit mittels CIT nicht ausreichend klar umschrieben. Aus der Datenrichtlinie (B 9) ist dazu ebenfalls nichts zu entnehmen.

Die Registrierungsseite von Facebook weist auf die – verlinkte – Datenrichtlinie hin. Dort wurde der Nutzer jedoch nicht darüber aufgeklärt, dass und wie seine Telefonnummer im Rahmen des Einsatzes des CIT verwendet wird. Insbesondere wurde ihm nicht verdeutlicht, dass die Telefonnummer ohne Veränderungen der Einstellungen angesichts der Standardvoreinstellung für die Suchbarkeit über die Telefonnummer auf „für alle“ bereits mit deren Angabe genutzt werden kann, um ihn auf Facebook und insbesondere auch über das CIT zu finden.

Dazu hätte dem Nutzer erläutert werden müssen, dass die Verwendung des CIT der Messenger App es anderen Benutzern ermöglicht, mittels Abgleichs von in deren Smartphone gespeicherten Telefonkontakten mit der Mobilfunknummer des Nutzers im Falle eines „Treffers“ dessen Benutzerprofil als „Freund“ hinzufügen und auf die entsprechenden Daten zuzugreifen (so LG Freiburg (Breisgau); Urteil vom 15.09.2023 - 8 O 21/23, Rn 90 - juris).

cc)
Im Hinblick auf die unter aa) und bb) festgestellten Verstöße der Beklagten kann offenbleiben, ob sie zudem gegen ihre Verpflichtung verstoßen hat, ausreichende geeignete technische und organisatorische Maßnahmen zu treffen, um die personenbezogenen Daten gegen unbefugte Zugriffe Dritter zu schützen, Art. 24, 32 DSGVO.

dd)
Offenbleiben kann ebenfalls, ob die Beklagte ihre Benachrichtigungspflicht aus Art. 34 DSGVO gegenüber der Klagepartei, aus Art. 33 DSGVO gegenüber der Aufsichtsbehörde oder die Auskunftspflicht nach Art. 15 DSGVO verletzt hat, denn ein kausaler Schaden der Klagepartei, der auf der Verletzung von Benachrichtigungspflichten beruhen könnte, ist nicht ersichtlich (vgl. hierzu auch OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 147 - juris). Die Klagepartei hat nicht dargelegt, welcher Schaden ihr daraus entstanden sein soll. Der Kontrollverlust und die Veröffentlichung der Daten und die nach der Behauptung der Klagepartei darauf beruhenden ungebetenen Anrufe sowie spam sms und spam e-mails können nur auf dem Scraping Vorfall und nicht auf der Verletzung von Benachrichtigungs- und Auskunftspflichten zurückzuführen sein.

Unabhängig davon kann ein Schadensersatzanspruch nach Art. 82 DSGVO ohnehin nicht auf die Verletzung der vorgenannten Pflichten gestützt werden, da keine „Verarbeitung personenbezogener Daten“ vorliegt. Nach der Rechtsprechung des EuGH setzt der Anspruch die Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmung der DSGVO voraus (vgl. EuGH, Urteil vom 04.05.2023 - C - 300/21, Rn 36 - juris; vgl. Moos/Schlefzig in Taeger/Gabel (Hrsg.) DSGVO, 2022, Art. 82 Rn 22). Dies belegt auch die Formulierung in Erwägungsgrund Nr. 146, wonach Schäden ersetzt werden, die „aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht“.

b)
Dem Kläger ist ein immaterieller kausaler Schaden entstanden, den der Senat mit 100 EUR bemisst, § 82 DSGVO.

Art. 82 Abs. 2 DSGVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt die drei Voraussetzungen für die Entstehung des Schadenersatzanspruchs, nämlich eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (so EuGH Urteil vom 04.05.2023 - C - 300/21, Rn 36 - juris). Der europäische Gerichtshof stützt sich auf den 146. Erwägungsgrund, der auf „Schäden“ abstellt, „die einer Person aufgrund einer Verarbeitung entstehen“. Zwar muss der Schaden nicht eine gewisse Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urteil vom 04.05.2023 - C - 300/21, 49, 50 - juris; vgl. Urteil vom 20.06.2024 - C - 590/22 - juris). Der Schaden muss tatsächlich und sicher entstanden sein (vgl. EuGH, Urteil vom 04.04.2017 - C - 337/15, Rn 91 - juris; vgl. EuGH, Urteil vom 20.06.2024 - C - 590/22, Rn 35, 36 - juris).

aa)
Durch den Kontrollverlust der Mobiltelefonnummer und deren Veröffentlichung im Darknet ist kein materieller Schaden eingetreten. Dies behauptet die Klagepartei auch nicht.

bb)
Der Kontrollverlust der Daten und deren Veröffentlichung im Darknet hat im vorliegenden Fall zu einem - wenngleich nur geringfügigen - immateriellen Schaden im Sinne von Art. 82 DSGVO bei der Klagepartei geführt.

Soweit die Daten der Klagepartei ohnehin öffentlich einsehbar sind - wie Vor- und Nachname, Geschlecht und Nutzer ID - liegt schon objektiv kein Kontrollverlust vor. Denn diese Daten sind mit der Registrierung anzugeben und zwingend stets öffentlich und für jedermann weltweit einsehbar. Auch ohne Scraping ist ein Auslesen dieser Daten und deren Verbreitung im Internet jederzeit möglich. Mit der Registrierung bei der Beklagten standen diese stets öffentlichen Daten nicht mehr unter der ausschließlichen Kontrolle der Klagepartei. Sie hat vielmehr bewusst auf die Kontrolle verzichtet. Dem Erfordernis eines konkreten Schadens liefe es zuwider, würde man in Bezug auf diese Daten bereits einen abstrakten "Kontrollverlust" des - im Ergebnis sogar eines jeden - Plattformnutzers ausreichen lassen. Durch das Scraping dieser vom Nutzer freiwillig zur Verfügung gestellten Daten wird der bereits durch die Anmeldung eingetretene Kontrollverlust nach Auffassung des Senats nicht in einer Weise vertieft, dass hieraus ein konkreter immaterieller Schaden abgeleitet werden könnte.

Nach der Rechtsprechung des EuGH (Urteil vom 14.12.2023 C - 340/21 - juris; vgl. Urteil vom 20.06.2024 - c - 590/22 - Rn 33, juris)) kann der Kontrollverlust grundsätzlich einen immateriellen Schaden begründen. Aus dieser beispielhaften Aufzählung im Erwägungsgrund Nr. 85 der „Schäden“, die den betroffenen Personen entstehen können geht hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen „Verlust der Kontrolle“ über ihre eigenen Daten infolge eines Verstoßes gegen die DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (vgl. EuGH, Urteil vom 14.12.2023 - C - 340/21, Rn 82 - juris). Allerdings muss eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (vgl. EuGH, a.a.O. Rn 84; vgl. EuGH, Urteil vom 20.06.2024 - C - 590/22 - juris). Wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, ist aber gleichwohl zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. EuGH a.a.O., Rn 85). An dem Erfordernis eines kausalen Schadens hat der Europäische Gerichtshof festgehalten.

Dies deckt sich mit der Funktion des aus Art. 82 Abs.1 DSGVO folgenden Anspruches auf Schadensersatz, einen konkreten Schaden auszugleichen. Ließe man einen für den Betroffenen folgenlosen Kontrollverlust als immateriellen Schaden zu, müsste die Höhe des Schadensersatzes konsequent auf null EUR lauten. Denn für die Bemessung des Ersatzes des immateriellen Schadens kommt es letztlich im Hinblick auf die Ausgleichsfunktion des Art. 82 Abs. 1 DSGVO nur auf die konkreten Auswirkungen für die betroffene Person an, nicht aber beispielsweise auf Strafzwecke, Schwere des Verschuldens, Schwere des Verstoßes gegen die DSGVO oder die Anzahl der Verstöße gegen die Datenschutzgrundverordnung (vgl. OLG Hamm, Urteil vom 21.06.2024 - 7 U 154/23, Rn 48 - juris, bezugnehmend auf EuGH, Urteil vom 20.06.2024 - C - 590/22, Rn 24 - juris).

Die betroffene Person muss die Tatsachen, die dazu führen können, dass ein „tatsächlich erlittener immaterieller Schaden“ infolge der Verletzung des Schutzes personenbezogener Daten anerkannt werden kann, genau und nicht nur allgemein darlegen, auch wenn er nicht eine im Voraus festgelegte Schwelle von besonderer Schwere erreicht. Entscheidend ist, dass es sich nicht um eine bloße subjektive Wahrnehmung handelt, die veränderlich ist und auch vom

Charakter und von persönlichen Faktoren abhängt, sondern um die Objektivierung einer, wenn auch geringfügigen aber nachweisbaren Beeinträchtigung der physischen oder psychischen Sphäre oder des Beziehungslebens einer Person; die Art der betroffenen personenbezogenen Daten und die Bedeutung, die sie im Leben der betroffenen Person haben und vielleicht auch die Wahrnehmung, die die Gesellschaft zu diesem Zeitpunkt von dieser spezifischen, mit der Datenverletzung verbundenen Beeinträchtigung hat (vgl. Schlussanträge des GA Pitruzella vom 27.04.2023 - C 340/21, Rn 83 - juris).

Unter Berücksichtigung der Umstände kann die Befürchtung der Klagepartei, dass die Daten missbräuchlich verwendet werden, nicht als unbegründet angesehen werden.

Der Kläger hat einen immateriellen Schaden nachgewiesen. Er hat vor dem Landgericht eine zwar kurzzeitige, jedoch störende Beeinträchtigung mit andaurenden Telefonaten geschildert, der er nur durch Wechsel seiner Telefonnummer habe entgehen können. Der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten kann einen „immateriellen Schaden“ im Sinne von Art. 82 Abs. 1 DSGVO darstellen, der einen Schadensersatzanspruch begründet, sofern die betroffene Person den Nachweis erbringt, dass sie tatsächlich einen solchen Schaden – so geringfügig er auch sein mag – erlitten hat, wobei der bloße Verstoß gegen die Bestimmungen der DSGVO nicht ausreicht, um auf dieser Grundlage einen Schadensersatzanspruch zu begründen (vgl. EuGH, Urteil vom 20.06.2024 - C - 590/22, Rn 33 - juris). Der Kläger hat vor dem Landgericht geschildert, dass er 2022 und 2023 mit einer Vielzahl von sms „bombardiert“ worden sei. Anrufe hätten sich teilweise nicht zurückverfolgen lassen, in einem Fall sei ihm auf seinen Rückruf hin mit verfremdeter Stimme gedroht worden, er habe eine Straftat begangen und werde international gesucht, was er mit einer Zahlung abwenden solle. Obwohl er den Anruf abgeblockt habe, sei er aber dann innerhalb einer Stunde mehrfach telefonisch wieder kontaktiert worden. Das Telefonat habe er nicht mehr annehmen können. Dies sei so oft passiert, dass er seinen Telefonprovider angerufen und binnen 5 Tagen seine Rufnummer geändert habe. Danach habe es keine Anrufe mehr gegeben. Es seien danach aber noch sms und e-mails gekommen, die im Spamordner gelandet seien.

Der Senat war nicht gehalten den Kläger erneut zu hören. Denn die vom Landgericht abweichende Würdigung der Angaben des Klägers wird auf seine protokollierten Angaben in der mündlichen Verhandlung vom 07.02.2024 gestützt, an deren Wahrheitsgehalt das Landgericht keine Zweifel geäußert hat, denen es aber - anders als der Senat - keinen immateriellen Schaden entnommen hat. Eine erneute Vernehmung kann dann unterbleiben, wenn das Berufungsgericht seine abweichende Würdigung auf solche Umstände stützt, die weder die Urteilsfähig-

keit, das Erinnerungsvermögen oder die Wahrheitsliebe des Zeugen noch die Vollständigkeit und Widerspruchsfreiheit seiner Aussage betreffen (vgl. BVerfG, Beschluss vom 14.09.2010 - 2 BvR 2638/09 - juris; vgl. BGH, Beschluss vom 30.11.2011 - III ZR 165/11 - juris). Dies ist hier der Fall.

Ein Kausalzusammenhang zwischen dem Scraping Ereignis und dem belästigenden Anrufen, die zu dem Rufnummernwechsel geführt hat, ist zu bejahen. Zwar ist das Scraping Ereignis im Jahr 2019 erfolgt. Gleichwohl können die häufigen Anrufe, die nicht mehr angenommen werden konnten auf die Veröffentlichung der Telefonummer, die im Jahr 2021 im Darknet veröffentlicht wurde, zurückgeführt werden. Soweit er nach der Änderung seiner Handynummer noch spam sms erhalten haben will, kann dies nicht mehr auf dem Scraping beruhen. Der Erhalt von spam e-mails steht in keinem erkennbaren Zusammenhang mit dem Scraping Ereignis, denn die e-mail Adresse war davon nicht betroffen.

Mit 100 Eur ist der immaterielle Schaden des Klägers angemessen ausgeglichen. Dem Schadensersatzanspruch kommt keine Straffunktion zu (vgl. EuGH, Urteil vom 25.01.2024 - C-687/21, Rn 46 ff. - juris). Der EuGH hat angenommen, dass in Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs eine auf diesen Artikel gestützte finanzielle Entschädigung als „vollständig und wirksam“ anzusehen ist, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen, ohne dass ein solcher vollumfänglicher Ausgleich die Verhängung von Strafschadenersatz erfordert (vgl. EuGH, Urteil vom 21.12.2023 - C-667/21, Rn 84 - juris). Ebensowenig ist die Schwere des Verstoßes zu berücksichtigen (vgl. EuGH, Urteil vom 25.01.2024 - C-687, Rn 54 - juris). Im Hinblick auf die lediglich kurzzeitige Beeinträchtigung des Klägers seiner Handynutzung von einer knappen Woche ist kein höherer Ansatz gerechtfertigt, auch wenn mit einem Wechsel der Rufnummer eine gewisse Lästigkeit verbunden sein mag.

2.
Der Klagepartei steht kein Anspruch auf Feststellung der Verpflichtung der Beklagten, alle künftigen (materiellen) Schäden zu erstatten, zu. Der Antrag ist bereits unzulässig, weil ihm das Rechtsschutzbedürfnis fehlt, § 256 ZPO.

Grundsätzlich hängt die Zulässigkeit einer Feststellungsklage bei reinen Vermögensschäden von der Wahrscheinlichkeit eines auf die Verletzung zurückzuführenden Schadenseintrittes ab (vgl. BGH, Urteil vom 10.07.2014 - IX ZR 197/12, Rn. 11 - juris). Ausreichend ist, dass nach

der Lebenserfahrung und dem gewöhnlichen Verlauf der Dinge mit hinreichender Wahrscheinlichkeit ein erst künftig aus dem Rechtsverhältnis erwachsender Schaden angenommen werden kann (BGH, a.a.O.). Bei der Verletzung eines absoluten Rechtes genügt aber die ausreichende Möglichkeit des Eintrittes eines Schadens (vgl. BGH, Urteil vom 29.06.2021 - VI ZR 52/18, Rn. 30 - juris). Die Möglichkeit materieller Schäden reicht hier für die Annahme eines Feststellungsinteresses mithin aus (so BGH, Urteil vom 29.06.2021 - VI ZR 52/18, Rn. 30 - juris). Ein Feststellungsinteresse ist nur dann zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen (vgl. BGH, Beschluss vom 09.01.2007 - VI ZR 133/06, Rn. 5 - juris). Dies ist der Fall. Vorliegend ist auch vier Jahre nach dem Vorfall kein Schaden eingetreten. Die Klagepartei macht zwar geltend, dass gleichwohl in der Zukunft aufgrund der Veröffentlichung ihrer Telefonnummer eine erhebliche Belästigung durch betrügerische Anrufe möglich sei, weil es nicht selten passiere, dass sich Anrufer als Bankmitarbeiter ausgäben, um an sensible Kontaktdaten der angerufenen Person zu gelangen. Es bestehe daher weiter die Gefahr der missbräuchlichen Nutzung der entwendeten Daten. Diese Auffassung teilt der Senat schon deshalb nicht, weil die Wahrscheinlichkeit eines Schadenseintritts mit zunehmender Distanz zum Scraping-Ereignis abnimmt und sich der Kausalzusammenhang dadurch immer schwerer beweisen lässt. Dies gilt hier auch deshalb, weil die Klagepartei ihre Handy-Nummer im Internet auch bei anderen Gelegenheiten, z. B. bei Paypal und bei der Bank verwendet. Im Hinblick darauf, dass vier Jahre nach dem Scraping-Vorfall und dem unbefugten Zugriff Dritter auf die Daten ein kausaler materieller Schaden nicht entstanden ist und auch keine konkreten Anhaltspunkte dafür bestehen, dass der Klagepartei eine Gefährdung ihres Vermögens drohen könnte, kann nach alledem davon ausgegangen werden, dass mit dem Eintritt eines materiellen Schadens nicht mehr zu rechnen ist (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn. 215 - juris).

Die Auffassung des OLG Stuttgart (Urteil vom 22.11.2023 – 4 U 20/23 - Rn 233 ff. - juris), das Feststellungsinteresse sei infolge des Kontrollverlusts über die Daten gegeben, teilt der Senat nicht. Dem Vortrag der Klagepartei lassen sich keine Anhaltspunkte dafür entnehmen, dass im Hinblick auf die konkret betroffenen Daten und sein Verhalten noch ein materieller Schaden drohen könnte (vergleiche auch OLG Hamm, Urteil vom21.06.2024 - 7 U 154/23, Rn 64 - juris; OLG Hamm, Urteil vom 15 2823 – 7 U 19/23 – juris, Rn. 214 ff., so auch OLG Köln, Urteil vom 07.12.2023 - 15 U 33/23 - juris).

3.

a)

Die Klagepartei hat keinen Anspruch auf Unterlassung gemäß Ziffer 3 a) ihres Antrages. Der Antrag ist zu unbestimmt und daher unzulässig.

Ein Klageantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt. Dies ist bei einem Unterlassungsantrag regelmäßig der Fall, wenn die konkret angegriffene Verletzungsform antragsgegenständlich ist (vgl. BGH; Urteil vom 09.03.2021 - VI ZR 73/20, Rn 15 - juris).

Der Antrag Ziffer 3 a) hat indes keinen vollstreckungsfähigen Inhalt. Die Begriffe „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen“ und „unbefugten Dritten“ sind zu unbestimmt und nicht vollstreckbar. Der Formulierung lässt sich nicht entnehmen, welche konkreten Maßnahmen die Beklagte ergreifen soll (vgl. LG Köln, Urteil vom 24.05.2023, Rn 46 - juris). Sie beschränkt sich nicht auf die Wiedergabe des gesetzlichen Verbotstatbestandes 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. Es ist aus dem Antrag bei dieser Fassung nicht hinreichend ersichtlich, welche Maßnahmen konkret gefordert werden. 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 (vgl. LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn 59 - juris). 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 (vgl. LG Lübeck a.a.O.). Schließlich steht zwischen den Parteien im Streit, welche Maßnahmen dem Stand der Technik entsprechen. Die auslegungsbedürftige Antragsformulierung lässt sich auch nicht durch Auslegung unter Heranziehung des Vortrags der Klagepartei eindeutig präzisieren. Das Verlangen von „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ würde somit dazu führen, dass der Streit, welche Maßnahmen nach dem jeweils aktuellen Stand der Technik erforderlich sind und damit auf welche Art und Weise die Datenverarbeitung auf der Plattform der Beklagten abzusichern ist, in unzulässiger Weise

in das Vollstreckungsverfahren verlagert wird (vgl. OLG Stuttgart, Urteil vom 26.06.2024 - 4 U 114/23, Rn 41 - juris).

Darüber hinaus ist der Antrag Ziffer 3 a mit der geforderten Androhung nach § 890 Abs. 2 ZPO unzulässig. Die Titulierung einer Unterlassungsverpflichtung kann - auch unter Berücksichtigung der Grundsätze der Effektivität und Äquivalenz - eine gleichfalls nach § 890 ZPO vollstreckbare Verpflichtung zur Handlung nur beinhalten, wenn der Schuldner der Pflicht zur Unterlassung ausschließlich genügen kann, indem er die hierfür erforderliche positive Handlung vornimmt. Ob ein Titel Handlungspflichten auferlegt oder Unterlassung fordert, ist im Wege der Auslegung mit Blick auf den Schwerpunkt der jeweils in Rede stehenden Verpflichtung zu beurteilen (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 221 - juris).

Vorliegend fordert die Klagepartei mit dem Antrag Ziffer 3 a im Schwerpunkt ein aktives Tun, das nicht nach § 890 ZPO, sondern als vertretbare Handlung nach § 887 ZPO zu vollstrecken ist - nämlich zukünftig Kontaktimportfunktionen nur im Einklang mit den einzuhaltenden Sicherheitsvorkehrungen "freizuschalten", um Zugriffe unbefugter Dritter nach Möglichkeit von vorneherein zu verhindern - so wie es die DSGVO verlangt (vgl. OLG Hamm, Urteil vom 15.08.2023 - 7 U 19/23, Rn 222 - juris). Die Klagepartei will gar kein Unterlassen der Nutzung der Kontaktimportfunktion, was sie durch eine schlichte Umstellung der Suchbarkeitseinstellungen hätte erreichen können und tatsächlich inzwischen erreicht hat, sondern sie will, dass sie die bzw. zukünftig irgendeine andere Kontaktimportfunktion unter Wahrung der Sicherheitsanforderungen nutzen kann (vgl. OLG Hamm a.a.O.).

b)
Der unter Ziff. 3 b geltend gemachte Antrag, es zu unterlassen, die Telefonnummer der Klagepartei unter den dort genannten Einschränkungen weiterzuverarbeiten, ist unzulässig. Zum einen ist nach der Formulierung unklar, ob es sich hierbei überhaupt um einen Unterlassungs-, oder nicht vielmehr um einen Antrag auf zukünftige Leistung handelt, ohne dass die Voraussetzungen des § 259 ZPO vorlägen. Es fehlt aber insbesondere an einem Rechtsschutzbedürfnis (vgl. Senat, Urteil vom 05.12.2023 - 4 U 1094/23 - juris). Der Antrag ist darauf gestützt, der Beklagten die Weiterverarbeitung auf der Grundlage einer für unwirksam erachteten Einwilligung zu untersagen. Diesem Begehren kann aber mit einem Widerruf dieser Einwilligung nach Art. 7 Abs. 3 DSGVO jederzeit Rechnung getragen werden, ohne dass hierfür ein Unterlassungsanspruch geltend gemacht werden müsste (vgl. auch OLG Stuttgart, Urteil vom 26.06.2024 - 4 U 114/23, Rn 44 - juris). Angesichts des Umstandes, dass der Unterlassungsanspruch insoweit auch ausdrücklich mit der möglichen Verwendung der Telefonnummer

über das CIT begründet wird, dieses Tool aber unstreitig spätestens seit Oktober 2019 nicht mehr besteht, ist jedenfalls ein Rechtsschutzbedürfnis für einen in die Zukunft gerichteten Unterlassungsantrag nicht mehr zu erkennen (vgl. Senat, Urteil vom 05.12.2023 - 4 U 1094/23 - juris; vgl. auch OLG Stuttgart, Urteil vom 26.06.2024 - 4 U 114/23, Rn 47 - juris). Eine Wiederholungsgefahr wäre jedenfalls zu verneinen. Die Verletzung einer Unterlassungsverpflichtung begründet die Vermutung der Wiederholungsgefahr nicht nur für identische Verletzungsformen, sondern auch für andere Vertragspflichtverletzungen, soweit die Verletzungshandlungen im Kern gleichartig sind (BGH, Urteil vom 29.07.2021 – III ZR 192/20 –, Rn. 115 - 116,- juris; vgl. Senat, Urteil vom 05.12.2023 - 4 U 1094/23 - juris). An die Entkräftung dieser Vermutung sind strenge Anforderungen zu stellen. Sie ist ausnahmsweise dann als widerlegt anzusehen, wenn der Eingriff durch eine einmalige Sondersituation veranlasst war (BGH, Urteil vom 27.04.2021 – VI ZR 166/19 –, Rn. 23, -juris; Senat, Beschluss vom 4.10.2021 – 4 W 625/21 –, Rn. 5, - juris). Eine solche Sondersituation ist vorliegend allerdings mit Blick auf die Deaktivierung des CIT und dessen Ersatz durch die people-you-may-know (social-connection-check) Funktion gegeben. Eine solche aufwändige Umprogrammierung der Suchfunktion eines Unternehmens mit weit über einer Milliarde Nutzern erfordert einen derartigen Aufwand, dass nicht davon auszugehen ist, dass diese Umprogrammierung alsbald wieder rückgängig gemacht und die hiervon ausgehende Gefahr erneut in Kauf genommen würde (vgl. Senat, Urteil vom 05.12.2023 - 4 U 1094/23 - juris). Dass sich der hier festgestellte Schadenshergang wiederholt, könnte der Nutzer überdies selbst in diesem Fall durch eine einfache Änderung der Voreinstellungen bewirken. Stellt er die Einstellungen von „alle“ auf „nur ich“ zurück, und würden seine Daten dann (erneut) gescraped, so wäre das indes ein anderer Schadenshergang.

4.

Der Klagepartei steht kein Anspruch auf Auskunft nach Art. 15 DSGVO zu, denn der Anspruch ist durch das Schreiben der Beklagten erfüllt worden, § 362 BGB.

Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung (vgl. OLG Hamm im Urteil vom 15.08.2023 - 7 U 19/23, Rn 244 ff. - juris). 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 Unrichtig-

keit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (vgl. BGH Urt. v. 15.6.2021 - VI ZR 576/19, - juris).

Das zur Akte gereichte anwaltliche Antwortschreiben der Beklagten enthält eine Beschreibung des Scrapings, die Mitteilung, dass die Beklagte keine Kopie der Rohdaten hält, welche abgerufen worden waren und eine Auflistung der Datenpunkte, die gescraped wurden. Des Weiteren enthält das Schreiben eine Erläuterung des Datenabrufs über die immer öffentlichen Daten, das Facebook-Profil und die Kontaktimportfunktion, die zeitliche Angabe "im Zeitraum bis September 2019" und den Hinweis auf das Handeln möglicherweise mehrerer Scraper. Die Beklagte hat einen Link übersandt, auf der über den individuellen Nutzer gespeicherte Daten eingesehen werden können. Damit hat die Beklagte zu erkennen gegeben, dass sie vollständig Auskunft erteilt hat.

Soweit die Klagepartei weitergehend Auskunft darüber verlangt, welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des CIT erlangt werden konnten, steht ihrem Anspruch § 275 Abs. 1 BGB entgegen. Insofern weist die Beklagte unwidersprochen darauf hin, dass ihr die Identitäten der Scraper nicht bekannt seien, weswegen ihr eine Auskunftserteilung unmöglich ist.

C

1.

Eine Aussetzung des Verfahrens entsprechend § 148 ZPO war nicht veranlasst. Schließlich entscheidet der Senat nicht als letztinstanzliches Gericht und ist zur Vorlage daher nicht verpflichtet.

2.

Die Entscheidung über die Kosten folgt aus §§ 92 Abs.2, 97 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 ZPO.

3.

Die Revision war gemäß § 543 Abs.2 Nr. 2 ZPO zur Sicherung einer einheitlichen Rechtsprechung zuzulassen. Es sind Tausende von Parallelverfahren in Deutschland anhängig. Soweit die Zulässigkeit der Feststellungsklage betroffen ist, weicht der Senat zudem von der Rechtsprechung des OLG Stuttgart (Urteil vom 22.11.2023 - 4 U 20/23, Rn 238 - juris) ab.

4.

Die Streitwertfestsetzung beruht auf § 3 ZPO. Zur Begründung wird auf die Beschlüsse des Senates vom 31.07.2023 (4 W 396/23 und 4 W 388/23 - beides juris) Bezug genommen.