Abschrift z.K. vorab

Landgericht Halle

Geschäfts-Nr.:
4 O 250/22

Verkündet am:
5. Juni 2023
Gez.
als Urkundsbeamtin/beamter der Geschäftsstelle

Im Namen des Volkes!

Urteil

In dem Rechtsstreit

des

Kläger,

Prozessbevollmächtigte: Wilde Beuger Solmecke Rechtsanwälte Partnerschaft mbB,
vertreten durch die Rechtsanwälte ,
Kaiser-Wilhelm-Ring 27-29, 50672 Köln,

gegen

Meta Platform Ireland Ltd., vertreten durch die Mitglieder des Board of Directors, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte:
Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB,
vertreten durch ,
Bockenheimer Anlage 44, 60322 Frankfurt/Main,

hat die 4. Zivilkammer des Landgerichts Halle auf die mündliche Verhandlung vom 28. April 2023 durch den Vorsitzenden Richter am Landgericht , die Richterin am Landgericht und den Richter

für **R e c h t** erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 400 Euro nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21. September 2022 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger sämtliche materiellen Schäden zu ersetzen, die diesem durch die seitens der Beklagten erfolgten Verknüpfung seiner personenbezogenen Daten beim Abschöpfen von Daten durch Dritte im Jahre 2019 entstanden sind bzw. 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 zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten der Klägerseite, namentlich Telefonnummer, Facebook-Nutzername, Vor- und Nachname und Geschlecht Dritten über eine Anwendung zum Importieren von Kontakten (sog. Contact-Import-Tool) zugänglich zu machen, ohne die nach dem Stand der Technik angemessenen Sicherheitsmaßnahmen vorzusehen, die eine Ausnutzung der Anwendung zu anderen Zwecken, als zur Kontaktaufnahme verhindern.

4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsverfolgungskosten in Höhe von 220,27 € nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 21. September 2022 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Die Kosten des Rechtsstreits werden gegeneinander aufgehoben.

7. Das Urteil ist vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung gegen Sicherheitsleistung in Höhe von 1.000 Euro abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit entsprechender Höhe des jeweils zu vollstreckenden Betrags leistet. Der Kläger kann die Vollstreckung gegen Sicherheitsleistung in Höhe von 120 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der

Vollstreckung Sicherheit in Höhe von 120 % des jeweils zu vollstreckenden Betrags leistet.

Und beschlossen:

> Der Gegenstandswert für die Gerichtsgebühren des Rechtsstreits wird auf die Stufe bis 3.000 Euro festgesetzt.

****

Tatbestand

Der Kläger nimmt die Beklagte von dem Kläger angenommener Verstöße gegen die DSGVO in Anspruch.

Die Beklagte betreibt das soziales Netzwerk "Facebook", welches es Nutzern nach Registrierung ermöglicht, mit anderen Nutzern in Kontakt zu treten, Nachrichten zu versenden und persönliche Informationen zu teilen. Eine Nutzung ist nicht nur über die Internetseite "www.facebook.com" möglich, sondern auch durch die gleichnamige Anwendung für Smartphones oder Tablet-PC. Zudem kann die Nachrichtenfunktion des Portals mittels einer auf diesen Nutzen reduzierten App ("Messenger-App") unter Verwendung desselben Nutzerprofils bedient werden.

Damit Nutzer sich leichter mit anderen Nutzern vernetzen und ihrerseits über eine Suchmaske aufgefunden werden können, müssen folgende Datenpunkte zwingend öffentlich angegeben werden: Name, Geburtstag, Geschlecht. Die Angabe einer Mobilfunktelefonnummer ist optional. Diese kann sowohl bei der Registrierung auf der Plattform, bei Entscheidung zugunsten einer 2-Faktor-Authentifizierung zur Erhöhung der Kontosicherheit sowie bei Nutzung des Messenger-App angegeben werden.

Nach der erstmaligen Registrierung erhalten Nutzer ein persönliches Profil, auf dem sie weitere Angaben zu ihrer Person tätigen und im von der Beklagten vorgegebenen Rahmen darüber befinden können, welche anderen Nutzer ihre Daten einsehen bzw. abrufen können. So stellt die Beklagte Anwendungen und Informationen zur Verfügung, die Nutzern eine Konfiguration ihrer sog. Privatsphäre-Einstellungen und damit auch ihrer Auffindbarkeit über die Suchmaske oder andere Suchanwendungen ermöglicht. Innerhalb

der Privatsphäre-Einstellungen zur Suchbarkeit wird zwischen verschiedenen Möglichkeiten differenziert, welche von der privatesten Einstellung, der Abrufbarkeit der Daten nur für den Nutzer selbst ("Nur ich"), bis hin zur Abrufbarkeit für sämtliche Personen reicht, die als Nutzer registriert sind ("Alle"). Wegen der zur Verfügung gestellten Konfigurationsmöglichkeiten sowie der diesbezüglichen Informationen insbesondere zur Nutzung einer angegebenen Mobilfunknummer wird auf die Seiten 8 – 15 der Klageschrift sowie die Anlagen B1 – B9 Bezug genommen.

Der Kläger meldete sich vor Oktober 2016 zu einem nicht näher benannten Zeitpunkt auf der von der Beklagten betriebenen Plattform an. Auf einem der oben beschriebenen Wege gab der Kläger auch seine Telefonnummer preis, wobei von der Klägerseite nicht näher konkretisiert worden ist, im Rahmen welchen Vorgangs dies erfolgte. Die standardmäßige Konfiguration zur Suchbarkeit seines Profils unter Eingabe der Telefonnummer war auf "Alle" festgelegt, ermöglichte es also sämtlichen Nutzern das klägerische Profil jedenfalls mit den dort zwingend öffentlich einsehbaren Daten Name, Nutzername (sog. Facebook-ID), Geschlecht und Geburtsdatum aufzufinden. Diese passte der Kläger nicht nach Registrierung den eigenen Vorstellungen entsprechend an, sondern ließ diese unangetastet. Die Telefonnummer des Klägers war wiederum im Rahmen der hiervon getrennten sog. Zielgruppeneinstellung nicht als öffentlich freigegeben, also auch auf seinem Profil nicht für jedermann einsehbar.

Im Jahre 2019 kam es auf der Plattform der Beklagten zu einem breit angelegten, automatisierten Abschöpfen von Millionen von Nutzerdaten durch unbekannte Dritte, von denen auch der Kläger mit seinen Datenpunkten Name, Nutzername und Geschlecht betroffen war (sog. Scraping-Vorfall). Scraping ist eine der Beklagten bereits seit 2018 bekannte, informationstechnische Methode, mithilfe derer typischerweise öffentlich einsehbare Daten von Internetseiten durch automatisierte Softwareprogramme massenhaft abgerufen werden. Die Methode bedient sich dabei in der Regel Anwendungen, die für eine ordnungsgemäße Nutzung der Internetseite entworfen worden sind. Scraping war nach den Nutzungsbedingungen der Beklagten untersagt.

Im hiesigen Fall erfolgte der Datenabruf unter Verwendung des sog. Contact-Import-Tool (im Folgenden: CIT). Hierbei handelte es sich um eine Anwendung der Beklagten, die es an sich Nutzern ermöglichen sollte, im digitalen Adressbuch des Nutzergeräts vorhandene Kontakte mit den bereits vernetzten virtuellen Kontakten auf Facebook abzuglei-

chen und gegebenenfalls weitere, noch nicht vernetzte Kontakte aufzufinden. Nach Eingabe einer Mobilfunktelefonnummer prüfte die Beklagte automatisiert, ob zu dieser ein Facebook-Profil bestand und stellte im Falle dessen die Verknüpfung zum jeweiligen Profil her, indem es der suchenden Person das Profil mit den öffentlich verfügbaren Daten als zur Telefonnummer gehörig anzeigte. Die Parteien gehen davon aus, dass der Abruf der Daten im Wege einer randomisierten Eingabe einer Vielzahl an möglichen Zahlenkombinationen zu Telefonnummern erfolgte, wobei die Beklagte bei Übereinstimmung einer Telefonnummer entsprechend der obigen Verfahrensweise das dazugehörige Profil angab. Wegen des konkreten Ablaufs des in Rede stehenden Datenabrufs mittels Scraping und des Kenntnisstandes der Beklagten Ende 2019 wird auf die Anlagen B10, B11 und B16 Bezug genommen. Durch dieses Vorgehen gelang es unbekannten Dritten die öffentlich einsehbaren o.g. Daten des Klägers als um dessen Nummer erweitertes Datenbündel für andere Zwecke zu speichern.

Im April 2021 veröffentlichten Unbekannte das Datenbündel des Klägers im Internet in einer vor dem Zugriff durch Dritte ungesicherten Datenbank. Erst nach Medienberichten (Business Insider, 3 April 2021, abrufbar unter https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leakedonline-2021-4?r=US&IR=T) über den Vorfall veröffentlichte die Beklagte am 6. April 2021 Einträge auf ihrer Website, wo sie zu dem Scraping-Vorfall Stellung bezog. Dabei gab sie zu erkennen, dass sie bereits Ende 2019 vom Scraping Kenntnis erlangt hatte. Eine Information der irischen Datenschutzaufsichtsbehörde DPC oder des Klägers selbst erfolgte im Nachgang zur Kenntniserlangung nicht.

Mit E-Mail vom 23. September 2021 forderte der Kläger die Beklagte zur Auskunft über die Verarbeitung der klägerischen Daten im Zusammenhang mit dem Scraping-Vorfall auf. Wegen des konkreten Inhalts des Auskunftsersuchens wird auf die Anlage K1 Bezug genommen. Mit Schreiben vom 21. Oktober 2021 erteilte die Beklagte dem Kläger hierauf konkrete Informationen, derentwegen auf die Anlage B16 Bezug genommen wird.

Der Kläger behauptet, sein Datenbündel sei auch auf einer Internetseite veröffentlicht worden, die illegale Aktivitäten begünstigt habe ("www.raidforums.com"), was die Beklagte mit Nichtwissen bestreitet. Weiterhin habe die Veröffentlichung der Daten dazu geführt, dass er nunmehr vermehrt Kontaktaufnahmen via E-Mail, SMS oder Anruf mit Betrugsabsichten von unbekannten Personen erhalte. Seither habe er ein gewachsenes Misstrauen gegenüber Kontaktaufnahmen durch unbekannte Dritte.

Der Kläger beantragt,

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

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

3. die Beklagte zu verurteilen, 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 Widerholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Beziehungsstatut unbefugten Dritten über eine Software zum Importieren von Kontaktdaten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahamen 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 zu verurteilen, 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 zu verurteilen, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, sie habe im Zeitraum des Abschöpfens der Daten Maßnahmen zur Verhinderung des massenhaft automatisierten Auslesens öffentlicher Nutzerdaten in Form von Übertragungsbeschränkungen, Bot-Erkennungssystemen und Captcha-Tests, also Tests zur automatisierten Differenzierung von menschlichen und computersteuerten Abfragen, insbesondere für die Fälle vorgehalten, in denen eine eindeutig exzessive Aktivität des Abfragenden erkannt werden konnte. Hierzu ist sie der Ansicht, dass die getroffenen Maßnahmen dem Stand der Technik angemessen gewesen seien. Hinsichtlich der Gestaltung des Hilfebereichs zu Privatsphäre-Einstellungen behauptet die Beklagte schließlich, dass zu sämtlichen relevanten Themen die erforderlichen Informationen durch Eingabe eines Schlagworts einfach aufgefunden werden konnten.

Die Klage ist der Beklagten am 20. September 2022 zugestellt worden.

Entscheidungsgründe

A. Die Klage ist zulässig, hat in der Sache aber nur teilweise Erfolg.

I. Der zulässige Klageantrag zu 1. ist nur teilweise begründet.

1. Der Antrag ist hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Entgegen der Auffassung der Beklagten ist darin keine alternative Klagehäufung zu erkennen, dass der Kläger sich zum einen auf mehrere Verstöße gegen die DSGVO zeitlich vor dem Scraping-Vorfall bezieht und andererseits die Verletzung von Melde- und Benachrichtigungspflicht, also dem Vorfall nachgelagerte Pflichten, rügt. Eine alternative Klagehäufung liegt erst dann vor, wenn der Kläger ein einheitliches Klagebegehren aus mehreren prozessualen Ansprüchen (Streitgegenständen) herleitet und dem Gericht die Auswahl

überlässt, auf welchen Klagegrund es die Verurteilung stützt (BGH, Urteil vom 21. November 2017 – II ZR 180/15 –, Rn. 8, juris). Dies ist jedoch nicht der Fall. Denn der vom Kläger vorgetragene Lebenssachverhalt vor dem Datenabruf erstreckt sich zwar über einen längeren Zeitraum, bezieht sich jedoch durchwegs auf eine einheitliche immaterielle Einbuße infolge des Scraping-Vorfalls, der seinerseits kumulativ auf den gerügten Verstößen gegen die DSGVO beruhen soll. Es besteht auch kein Anlass, den Vortrag zu einer unterbliebenen Meldung an die Aufsichtsbehörde, Benachrichtigungen an den Kläger oder der Auskunftserteilung ihm gegenüber einem abweichenden Lebenssachverhalt zuzuordnen. Bei der Bemessung des Schmerzensgeldes können nämlich – mit Blick auf dessen Ausgleichsfunktion – in der Gesamtbetrachtung auch solche Gesichtspunkte Berücksichtigung finden, die den einmal erlittenen Schaden abgemildert oder aber weiter vertieft haben (vgl. OLG Naumburg, Urteil vom 10. Juli 2014 – 2 U 101/13 –, Rn. 61, juris).

2. Der Antrag ist aber nur teilweise begründet, da der dem Grunde nach bestehende Anspruch auf Ersatz immaterieller Schäden den klägerseits geforderten Mindestbetrag in der Höhe nicht erreicht.

a) Dem Kläger steht gegen die Beklagte ein Anspruch gem. Art. 82 Abs. 1 DSGVO zu, da diese schuldhaft die Anforderungen an die rechtmäßige Datenverarbeitung im Sinne von Art. 6 Abs. 1 S.1 DSGVO nicht eingehalten hat.

aa) Die Verarbeitung der klägerischen Daten war nicht gem. § 6 Abs. 1 S.1 lit. b) DSGVO rechtmäßig. Soweit die Beklagte vorträgt, dass die streitgegenständliche Datenverarbeitung für die Erfüllung des Vertrages in Bezug auf die Bereitstellung eines sozialen Netzwerks nach Art. 6 Abs. 1 S. 1 lit. b DSGVO erforderlich und damit rechtmäßig gewesen sei, kann dem nicht gefolgt werden. Die Datenverarbeitung setzt in Erfüllung eines Vertrags notwendigerweise zu ihrer Rechtmäßigkeit voraus, dass technisch ausreichende und gesetzgeberisch geschuldete Sicherheitsmaßnahmen vorgehalten werden, um wie im Streitfall Unbefugten das Zugänglichmachen personenbezogener Daten zu verhindern.

Diesen Anforderungen hat die Beklagte jedoch gerade nicht genügt. Während ein Verstoß gegen Art. 13 Abs. 1 lit. c) i.V.m. Art. 5 Abs. 1 lit. a) nicht zu erkennen ist, hat die Beklagte bei der Datenverarbeitung sowohl gegen Art. 24, 25 Abs. 1, 32 Abs. 1 Hs. 1, Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f) DSGVO (dazu (1)), als auch gegen Art. 25 Abs. 2 DSGVO (dazu (2)) verstoßen.

(1) Soweit der Kläger der Ansicht ist, die Beklagte habe gegen die aus Art. 13 Abs. 1 lit. c) i.V.m. Art. 5 Abs. 1 lit. a) DSGVO folgenden Informationspflichten bei der Erhebung der Telefonnummer verstoßen, genügen seine Darlegungen insoweit nicht.

Selbst wenn man zugunsten des Klägers annimmt, dass die Beklagte infolge des Inkrafttretens der gegenüber § 4a BDSG a.F. engeren Regelungen der DSGVO eine neuerliche Information auf der Basis der veränderten Pflichten in Bezug auf die bereits 2016 angegebene Nummer hätte vornehmen müssen, so verbleibt unklar, welcher Sachverhalt der gerichtlichen Prüfung zugrunde zu legen ist. Denn auch in der mündlichen Verhandlung hat der Kläger nach widersprüchlichen Angaben in Klage und Replik nicht zu präzisieren vermocht, auf welchem der drei von ihm aufgezeigten Wege er seine Mobilfunknummer auf der Plattform der Beklagten angegeben hat.

Dem Vortrag der Beklagten ist jedoch zumindest in Bezug auf die Angabe der Nummer im Zuge der Registrierung auf der Plattform eine hinreichend transparente und übersichtliche Information zu den möglichen Verwendungen der Nummer bezüglich der Auffindbarkeit sowie zur Konfigurabilität der Privatsphäre-Einstellungen zu entnehmen, selbst wenn man den – bestrittenen – Vortrag zur Suchmöglichkeit bezüglich Informationen im Hilfebereich mittels einfacher Eingabe von Schlagwörtern außer Betracht lässt. Auch die organisatorische Gestaltung durch Verwendung von Unterverknüpfungen führt nicht grundsätzlich zur Intransparenz, sondern stellt ein geeignetes Mittel dar, umfangreiche Informationen dem Nutzer übersichtlich zur Verfügung zu stellen (vgl. Leitlinien für Transparenz gemäß der Verordnung 2016/679 der Art. 29 Datenschutzgruppe, WP260 rev.01, Rn. 34 - 37). Der Kläger ist weiterhin den Angaben der Beklagten nicht entgegengetreten, dass die vorgetragenen Informationen und Einstellungsmöglichkeiten im hier relevanten Zeitpunkt den damals zur Verfügung gestellten Informationen entsprachen. Da allerdings offengeblieben ist, ob der Kläger nicht doch im Rahmen der datenschutzkonformen Erhebung seine Mobilfunknummer bei der Registrierung angegeben hat, entbehrt der Vortrag hinsichtlich der Einhaltung der Transparenzpflicht der zur Subsumtion erforderlichen Konkretisierung.

(2) Die Beklagte hat aber durch die Verarbeitung der personenbezogenen Daten des Klägers gegen deren Verpflichtungen aus Art. 24, 25 Abs. 1, 32 Abs. 1 Hs. 1, Abs. 2 i.V.m. Art. 5 Abs. 1 lit. f) DSGVO bei der Datenverarbeitung verstoßen.

(a) Die Beklagte hat gem. § 4 Nr. 1, 2 DSGVO personenbezogene Daten des Klägers verarbeitet, indem sie im Rahmen des Scraping-Sachverhalts die im CIT eingegebenen

Telefonnummer mit den bei ihr bereits gespeicherten Daten zum Namen, Nutzernamen sowie Geschlecht abgeglichen und schlüssig verknüpft hat. Denn nach der Funktionsweise des CIT genügte die Eingabe einer mit einem Konto verknüpften Telefonnummer, um die Beklagte zu veranlassen, das dazugehörige Konto im öffentlich einsehbaren Umfang mitzuteilen und damit zugleich konkludent die Existenz und die Zugehörigkeit der Mobilfunknummer zum mitgeteilten Profil zu bestätigen.

(b) Die Kammer geht davon aus, dass die Daten nicht in einer dem Grundsatz der Integrität und Vertraulichkeit genügenden Weise verarbeitet worden sind.

(aa) Gem. Art. 32 Abs. 1 Hs. 1 DSGVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zugleich finden nach Art. 32 Abs. 2 DSGVO insbesondere die Risiken Berücksichtigung, die mit der Verarbeitung verbunden sind. Namentlich betrifft dies – ob unbeabsichtigt oder unrechtmäßig – unter anderem die unbefugte Offenlegung von beziehungsweise den unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(bb) In Anwendung des vorstehenden Maßstabs hat die Beklagte nicht hinreichend dargelegt, dass sie ihrer Verpflichtung zur Gewährleistung eines angemessenen Schutzniveaus bei der Datenverarbeitung in zureichendem Umfang nachgekommen ist.

(aaa) Nach den allgemeinen Regeln ist grundsätzlich der Kläger hinsichtlich der anspruchsbegründenden Tatsachen wie beispielsweise einer den Anspruch tragenden Rechtsverletzung darlegungs- und beweisbelastet. Dies gilt jedoch nicht, soweit die Rechtmäßigkeit der Datenverarbeitung im Sinne von Art. 5 Abs. 1 lit. a) DSGVO in Streit steht. Denn aus dem Grundsatz der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO folgt, dass es an der Beklagten als für die Verarbeitung der Daten im Sinne des Art. 4 Nr. 7 DSGVO Verantwortliche ist, darzulegen und gegebenenfalls zu beweisen, dass sie die in Art. 5 Abs. 1 DSGVO festgehaltenen Grundsätze für die Verarbeitung personenbezogener Daten eingehalten hat (vgl. EuGH, Urteil vom 24.02.2022, C-175/20, Rn. 77 ff., juris; a.A. LG Heilbronn, Urteil vom 3. März 2023 – Bö 1 O 78/22 –, Rn. 67, juris m.w.N.).

(bbb) Aus dem Vortrag der Beklagten ergibt sich indes nicht, dass die von ihr getroffenen Maßnahmen im maßgeblichen Zeitpunkt des Scraping-Vorfalls ein angemessenes Schutzniveau erreicht hatten.

(aaaa) Zur Beurteilung des erforderlichen Schutzniveaus ist zunächst hinsichtlich der Gefährdungslage zu berücksichtigen, dass zum damaligen Zeitpunkt sowohl die hier relevante Scraping-Methode zum missbräuchlichen Abschöpfen von Daten bereits bekannt war, wie auch gängige technische Gegenmaßnahmen z.B. durch Sicherheitscaptchas, die der verarbeitenden Software eine Differenzierung zwischen menschlicher und computergesteuerter Abfrage erlauben, zur Verfügung standen.

Weiterhin sind die Risiken des Eintritts von materiellen und immateriellen Schäden, die sich aus der Möglichkeit der Zuordnung von Telefonnummern zum Plattform-Profil und den öffentlich einsehbaren Daten gerade bei massenhaftem Auslesen und ggf. auch automatisierter missbräuchlicher Folgenutzung ergeben, nicht von geringer Erheblichkeit. Nimmt man nämlich in den Blick, dass einerseits mit der fortschreitenden Digitalisierung für die Identifikation des Vertragspartners im Massengeschäftsverkehr mittlerweile häufig auf die sog. 2-Faktor-Authentifizierung unter Zuhilfenahme der Mobilfunknummer zurückgegriffen wird (z.B. SMS-TAN-Verfahren im Online-Zahlungsverkehr) und andererseits die Möglichkeit besteht, ohne wesentliche Schwierigkeiten die Telefonnummer durch den Mobilfunkanbieter auf eine neue SIM-Karte überschreiben zu lassen (sog. SIM-Swapping), so lässt sich erkennen, dass das Risiko der missbräuchlichen Ausnutzung beträchtlich ist. Dass bei isolierter Betrachtung die Profildaten des Klägers öffentlich waren, ist dagegen insoweit unerheblich (a.A. LG Halle, Urteil vom 7. Dezember 2022, – 6 O 195/22). Denn gerade die durch die Beklagte vorgenommene Verknüpfung der zwar für alle Nutzer suchbaren, jedoch nicht öffentlich einsehbaren Telefonnummer zu einem erweiterten Datenbündel, begründet Risiken von eigenständigen Gewicht. Den damit einhergehenden Verpflichtungen zum Schutz der informationellen Selbstbestimmung hat die Beklagte als Betreiberin eines sozialen Netzwerks, das zur gesellschaftlich-kommunikativen Teilhabe eine dominante Position einnimmt, und der daraus folgenden Annährung an eine Grundrechtsbindung in besonderem Maße Rechnung zu tragen (vgl. BGH, Beschluss vom 23. Juni 2020 – KVR 69/19 –, Rn. 105).

Beim Ansatz des Schutzniveaus hat die Kammer allerdings auch in die Beurteilung eingestellt, dass Art. 32 Abs. 1 DSGVO keine absolute Obergrenze eines Schutzes verpflichtend normiert, sondern im jeweiligen Verarbeitungskontext lediglich angemessen sein

muss. Dies ist hier zum einen insoweit von Bedeutung, als dass die Bereitstellung bestimmter Nutzeranwendungen wie des CIT der angebotenen Dienstleistung zur Vernetzung mit anderen Personen zugutekommt und damit eine Abschaltung der Anwendung in der Abwägung mit den oben genannten Risiken einseitig zulasten der Nutzbarkeit der von der Beklagten angebotenen Dienstleistungen ginge. Da es sich beim CIT jedoch um eine optionale Anwendung handelt, die die Kontaktsuche vereinfachen soll, aber nicht zwingend voraussetzt, fällt der Gesichtspunkt der vereinfachten Nutzbarkeit im Übrigen jedoch nur in geringem Maße ins Gewicht. Zum anderen kommt der Angemessenheit des Schutzniveaus dahingehend eine Bedeutung zu, als eine missbräuchliche Verwendung von informationstechnischen Anwendungen mit vollendeter Sicherheit nie ausgeschlossen werden kann. Die Gefährdung der Daten des Einzelnen nimmt bei wirtschaftlicher Betrachtung daher vor allem dort streiterhebliche Form an, wo nicht nur aufgrund einer einzelnen Abfrage Daten verknüpft werden, sondern die Verknüpfung in einer Masse stattfindet, die auch für böswillige Dritte einen Nutzen generiert (vgl. hierzu Erwägungsgrund 75 a.E. der DSGVO).

(bbbb) Soweit die Beklagte behauptet, sie habe im relevanten Zeitraum Sicherheitscaptchas, Bot-Erkennung und Übertragungsbeschränkungen eingesetzt, hat sie nicht hinreichend substantiiert, inwiefern die Maßnahmen auch Anwendung fanden, um nicht erkannte, automatisierte sowie umfangreiche Datenabfragen zu verhindern. Dies wäre jedoch gemessen am Ausmaß der durch das Scraping drohenden Gefahren geboten gewesen (so auch die Irische Datenschutzaufsichtsbehörde DPC, Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Article 60 of the General Data Protection Regulation, S. 44 ff.).

Es kann in diesem Sinne zugunsten der Beklagten unterstellt werden, dass sie die beschriebenen Sicherheitsmaßnahmen zumindest dann einsetzte, wenn zuvor Abfrageaktivitäten festgestellt worden sind, die wahrscheinlich auf unauthentischem Verhalten beruhten. Wie die Beklagte allerdings selbst vorträgt, beruht Scraping gerade auf einer missbräuchlichen Nutzungsweise von normalen Funktionen, im Rahmen derer das verarbeitende System im Einzelfall den Missbrauch nicht von einer ordnungsgemäßen Nutzung zu unterscheiden vermag. Gerade daher war die Beklagte hier gehalten, verhältnismäßig leichte Einschränkungen im Nutzererlebnis zu implementieren, die wegen des nicht fernliegenden Ausfalls der Missbrauchserkennung ein umfangreiches Abschöpfen von Daten effektiv verhinderten. Die einzige präventiv-effektive Gegenmaßnahme im Einzelfall, die dem Vortrag der Beklagten hierzu zu entnehmen ist, ist die Durchführung einer

Captcha-Abfrage vor der Verarbeitung. Selbst wenn man aber beispielsweise eine Captcha-Abfrage für jeden Fall der Suche einer Telefonnummer für unangemessen hielte, ist nicht einzusehen, warum die Beklagte nicht zumindest in regelmäßigen Abständen billigerweise eine solche hätte vorsehen können, um jedenfalls den massenhaften Datenabruf zu verhindern und so für böswillige Dritte unattraktiv zu gestalten. Captcha-Abfragen im benannten Umfang oder zumindest gleich geeignete Maßnahme sind dem Vortrag der Beklagten aber nicht zu entnehmen.

Soweit die Beklagte darüber hinaus umfangreich zu ihrer Reaktion auf den "Scraping-Vorfall" und die infolgedessen entwickelten Gegenmaßnahmen vorgetragen hat, kommt es hier darauf nicht an, da maßgeblicher Beurteilungszeitpunkt das Schutzniveau im Zeitpunkt der rechtswidrigen Verarbeitung ist.

(cccc) Schließlich kann der neue Vortrag der Beklagten, "im Nachgang" zu Scraping-Vorfällen 2018 im CIT weitere Schutzmechanismen in Form des sog. Social-Connection-Checks oder der sog. PMYK-Funktion nach Schluss der mündlichen Verhandlung gem. § 296a S.1 ZPO nicht mehr in die erste Instanz eingeführt werden. Wird ein Schriftsatz innerhalb eines Schriftsatznachlasses eingereicht, gilt gerade nicht jeder Inhalt dieses Schriftsatzes als noch in der Instanz beigebracht, sondern nur solcher Vortrag, der sich innerhalb der thematischen Begrenzung des Nachlasses hält (BGH, Urteil vom 2. Juni 2022, III ZR – 216/20 –, Rn. 31, juris). Mit Beschluss vom 28. April 2023 gewährte die Kammer der Beklagten – beschränkt auf tatsächlich neues Vorbringen im Schriftsatz des Klägers vom 20. April 2023 – Stellung zu nehmen und gerade nicht den eigenen Tatsachenvortrag noch zu erweitern.

(3) Der Beklagten fällt auch ein Verstoß gegen die Verpflichtung zur datenschutzfreundlichsten Voreinstellung gem. Art. 25 Abs. 2 DSGVO zur Last.

(a) Die Beklagte hat es versäumt, im Vorfeld der Verarbeitung geeignete Maßnahmen zu ergreifen, um sicherzustellen, dass standardmäßig nur diejenigen personenbezogenen Daten des Klägers verarbeitet wurden, die für den Zweck der Verarbeitung erforderlich waren. Denn die Telefonnummer war laut Angaben der Beklagten in der Suchbarkeit im Zeitpunkt des Scraping-Vorfalls auf "Alle" voreingestellt. Indem die Beklagte die Einstellungen für die Auffindbarkeit des Klägers in Bezug auf die relevanten Merkmale automatisch dessen Telefonnummer einschloss, machte sie dessen personenbezogene Daten ohne weiteres Zutun einer unbestimmten Anzahl natürlicher Personen zugänglich. Da im Übrigen die Angabe bzw. die Auffindbarkeit der Telefonnummer auch nicht zwingend zur

Nutzung der Plattform erforderlich gewesen ist, hätte die Suchbarkeit der Telefonnummer standardmäßig auf der privatesten Einstellung konfiguriert sein müssen. Die Veröffentlichung der Telefonnummer war nach dem Zweck der Anmeldung auf der Plattform dementsprechend nur als nützlich, nicht aber notwendig anzusehen (vgl. zu einer notwendigen Funktion: BGH, Urteil vom 13. Dezember 2022 – VI ZR 60/21 –, Rn. 21, juris).

(b) Die Verletzung von Art. 25 Abs. 2 DSGVO kann auch einen Schadensersatzanspruch gem. Art. 82 Abs. 1 DSGVO begründen. Wie sich aus dem systematischen Zusammenhang mit Art. 82 Abs. 2 S.1 DSGVO ergibt, vermag nicht jeder Verstoß gegen die DSGVO einen Schadensersatzanspruch zu begründen, sondern setzt eine rechtswidrige Verarbeitung voraus. Anders als die Beklagte meint, folgt daraus jedoch nicht, dass der in Rede stehende Verstoß gegen Art. 25 Abs. 2 DSGVO nicht vom Anwendungsbereich umfasst ist, weil dieser unmittelbar an einen Zeitraum vor der erstmaligen Verarbeitung anknüpft. Die Voreinstellungen sind mit der späteren Datenverarbeitung eng verwoben, vgl. Art. 25 Abs. 2 S.3 DSGVO. Denn in der Anwendung der Voreinstellungen materialisiert sich letztlich bei der Verarbeitung, was bereits im Zeitpunkt der erstmaligen Konfiguration unter Missachtung der gesetzlichen Bestimmungen angelegt war (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 7; Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 6; a.A. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 34). Wäre die datenschutzfreundlichste Einstellungsvariante für den Kläger vorausgewählt worden, so hätte die Beklagte nämlich den Dritten im Rahmen des "Scrapings" auch keinen zur Mobilfunknummer passenden Facebook-Kontakt zur Verfügung gestellt.

(c) Der Anwendung des Art. 25 Abs. 2 DSGVO steht schließlich auch nicht entgegen, dass die Norm gem. Art. 99 Abs. 2 DSGVO zeitlich erst nach Registrierung des Klägers auf der Plattform der Beklagten Geltungskraft erlangt hat. Denn die Beklagte war mit Ablauf der zweijährigen Übergangsfrist ab Mai 2018 verpflichtet, die zuvor "angemessene" Standardkonfiguration (vgl. § 9 S.2 BDSG in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618)) nunmehr auf die datenschutzfreundlichste Konfiguration umzustellen. Dem klarstellenden Vortrag des Klägers in der mündlichen Verhandlung, er habe zwischen der Registrierung und dem Scraping-Vorfall seine Suchbarkeitseinstellungen nicht verändert, ist die Beklagte nicht entgegengetreten. Da beim Kläger also noch die Standardkonfiguration vorhanden war als Art. 25 Abs. 2 DSGVO geltungskräftig wurde, und die Einstel-

lungen zuvor auch nicht individualisiert worden waren, wäre die Beklagte verpflichtet gewesen, von sich aus die Voreinstellungen des Klägers nachträglich auf die datenschutzfreundlichste Alternative umzustellen.

bb) Auch war die Datenverarbeitung nicht aus anderen Gründen im Sinne von Art. 6 Abs. 1 S.1 DSGVO rechtmäßig.

(a) Zu einer etwaigen Einwilligung des Klägers gem. § 6 Abs. 1 S.1 lit. a) DSGVO in die Verknüpfung der Daten gegenüber Dritten hat die Klägerin nicht vorgetragen, da sie davon ausgegangen ist, dass für die Rechtmäßigkeit der Datenverarbeitung nicht erforderlich gewesen sei.

(b) Schließlich überwiegen die Interessen der Beklagten sowie anderer Nutzer an der vereinfachten Auffindbarkeit von anderen Nutzern mithilfe des CIT gem. Art. 6 Abs. 1 S.1 lit. f) DSGVO auch nicht die berechtigten Interessen des Klägers. Die bloße Unannehmlichkeit, mehr Ressourcen zur Vernetzung mit anderen Nutzern aufwenden zu müssen, fällt gegenüber den mit der Verarbeitung einhergehenden Gefährdungen der klägerischen Daten nicht ins Gewicht.

cc) Der Beklagten ist es des Weiteren nicht gelungen, sich gem. Art. 82 Abs. 3 DSGVO zu entlasten, weshalb ihr Verschulden gesetzlich vermutet wird. Dem Vortrag der Beklagten ist – wie bereits ausgeführt – nicht zu entnehmen, dass sie zureichende Maßnahmen getroffen hat, um die ihr bekannte Scraping-Methode zum massenhaften Auslesen von Daten zu unterbinden und damit die bei der Datenverarbeitung gem. Art. 5 DSGVO erforderliche Sorgfalt einzuhalten.

b) Die Höhe des ersatzfähigen, durch die Verstöße verursachten immateriellen Schadens beläuft sich hier auf 400 Euro.

aa) Dem Kläger ist ein immaterieller Schaden entstanden, der gem. Art. 82 Abs. 1 DSGVO ersatzfähig ist.

(1) Entgegen der Auffassung des Klägers begründet nicht schon jeder Verstoß gegen die DSGVO einen Schadensersatzanspruch. Vielmehr folgt bereits aus dem Wortlaut des Art. 82 Abs. 1 DSGVO und den Erwägungsgründen 75, 85 und 146 der DSGVO, dass der Schaden ein eigenständiges Tatbestandsmerkmal darstellt, der der Feststellung durch das erkennende Gericht bedarf (EuGH, Urteil vom 04.05.2023, C-300/21, Rn. 33

ff., juris; a.A. BAG, Beschluss v. 26.8.2021 – 8 AZR 253/20). Andererseits folgt insbesondere aus der gebotenen weiten Auslegung des Schadensbegriffs in Art. 82 Abs. 1 DSGVO entsprechend der Ziele der DSGVO (Erwägungsgrund 146 S.3 der DSGVO), dass die Ersatzfähigkeit – anders als die Beklagte meint – nicht auf solche immateriellen Schäden beschränkt ist, die eine wie auch immer geartete Erheblichkeitsschwelle überschreiten (EuGH, Urteil vom 04.05.2023, C-300/21, Rn. 44 ff., juris). Es genügt daher im Sinne der Erwägungsgründe 75 und 85 für die Annahme eines Schadens, dass aus einem Kontrollverlust über die eigenen personenbezogenen Daten hinreichend konkretisierte Risiken für die Rechte und Freiheiten z.B. in Form eines Identitätsdiebstahls erwachsen.

(2) Dies zugrunde gelegt, liegt ein immaterieller Schaden beim Kläger vor. Dabei kann dahinstehen, ob die Behauptungen des Klägers zutreffen, sein Datenbündel sei auch auf einer Internetseite veröffentlicht worden, die illegale Aktivitäten begünstigt habe oder aber, dass er nunmehr vermehrt Kontaktaufnahmen via E-Mail, SMS oder Anruf mit Betrugsabsichten erhalte und infolgedessen misstrauischer gegenüber Kontaktaufnahmen durch unbekannte Dritte sei. Denn zwischen den Parteien ist unstreitig, dass die Beklagte die bei ihr vorhandenen Daten des Klägers im Rahmen des Scraping-Vorfalls Dritten gegenüber verknüpft und damit die Kontrolle über die Verwendung von in dieser Verknüpfung nicht öffentlichen Daten dem Kläger entzogen hat. Zum anderen steht fest, dass das Datenbündel im Jahr 2021 in einer ungesicherten Datenbank im Internet veröffentlicht wurde und dementsprechend dem ungehinderten Zugriff durch weitere Dritte ausgesetzt war. Damit steht zur Überzeugung der Kammer fest, dass der Kläger einen hinreichend konkreten Verlust der Kontrolle über seine personenbezogenen Daten und folglich auch einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO erlitten hat.

bb) Die Verletzung von Vorschriften über die Datenverarbeitung war ursächlich für den festgestellten Schaden. Dabei schadet es der Zurechenbarkeit von Schäden nicht per se, wenn auch Dritte – wie vorliegend – bei der Schadensentstehung mitwirken. Vielmehr genügt es, wenn die hier von der Beklagten gesetzten Verursachungsbeiträge mitursächlich waren (vgl. OLG Hamm, Urteil vom 20. Januar 2023 – I-11 U 88/22 –, Rn. 125, juris; vgl. auch EuGH, Urteil vom 5. Juni 2014 – C-557/12 –, juris) und auch in einem Adäquanzzusammenhang stehen.

In Anwendung des § 287 Abs. 1 ZPO ist die Kammer davon überzeugt, dass zureichende Anhaltspunkte für einen adäquaten Kausalzusammenhang mit den vorgenannten Verstößen vorliegen. Der mögliche Missbrauch von Nutzeranwendungen zum massenhaften Auslesen von Daten mit der Scraping-Methode war schon damals bekannt, weshalb ohne Weiteres vorhersehbar war, dass unzureichende Schutzmaßnahmen eine latente Gefahr für die unberechtigte Datenabschöpfung bildeten. Darüber hinaus kann auch mit hinreichender Wahrscheinlichkeit davon ausgegangen werden, dass das Datenbündel des Beklagten nicht durch Scraping hätte abgerufen werden können, wenn die Beklagte die ihr aus Art. 25 Abs. 2 DSGVO und Art. 32 DSGVO erwachsenen Verpflichtungen eingehalten hätte. Denn während – wie bereits ausgeführt – die Einhaltung der Verpflichtung zur datenschutzfreundlichsten Standardkonfiguration der Suchbarkeitseinstellungen im Zeitpunkt der streitgegenständlichen Verknüpfung eine solche ausgeschlossen hätte, hätten angemessene Schutzvorkehrungen mit hinreichender Wahrscheinlichkeit den Abruf der betroffenen Daten beim Scraping-Vorfall verhindert. Aus dem Umstand folgende Zweifel, dass dem Missbrauch informationstechnischer Nutzungsfunktionen nicht mit Sicherheit Einhalt geboten werden kann, verblassen hier insoweit, als die oben beschriebenen Maßnahmen jedenfalls einen prozessökonomischen, massenhaften Abruf der Daten von der Plattform der Beklagten mit hinreichender Sicherheit verhindert hätten. Es steht schon zu bezweifeln, dass die unbekannten Dritten bei Bestehen effektiver Abrufbeschränkungen im CIT überhaupt Daten von der Plattform der Beklagten in der streitgegenständlichen Form ausgelesen hätten, da die Funktionen der Anwendung auf dem damaligen Stand das Scraping im großen Stil erst ermöglicht haben. Jedenfalls wäre aber in diesem Fall in Anbetracht des hier erfolgten millionenfachen Datenabrufs die Wahrscheinlichkeit eines zufälligen Abrufs der klägerischen Daten bei bestehenden effektiven Beschränkungen auf ein Minimum reduziert gewesen, da wegen des erheblichen Mehraufwands ein Abschöpfen lediglich in deutlich verringertem Maß erfolgen hätte können.

cc) Die Kammer hält in Bemessung nach § 287 Abs. 1 ZPO einen Ersatz für die immateriellen Einbußen in Höhe von 400 Euro für angemessen.

(1) Ausgangspunkt für die Bemessung der Höhe ist – wie auch im Rahmen des § 253 Abs. 2 BGB – die Ausgleichs- und Genugtuungsfunktion des immateriellen Schadensersatzes, deren Schwerpunkt auf dem Ausgleich der erlittenen Einbußen liegt (vgl. BGH, Beschluss vom 16. September 2016 – VGS 1/16 –, Rn. 48, juris). So soll nach Erwägungsgrundes 146 S.6 der DSGVO die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. In welchem Umfang der

Schadensersatz Vollständigkeit und Wirksamkeit erreicht, hängt von den Umständen des Einzelfalles ab. Dabei können beispielsweise unter Berücksichtigung der Wertungen aus Art. 9, 10 und Art. 82 Abs. 3 DSGVO die Schutzbedürftigkeit und der Umfang der betroffenen Daten, Art und Erheblichkeit der Datenschutzverstöße, das Ausmaß der subjektiven Gefühlsbeeinträchtigung ebenso Beachtung finden, wie Maßnahmen des Schädigers zur Minderung oder Intensivierung des der betroffenen Person entstandenen Schadens. Schließlich ist auch eine etwaige Mitverursachung der Schäden durch den Betroffenen selbst nicht außer Betracht zu lassen.

(2) Hieran gemessen ist der Ansatz in der genannten Höhe gerechtfertigt.

Dabei hat die Kammer zunächst zugrunde gelegt, dass die betroffenen Daten teilweise bereits öffentlich waren, in ihrer Gesamtheit keiner besonders schutzbedürftigen Datenkategorie unterfallen und folglich der Kontrollverlust relativ betrachtet nicht von besonders starkem Gewicht ist. Zugleich war aber auch zu beachten, dass aufgrund der aufgezeigten Missbrauchspotenziale der Kontrollverlust über den verknüpften Datensatz und das nach allgemeiner Lebenserfahrung naturgemäß damit einhergehende Unwohlsein über die zweckwidrige Verwendung auch nicht unerheblich sind. Dass dies nicht noch mehr ins Gewicht fällt, wurzelt darin, dass der Kläger seine – mangels entsprechend weit reichender Informationspflicht (vgl. hierzu BGH, Urteil vom 23. Juli 2019 – VI ZR 337/18 –, Rn. 10, juris) – zulässigerweise mit Nichtwissen bestrittene Behauptung nicht näher substantiiert hat, seine Daten seien tatsächlich auf einer spezifisch kriminelle Machenschaften fördernden Internetseite hochgeladen worden.

Darüber hinaus ist auch die rechtswidrige Verarbeitung unter mehrfachem Verstoß gegen die DSGVO ebenso in die Bewertung eingeflossen, wie in zeitlicher Hinsicht, dass seit Abruf der Daten durch das Scraping ca. zwei Jahre vergangen sind, ehe die Öffentlichkeit hiervon erfuhr. Unstreitig hat die Beklagte überdies weder den Kläger selbst gem. Art. 34 DSGVO, noch die gem. Art. 55 DSGVO zuständige irische Datenschutzaufsichtsbehörde DPC gem. Art. 33 DSGVO im gebotenen Zeitraum informiert, um dafür Sorge zu tragen, dass mögliche Gegenmaßnahmen wie z.B. die Änderung der Mobilfunknummer zeitnah ergriffen werden können.

Ohne Bedeutung ist dagegen im vorliegenden Fall, dass der Kläger sich frei verantwortlich auf der Plattform registriert, seine Telefonnummer dort angegeben und die Suchbarkeitseinstellungen nicht nach Registrierung verändert hat. Eine Berücksichtigung würde den der DSGVO zugrundeliegenden Gedanken konterkarieren, dass Nutzer von einer

rechtmäßigen und integren Datenverarbeitung ausgehen dürfen. Dies gilt erst recht dann, wenn sich Nutzer unter anderem dann zu einer Registrierung entscheiden, weil das soziale Netzwerk Facebook im Zeitpunkt der Anmeldung bereits eine gesellschaftlich dominante Position zur Teilhabe an zwischenmenschlicher Kommunikation eingenommen hat. Zuletzt steht einer Berufung auf die unveränderten Voreinstellungen auch entgegen, dass die verordnungswidrige Standardkonfiguration zur Suchbarkeit von der Beklagten gerade präferiert war, um die von ihr verfolgten Zwecke der Vernetzung von Nutzern zu erreichen. Ihr ist es dann aber verwehrt, sich darauf zu berufen, dass es am Kläger gewesen wäre, ihre rechtswidrigen Einstellungsmodalitäten zu korrigieren (vgl. LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, Rn. 101, juris).

3. Der Zinsanspruch zum Antrag zu 1. ergibt sich aus §§ 288, 291 BGB. Die Kammer geht davon aus, dass eine wirksame Zustellung der Klage spätestens am 20. September 2022 eingetreten ist. Ein Rückschein zur Auslandszustellung der Klage ist nicht zur Akte gelangt ist. Allerdings lässt sich der Sendungsverfolgung der Deutschen Post AG entnehmen, dass das Einschreiben am 16. September 2022 in Irland zum Briefzentrum des Bestimmungsortes weitergeleitet worden ist. Dies Kammer geht daher davon aus, dass das Einschreiben jedenfalls am dritten Werktag nach Eingang im Briefzentrum auch an die Beklagte ausgeliefert worden ist. In entsprechender Anwendung des § 187 Abs. 1 BGB beginnt der Zinslauf am auf die Zustellung folgenden Tag.

II. Der Antrag zu 2. zulässig und begründet.

1. Die Zulässigkeit des Antrags steht nicht in Frage. Anders als die Beklagte meint, fehlt es dem Antrag weder an der gem. § 253 Abs. 2 Nr. 2 ZPO erforderlichen Bestimmtheit, noch an der besonderen Sachurteilsvoraussetzung des Feststellungsinteresses gem. § 256 Abs. 1 ZPO.

a) Der gem. § 133 BGB nach dem wirklichen Willen des Klägers auszulegende Antrag ist nicht unbestimmt. Denn unter Berücksichtigung des Vorbringens in der Replik ist ersichtlich, dass der Kläger die Feststellung der Ersatzfähigkeit von sämtlichen künftigen materiellen Schäden begehrt. Dabei lässt der Kläger erkennen, dass er unter künftigen Schäden sowohl diejenigen versteht, die aus dem der Klage zugrundeliegenden Scraping-Vorfall bereits entstanden und insoweit noch nicht bezifferbar sind, als auch jene, die künftig im engeren Sinne z.B. durch die missbräuchliche Ausnutzung der abgeschöpften Daten noch entstehen werden.

b) Der Kläger hat auch ein Interesse an der begehrten Feststellung.

aa) Ein solches Feststellungsinteresse ist gegeben, wenn dem konkreten vom Feststellungsantrag betroffenen Recht des Klägers eine gegenwärtige Gefahr der Unsicherheit droht und der erstrebte Feststellungausspruch geeignet ist, diese Gefahr zu beseitigen. Der der Gefahr zugrunde zu legende Gewissheitsgrad hängt dabei von der Art des betroffenen Rechtsguts ab. Macht die Klägerin – wie vorliegend in Form des Rechts auf Schutz der sie betreffenden personenbezogenen Daten – die Beeinträchtigung absolut geschützter Rechtsgüter und nicht nur Vermögensschäden geltend, so kommt es entgegen der Auffassung der Parteien in Bezug auf künftigen Schäden nicht darauf an, ob der Eintritt von weiteren Schäden wahrscheinlich ist (vgl. BGH, Urteil vom 29. Juni 2021 – VI ZR 52/18 –, Rn. 30, juris). Vielmehr genügt es, dass der Eintritt derartiger Schäden nicht ausgeschlossen werden kann, die Möglichkeit von Spätschäden also gegeben ist (vgl. BGH, Beschluss vom 09. Januar 2007 – VI ZR 133/06 –; BGH, Urteil vom 20. März 2001 – VI ZR 325/99 –, Rn. 11, juris).

bb) Dies ist hier der Fall. In Ansehung der bereits beschriebenen latenten Gefahren, die mit einer Veröffentlichung eines Datenbündels unter Einschluss einer Mobilfunknummer einhergehen, ist nicht ausgeschlossen, dass unbefugte Dritte durch betrügerisches Verhalten z.B. im Online-Banking oder -Handel zulasten des Klägers diesem weiteren materiellen Schaden zufügen.

2. Der Feststellungsantrag ist auch begründet, da ein haftungsrechtlich relevanter Eingriff gegeben ist, der zu möglichen künftigen Schäden führen kann. Die sachlichen und rechtlichen Voraussetzungen eines Schadensersatzanspruchs liegen nämlich im geltend gemachten Umfang vor. Auf eine gewisse Wahrscheinlichkeit des Eintritts kommt es dagegen auch hier nicht an. Bei Verletzung eines absolut geschützten Rechtsguts nebst Vorliegen eines hieraus resultierenden Schadens, besteht kein Anlass, die Feststellung der Ersatzpflicht für weitere, künftige Schäden von der Wahrscheinlichkeit ihres Eintritts abhängig zu machen. Materiell-rechtlich wird es den Anspruch auf Ersatz dieser Schäden ohnehin nicht geben, solange diese nicht eingetreten sind. Von der Wahrscheinlichkeit des Schadenseintritts hängt die Entstehung des Anspruchs also nicht ab. Die Leistungspflicht soll bei künftige Schäden erfassenden Feststellungsklagen deshalb nur für den Fall festgestellt werden, dass die befürchtete Schadensfolge wirklich eintritt. Da dementsprechend 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 (vgl. BGH, Urteil vom 17. Oktober 2017 – VI ZR 423/16 –, Rn. 49, juris). Nach den vorstehenden Grundsätzen genügt hier, dass die festgestellten Verstöße kausal für ersatzfähige immaterielle oder materielle Schäden waren und folglich nicht ausgeschlossen werden kann, dass der Kläger infolge der Verstöße gegen die DSGVO auch weitere materielle Schäden erleidet.

III. Die teilweise ebenfalls auslegungsbedürftigen Anträge zu 3. sind zulässig, aber nicht vollumfänglich begründet.

1. Der Antrag zu 3.b. ist – unter Befreiung von rechtlichen Wertungen in der Antragsformulierung – dahingehend auszulegen, dass der Kläger die Unterlassung einer dem Scraping-Vorfall entsprechenden Datenverarbeitung durch die Beklagte mithilfe des CIT insoweit begehrt, als diese die Verarbeitung auf eine Einwilligung stützt, ohne dass sie zuvor den Kläger über die Folgen der möglichen Suchbarkeitseinstellungen aufgeklärt hat

2. Die Anträge zu 3 sind zulässig. Die Kammer folgt der Auffassung der Beklagten nicht, dass dies zu unbestimmt seien und es dem Kläger auch am Rechtsschutzbedürfnis fehle.

a) Der Bestimmtheit des Antrags stehen keine Bedenken entgegen, soweit der Kläger dem "Stand der Technik" nach mögliche Sicherheitsmaßnahmen begehrt.

aa) 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 die beklagte Partei deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was ihr verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (BGH, Urteil vom 9. September 2021 – I ZR 90/20 –, BGHZ 231, 38-87, Rn. 19). In besonders gelagerten Fällen können aber bei der Bemessung der Anforderungen, die zur Sicherung der Bestimmtheit des Unterlassungsantrags und des entsprechenden Urteilsausspruchs aufzustellen sind, die Erfordernisse der Gewährung eines wirksamen Rechtsschutzes zu berücksichtigen sein (vgl. BGH, Urteil vom 4. März 2004 – I ZR 221/01 –, Rn. 40 f., juris).

bb) Nach diesen Maßstäben ist die Antragsformulierung hinreichend bestimmt. Obgleich die Verurteilung zur Einhaltung des "Standes der Technik" bei der Verarbeitung für die Prozessökonomie im Vollstreckungsverfahren eine möglicherweise hinderliche Unschärfe erwarten lässt, kann es dem Kläger nicht zugemutet werden, sämtliche künftigen

technischen Entwicklungen präzise benennen zu können. Die insoweit verbleibende Unsicherheit steht einer wertenden Prüfung im Vollstreckungsverfahren gegebenenfalls unter Zuhilfenahme eines Sachverständigen jedoch nicht grundsätzlich entgegen (vgl. z.B. § 100 GVGA oder § 756 ZPO, wenn die vom Gerichtsvollzieher zu überprüfende geschuldete Gegenleistung in der Mängelbeseitigung besteht) und ist daher hier zugunsten der effektiven Rechtsschutzgewähr hinzunehmen.

b) Der Einwand des fehlenden Rechtsschutzbedürfnisses der Beklagten unter Verweis auf die Möglichkeit zur Anpassung von Nutzereinstellung überzeugt nicht. Es erscheint zumindest möglich, dass eine zukünftige unrechtmäßige Datenverarbeitung dadurch nicht verhindert werden kann, da der Kläger nämlich keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat (vgl. LG Itzehoe, Urteil vom 27. Februar 2023 – 10 O 159/22 –, Rn. 52, juris).

3. Während der Antrag zu 3.a. nur teilweise begründet ist, ist der Antrag zu 3.b. unbegründet.

a) Hinsichtlich des Antrag zu 3.a. steht dem Kläger gegen die Beklagte ein Unterlassungsanspruch gem. Art. 17 Abs. 1 lit. d) DSGVO zu, jedoch nicht im geltend gemachten Umfang.

aa) Aus dem Löschanspruch gem. Art. 17 DSGVO ergibt sich a maiore ad minus zugleich ein Anspruch auf Unterlassung (BGH, Urteil vom 13. Dezember 2022 – VI ZR 60/21 –, Rn. 10, juris), soweit der zugrunde zu legende Sachverhalt die Anspruchsvoraussetzungen im geltend gemachten Umfang trägt.

bb) Der Kläger kann von der Beklagten lediglich verlangen, die nach dem Stand der Technik angemessenen Maßnahmen vorzusehen.

(1) Wie ausgeführt hat die Beklagte rechtswidrig personenbezogene Daten des Klägers verarbeitet, indem sie keine hinreichenden Vorkehrungen getroffen hat, um eine ihrerseits vorgenommene Verknüpfung der klägerischen Daten bei missbräuchlicher Ausnutzung des CIT durch Dritte zu verhindern.

(2) Darüber hinaus begründet die Verletzung des klägerischen Rechts auf informationelle Selbstbestimmung die tatsächliche Vermutung dafür, dass eine Wiederholungsgefahr für die entsprechende Verletzung vorliegt (vgl. BGH, Urteil vom 4. Dezember 2018 – VI ZR 128/18 –, Rn. 9, juris m.w.N.).

(a) Diese Vermutung hat die Beklagte nicht entkräftet. Weder hat sie eine strafbewehrte Unterlassungserklärung abgegeben, noch andere Umstände dargetan, die die Vermutung hier widerlegen.

(b) Allerdings erstreckt sich die Wiederholungsgefahr hier nur auf die Datenverarbeitung ohne die dem Stand der Technik nach angemessenen und nicht etwa – wie der Kläger beantragt – möglichen Maßnahmen vorzusehen. Die tatsächliche Vermutung der Wiederholungsgefahr und damit auch der Anspruchsinhalt werden durch die geltend gemachte Rechtsverletzung determiniert. Der Kläger kann hier durch seinen Antrag also nicht berechtigterweise ein Unterlassen von solchen Handlungen erzwingen, die mit der gesetzlichen Regelung im Einklang stehen. Wie oben dargelegt normiert Art. 32 Abs. 1 DSGVO keine Verpflichtung zu einem Höchstmaß an Vorkehrungen, sondern lediglich zu einem angemessenen Schutzniveau.

b) Der Antrag zu 3.b. ist hingegen nicht begründet. Es ist schon mit Blick auf die unterschiedlichen Rechtfertigungsgründe in Art. 6 Abs. 1 S.1 lit. b) – f) DSGVO nicht einzusehen, warum allein eine unwirksam erteilte Einwilligung zwingend die Rechtswidrigkeit der Verarbeitung und damit auch eine den Unterlassungsanspruch stützende Rechtsverletzung begründet. Zwischen den Parteien ist zudem unstreitig, dass eine Einwilligung seitens der Beklagten nicht eingeholt wurde. Es erschließt sich folglich nicht, woraus mangels in der Vergangenheit erfolgter Verarbeitung der Telefonnummer auf Grundlage einer Einwilligung das klägerische Recht resultieren soll, dies künftig der Beklagten zu untersagen.

IV. Der Antrag zu 4 ist zulässig, aber unbegründet, da die Beklagte mit Schreiben vom 21. Oktober 2021 den Anspruch des Klägers auf Auskunft aus § 15 DSGVO bereits vorprozessual i.S.d. § 362 Abs. 1 BGB erfüllt hat. Dabei ist ohne Belang, ob die Auskunft auch inhaltlich der Richtigkeit entspricht. Es kommt lediglich darauf an, dass die Auskunft nach dem Willen des Schuldners im geschuldeten Gesamtumfang erteilt wird (BGH, Urteil vom 3. September 2020 – III ZR 136/18 –, Rn. 43, juris).

Dies war hier der Fall. Die Beklagte hat mitgeteilt, dass sie über eine Kopie der verlangten Rohdaten, welche die durch Scraping abgerufenen Daten enthielten, nicht verfüge. Auf Grundlage der bislang vorgenommenen Analysen sei es ihr jedoch gelungen, der Nutzer-ID des Klägers die bestimmten Daten zuzuordnen, die nach ihrem Verständnis in den durch Scraping abgerufenen Daten erschienen und mit den auf dem Facebook-Profil des Klägers verfügbaren Informationen übereinstimmten. Weiter hat die Beklagte erläutert,

wie das Daten-Scraping ihrer Einschätzung nach erfolgte. Schließlich hat die Beklagte auch erklärt, dass sie davon ausgehe, dass die Telefonnummer des Klägers in den durch Scraping abgerufenen Daten enthalten gewesen sei. Mit dem umfangreichen Schreiben hat die Beklagte nicht zuletzt in Ansehung des letzten Absatzes zum Ausdruck gebracht, dass sie die von ihr geschuldeten Angaben mitgeteilt hat.

V. Der Kläger hat Anspruch auf Ersatz seiner vorgerichtlichen Anwaltskosten gem. § 82 Abs. 1 DSGVO, da sich dieser zur Rechtsverfolgung zunächst im Wege eines Auskunftsersuchens in Vorbereitung des späteren Klageverfahrens anwaltlicher Hilfe bediente und die Inanspruchnahme sachkundiger Personen in Anbetracht der Komplexität der Materie auch notwendig war. Der materiell-rechtliche Kostenerstattungsanspruch besteht allerdings nur in der Höhe, in der dieser in Abhängigkeit zur zugesprochenen Hauptforderung auch tatsächlich begründet war (hier: Gebührenstufe bis 1.500 €).

B. Die Kostenentscheidung beruht auf §§ 91 Abs. 1, 92 Abs. 1 S.1 Alt. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711, 709 S.1, 2 ZPO.

C. Der von Amts wegen durch die Kammer gem. § 63 Abs. 2 S.1 GKG festzusetzende Gegenstandswert liegt in Bemessung nach §§ 39, 40, 43, 48 Abs. 1 GKG i.V.m. § 3 ZPO innerhalb der festgesetzten Stufe.

Die Entscheidung über die Festsetzung des Streitwertes kann mit der Beschwerde angefochten werden. Sie ist nur zulässig, wenn sie innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache rechtskräftig geworden ist oder das Verfahren sich anderweitig erledigt hat, bei dem Landgericht Halle, 06108 Halle, Hansering 13 eingeht.
Wird der Streitwert später als einen Monat vor Ablauf dieser Frist festgesetzt, kann die Beschwerde innerhalb eines Monats nach Zustellung oder formloser Mitteilung der Festsetzung bei dem Gericht eingelegt werden. Die Beschwerde ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200,00 € übersteigt oder das Gericht die Beschwerde in diesem Beschluss zugelassen hat.
Beschwerdeberechtigt ist, wer durch diese Entscheidung in seinen Rechten beeinträchtigt ist. Die Beschwerde wird durch Einreichung einer Beschwerdeschrift oder zur Niederschrift der Geschäftsstelle des genannten Gerichts eingelegt. Sie kann auch zur Niederschrift der Geschäftsstelle eines jeden Amtsgerichts erklärt werden, wobei es für die Einhaltung der Frist auf den Eingang bei dem genannten Gericht ankommt. Sie ist von dem Beschwerdeführer oder seinem Bevollmächtigten zu unterzeichnen.
Die Einlegung kann auch in elektronischer Form erfolgen. Informationen zu den weiteren Voraussetzungen zur Signatur und Übermittlung sind auf dem Justizportal des Bundes und der Länder (www.justiz.de) im Themenbereich zur elektronischen Kommunikation zu finden. Eine Einlegung per einfacher E-Mail ist unzulässig.

Die Beschwerde muss die Bezeichnung des angefochtenen Beschlusses sowie die Erklärung enthalten, dass Beschwerde gegen diesen Beschluss eingelegt wird. Soll die Entscheidung nur zum Teil angefochten werden, so ist der Umfang der Anfechtung zu bezeichnen.

Richterin am Landgericht
ist wegen Erkrankung abwesend und
deshalb gehindert zu unterzeichnen.