Aktenzeichen:
4 O 244/22

Landgericht Ulm

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.Legal**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platform Ireland Limited (zuvor Facebook Ireland Ltd.), vertreten durch d. Geschäftsführer (Director) Gareth Lambe, ebenda, Merrion Road, Dublin 4, D04 X2K5, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater Partnergesellschaft mbB**, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.:

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat das Landgericht Ulm - 4. Zivilkammer - durch die Vorsitzende Richterin am Landgericht als Einzelrichterin am 09.02.2024 aufgrund der mündlichen Verhandlung vom 10.01.2024 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 350,00 € nebst Zinsen seit 20.09.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen materiellen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahr 2019 noch entstehen werden.

3. Im Übrigen wird die Klage abgewiesen.

4. Von den Kosten des Rechtsstreits haben der Kläger 88 % und die Beklagte 12 % zu tragen.

5. Das Urteil ist vorläufig vollstreckbar.

   Der Beklagten wird nachgelassen, die Vollstreckung durch den Kläger gegen Sicherheitsleistung i.H.v. 110 Prozent des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Klägerin vor der Vollstreckung Sicherheit i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages leistet.

   Für die Beklagte ist das Urteil gegen Sicherheit i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

(Klageantrag Ziff. 1 - Leistungsantrag: 1.000,00 €
Klageantrag Ziff. 2 - Feststellungsantrag: 500,00 €
Klageantrag Ziff. 3 - Unterlassungsantrag: 5.000,00 €

Klageantrag Ziff. 4 - Auskunftsantrag: 500,00 €

Klageantrag Ziff. 5 - vorger. Rechtsanwaltskosten: 0,00 €)

Tatbestand

Der Kläger fordert mit seiner Klage wegen eines sog. Scraping (dem Abgreifen personenbezogener Daten aus dem Contact-Import-Tool der Beklagten) Schadensersatz, die Feststellung einer weiteren Ersatzpflicht der Beklagten, Unterlassung, Auskunftserteilung sowie Erstattung vorgerichtlich entstandener Rechtsanwaltskosten.

Der Kläger unterhält seit 2010 ein Nutzerkonto bei der Beklagten, die das soziale Netzwerk Facebook betreibt, unter Verwendung der E-Mail-Adresse: .

Bei der Eröffnung eines Facebook-Kontos müssen die Nutzer Informationen über sich erteilen. Durch entsprechende Einstellungen des Facebook-Kontos können die Nutzer bestimmen, welche der angegebenen Informationen für welchen Personenkreis einsehbar sind. Die Nutzer-ID, der Vor- und Nachname sowie das Geschlecht sind immer öffentlich einsehbar. Die Angabe der Handynummer ist nicht zwingend.

Hinsichtlich der weiteren Daten gibt es im Rahmen der Privatsphäre-Einstellungen Wahlmöglichkeiten für jeden Nutzer.

Bei der sog. *„Zielgruppenauswahl“* legt der Nutzer fest, wer einzelne Informationen auf seinem Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann.

In den *„Suchbarkeits-Einstellungen“* wird festgelegt, wer das Profil eines Nutzers durch die Telefonnummer finden kann.

In der App für Mobiltelefone ist eine Software namens Contact-Import-Tool (CIT) integriert. Das CIT gleicht die bei Facebook hinterlegten Telefonnummern mit Telefonnummern ab, die bei einem Nutzer in seinem Smartphone als Kontakte gespeichert sind. Dann werden dem Nutzer die entsprechenden Facebook-Profile angeboten, die zu seinen im Smartphone abgespeicherten Telefonnummern passen. Maßgeblich für diese Funktion sind allein die Angaben des Nutzers unter der *„Suchbarkeits-Einstellung“*, nicht die der Zielgruppenauswahl.

Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre *„Suchbarkeits-Einstellung“* für Telefonnummern auf der Standard-Voreinstellung *„Alle“* eingestellt war. Daneben waren die Einstellungen nur *„Freunde von Freunden“* oder *„Freunde“* auswählbar. Ab Mai 2019 stand Nutzern auch die Option *„Nur ich“* zur Verfügung.

Die Datenrichtlinie der Beklagten in der Fassung von 2018 teilten mit, welche Nutzerinformationen öffentlich sind (Name, Geschlecht, Nutzername, Nutzer-ID), wie ein Nutzer festlegen kann, welche Informationen zugänglich gemacht werden können (Zielgruppenauswahl) und wie er aufgrund Mailadresse oder Telefonnummer aufgefunden werden kann (Suchbarkeitseinstellungen) (vgl. Anl. B9).

Im Jahr 2019 kam es zu einem Abgreifen persönlicher Daten von Facebook-Nutzern durch Dritte. Hierbei wurden die immer öffentlich zugänglichen Daten (Name, Geschlecht, Nutzername, Nutzer-ID) mit der angegebenen Telefonnummer verknüpft, indem über die Contact-Import-Funktion die Telefonnummern hochgeladen wurden, die mit einem Konto verknüpft waren, und diese Daten dann zusammengeführt wurden.

Mit E-Mail vom 18.03.2022 forderte der Prozessbevollmächtigte des Klägers die Beklagte auf, *„die rechtswidrige Verarbeitung der personenbezogenen Daten (...) - hier das Zugänglichmachen für Unbefugte (...) - zu unterlassen“.* Ferner forderte er eine Schadensersatzzahlung in Höhe von 500,00 € unter Fristsetzung bis 19.04.2022, Auskunftserteilung darüber, welche konkreten Daten des Klägers abgegriffen und veröffentlicht wurden, sowie Erstattung vorgerichtlich entstandener Rechtsanwaltskosten (vgl. Anl. K1).
Mit Antwortschreiben vom 14.04.2022 nahm die Beklagte zu den Vorwürfen des Klägers erneut Stellung (vgl. Anl. B16).

Der Kläger behauptet und vertritt die Auffassung,
seine Handynummer habe wegen einer Sicherheitslücke mit seinen restlichen Personendaten korreliert werden können. Diese seien somit Bestandteil des unbefugt verbreiteten Datensatzes gewesen. Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben worden sei, sei es Unbekannten gelungen, Telefonnummern konkreten Facebook-Profilen zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben gewesen seien. Um die Telefonnummern jeweils zu korrelieren, sei mit Hilfe des Contact- Import-Tools jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer angezeigt worden. Auf seinem Profil sei er dann besucht und von dort seien die öffentlichen Daten gescrapt *(“abgeschöpft“)* worden.

Ihm stehe ein Schadensersatzanspruch gegen die Beklagte gemäß § 82 Abs. 1 DSGVO zu, da deren Verhalten mehrere Verstöße gegen die DSGVO begründe.

Die Beklagte habe ihn nicht in ausreichendem Maße über die Verarbeitung ihn betreffender Daten, die er angegeben habe, informiert bzw. aufgeklärt. Insbesondere stelle die Art der Belehrung über die Verwendung und Geheimhaltung seiner Telefonnummer einen Verstoß gegen die DSGVO dar. Er macht in diesem Zusammenhang einen Verstoß der Beklagten gegen das Transparenzgebot gemäß Art. 5 Abs. 1 lit. a) DSGVO sowie einen Verstoß gegen Informationspflichten der Beklagten gemäß Art. 13, 14 DSGVO geltend.

Die Beklagte habe darüber hinaus seine personenbezogenen Daten im Jahr 2019 nicht in ausreichendem Maße und den Anforderungen von Art. 5 Abs. 1 lit. f) DSGVO entsprechend geschützt. So seien technische Maßnahmen wie z.B. *„Sicherheits-Capchas“*, die garantierten, dass es sich bei der Person, die eine Suchanfrage stellt, um einen Menschen und nicht um eine automatische Software handle, nicht verwendet worden.

Unabhängig von etwaigen Sicherheitslücken habe die Beklagte mit den von ihr vorgenommenen Einstellungen zur Privatsphäre gegen die in Art. 25 DSGVO niedergelegten Grundsätze der *„Privacy by design“* und *„Privacy by default“* verstoßen.

Die Beklagte habe darüber hinaus weder ihn noch die zuständige Aufsichtsbehörde, die Irish Data Protection Commission, von dem Datenschutzverstoß informiert. Sie sei damit weder ihrer Informationspflicht nach Art. 34 DSGVO noch nach Art. 33 DSGVO nachgekommen.

In einer für jedermann abrufbaren Datenbank seien nachfolgende personenbezogene Daten enthalten:

„
,,“

Dabei handle es sich um seine Telefonnummer, seine Facebook-ID und seinen Alias-Namen.

Durch die unbefugte Veröffentlichung seiner personenbezogenen Daten habe er einen konkreten ersatzfähigen Schaden erlitten. Dieser bestehe darin, dass er einen erheblichen Kontrollverlust über seine Daten erlitten habe und in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten verbleibe. Dies habe sich u.a. in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen, aber auch in der ständigen Sorge, dass die veröffentlichten Daten von Kriminellen für unlautere Zwecke verwendet werden könnten, manifestiert.

Seit April 2021 erhalte er vermehrt Anrufe von unbekannten Telefonnummern, dubiose Nachrich-

ten, Spam- und Werbe-Emails sowie SMS-Benachrichtigungen mit dubiosen Aufforderungen zum Anklicken von Links.

Hätte die Beklagte ihn ausreichend und in angemessenem Umfang über die Folgen der Preisgabe seiner Telefonnummer informiert, so hätte er keine Einwilligung erteilt und seine Telefonnummer nicht angegeben. Insbesondere, wenn klar darauf hingewiesen worden wäre, dass kein Schutz vor dem Abgreifen durch automatische Verfahren bestehe, wäre eine Einwilligung zur Verarbeitung nicht erteilt und die Telefonnummer nicht veröffentlicht worden.

Auch die Nichtvornahme entsprechender Schutzmaßnahmen gegen das automatische Abgreifen der Daten sowie gegen die Ausnutzung der Sicherheitslücke, die ein Abgreifen von nicht-öffentlichen Daten ermöglicht habe, sei ursächlich für seinen Schaden geworden. Wären von der Beklagten derartige Maßnahmen vorgenommen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen. Das Abgreifen habe durch die anschließende Veröffentlichung unmittelbar in seinen Schaden gemündet.

Ebenso habe die unterlassene Information zu einer Intensivierung seines Schadens geführt. Durch einen auf mangelnder Unterrichtung beruhenden Zeitraum der Ungewissheit hätten sich die Risiken, dass seine Daten unbemerkt missbraucht werden und damit sein Unwohlsein und seine Sorgen entschieden gesteigert. Wäre angemessen zügig eine Benachrichtigung erfolgt, so hätten zeitnah Schritte zur Risikominimierung und Absicherung eingeleitet werden können, um einen Schaden zu vermeiden.

Ein Schadensersatzanspruch in Höhe von mindestens 1.000,00 € sei vorliegend angemessen.

Aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz folge auch ihre Pflicht, zukünftige Schäden, die aufgrund der entwendeten Daten entstehen, zu tragen. Ihrem Wesen nach zeigten sich die Folgen von Datenschutzverletzungen erst spät, oft blieben sie lange unerkannt. Es sei daher in seinem Interesse und auch im Interesse der allgemeinen Rechtssicherheit, eine Haftung der Beklagten schon jetzt festzustellen, um später aufgrund des Zeitablaufs entstehende Unsicherheiten zu vermeiden.

Ihm stehe ferner ein Anspruch auf Auskunftserteilung gemäß Art. 15 DSGVO zu, da die Beklagte seinem Verlangen auf Auskunftserteilung nicht in ausreichendem Maße nachgekommen sei. Sie habe lediglich allgemein angezeigt, welche Arten von Daten sie von ihm verarbeite, jedoch keine konkrete Auskunft zu dem in Rede stehenden Datenschutzvorfall gemacht. Weder sei er darüber

informiert worden, wer auf die Daten zugegriffen habe noch sei er darüber aufgeklärt worden, welche Daten genau auf diesem Wege abgegriffen worden seien. Konkret seien keine Informationen darüber erteilt worden, welche Daten zum Zeitpunkt des Datenschutzvorfalls für wen einsehbar gewesen seien. Der Beklagten sei aber durch einfachste Log-Dateien möglich, diese Vorgänge nachzuvollziehen und mitzuteilen, ob Telefonabgleiche etc. stattgefunden haben.

Ihm stehe auch nach §§ 1004 analog, 823 Abs. 1 und Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO ein Anspruch gegen die Beklagte auf Unterlassung, seine personenbezogenen Daten in Zukunft unbefugt, d.h. konkret ohne vorherige ausreichende Belehrung, zu veröffentlichen und diese zukünftig unbefugten Dritten zugänglich zu machen, zu.

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 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet und vertritt die Auffassung,
die Klage sei bereits weitgehend unzulässig.

Klageantrag Ziff. 1 sei mangels hinreichender Bestimmtheit im Sinne des § 253 Abs. 2 Nr. 2 ZPO unzulässig. Zwar mache der Kläger einen Zahlungsantrag geltend, er stütze sein Begehren jedoch auf zwei zeitlich auseinanderfallende angebliche Verstöße gegen die DSGVO und damit auf unterschiedliche Lebenssachverhalte.
Einerseits trage der Kläger vor, ihm sei durch die dem Scraping-Vorfall vorgelagerten vermeintlichen Verstöße gegen die DSGVO ein Schaden in Form eines Kontrollverlusts über seine Daten entstanden. Gleichzeitig stütze er seine Klage auf einen pauschal behaupteten Schaden aus der Verletzung von Benachrichtigungspflichten, ohne diesen konkret zu benennen. Der Klage lägen damit zwei verschiedene - separate und eigenständige - Streitgegenstände zugrunde. Der Kläger habe es versäumt zu konkretisieren, in welchem Verhältnis jeder der unterstellten Schäden den geltend gemachten Ersatzanspruch anteilig tragen soll. Das Verhältnis der eigenständigen Le-

benssachverhalte sei damit unklar, dessen Bestimmung dürfe nicht in das Ermessen des Gerichts gestellt werden und sei auch im Wege der Auslegung nicht zu ermitteln.

Auch Klageantrag Ziff. 2 sei nicht hinreichend bestimmt.
Der Kläger begehre die Feststellung ihrer Ersatzpflicht für *„künftige* [...] *Schäden“*, die *„entstanden sind“*. Der Antrag sei daher seinem Wortlaut nach derart widersprüchlich, dass unklar sei, welche Feststellung er tatsächlich begehre. Ob lediglich zukünftige oder bereits in der Vergangenheit entstandene Schäden erfasst werden sollen, lasse sich dem Antrag nicht mit hinreichender Bestimmtheit entnehmen oder im Wege der Auslegung ermitteln.

Daneben fehle es an dem für die Zulässigkeit des Antrags gemäß § 256 Abs. 1 ZPO erforderlichen Feststellungsinteresse.
Der Kläger werde den vom Bundesgerichtshof an das Feststellungsinteresse gemäß § 256 Abs. 1 ZPO gestellten Anforderungen mit seinem pauschalen und unsubstantiierten Verweis darauf, dass die Folgen von Datenschutzverletzungen lange unerkannt blieben, nicht gerecht. Er habe weder konkret vorgetragen, welche materiellen Schäden ihm aus dem behaupteten Datenschutzverstoß entstehen könnten noch dazu, warum er einen Schadeneintritt für wahrscheinlich halte. Im Gegenteil habe er sich dahingehend eingelassen, dass *„noch nicht abgesehen werden* [kann], *welche Dritten Zugriff auf die Daten* [...] *erhalten haben und für welchen konkreten kriminellen Zwecke die Daten missbraucht werden“*. Damit räume er ein, dass der Eintritt künftiger Schäden derzeit ungewiss sei; eine hinreichende Wahrscheinlichkeit des Schadenseintritts bestehe daher schon nach den Darstellungen des Klägers nicht und sei bei objektiver Betrachtung auch nicht ersichtlich. Das Missbrauchspotenzial der streitgegenständlichen Daten sei äußerst gering. Insofern sei es fernliegend, dass unbefugte Dritte mit den Daten einen Vermögensschaden des Klägers herbeiführen werden oder könnten. Zudem sei nach dem Vortrag des Klägers der Zugriff auf seine Daten bereits im Jahr 2019 erfolgt. Sie seien aber bisher nicht für kriminelle Aktivitäten genutzt worden. Ohne weitere Anhaltspunkte könne nicht angenommen werden, dass die Daten erst drei Jahre nachdem unbefugte Dritte angeblich erstmalig darauf zugegriffen hätten, für kriminelle Zwecke missbraucht werden.

Auch der vom Kläger behauptete Kontrollverlust über seine Daten begründe keine hinreichende Wahrscheinlichkeit eines künftigen Schadens. Dieser könne sich nämlich denklogisch nicht wiederholen. Die vom Kläger behauptete Gefahr, Opfer von Internetkriminalität beziehungsweise Identitätsdiebstahl zu werden, sei Teil des allgemeinen Lebensrisikos. Es handle sich dabei um ein abstrakt-generelles und überdies nicht sonderlich wahrscheinliches Risiko, dem jeder Nutzer des Internets ausgesetzt sei.

Schließlich fehle das Feststellungsinteresse nach dem Grundsatz der Einheitlichkeit des Schmerzensgeldes jedenfalls hinsichtlich künftiger immaterieller Schäden. Dementsprechend habe der Kläger kein berechtigtes Interesse an einem Feststellungsurteil über den Ersatz künftiger immaterieller Schäden, da solche Schäden bereits durch die Rechtskraft der Entscheidung über den Klageantrag zu Ziffer 1) abgedeckt wären.

Zuletzt sei auch Klageantrag Ziff. 3. zu unbestimmt.

Klageantrag Ziff. 3. lit. a), mit welchem der Kläger die Unterlassung der Zugänglichmachung von personenbezogenen Daten ohne *„nach dem Stand der Technik mögliche(n) Sicherheitsmaßnahmen“* fordere, entspreche nicht dem für Unterlassungsanträge geforderten Standard. Hiernach müssten Unterlassungsanträge im Besonderen über den Wortlaut einer etwaigen Verbotsnorm hinaus genau an die konkrete Verletzungsform angepasst sein, um inhaltlich nicht über den materiell-rechtlichen Anspruch hinauszugehen. Der Streitgegenstand müsse so klar gefasst sein, dass sie sich im Erkenntnisverfahren erschöpfend verteidigen könne. Im Hinblick auf die Formulierung des Klageantrages Ziff. 3. lit. a) müsste im Vollstreckungsverfahren geklärt werden, welche Sicherheitsmaßnahmen dem aktuellen *„Stand der Technik“* entsprechen. Unklar bleibe zudem, wo die Grenze zwischen *„aktueller“* und *„nicht mehr aktueller“* Technik liege.

Der Klageantrag Ziff 3. lit. a) sei im Übrigen auch widersprüchlich, wenn der Kläger fordere, dass sie es unterlassen müsse, *„personenbezogene Daten der Klägerseite, namentlich* […] *FacebookID, Familiennamen, Vornamen, Geschlecht* […] *unbefugten Dritten* […] *zugänglich zu machen“.* Es handle sich bei diesen Datenpunkten um immer öffentliche Nutzerinformationen, so dass es schon keine unbefugten Dritten geben könne, welchen der Zugriff verweigert werden könne. Sollte der Antrag so zu verstehen sein, dass der Kläger darauf abziele, dass sein Facebook-Nutzerkonto nicht über seine Handynummer suchbar sein soll, würde ihm hierfür jedenfalls das Rechtsschutzbedürfnis fehlen, da er dieses Ziel durch die Anpassung seiner Einstellungen erreichen könne. Es bestehe daher ein gegenüber der klageweisen Geltendmachung schnelleres, aber genauso effektives Mittel.

Auch der Klageantrag Ziff. 3. lit. b) sei nicht hinreichend bestimmt, soweit sie verurteilt werden solle, die Verwendung der Telefonnummer zu unterlassen, die aufgrund *„unübersichtlicher oder unvollständiger Informationen“* erlangt worden sei. Die Begriffe *„unübersichtlich“* und *„unvollständig“* bedürften einer Wertung, die wegen ihrer Komplexität und ihres Umfangs nicht im Vollstreckungsverfahren vorgenommen werden könne.

Die Klage sei darüber hinaus unbegründet.

Es sei davon auszugehen, dass Telefonnummern gerade nicht von Facebook-Profilen abgerufen worden seien, sondern von den Scrapern mit einem Prozess der sog. Telefonnummernaufzählung bereitgestellt worden seien. Nutzer hätten während des relevanten Zeitraums ihre Kontakte von ihren Mobilgeräten auf Facebook hochladen können, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten (Kontakt-Importer-Funktion). Zu diesem Zweck hätten die Scraper mit Hilfe der Kontakt-Importer-Funktion Kontakte hochgeladen, welche mögliche Telefonnummern von Nutzern enthalten hätten, um so festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden seien. Soweit die Scraper hätten feststellen hätten, dass eine Telefonnummer mit einem Facebook-Konto (in Übereinstimmung mit der jeweiligen Suchbarkeitseinstellung des Nutzers) verknüpft gewesen sei, hätten sie die öffentlich einsehbaren Informationen (in Übereinstimmung mit der Zielgruppenauswahl des Nutzers) aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten sodann hinzugefügt.

Der vom Kläger geltend gemachte Schadensersatzanspruch scheitere bereits daran, dass die Vorschriften, auf die er seine vermeintlichen Ansprüche stütze, also Art. 13, 14 DSGVO, Art. 24, 25 DSGVO, Art. 34 DSGVO und Art. 15 DSGVO, nicht vom Anwendungsbereich des Art. 82 DSGVO erfasst seien.

Art. 82 DSGVO erfasse von vornherein nur solche Pflichtverstöße, die ihm Rahmen einer *„Verarbeitung“* geschehen würden. Art. 13, 14 DSGVO, 34 DSGVO und Art. 15 DSGVO begründeten Informationspflichten gegenüber betroffenen Personen. Die Erteilung von Informationen über die Verarbeitung personenbezogener Daten, die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten gegenüber Nutzern und die Erteilung einer beantragten Auskunft stellten jedoch selbst keine Verarbeitung personenbezogener Daten im Sinne von Art. 4 Nr. 2 DSGVO dar. Dementsprechend könne ein Schadensersatzanspruch nach Art. 82 DSGVO nicht aus einer Verletzung dieser Vorschriften resultieren.

Auch Art. 24 DSGVO scheide als möglicher Anknüpfungspunkt für einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO aus. Bei Art. 24 DSGVO handle es sich um eine Überblicks- und Generalnorm, die die Rolle und Verantwortung des Verantwortlichen als Hauptadressaten der DSGVO konkretisiere, jedoch selbst keine konkreten Verpflichtungen begründe, die einen Schadensersatzanspruch auslösen könnten.

Ebenso wenig könne ein Verstoß gegen die Grundsätze *„Privacy by design“* und *„Privacy bei default“* gemäß Art. 25 Abs. 1 und Abs. 2 DSGVO einen Schadensersatzanspruch nach Art. 82

Abs. 1 DSGVO auslösen, weil die Normen nicht in direktem Zusammenhang mit einer konkreten Verarbeitung stünden. Jedenfalls könne ein Verstoß gegen Art. 25 DSGVO niemals kausal für einen etwaigen Schaden sein, da ein datenschutzrechtliches Schadensereignis nur durch eine konkrete Verarbeitung ausgelöst werde könne, nicht hingegen durch die vom Verantwortlichen getroffene Wahl der technischen Gestaltung des betreffenden Dienstes oder der gewählten Voreinstellungen.

Der geltend gemachte Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO bestehe auch deshalb nicht, weil der darlegungs- und beweisbelastete Kläger einen Verstoß gegen die DSGVO nicht dargelegt oder bewiesen habe.

Dem Scraping-Sachverhalt habe weder eine Sicherheitslücke in ihrem System zugrunde gelegen noch treffe die klägerische Behauptung zu, dass sie keinen Schutz vor dem *„Abgreifen durch automatische Verfahren“* geleistet habe.

Sie stelle ihren Nutzern sämtliche in Art. 13, 14 DSGVO aufgeführten Informationen in Bezug auf die von ihr durchgeführten Datenverarbeitungen zum Zeitpunkt der Datenerhebung im Rahmen ihrer Datenrichtlinie zur Verfügung. Die Darstellung der Informationen erfolge im Einklang mit den Vorgaben der DSGVO (vgl. Art. 12 Abs. 1 DSGVO). Insbesondere die Verwendung einer sog. Mehrebenen-Datenschutzerklärung, bei welcher der Nutzer auf der ersten Ebene einen ersten Überblick über die ihm hinsichtlich der Verarbeitung seiner personenbezogenen Daten zur Verfügung stehenden Informationen erhalte und die weiterführenden Informationen durch Ansteuern des jeweiligen Abschnitts eingesehen werden könnten, entspreche den Empfehlungen der europäischen Datenschutzbehörden. Die Mehrebenen-Datenschutzerklärung sei auch im relevanten Zeitraum durch weitergehende Informationen im Hilfebereich ergänzt worden. Hierdurch würden den Nutzern nicht nur die nach Art. 5 Abs. 1 lit. a), 13 und 14 DSGVO gesetzlich vorgeschriebenen Pflichtinformationen zur Verfügung gestellt, sondern auch übersichtliche Zusammenfassungen besonders relevanter Themen. Auch dieses Vorgehen entspreche den Empfehlungen der europäischen Datenschutzbehörden.

Auch ein Verstoß gegen Art. 24 und 32 DSGVO, welche die Pflicht zur Gewährleistung angemessener technischer und organisatorischer Maßnahmen vorsehen, sei vom darlegungs- und beweisbelasteten Kläger nicht schlüssig und hinreichend substantiiert dargelegt worden. Zudem führe ein Verstoß gegen Art. 24 DSGVO schon deshalb nicht zu einem Schadensersatzanspruch, weil die Regelung kein subjektives Recht des Betroffenen begründe.

Soweit der Kläger das Fehlen einzelner technischer und organisatorischer Maßnahmen behaup-

te, könne dies bereits dem Grunde nach keinen Verstoß begründen, da ihr hinsichtlich der Auswahl der konkreten Maßnahmen ein Ermessensspielraum zukomme und sie demnach zur Ergreifung einzelner, konkreter Maßnahmen nicht verpflichtet sei.

Soweit der Kläger das Fehlen angemessener technischer und organisatorischer Maßnahmen im Ganzen behaupte, könne auch dies keinen Verstoß gegen Art. 24, 32 DSGVO.

Denn der Verantwortliche habe vor Beginn der eigentlichen Datenverarbeitung zu prüfen, welche Risiken mit der Datenverarbeitung einhergehen und welche technischen und organisatorischen Maßnahmen erforderlich sind, um etwaigen Risiken angemessen zu begegnen. Es sei daher widersprüchlich und mit dem risikobasierten Ansatz der DSGVO unvereinbar, wenn der Kläger einerseits die Notwendigkeit einer ex-ante-Beurteilung erkenne, wenige Absätze später indes versuche, aus dem Stattfinden des Scraping-Sachverhalts ex post die Mangelhaftigkeit ihrer technischen und organisatorischen Maßnahmen abzuleiten.

Schließlich habe der Scraping-Sachverhalt Daten betroffen, die im Einklang mit der Zielgruppenauswahl des jeweiligen Nutzers öffentlich einsehbar gewesen seien. Hieraus folge, dass sie in Bezug auf die Systeme und Dienste mit der Verarbeitung von vornherein nicht verpflichtet gewesen sei, Vertraulichkeit sicherzustellen.

Selbst wenn man dies anders sähe, hätte sie im relevanten Zeitraum ohnehin verschiedene effektive Anti-Scraping-Maßnahmen eingesetzt, die jedenfalls vollumfänglich den Anforderungen des Art. 32 DSGVO Rechnung tragen würden. Schließlich sei auch die Integrität, Verfügbarkeit und Belastbarkeit ihrer Systeme durch den Scraping-Sachverhalt nicht beeinträchtigt.

Sie habe im relevanten Zeitraum auch die Grundsätze des Art. 25 DSGVO (data protection by design and by default) gewahrt. Eine Festlegung der Standardeinstellungen für die Suchbarkeit von Telefonnummer, d.h. eine Suchbarkeitseinstellung auf eine andere Einstellung als *„alle“*, würde den eigentlichen Zweck, zu dem ein Nutzer Facebook beitrete, zunichtemachen, da dies dazu führen würde, dass die Nutzer auf der Facebook-Plattform isoliert wären, ohne dass sie eine einfache Möglichkeit hätten, mit anderen in Kontakt zu treten. Wenn indes eine Standardeinstellung für den Zweck der Verarbeitung erforderlich sei, müsse sie auch als mit Art. 25 Abs. 2 DSGVO vereinbar angesehen werden, solange der Nutzer die Möglichkeit habe, durch Anpassung der betreffenden Einstellung *„einzugreifen“.*

Auch eine Verletzung der Benachrichtungs- oder Meldepflichten gemäß Art. 34, 33 DSGVO habe der Kläger weder dargelegt noch bewiesen. Es fehle an einer Verletzung der Sicherheit im Sinne

des Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten.

Ebenso wenig falle ihr ein Verstoß gegen Art. 6 DSGVO zur Last, weil die Verarbeitung der personenbezogenen Daten des Klägers im Rahmen der Bereitstellung der Facebook-Plattform rechtmäßig gewesen sei. Sie verfüge über eine wirksame Rechtsgrundlage für die Verarbeitung der Daten des Klägers. Diese Rechtsgrundlage sei im Rahmen der Bereitstellung der Facebook-Plattform Art. 6 Abs. 1 lit. b) DSGVO. Dabei handle es sich um den hier erheblichen Verarbeitungszweck, welcher bedinge, dass bestimmte Daten der Privatsphäreeinstellungen des Klägers entsprechend öffentlich zugänglich seien.

Der mit Klageantrag Ziff. 4 geltend gemachte Auskunftsanspruch des Klägers bestehe ebenfalls nicht. Sie habe das Auskunftsersuchen der Klägerseite vom 18.03.2022 mit Antwortschreiben vom 14.04.2022 ordnungsgemäß beantwortet. Entgegen dem Vortrag des Klägers sei eine Verletzung der Auskunftspflicht gemäß Art. 15 DSGVO nicht darin zu sehen, dass in ihrem Schreiben *„keinerlei konkrete Aussagen dazu* [enthalten waren], *welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen wurden“,* da Art. 15 Abs. 1 DSGVO den Verantwortlichen lediglich zur Auskunft in Bezug auf seine eigene Verarbeitungstätigkeit verpflichte.

Der darlegungs- und beweisbelastete Kläger habe keinen immateriellen Schaden dargelegt. Der angeblich erlittene Kontrollverlust, auf den er sich berufe, begründe keinen ihr zurechenbaren Schaden. Ebenso wenig genüge der Umstand, dass der Kläger angeblich bestimmte Risiken befürchte.

Der Anspruch des Klägers auf immateriellen Schadensersatz bestehe auch deshalb nicht, weil er nicht dargelegt habe, dass ein Schaden gerade aus den angeblichen Verstößen gegen die DSGVO resultiere. Selbst wenn man einen Verstoß ihrerseits gegen die Vorschriften unterstellte, so fehle es jedenfalls an dem erforderlichen Kausalzusammenhang zwischen einem solchen hypothetischen Rechtsverstoß und einem Schaden des Klägers. Schließlich scheide eine Haftung ihrerseits mangels Verschuldens aus, weil ihr - ein Verstoß gegen die DSGVO unterstellt - diesbezüglich weder Vorsatz noch Fahrlässigkeit zur Last falle.

Der Feststellungsantrag sei ebenfalls unbegründet, da der Kläger nicht dargelegt habe, dass ein zukünftiger Eintritt eines materiellen oder immateriellen Schadens wahrscheinlich sei.

Schließlich stehe dem Kläger auch der mit Klagantrag zu 3) a) und 3) b) geforderte Unterlassungsanspruch nicht zu, da sich aus §§ 1004 analog, 823 Abs. 1, Abs. 2 BGB i.V.m. Art. 6 Abs. 1

DSGVO sowie Art. 17 DSGVO kein derartiger Anspruch ergebe.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie auf die Sitzungsniederschrift vom 10.01.2024 (Bl. 393/398 d. e.A.) Bezug genommen.

Entscheidungsgründe

Die Klage hat lediglich zum Teil Erfolg.

I.

Die Klage ist lediglich teilweise zulässig.

Das Landgericht Ulm ist für die Klage zuständig **[1.]**.

Die Klageanträge Ziff. 1 (Leistungsantrag), Ziff. 2 (Feststellungsantrag), Ziff. 4 (Auskunftsantrag) und Ziff. 5 (vorgerichtliche Rechtsanwaltskosten) sind zulässig gestellt. Klageantrag Ziff. 3 (Unterlassungsantrag) ist teilweise nicht hinreichend bestimmt (Ziff. 3 lit. a)) und teilweise fehlt ihm das erforderliche Rechtsschutzbedürfnis (Ziff. 3 lit b)) **[2.]**.

1.

1.1.

Die von Amts wegen zu prüfende internationale Zuständigkeit ergibt sich ab dem zeitlichen Anwendungsbereich der DSGVO nach Art. 99 Abs. 2 DSGVO (25.05.2018) aus Art. 79 Abs. 2 S. 2 DSGVO, da die Beklagte in Deutschland eine Niederlassung und der Kläger als betroffene Person im Sinne von Art. 4 Nr. 1 DSGVO seinen gewöhnlichen Aufenthalt in Deutschland hat *(vgl. OLG Stuttgart*, Urt. v. 22.11.2023 - 4 U 20/23 -, juris Rn. 253; *OLG Hamm*, Urt. v. 15.08.2023 - I-7 U 19/23 -, juris Rn. 45 m.w.N.; *OLG Dresden,* Urt. v. 05.12.2023 - 4 U 1094/23 -, juris Rn. 23).

Vor dem zeitlichen Anwendungsbereich der DSGVO folgt die internationale Zuständigkeit der deutschen Gerichte aus Art. 7 Nr. 2, Art. 63 Abs. 1 lit a), lit. c), Abs. 2 EuGVVO, da die Beklagte ihren satzungsgemäßen Sitz, jedenfalls ihre Hauptniederlassung in Irland hat, das schädigende Ereignis aus unerlaubter Handlung in Deutschland eingetreten ist und das vorgeworfene Verhalten auch nicht - Vorrang begründend - als Verstoß gegen die vertraglichen Verpflichtungen angesehen werden kann (vgl. *OLG Stuttgart*, a.a.O., Rn. 255 m.w.N.; *OLG Hamm*, a.a.O., Rn. 46 m.w.N.).

Jedenfalls greift Art. 26 Abs. 1 Satz 1 EuGVVO, da sich die Beklagte - entsprechend Ziff. 4.4 der seit April 2018 geltenden Nutzungsbedingungen (Anl. B19) - rügelos eingelassen hat (vgl. *OLG Stuttgart*, a.a.O., Rn. 257 m.w.N.; *OLG Hamm*, a.a.O., Rn. 46 m.w.N.; *OLG Dresden,* a.a.O., Rn. 25).

1.2.

Die örtliche Zuständigkeit des Landgerichts Ulm folgt aus § 44 Abs. 1 S. 2 BDSG. Demnach können Klagen gegen einen Verantwortlichen an dem Ort erhoben werden, an dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Das ist vorliegend im Bezirk des Landgerichts Ulm der Fall, § 7 BGB.

1.3.

Die sachliche Zuständigkeit des Landgerichts Ulm ergibt sich aus § 71 Abs. 1 GVG i.V.m. § 23 Nr. 1 GVG.

2.

Die Klageanträge sind auch im Übrigen mit Ausnahme von Klageantrag Ziff. 3 (Unterlassungsantrag) zulässig.

2.1.

Klageantrag Ziff. 1 (Leistungsantrag), mit welchem der Kläger einen angemessenen immateriellen Schadensersatz fordert, ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Dem steht nicht entgegen, dass er diesen Anspruch auf das kumulative Zusammenwirken mehrerer Verstöße stützt. Entgegen der Ansicht der Beklagten liegt kein Fall von unzulässigen alternativen Klagegründen bzw. Streitgegenständen vor. Denn der Kläger macht vorliegend einen einheitlichen Anspruch (immateriellen Schadensersatz wegen unterschiedlicher Verstöße gegen die DSGVO) geltend, wobei er in der Sache auf das Abgreifen seiner Telefonnummer und die Verknüpfung mit seinen öffentlich zugänglichen Daten abstellt. Die Regelungen in der DSGVO, die dieses Verhalten betreffen, sind insoweit nicht erkennbar unterschiedlich ausgestaltet, sondern betreffen in der Sache jeweils den erforderlichen Schutz der persönlichen Daten des Klägers und regeln die Schutzanforderungen für unterschiedliche Phasen der Datenverarbeitung. Eine Mehrheit von Streitgegenständen kann deshalb nicht angenommen werden und es liegt auch keine verdeckte Teilklage vor (vgl. *OLG Stuttgart*, a.a.O., Rn. 230 ff. m.w.N.; *OLG Hamm*, a.a.O. Rn. 50 ff.; *OLG Dresden,* a.a.O. Rn. 26 f.; *OLG Köln,* Urt. v. 07.12.2023 -, juris Rn. 29 ff.).

2.2.

Klageantrag Ziff. 2, gerichtet auf Feststellung der weitergehenden Ersatzpflicht der Beklagten ist ebenfalls zulässig.

2.2.1.

Zunächst ist der Antrag dahingehend auszulegen, dass er sich auf die Feststellung der Ersatzpflicht der Beklagten hinsichtlich zukünftiger materieller Schäden beschränkt. In dieser Auslegung

ist er auch hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Wie bei einer Leistungsklage muss zur Individualisierung des Anspruchs der Anspruchsgrund bereits im Antrag so konkret benannt werden, dass der Umfang der Rechtshängigkeit und der Rechtskraft feststehen. Bei Ansprüchen auf Schadensersatz ist eine bestimmte Bezeichnung des zum Ersatz verpflichtenden Ereignisses erforderlich. Zur Ermittlung des Klagebegehrens ist nicht allein auf den Antrag selbst abzustellen, sondern auch die Klagebegründung heranzuziehen (vgl. *BGH,* Urt. v. 15.07.2021 - VI ZR 576/19 -, juris Rn. 32 m.w.N.).

Zwar ist die Formulierung des auf Feststellung der Ersatzpflicht für *„künftige (...) Schäden“,* die *„entstanden sind“* gerichteten Klageantrages in sich widersprüchlich, schon, weil sie keine Abgrenzung zu dem mit Ziff. 1 begehrten Ersatz des immateriellen Schadens erkennen lässt. Allerdings ergibt sich aus S. 49 der Replik v. 03.02.2023 (Bl. 216 d. e.A.), dass sich der Antrag ausschließlich auf materielle Schäden bezieht, die dem Kläger aus dem Scraping-Vorfall künftig noch entstehen werden und entstehen können. So verstanden, genügt der Antrag den Anforderungen an die Bestimmtheit (vgl. *OLG Dresden,* a.a.O. Rn. 50).

2.2.2.

Das Erfordernis eines rechtlichen Interesses des Klägers an einer entsprechenden alsbaldigen Feststellung steht der Zulässigkeit des Feststellungantrages entsprechend der vorgenommenen Auslegung nicht entgegen (§ 256 Abs. 1 ZPO).

Für die Zulässigkeit einer Klage, gerichtet auf Feststellung einer Ersatzpflicht bei künftigen Schäden wegen einer Persönlichkeitsverletzung, genügt die bloße Möglichkeit eines durch die Pflichtverletzung verursachten Schadenseintritts, wovon auszugehen ist, wenn bei verständiger Würdigung mit einem Schaden wenigstens zu rechnen ist (vgl. *BGH,* Urt. v. 29.06.2021 - XI ZR 52/18 -, juris Rn. 30 m.w.N.). Diese Rechtsprechung ist auf Ansprüche aus Art. 82 DSGVO zu übertragen (vgl. *OLG Stuttgart*, a.a.O., Rn. 236 m.w.N.). Da der Kläger die Kontrolle über seine Handynummer verloren hat und hierdurch ein weiterer Missbrauch der Nummer ermöglicht ist, besteht die Möglichkeit künftiger materieller Beeinträchtigungen (vgl. *OLG Stuttgart,* a.a.O., Rn. 237; **a.A.** *OLG Dresden*, a.a.O., Rn. 51; *OLG Hamm,* 212 ff.; *OLG Köln*, a.a.O., Rn. 63 ff.).

2.3.

Der auf Unterlassung gerichtete Klageantrag Ziff. 3 ist unzulässig.

2.3.1.

Mit dem Klageantrag Ziff. 3 lit. a) fordert der Kläger von der Beklagten insoweit Unterlassung, als

seine personenbezogenen Daten *„unbefugten Dritten“* über das Contact-Import-Tool (CIT) zugänglich gemacht werden, ohne dass die *„nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“* vorgesehen sind, um die *„Ausnutzung des Systems“* zu verhindern.

Für die Frage der Zulässigkeit des Klageantrages kann die zwischen dem OLG Hamm und dem OLG Stuttgart unterschiedlich beantwortete Frage, ob der Kläger in der Sache ein aktives Tun (so *OLG Hamm,* a.a.O., Rn. 222 ff.) oder ein Unterlassen (so *OLG Stuttgart*, a.a.O., Rn. 244) begehrt, offengelassen werden, da Klageantrag Ziff. 3 lit. a) bereits wegen fehlender hinreichender Bestimmtheit (§ 253 Abs. 2 Nr. 2 ZPO) unzulässig ist.

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, denn die Entscheidung darüber, was der Beklagten verboten ist, würde anderenfalls letztlich dem Vollstreckungsgericht überlassen bleiben. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit als unzulässig anzusehen. Abweichendes kann gelten, wenn der gesetzliche Verbotstatbestand eindeutig und konkret gefasst ist, sein Anwendungsbereich durch eine gefestigte Auslegung geklärt ist oder der Kläger hinreichend deutlich macht, dass er kein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert (vgl. *BGH,* Urt. v. 26.01.2017 - I ZR 207/14 -, juris Rn. 18 m.w.N.).

Der Unterlassungsantrag in der Fassung von Klageantrag Ziff. 3 lit. a) beschränkt sich hinsichtlich der begehrten Unterlassung nicht auf die Wiedergabe des gesetzlichen Verbotstatbestandes (Art. 32 Abs. 1 DSGVO), sondern greift einzelne Elemente hieraus auf. Hierbei bleibt er derart unbestimmt, dass der Antrag praktisch inhaltsleer ist.

Es bleibt unklar, wie etwa geklärt werden soll, wodurch ein *„angemessenes Schutzniveau gewährleistet werden soll“*, was *„nach dem Stand der Technik mögliche Sicherheitsmaßnahmen“* sind, mit denen *„die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern“* ist. Darüber hinaus ist nicht ersichtlich, welche Maßnahmen die Beklagte konkret zur Erfüllung ihrer Pflicht zu ergreifen hat. Ohne eine solche Konkretisierung ist für die Beklagte aber nicht klar, wann sie ihrer Pflicht Genüge getan hat und wann sie sich einer Haftung bzw. einer Vollstreckung aussetzen würde. Schließlich würde aufgrund der unklaren Fassung des Antrags die Frage, welche Maßnahmen zu welchem Zeitpunkt von der Beklagten veranlasst

werden müssten, um *„die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme“* zu verhindern, in unzulässiger Weise in das Vollstreckungsverfahren verlagert, was darauf hinausliefe, dass die Beklagte verpflichtet wäre, jedwede zukünftige Entwicklung vorherzusehen, mit der unbefugte Dritte versuchen könnten, an Daten aus ihrem Netzwerk zu gelangen, wobei andererseits aber *"die Kontaktaufnahme"* auch weiterhin noch ermöglicht werden soll. Damit würde aber letztlich unter Androhung von Ordnungsgeld/Ordnungshaft ein absoluter Schutz gefordert, der tatsächlich nicht geleistet werden kann. Die auslegungsbedürftige Antragsformulierung lässt sich auch durch Auslegung nicht eindeutig präzisieren (vgl. *OLG Dresden*, a.a.O., Rn. 56; *OLG Köln*, a.a.O., Rn. 75 ff.; *OLG Hamm,* a.a.O. Rn. 228 ff.; **a.A.** *OLG Stuttgart*, a.a.O., Rn. 248).

2.3.2.

Mit Klageantrag Ziff. 3 lit. b) fordert der Kläger von der Beklagten die Unterlassung der Verarbeitung seiner Telefonnummer ohne informierte Einwilligung.

Klageantrag Ziff. 3 lit. b) ist ebenfalls unzulässig, ohne dass es darauf ankommt, ob die vom Kläger begehrte Unterlassungsverpflichtung im Hinblick auf die Formulierungen "*unübersichtlich*" und "*unvollständig*" zu unbestimmt ist (verneinend *OLG Stuttgart,* a.a.O., Rn. 250). Denn es fehlt jedenfalls das notwendige Rechtsschutzbedürfnis (vgl. *OLG Hamm*, a.a.O., Rn. 233 ff.; *OLG Köln,* a.a.O., Rn. 79 ff.; *OLG Dresden*, a.a.O. Rn. 64).

Spätestens seit Zugang des Auskunftsschreibens der Beklagten vom 10.01.2022 (Anl. B16) war der Kläger über die Sichtbarkeits- und Suchbarkeitsfunktion informiert oder hätte zumindest von seinen Prozessbevollmächtigten informiert werden müssen. Dann hätte er die Suchbarkeit - soweit dies nicht ohnehin bereits durch die Systemumstellung der Beklagten bzw. durch die Umgestaltung des CIT im September 2019 obsolet geworden sein sollte - umstellen können. Es besteht daher kein Bedürfnis des Klägers für einen entsprechenden Unterlassungstitel. Ein Rechtsschutzbedürfnis für die Geltendmachung eines Unterlassungsanspruchs zugunsten anderer Nutzer besteht ebenfalls nicht (vgl. *OLG Köln*, a.a.O., Rn. 81).

II.

Die Klage ist lediglich hinsichtlich Klageantrag Ziff. 1 (Leistungsantrag) teilweise und hinsichtlich Klageantrag Ziff. 2, gerichtet auf Feststellung der Einstandspflicht der Beklagten für dem Kläger zukünftig entstehende materielle Schäden begründet.

1.

Auf das zwischen den Parteien vor Inkrafttreten der DSGVO geschlossene Vertragsverhältnis ist deutsches Recht anzuwenden.

Ziffer 4 der Nutzungsbedingungen der Beklagten enthält hinsichtlich des anwendbaren Rechts folgende Klausel:

> *„Wenn du ein Verbraucher bist und deinen ständigen Wohnsitz in einem Mitgliedstaat der Europäischen Union hast, gelten die Gesetze dieses Mitgliedstaats für jeglichen Anspruch, Klagegegenstand oder Streitfall, den du uns gegenüber hast und der sich aus diesen Nutzungsbedingungen oder aus den Facebook-Produkten oder im Zusammenhang damit ergibt (“Anspruch“).*
>
> (vgl. Anl. B19).

Gemäß Art. 3 Abs. 1, 6 Abs. 2 der Verordnung (EG) Nr. 593/2008 (Rom I-VO) unterliegt damit das Vertragsverhältnis dem von den Parteien in Ziff. 4 der Nutzungsbedingungen gewählten Recht, nämlich dem Recht des Mitgliedsstaates der Europäischen Union, in welchem der Kläger seinen ständigen Wohnsitz hat, was in Deutschland der Fall ist.

2.

Dem Kläger steht ein Anspruch auf Ersatz immateriellen Schadens in Höhe von 350,00 € gem. § 82 Abs. 1 DSGVO zu (Klageantrag Ziff. 1).

Gem. Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Voraussetzung für das Bestehen eines Schadensersatzanspruchs gem. Art. 82 Abs. 1 DSGVO ist, dass ein Verstoß gegen die DSGVO kausal einen immateriellen Schaden herbeigeführt hat (vgl. *EuGH*, Urt. v. 04.05.2023 - C 300/21 -, juris Rn. 32).

Die DSGVO ist zeitlich, sachlich und räumlich anwendbar **[2.1.].** Von der Beklagten wurden personenbezogene Daten des Klägers unter Verstoß gegen die Bestimmungen der DSGVO verarbeitet **[2.2.]**. Die Beklagte hat sich nicht mit Erfolg exkulpiert (Art. 82 Abs. 3 DSGVO) **[2.3.].** Dem Beklagten ist ein immaterieller Schaden enstanden **[2.4.].**

2.1.

Der sachliche **[2.1.2.]** und räumliche Anwendungsbereich **[2.1.3.]** der DSGVO ist eröffnet, in zeitlicher Hinsicht können Verstöße erst nach deren Inkrafttreten zum 25.05.2018 erfasst werden

[2.1.1.].

2.1.1.

a.

Die DSGVO gilt seit dem 25.05.2018 (Art. 99 Abs. 2 DSGVO) unmittelbar in jedem Mitgliedstaat der europäischen Union (Art. 288 Abs. 2 AEUV; vgl. *BGH,* Urt. v. 27.07.2020 - VI ZR 405/18 -, BGHZ 226, 285 [290 Rn. 12]).

b.

Der Abgriff der Daten des Klägers durch Dritte ist im Jahr 2019 erfolgt.

c.

Vom Kläger behauptete Verstöße der Beklagten im Rahmen des Anmeldeprozesses (Registrierungsprozess und Datenerhebung) fallen vorliegend aus dem Anwendungsbereich der DSGVO heraus, da das Nutzerkonto des Klägers bereits vor dem 25.05.2018 und damit vor dem Inkrafttreten der DSGVO registriert wurde. Der Kläger hat angegeben, er habe sein Facebook-Nutzerkonto bereits im Jahr 2010 eröffnet (vgl. S. 2 der Sitzungsniederschrift v. 10.01.2024, Bl. 394 d. eA.). (vgl. *OLG Stuttgart,* a.a.O. Rn. 360; *OLG Hamm*, a.a.O. Rn. 70).

Dementsprechend kann der Beklagten kein Verstoß gegen Art. 13, 14 DSGVO im Hinblick auf die Datenerhebung beim Kläger im Rahmen des Registrierungsprozesses zur Last gelegt werden. Denn die Informationspflichten aus Art. 13, 14 DSGVO beziehen sich nach dem ausdrücklichen Wortlaut der Norm allein auf den Zeitpunkt der Datenerhebung, die im vorliegenden Streitfall vor dem nach Art. 99 Abs. 2 DSGVO maßgeblichen 25.05.2018 abgeschlossen war (vgl. *OLG Stuttgart*, a.a.O., Rn. 361 m.w.N.; *OLG Hamm*, a.a.O., Rn. 71; *OLG Dresden*, a.a.O., Rn. 32).

Im Fall einer Datenerhebung vor dem 25.05.2018 unterfällt ausschließlich die Weiterverarbeitung der Daten ab dem 25.05.2018 den Anforderungen der DSGVO; denn aus Erwägungsgrund 171 Satz 2 DSGVO, aus Art. 4 Nr. 2 DSGVO und aus Art. 24 Abs. 1, insbesondere Satz 2 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,* a.a.O., Rn. 72 m.w.N.).

In Erwägungsgrund 171 DSGVO ist hierzu in den Sätzen 2 und 3 ausgeführt:

> *„2Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. 3Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, so dass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verord-*

nung fortsetzen kann.“

Die Frage einer hinreichenden Information ist damit (nur) entscheidend für die Frage der Wirksamkeit einer ursprünglich erteilten Einwilligung und deren Fortgeltung über den 25.05.2018 hinaus (vgl. *OLG Hamm*, a.a.O., Rn. 74; *OLG Stuttgart*, a.a.O. Rn. 363).

d.

Ebenso fällt ein etwaiger Verstoß der Beklagten gegen Art. 35 DSGVO nicht in den zeitlichen Anwendungsbereich der DSGVO; denn nach Art. 35 Abs. 1 Satz 1 DSGVO geht es um eine *"vorab"* - also vor dem Beginn des allgemein vorgesehenen und damit nicht vor jedem konkret-individuellen Datenverarbeitungsvorgang - durchzuführende Datenschutz-Folgenabschätzung. Da die hier streitgegenständlichen zum Scraping genutzten Funktionen unstreitig bereits vor der Einführung der DSGVO vorhanden waren, können diese von Art. 35 DSGVO ersichtlich nicht erfasst sein (vgl. *OLG Hamm*, a.a.O. Rn. 75 f.; *OLG Dresden*, a.a.O., Rn. 32; *OLG Stuttgart,* a.a.O., Rn. 364). Jedenfalls kann offenbleiben, ob die Beklagte im Hinblick auf Art. 35 Abs. 11 DSGVO nach der Feststellung der ersten Scraping-Vorfälle zur Erstellung einer Datenschutz-Folgenabschätzung verpflichtet war, weil im Hinblick auf die Verstöße der Beklagten gegen Art. 5 Abs. 1 lit. f, Art. 32 DSGVO und gegen Art. 5 Abs. 1 lit. b, Art. 25 Abs. 1 DSGVO (Einzelheiten hierzu folgen) durch einen etwaigen Verstoß gegen Art. 35 Abs. 11 DSGVO kein zusätzlicher Schaden entstehen oder ein entstandener Schaden vertieft werden konnte (vgl. *OLG Hamm*, a.a.O. Rn. 76).

2.1.2.

Der sachliche Anwendungsbereich der DSGVO ist ebenfalls eröffnet, denn der Betrieb eines sozialen Netzwerks mit der Sammlung und Speicherung von Nutzerdaten (Name, ID., Geschlecht, Telefonnummer etc.), die Vernetzung der Mitglieder und die Beschickung mit individualisierter Werbung ist Verarbeitung und Speicherung von personenbezogenen Daten gemäß Art. 2 Abs. 1 DSGVO (vgl. *EuGH*, Urt. v. 04.07.2023 - C-252/21 -, juris Rn. 27; Urt. v. 05.06.2018 - C-210/16 -, juris Rn. 30; *OLG Stuttgart*, a.a.O. Rn. 367 m.w.N.).

Bei den genannten Daten handelt es sich um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO (*OLG Stuttgart*, a.a.O., Rn. 367 m.w.N.; *OLG Hamm*, a.a.O., Rn. 79).

2.1.3.

Die DSGVO ist schließlich auch räumlich anwendbar, denn die Beklagte ist Verantwortliche der Datenverarbeitung im Sinne von Art. 4 Nr. 7 DSGVO (*EuGH*, Urt. v. 04.07.2023 - C-252/21 -, juris Rn. 30, 44; Urt. v. 05.06.2018 - C-210/16 -, juris Rn. 30) und betreibt für ihre Tätigkeit eine Niederlassung in Irland und damit innerhalb der Union (*OLG Stuttgart,* a.a.O., Rn. 370 m.w.N.; OLG Hamm, a.a.O. Rn.

81 ff.).

2.2.

Der Beklagten fallen verschiedene Verstöße gegen die DSGVO zur Last

2.2.1.

Art. 82 DSGVO erfasst jedweden Verstoß gegen die DSGVO.

Der Anspruch auf Schadenersatz nach Art. 82 Abs. 1 DSGVO setzt nicht voraus, dass eine Schutznorm verletzt wird oder eine rechtswidrige Datenverarbeitung vorliegt, es genügt jede Verletzung materieller oder formeller Bestimmungen der DSGVO (vgl. BeckOK DatenschutzR/*Quaas*, 46. Ed. 1.11.2023, DS-GVO Art. 82 Rn. 14; *OLG Stuttgart*, a.a.O. Rn. 380 m.w.N. mit ausführlicher Begründung).

2.2.2.

Im Rahmen einer auf Art. 82 DSGVO gestützten Schadenersatzklage trägt grundsätzlich der Anspruchsteller die Beweislast für die tatbestandsbegründenden Umstände (vgl. *Quass*, a.a.O. Rn. 16). Dennoch ist nicht der Kläger für den für die Haftung nach Art. 82 DSGVO erforderlichen Verstoß gegen die DSGVO im Zuge der Datenverarbeitung darlegungs- und beweisbelastet, obgleich es sich hierbei um eine anspruchsbegründende Voraussetzung handelt. Denn die DSGVO enthält in Art. 5 Abs. 2 DSGVO eine spezifische Beweislastregelung, wonach der für die Datenverarbeitung Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO enthaltenen Grundsätze der Datenverarbeitung verantwortlich ist und deren Einhaltung nachweisen können muss (*"Rechenschaftspflicht").*

Der für die betreffende Verarbeitung Verantwortliche trägt auch die Beweislast dafür, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 DSGVO geeignet waren (vgl. *EuGH,* Urt. v. 14.12.2023, C-340/21, Celex-Nr. 62021CJ0340 Rn. 57; *OLG Stuttgart*, a.a.O., Rn. 403; *OLG Hamm,* a.a.O. Rn. 85; **a.A.** *OLG Dresden*, a.a.O. Rn. 41 f.).

2.2.3.

Die Beklagte hat gegen die DSGVO verstoßen.

Mit der Belassung der Voreinstellung *"alle"* in der Suchfunktion hat sie gegen Art. 5 Abs. 1 lit. a), b), Art. 6 Abs. 1 Unterabs. 1 DSGVO und Art. 25 Abs. 2 DSGVO verstoßen **[a.]**. Des Weiteren hat sie gegen ihre aus Art. 6 Abs. 1 lit a) i.V.m. Art. 12 DSGVO folgende Pflicht verstoßen, den Kläger bei Inkrafttreten der DSGVO transparent und ausreichend über die zu diesem Zeitpunkt bestehende Suchbarkeitseinstellung zu informieren und hierzu eine erneute wirksame Einwilligung einzu-

holen **[b.]**. Es ist auch von einem Verstoß der Beklagten gegen ihre Pflicht zur Schaffung eines angemessenen Schutzniveaus durch geeignete technische und organisatorische Schutzmaßnahmen unter Berücksichtigung des Standes der Technik (Art. 5 Abs. 1 lit. f.), 32 DSGVO) auszugehen **[c.]**. Ob der Beklagten ein Verstoß gegen Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO zur Last fällt, kann dahinstehen **[d.]**.

a.

Die Beklagte als die für die Datenverarbeitung Verantwortliche hat weder schlüssig dargelegt noch bewiesen, dass ihre streitgegenständliche, zum Scraping-Vorfall beim Kläger führende Verarbeitung entgegen dem klägerischen Vorbringen nicht gegen die in Art. 5 Abs. 1 lit. a), b), Art. 6 Abs. 1 Unterabs. 1 DSGVO, Art. 25 Abs. 1, Abs. 2 DSGVO normierten Grundsätze verstoßen hat.

aa.

In Art. 25 Abs. 1 DSGVO wird der Verantwortliche verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen. Dabei wird die Möglichkeit der Abwägung eröffnet. Die Norm gibt die Möglichkeit, Umstände wie den Stand der Technik, die Implementierungskosten und auch Risiken für die Rechte und Freiheiten natürlicher Personen mit in die Abwägung bei der Wahl der Maßnahmen einzubeziehen.

Durch Art. 25 Abs. 2 DSGVO *(“privacy by default“)* wird der Verantwortliche verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch die Voreinstellung im technischen Verfahren nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind (vgl. BeckOK DatenschutzR/*Paulus* DS-GVO Art. 25 Rn. 8 m.w.N.).

Die Erwägungsgründe zur DSGVO konkretisieren diese Maßnahmen (Erwägungsgrund 78). Danach könnten solche Maßnahmen u.a. darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird und personenbezogene Daten so schnell wie möglich pseudonymisiert werden. Weiter sieht der Erwägungsgrund 78 vor, dass Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird und es der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen. Der Verantwortliche ist danach in der Rolle, Sicherheitsfunktionen zu schaffen und zu verbessern (vgl. *Paulus*, a.a.O., Rn. 11). Es müssen danach die Grundsätze und die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beachtet werden. Ausgerichtet an den Art. 5 und 6 DSGVO sind entsprechende Maßnahmen zu ergreifen (vgl. *Paulus*, a.a.O., Rn. 11a). Die technischen und organisatorischen Maßnahmen, die den Rahmen für die Voreinstellung der Verarbeitung geben, sollen insbesondere

sicherstellen, dass personenbezogene Daten nicht einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (vgl. *Paulus*, a.a.O., Rn. 12).

Die aufgeführte Verpflichtung richtet sich insbesondere an soziale Netzwerke, die für gewöhnlich eine große Einstellungsbandbreite in Bezug auf die Privatsphäre der Nutzer bereithalten. Geschützt werden sollen insbesondere diejenigen Internet-Nutzer, die die technischen Implikationen der Verarbeitungsvorgänge nicht überblicken und sich deshalb nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen. Der Verantwortliche hat die Voreinstellungen und Optionen für die Verarbeitung so auszuwählen, dass nur die Verarbeitung standardmäßig ausgeführt wird, die (unbedingt) erforderlich ist, um den vorgegebenen rechtmäßigen Zweck zu erreichen (vgl. *OLG Dresden*, a.a.O., Rn. 34 m.w.N.).

bb.

Diesen Anforderungen wird die hier gewählte Voreinstellung *"alle"* in der Suchfunktion nicht gerecht, weil damit nicht sichergestellt ist, dass ein Nutzer, der in der Zielgruppenauswahl das von ihm gewünschte Maximum an Privatheit dahingehend umrissen hat, dass er seine Telefonnummer gerade nicht unbegrenzt zur Verfügung stellen will, auch von der Suchbarkeit über diese Telefonnummer ausgeschlossen ist (vgl. *OLG Dresden,* a.a.O.; *OLG Stuttgart*, a.a.O., Rn. 490; *OLG Hamm,* a.a.O., Rn. 127).

Dass eine solche Suchbarkeit gleichwohl regelmäßig dem Wunsch eines Nutzers von sozialen Netzwerken entsprechen und der Nutzer daher Änderungen an dieser Voreinstellung nicht vornehmen wird, kann zumindest bei dieser Nutzergruppe nicht ohne weiteres unterstellt werden (vgl. *OLG Dresden*, a.a.O.).

Eine solche Einstellung ist auch nicht erforderlich, um den vorgegebenen Zweck des sozialen-Netzwerkes und der Suchfunktion zu erreichen. Bereits aus dem Umstand, dass die Beklagte nur hinsichtlich bestimmter personenbezogener Daten vorgab, dass diese *"immer öffentlich",* also zwecks Vernetzung sichtbar und damit suchbar sein müssen, und dem Umstand, dass sie den Nutzern im Rahmen der Zielgruppenauswahl und der Suchbarkeitseinstellungen freistellt, ob und wem die nicht *"immer öffentlichen"* Daten gezeigt werden bzw. ob und wer nach ihnen suchen kann, folgt, dass diese Daten nicht objektiv unerlässlich waren, um eine (hinreichende) Verknüpfung der Nutzer der Beklagten zu ermöglichen (vgl. *OLG Hamm*, a.a.O., Rn. 99).

Die Möglichkeit weitere Nutzer ausfindig zu machen, um sich anschließend mit ihnen *"befreunden"* zu können, war nicht an den Einsatz der Telefonnummer gebunden, sondern es konnte nach einer Vielzahl weiterer Kriterien (Name, Vorname, Wohnort, etc.) gesucht werden. Die Ein-

gabe der Telefonnummer erleichtert zwar bei Namensgleichheit die Zuordnung zu einer Person, ist angesichts dessen für die Nutzbarkeit der Suchfunktion aber nicht in dem Sinne erforderlich, dass hierauf nicht auch verzichtet werden könnte (vgl. *OLG Dresden*, a.a.O.; *OLG Stuttgart,* a.a.O., Rn. 504). Die fehlende Erforderlichkeit ergibt sich auch daraus, dass die Suchbarkeitsfunktion zum 06.06.2019 vollständig deaktiviert worden ist (vgl. *OLG Hamm*, a.a.O., Rn. 110; *OLG Stuttgart*, a.a.O., Rn. 504).

cc.

Ein Verstoß gegen die Pflicht zur Wahl datenschutzfreundlicher Voreinstellungen nach Art. 25 Abs. 2 DSGVO stellt damit zugleich einen Verstoß gegen die in Art. 5 Abs. 1 lit b), c), e) genannten Datenschutzgrundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung dar (vgl. *OLG Dresden*, a.a.O. m.w.N.).

dd.

Da der Kläger am 25.05.2018, also zum Beginn des zeitlichen Geltungsbeginn der DSGVO, bereits registriert war, es aber zuvor entgegen Art. 25 Abs. 2 DSGVO (*"privacy by default"*) die nicht datenschutzfreundliche Grund- / Voreinstellung der Suchbarkeitseinstellung auf *"alle"* gab, musste die Beklagte sicherstellen, dass nicht geänderte unfreundliche Voreinstellungen zum 25.05.2018 unter Abkehr vom *"Opt-Out"*-System geändert wurden (vgl. *OLG Hamm*, a.a.O., Rn. 128; *OLG Dresden,* a.a.O., Rn. 35). Eine solche Änderung hat die Beklagte nicht vorgenommen.

ee.

Das Verhalten der Beklagten ist nicht über Art. 6 Abs. 1 lit. f) DSGVO gerechtfertigt.

Nach Art. 6 Abs. 1 S. 1 lit. f) ist die Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Nach Art. 13 Abs. 1 lit. d) DSGVO obliegt es dem Verantwortlichen, einer betroffenen Person zu dem Zeitpunkt, zu dem personenbezogene Daten bei ihr erhoben werden, die verfolgten berechtigten Interessen mitzuteilen, wenn diese Verarbeitung auf Art. 6 Abs. 1 lit. f) DSGVO beruht (vgl. *EuGH,* Urt. v. 04.07.2023 - C-252/21 -, juris Rn. 107).

Die Voraussetzung der Erforderlichkeit der Datenvereinbarung ist gemeinsam mit dem sog. Grundsatz der *„Datenminimierung“* zu prüfen, der in Art. 5 Abs. 1 lit. c) DSGVO verankert ist und verlangt, dass personenbezogene Daten *„dem Zweck angemessen und erheblich sowie auf*

das für die Zwecke der Verarbeitung notwendige Maß beschränkt“ sind (vgl. *EuGH,* a.a.O., Rn. 109 m.w.N.).

Wie bereits ausgeführt wurde, fehlt es vorliegend jedenfalls an der Erforderlichkeit der Suchbarkeit des Profils des Klägers über dessen Mobiljunktnummer unter Verwendung der Voreinstellung *„alle“.*

b.

Nicht ausgeräumt hat die Beklagte ferner einen Verstoß gegen ihre aus Art. 6 Abs. 1 lit. a) i.V.m. Art. 12 DSGVO folgende Pflicht, den Kläger bei Inkrafttreten der DSGVO transparent und ausreichend über die zu diesem Zeitpunkt bestehende Suchbarkeitseinstellung zu informieren und hierzu eine erneute wirksame Einwilligung einzuholen.

aa.

Nach Art. 6 Abs. 1 S. 1 DSGVO ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn mindestens eine der in Art. 6 Abs. 1 S. 1 unter lit. a) - f) genannte Bedingungen erfüllt ist.

Gem. Art. 6 Abs. 1 S. 1 lit. a) ist die Datenverarbeitung dann rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

bb.

Nach Art. 7 Abs. 1 DSGVO muss der Verantwortliche, wenn die Verarbeitung auf einer Einwilligung beruht, nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Art. 7 Abs. 1 DSGVO enthält eine ausdrückliche Beweislastregel für das Vorliegen einer wirksamen Einwilligung (vgl. *EuGH*, Urt. v. 11.11.2020 - C-61/19 -, juris Rn. 42; BeckOK DatenschutzR/*Stemmer*, 46. Ed. 1.11.2023, DS-GVO Art. 7 Rn. 89).

Art. 6 Abs. 1 lit. a), Art. 7 Abs. 1 DSGVO ist dahin auszulegen, dass es dem für die Verarbeitung von Daten Verantwortlichen obliegt, nachzuweisen, dass die betroffene Person ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten durch aktives Verhalten bekundet hat und, dass sie vorher eine Information über alle Umstände im Zusammenhang mit dieser Verarbeitung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erhalten hat, die sie in die Lage versetzt, die Konsequenzen dieser Einwilligung leicht zu ermitteln, so dass gewährleistet ist, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird (vgl. *EuGH*, a.a.O. Rn. 52).

cc.

Eine wirksame Einwilligung des Klägers im Sinne von Art. 6 Abs. 1 Unterabs. 1 lit. a), Art. 7 DS-GVO in die Suchbarkeit seines Nutzerprofils über die Mobilfunknummer lag nicht vor.

(1) Nach Art. 6 Abs. 1 Unterabs. 1 lit. a) DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn und soweit die betroffene Person ihre Einwilligung für einen oder mehrere bestimmte Zwecke freiwillig in informierter Weise und unmissverständlich im Sinne von Art. 4 Nr. 11 DSGVO erteilt hat (vgl. *EuGH,* Urt. v. 04.07.2023 - C- 252/21 -, juris Rn. 92). Dabei gilt es, auch den Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a) Var. 3 DSGVO zu berücksichtigen. (vgl. *OLG Stuttgart*, a.a.O., Rn. 444; *OLG Hamm*, a.a.O., Rn. 113, jew. m.w.N.).

(2) Eine möglicherweise vom Kläger vor dem 25.05.2018 in die Suchbarkeit seines Profils über die Mobilfunknummer erteilte Einwilligung, konnte unter Geltung der DSGVO nach dem oben (unter Ziff. 3.1.1. lit. c.) zitierten Erwägungsgrund 171 Satz 3 DSGVO keine rechtfertigende Wirkung mehr entfalten. Denn hiernach musste eine vorab erteilte Einwilligung bereits den Bedingungen der DSGVO entsprechen, um fortzugelten (vgl. *OLG Dresden*, a.a.O., Rn. 37; *OLG Hamm,* a.a.O., Rn. 114.)

Seit dem 25.05.2018 erfordert eine wirksame Einwilligung ein aktives Verhalten des Einwilligenden. Entsprechend Erwägungsgrund 32 Satz 3 DSGVO folgt aus Stillschweigen, bereits angekreuzten Kästchen oder Untätigkeit der betroffenen Person keine Einwilligung mehr (vgl. *EuGH,* Urt. v. 11.11.2020 - C-61/19 -, juris Rn. 35 f.; Urt. v. 01.10.2019 - C-673/17 -, juris Rn. 51 ff.). Bei einer Voreinstellung mit einer sog. Abwahlmöglichkeit (Opt-out-Voreinstellung), wie sie in den Nutzungsbedingungen der Beklagten v. 19.04.2018 vorgesehen sind (vgl. Anl. B19) kann damit nicht von einer wirksamen Einwilligung in die Datenverarbeitung ausgegangen werden (vgl. *OLG Stuttgart,* a.a.O., Rn. 446 m.w.N.; *OLG Hamm*, a.a.O. Rn. 116 ff.).

Der Annahme einer wirksamen Einwilligung steht ferner entgegen, dass die Beklagte nicht transparent und ausreichend über die Bedeutung der Suchbarkeitseinstellung informiert und damit gegen das sich aus Art. 5 Abs. 1 lit. a.) DSGVO ergebende Transparenzgebot verstoßen hat.

Nach Art. 5 Abs. 1 lit. a) DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden *(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).*

Art. 5 Abs. 1 lit. a) DSGVO verbindet mehrere Grundsätze, die miteinander in Verbindung stehen:

U. a. fordert die genannte Norm eine Nachvollziehbarkeit der Datenverarbeitung (im Klammerzu-

satz mit Transparenz umschrieben).

Im Erwägungsgrund 39 Satz 4 der DSGVO ist hierzu ausgeführt, dass dieser Grundsatz insbesondere Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen betrifft, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten. Eine Erweiterung und Konkretisierung erfährt der Grundsatz der Transparenz in Art. 13 DSGVO.

Nachvollziehbarkeit und Transparenz bedeutet neben dem in Art. 13 DSGVO normierten Pflichtenkatalog, dass neben der Kenntnis über den Verantwortlichen und die Zwecke der Verarbeitung auch über die Risiken der Verarbeitung zu informieren ist, welche die betroffene Person kennen muss, um die Auswirkungen einer Verarbeitung auf sich einzuschätzen (Erwägungsgrund 39 Satz 5 DSGVO). Dazu gehören auch die Konsequenzen einer Verarbeitung (vgl. *OLG Stuttgart*, a.a.O. Rn. 427 ff. m.w.N.).

Der Kläger hat hinsichtlich eines Verstoßes der Beklagten gegen das Transparenzgebot ausreichend schlüssig vorgetragen.

Die Beklagte hat als die für die Datenverarbeitung Verantwortliche nicht schlüssig dargelegt und nicht bewiesen, dass ihre streitgegenständliche Verarbeitung klägerischer personenbezogener Daten nicht gegen die in Art. 5 Abs. 1 DSGVO normierten Grundsätze verstoßen hat.

Tatsächlich findet sich in den von der Beklagten zum Nachweis einer umfassenden Information vorgelegten Anlagen kein Hinweis darauf, dass bei einer Nutzung des Contact-Import-Tools auch im Falle einer Beschränkung der Telefoneinstellungen die Möglichkeit eines Zugriffs auf das Nutzerkonto gegeben ist. Ebenso wenig geht aus der als Anlage B9 vorgelegten Datenrichtlinie und aus den als Anlage B19 vorgelegten Nutzungsbedingungen ein entsprechender übersichtlicher und leicht verständlicher Hinweis hervor (vgl. *OLG Dresden,* a.a.O., Rn. 38 ff.; *OLG Hamm*, a.a.O., Rn. 114 ff.; *OLG Stuttgart,* a.a.O., Rn. 514 ff.).

Dies folgt zwar noch nicht daraus, dass diese Dokumente im Bestätigungsverfahren vom April 2018 zur Anpassung des Nutzungsvertrages an die DSGVO lediglich über die Registrierungsseite durch Verlinkung zu erreichen waren. Derartige Mehrebenen-Datenschutzhinweise durch Verlinkung sind vielmehr als zulässig anzusehen. Allerdings waren die der Einwilligung zugrundeliegenden Informationen inhaltlich unzureichend, weil sie keinen Hinweis auf die übertragene Suchbarkeitseinstellung, den darin liegenden Verstoß gegen das *"privacy-by default"*-Konzept und die Möglichkeit des Klägers, diesem durch eine Änderung der Datenschutzeinstellung zu begegnen,

enthielten. Erforderlich wäre es gewesen, dem Nutzer zu erläutern, dass die Verwendung des CIT der Messenger-App es anderen Benutzern ermöglicht, mittels Abgleiches von in deren Smartphone gespeicherter Telefonkontakten mit der Mobilfunknummer des Nutzers im Falle eines *„Treffers“* dessen Benutzerprofil als *„Freund“* hinzufügen und auf die entsprechenden Daten zuzugreifen (vgl. *OLG Dresden,* a.a.O., Rn. 38 m.w.N.).

Damit ist objektiv keine ausreichende Information über diese Verarbeitungsmöglichkeit erfolgt. Da zur Verarbeitung auch jede andere Form der Bereitstellung von Daten gehört (Art. 4 Nr. 2 DS-GVO), liegt insoweit eine rechtswidrige Verarbeitung vor (vgl. *OLG Stuttgart*, a.a.O. Rn. 440).

c.

Weiterhin hat die Beklagte nicht dargelegt, dass ihre Datenverarbeitung den Anforderungen der Art. 5 Abs. 1 lit. f, Art. 32 DSGVO entsprach.

aa.

Da eine Datenverarbeitung im Sinne von Art. 4 Nr. 2 DSGVO schon dann vorliegt, wenn ein automatisierter Zugriff auf Daten möglich ist, nach dem Schutzzweck der DSGVO insoweit auch kein willensgesteuertes Verhalten erforderlich ist (unbeabsichtigte Beeinträchtigungen genügen), hat die Beklagte keine ausreichenden Sicherungsmaßnahmen ergriffen. Der Datenschutzverstoß liegt insoweit in der ungeschützten Bereitstellung der Daten (vgl. *OLG Stuttgart,* a.a.O., Rn. 449, 469 f.; OLG *Hamm*, a.a.O., Rn. 132).

bb.

Art. 5 Abs. 1 lit. f) DSGVO fordert, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen *(„Integrität und Vertraulichkeit”).* Der Begriff der Vertraulichkeit zielt auf den Schutz der Daten vor unbefugter Kenntnisnahme und damit unbefugter Verarbeitung. Die Daten sollen vor geplanten Zugriffen und unbeabsichtigten Beeinträchtigungen geschützt werden. Nach Erwägungsgrund 39 Satz 12 DSGVO gehört hierzu, dass unbefugte Personen weder Zugang zu den Daten, noch zu den Geräten haben, mit denen sie verarbeitet werden. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt insbesondere vom Risiko eines unberechtigten Zugriffs und der Art der Verarbeitung ab (vgl. *EuGH*, Urt. v. 08.08.2014 - C-293/12 -, juris Rn. 53 ff.; *OLG Stuttgart*, a.a.O., Rn. 450 m.w.N.).

Art. 32 Abs. 1 DSGVO konkretisiert dahingehend, dass der Verantwortliche unter Berücksichti-

gung 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 hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

cc.

Die im Zeitpunkt des Scraping-Vorfalls bestehenden Maßnahmen waren technisch und organisatorisch ungeeignet im Sinne des Art. 32 Abs. 1 Hs. 1 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, obwohl es in Bezug auf die Kontaktimportfunktionen bei Facebook und im Facebook-Messenger geeignete Maßnahmen gab (vgl. *OLG Hamm*, a.a.O., Rn. 138; *OLG Stuttgart,* a.a.O., Rn. 475).

Durch die eingeräumte Möglichkeit des Hochladens von Telefonnummern für eine Verknüpfung der Kontakte wurden die persönlichen Daten des Klägers (Name, Facebook-ID etc.) für eine Verknüpfung bereitgestellt beziehungsweise zur Verfügung gestellt, weshalb eine Zugriffsmöglichkeit vorhanden war, die nach den Nutzungsbedingungen der Beklagten untersagt ist (*OLG Stuttgart*, a.a.O., Rn. 471; *OLG Hamm*, a.a.O. Rn. 134). Insoweit war kein ausreichender Schutz der persönlichen Daten des Klägers vorhanden.

Die Beklagte hat bei der nach Art. 32 DSGVO vorzunehmenden ex-ante-Betrachtung trotz ihres Beurteilungsspielraums unter Abwägung der widerstreitenden Interessen spätestens ab April 2018 keine geeignete und gebotene Maßnahme gegen das Scraping getroffen (vgl. *OLG Stuttgart*, a.a.O. 473 ff.; *OLG Hamm*, a.a.O., Rn. 141).

Das Gericht schließt sich diesbezüglich den nachfolgend zitierten, umfassenden und überzeugenden Ausführungen des OLG Hamm an (a.a.O., Rn. 139 ff.):

> *„139 [1] Der Senat verkennt insoweit zunächst nicht, dass allein die Tatsache, dass es zum Scraping-Vorfall gekommen ist, kein Beweis dafür ist, dass die Beklagte im Vorfeld ungeeignete Maßnahmen ergriffen hätte (vgl. GA Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, BeckRS 2023, 8707 Rn. 29-37).*
>
> *140 Da Art. 32 DSGVO keine konkreten Vorgaben zu erforderlichen Maßnahmen enthält, ist es vielmehr ersichtlich eine Frage des konkreten und vom Gericht zu bearbeitenden Einzelfalls, ob die vom Verantwortlichen darzulegenden und zu beweisenden Maßnahmen das Risiko einer Datenverletzung Dritter - aus ex-ante-Sicht - hinreichend zu verhindern geeignet waren, wobei dem Verantwortlichen bei der Auswahl und Umsetzung der Maßnahmen ein gewisser subjektiver Beurteilungsspielraum zuzugestehen ist (vgl. GA Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, BeckRS 2023, 8707 Rn. 38-44).*

141 [2] Vorliegend hat die Beklagte bei einer ex-ante-Betrachtung trotz ihres Beurteilungsspielraums unter Abwägung der widerstreitenden Interessen spätestens ab April 2018 keine geeignete und gebotene Maßnahme gegen das Scraping getroffen.

142 Der Begriff "geeignet" setzt voraus, dass die zur Sicherung der Informationssysteme gewählten Maßnahmen sowohl in technischer (Angemessenheit der Maßnahmen) als auch in qualitativer Hinsicht (Wirksamkeit des Schutzes) ein akzeptables Niveau erreichen.

Um die Einhaltung der Grundsätze der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit zu gewährleisten, muss die Verarbeitung nicht nur geeignet sein, sondern auch den Zwecken entsprechen, denen sie dienen soll. Dabei spielt der Grundsatz der Minimierung eine entscheidende Rolle, wonach auf allen Stufen der Datenverarbeitung stets darauf geachtet werden muss, dass Sicherheitsrisiken minimiert werden (GA Pitruzzella Schlussanträge v. 27.4.2023 - C-340/21, BeckRS 2023, 8707 Rn. 20).

143 Es ist weder von der Beklagten dargetan noch sonst ersichtlich, dass trotz ex-ante-Betrachtung wie geboten ab Geltung der DSGVO im Mai 2018 ausreichende Sicherheitsvorkehrungen gegen Scraping getroffen wurden. Konkret durfte die Beklagte, der ein Scraping bereits spätestens im März 2018 aufgefallen war, sich nicht auf die Deaktivierung der Suchfunktion der Plattform im April 2018 beschränken. Es war für sie ohne Weiteres möglich und im Hinblick auf die Datensicherheit ihrer Nutzer geboten sowie zumutbar - auch wenn es ihrem wirtschaftlichen Interesse möglicherweise widersprach -, die Kontaktimportfunktion auf Facebook, im Friend Center und im Facebook-Messenger unverzüglich einzuschränken und somit einen massiven weiteren Datenverlust an Unbefugte zu unterbinden. Es ist nicht ersichtlich oder trotz Hinweises vom 30.06.2023 sowie auf Erörterung im Senatstermin vorgetragen, warum die Deaktivierung der Suchfunktion im April 2018 bereits nach nicht einmal ein bis vier Monaten seit der Kenntniserlangung vom Vorfall erfolgte, die vollständige Deaktivierung der Kontaktimportfunktionen aber noch weitere rund sechzehn Monate dauerte oder warum nicht wenigstens andere weniger einschneidende, aber wirkungsvolle Maßnahmen getroffen wurden.

144 Dass es eine, wenn auch im Vergleich zur "one-to-one"-Zuordnung über das Kontaktimporttool nicht gleicheffektive, Funktion zur Verknüpfung der Nutzer gab, zeigt die aktuelle "People-You-May-Know"-Funktion. Dass eine Umstellung auf diese erst nach und nach trotz erkannten fortgesetzten Scrapinggeschehens erfolgte, lässt sich mit den Vorgaben des Art. 32 DSGVO auch aus ex-ante-Perspektive und unter Berücksichtigung eines Beurteilungsspielraums nicht vereinbaren. Dass die zögerliche Vorgehensweise der Beklagten von der Hoffnung getragen gewesen sein mag, das Scrapen zu erschweren, reicht nicht aus, um das geforderte angemessene Schutzniveau zu erreichen. Dies gilt insbesondere vor dem Hintergrund, dass die Beklagte ihre Standardeinstellung "alle" für die Suchbarkeit über die Telefonnummer nicht - wie geboten - geändert hatte.

145 Soweit die Beklagte vorträgt, sie habe für die Kontaktimportfunktion der Plattform zu einem - im vorliegenden Verfahren trotz Hinweises vom 30.06.2023 sowie auf Erörterung im Senatstermin nicht näher genannten Zeitpunkt (in anderen Verfahren wird Mai 2018 behauptet) - einen nicht näher konkretisierten, auch nicht zum Gegenstand der Entscheidung der DPC vom 28.11.2022 gemachten - "Social Connection Check" eingeführt, war dieser im Hinblick auf die allein vorgesehene Ähn-

lichkeitskontrolle und die danach fortbestehende Notwendigkeit, die streitgegenständliche Kontaktimportfunktion im Rahmen der Plattform - wie schon im April 2018 die Suchfunktion der Plattform - gleichwohl im Oktober 2018 zu eliminieren, evident ungeeignet. Dass dieser Check für den Messenger eingeführt worden wäre, wird zudem schon nicht behauptet.“

Aus den zitierten Ausführungen des OLG Hamm ergibt sich auch ein Verstoß der Beklagten im Rahmen ihrer Datenverarbeitung gegen Art. 5 Abs. 1 lit. b), Art. 25 Abs. 1 DSGVO *("privacy by design")* (vgl. *OLG Hamm*, a.a.O. Rn. 146; *OLG Stuttgart*, a.a.O. Rn. 488).

d.

Ob die Beklagte ihrer Darlegungslast mit Blick auf mögliche weitere Verstöße gegen die DSGVO zeitlich nach dem Scraping-Vorfall und der Veröffentlichung im Darknet nachgekommen ist, kann dahinstehen; denn hinsichtlich der seitens des Klägers gerügten Verstöße gegen die Meldepflicht nach Art. 33 DSGVO sowie die Benachrichtigungspflicht nach Art. 34 DSGVO wurde kein konkreter auf die fehlenden Informationen zurückzuführender Schaden dargelegt noch ist ein solcher sonst ersichtlich (vgl. *OLG Stuttgart,* a.a.O., Rn. 522 ff.)

Dass das Scrapen durch eine rechtzeitige Information noch konkret bezüglich des Klägers hätte verhindert oder die Veröffentlichung des Leak-Datensatzes mitsamt den Daten des Klägers hätte verhindert werden können, ist schon nicht ersichtlich, hätte aber auch allenfalls zum Entfallen des aus Sicht des Klägers erst auf Grund der Veröffentlichung entstandenen Schadens und gerade nicht zu einer Vertiefung oder Begründung desselben geführt (vgl. *OLG Hamm,* a.a.O., Rn. 147 f.).

2.3.

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

Gemäß Art. 82 Abs. 3 DSGVO wird der Verantwortliche von der Haftung nach Art. 82 Abs. 2 DSGVO befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Unabhängig davon, ob man den Begriff der Verantwortlichkeit mit Teilen der Rechtsprechung und der Literatur mit dem Begriff des Verschuldens gleichgesetzt oder Art. 82 DSGVO als Gefährdungshaftungstatbestand versteht (vgl. zum Streitstand: BeckOK DatenschutzR/*Quaas*, 46. Ed. 1.11.2023, DS-GVO Art. 82 Rn. 17 f.) kann sich die Beklagte nicht entlasten.

Die Beklagte kann nicht nachweisen, dass sie kein Verschulden trifft. Das wäre nämlich nur dann der Fall, wenn sie sämtliche Sorgfaltsanforderungen erfüllt hätte und ihr nicht die geringste Fahrlässigkeit vorzuwerfen wäre (Kühling/Buchner/*Bergt*, 4. Aufl. 2024, DS-GVO Art. 82 Rn. 54). Hält der Anspruchsgegner etwa sämtliche erforderlichen Sicherheitsmaßnahmen (Art. 32 DSGVO) ein

und kommt es dennoch zu einem unbefugten Datenzugriff, fehlt es an einem Verschulden. War der Angriffsweg dagegen bekannt oder auch nur erkennbar, ist der Entlastungsbeweis nicht geführt (vgl. *Bergt,* a.a.O.). Da vorliegend die nach Art. 32 DSGVO erforderlichen Sicherheitsmaßnahmen von der Beklagten nicht eingehalten wurden (s.o.), kann die Beklagte nicht nachweisen, dass sie kein Verschulden trifft.

2.4.

Dem Kläger ist ein kausaler immaterieller Schaden entstanden ist, der mit einem angemessenen Schmerzensgeld i. H. v. 350,00 EUR abzugelten ist.

2.4.1.

Die aufgeführten Verstöße der Beklagten gegen die DSGVO sind als kausal für die Schadensverursachung zu betrachten.

Nicht ausdrücklich gesetzlich geregelt ist, wen die Beweislast hinsichtlich der Kausalität des Verstoßes für den Schaden trifft, es ist jedoch von einer Beweislastumkehr zu Lasten des Schädigers auszugehen (vgl. *Bergt,* a.a.O., Art. 82 Rn. 47).

Der Beklagten ist nicht der Beweis dafür gelungen, dass die vom Kläger beschriebenen Spam-Anrufe und Nachrichten nicht erfolgt wären, hätte sie nicht gegen die verschiedenen Vorschriften der DSGVO verstoßen. Für die Kausalität spricht vorliegend vor allem die konkrete Angabe des Klägers, er habe Anrufe erhalten, bei welchen er mit seinem ausschließlich bei Facebook verwendeten Alias-Namen „ “ angesprochen worden sei.

2.4.2.

Nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) verweisen die Worte *„materieller oder immaterieller Schaden“* nicht auf das Recht der Mitgliedstaaten, weshalb sie als autonome Begriffe des Unionsrechts anzusehen und in allen Mitgliedstaaten einheitlich auszulegen sind sowie eine einheitliche unionsrechtliche Definition erhalten müssen (vgl. *EuGH*, Urt. v. 04.05.2023 - C-300/21 - (UI/Österreichische Post AG), DB 2023, 1280 ff.; Rn. 30, 44; ebenso *OLG Stuttgart*, a.a.O., Rn. 274 m.w.N.).

Ein bloßer Verstoß gegen die DSGVO reicht nach der Rechtsprechung des EuGH nicht aus, um einen immateriellen Schadensersatzanspruch zu begründen (vgl. *EuGH*, a.a.O., Rn. 42).

Zum immateriellen Schaden hat der EuGH weiter ausgeführt, dass Art. 82 Abs. 1 DSGVO dahin auszulegen sei, dass er einer nationalen Regelung oder Praxis entgegenstehe, die den Ersatz ei-

nes immateriellen Schadens i.S. dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (vgl. *EuGH*, a.a.O. Rn. 51).

Im Urteil vom 14.12.2023 - C-340/21 - hat der EuGH ferner ausgeführt, dass Art. 82 Abs. 1 DSGVO dahin auszulegen sei, dass allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, ihre personenbezogenen Daten könnten durch Dritte missbräuchlich verwendet werden, einen *„immateriellen Schaden“* im Sinne dieser Bestimmung darstellen könne (Celex-Nr. 62021CJ0340 Rn. 86). Die betroffene Person müsse damit nicht nachweisen, dass Dritte diese Daten vor Erhebung ihrer Schadenersatzklage unrechtmäßig verwendet haben. Das angerufene nationale Gericht müsse jedoch, 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, 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).

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*, Urt. v. 04.05.2023 - C-300/21 -, a.a.O., Rn. 50; Urt. v. 14.12.2023 - C-340/21 -, a.a.O., Rn. 84).

Hinsichtlich des haftungsbegründenden - hier immateriellen - Schadens gilt das strenge Beweismaß des § 286 ZPO, das die volle Überzeugung des Gerichts verlangt (vgl. *OLG Hamm,* a.a.O. Rn. 178 m.w.N.; *OLG Dresden,* a.a.O., Rn. 47; **a.A.** *OLG Karlsruhe*, a.a.O., Rn. 52). Diese erfordert keine absolute oder unumstößliche Gewissheit und auch keine an Sicherheit grenzende Wahrscheinlichkeit, sondern nur einen für das praktische Leben brauchbaren Grad von Gewissheit, der Zweifeln Schweigen gebietet (vgl. *BGH*, Urt. v. 23.6.2020 - VI ZR 435/19 -, juris Rn. 13).

Diese Überzeugung hat das Gericht vorliegend aufgrund der detailreichen und nachvollziehbaren Angaben des Klägers erlangt.

Er hat anlässlich seiner persönlichen Anhörung ausgeführt:

> *„Ich nutze Facebook mittlerweile lediglich noch, um Anträge zu stellen, um mit diesen zu erfahren, welche Daten von mir gespeichert sind.*
>
> *Ich habe Fake-Anrufe und Spam-SMS erhalten. Den Zusammenhang mit Facebook konnte ich herstellen, weil ich in den Anrufen mit meinem bei Facebook genutzten Namen „ “ angesprochen wurde.*

Außerdem habe ich auf einer Webseite eines australischen Sicherheitsforschers festgestellt, dass zwei Datenlecks hinsichtlich meiner persönlichen Daten aufgetaucht sind. Bei dem Datenleck bei Facebook wurde auch meine Telefonnummer angegeben.

Auf Nachfrage, wie viele Fake-Benachrichtungen bzw. -Mitteilungen er in den letzten Jahren erhalten habe: Ich wurde von den Klägervertretern aufgefordert, derartige Benachrichtigungen zu dokumentieren. Daher kann ich sagen, dass ich in den letzten Monaten mehrfach Fake-Anrufe und Spam-SMS erhalten habe. Es handelt sich bei den Anrufen weniger um solche, bei denen man mit dem Anrufer ein Gespräch führt. Meistens erfolgen die Anrufe mit einer unterdrückten Nummer und sind lediglich kurz.

Mich reißen derartige Anrufe aus dem Arbeitsfluss. Ich habe zwischenzeitlich eine App aufgespielt, die mir anzeigt, woher ein Anruf kommt. Anrufe nehme ich nur dann entgegen, wenn mir die App anzeigt, dass sie nicht aus dem Ausland erfolgen. Insgesamt bin ich zwischenzeitlich maximal misstrauisch und stelle daher - wenn überhaupt ein Anrufer am Telefon ist - eine Vielzahl von Fragen.

(...)

In dem Moment, in dem bei mir ein Anruf mit unterdrückter Nummer eingeht, fängt bei mir immer das Gedankenkarussell an. Der Puls geht hoch. Ich überlege, wer dran sein könnte und ob ich möglicherweise einen wichtigen Anruf, z.B. von meinem Bruder, verpasse, der aus beruflichen Gründen auch häufiger mit unterdrückter Nummer anruft. Mein Misstrauen in diesem Zusammenhang geht meinem Umfeld bereits auf die Nerven.

(vgl. S. 3 der Sitzungsniederschrift v. 10.01.2024, Bl. 395 d. e.A.).

Der Kläger stellte die sich aus den Anrufen und seiner Kenntnis, dass persönliche Daten von ihm abhanden gekommen sind, entstandene Verunsicherung und den damit zusammenhängenden Stress überzeugend dar. Der Kläger schilderte seine hierdurch entstandenen Beeinträchtigungen konkret und vermittelte ein individualisiertes und realistisches Bild. Auch seine glaubhaften Angabe, dass er Facebook zwichenzeitlich nur noch sehr eingeschränkt nutze, und der Umstand, dass der Kläger bereits bei der Anmeldung seines Nutzerkontos bei Facebook im Jahr 2010 nicht seinen wahren Namen, sondern einen Alias-Namen verwendet hat, zeigen die besondere Vorsicht des Klägers im Umgang mit sozialen Medien und lassen Rückschlüsse auf seine durch den Scraping-Vorfall entstandenen pschischen Beeinträchtigungen zu, die über bloße Lästigkeiten und Unannehmlichkeiten hinausgehen. Bei den vom Kläger geschilderten Befindlichkeiten handelt es sich nicht nur um negative Gefühle, die Teil des allgemeinen Lebensrisikos und des täglichen Erlebens sind und noch keine Beeinträchtigung des Seelenlebens oder der Lebensqualität darstellen (vgl. *OLG Stuttgart* a.a.O., Rn. 146), sondern um ein immer wieder auftretendes Unwohlsein infolge der Belästigungen insbesondere durch Anrufe mit unterdrückter Nummer oder aus dem Ausland und des unkontrollierbaren Datenverlusts.

Der Kläger hat daher einen tatsächlichen immateriellen Schaden erlitten.

Aufgrund der mehrfachen Verstöße der Beklagten gegen die DSGVO, dem sehr weitgehenden Kontrollverlust der personenbezogenen Daten des Klägers, sowie den hieraus resultierenden Beeinträchtigungen des Klägers auch während seiner beruflichen Tätigkeit im Homeoffice, hält das Gericht ein Schmerzensgeld in Höhe von 350,00 € für angemessen, aber auch für ausreichend.

Der Schmerzensgeldbetrag ist gem. §§ 291, 288 Abs. 1 BGB in Höhe von 5 Prozentpunkten über dem Basiszinssatz ab 20.09.2022 zu verzinsen.

3.

Auch der mit Klageantrag Ziff. 2 geltend gemachte Anspruch auf Feststellung der Schadensersatzpflicht der Beklagten hinsichtlich künftig entstehender materieller Schäden des Klägers ist begründet.

Es besteht vorliegend die Möglichkeit, dass mit einer weiteren Verbreitung der Mobilfunknummer des Klägers weitere materielle Beeinträchtigungen beim Kläger eintreten können. Es wird insoweit auf die nachfolgenden Ausführungen des OLG Stuttgart Bezug genommen, denen sich das Gericht anschließt (vgl. a.a.O., Rn. 552 ff.):

> *„552 a. Hinsichtlich der Frage einer Ersatzpflicht für künftige Schäden können die Grundsätze der höchstrichterlichen Rechtsprechung für Feststellungsanträge nach einem Gesundheitsschaden übertragen werden.*
>
> *553 Der Anspruch auf Feststellung beim Schmerzensgeld als immaterieller Schaden ist begründet, bei einer nicht eben entfernt liegenden Möglichkeit künftiger Verwirklichung der Schadensersatzpflicht durch das Auftreten weiterer, bisher noch nicht voraussehbarer und erkennbarer Leiden oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung des Krankheitsverlaufs. Das trifft bei schweren Unfallverletzungen in aller Regel zu, es sei denn, es besteht überhaupt kein Grund, mit Spätschäden zu rechnen (BGH NJW-RR 1989, 1367 = VersR 1989, 1055; BGH NJW 1972, 198; BGH MDR 1974, 825 [826]; BGHZ 4, 133 [135]; RGZ 61, 164 [171]). Die Feststellungsklage ist bei noch nicht voraussehbaren und erkennbaren weiteren Beeinträchtigungen oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung begründet.*
>
> *554 b. Das ist der Fall, denn es besteht die evidente Möglichkeit, dass mit einer weiteren Verbreitung der Telefonnummer weitere materielle oder immaterielle Beeinträchtigungen beim Kläger eintreten können (a.A. OLG Hamm GRUR-RS 2023, 22505 Rn. 189 – 202, das allerdings bereits ein Feststellungsinteresse verneint hat).“*

4.

Der mit Klageantrag Ziff. 3 geltend gemachte - bereits unzulässige (vgl. Ausführungen unter Ziff. II.

2.3.) Unterlassungsanspruch steht dem Kläger auch in der Sache nicht zu.

Der Anspruch kann weder aus Art. 17 DSGVO noch aus einer Anspruchsgrundlage des nationalen Rechts (§§ 823, 1004 BGB) hergeleitet werden.

4.1.

In Rechtsprechung und Literatur ist umstritten, ob und inwieweit bei einem Verstoß gegen die DSGVO Unterlassungsansprüche bestehen können und woran diese anknüpfen. Hinsichtlich der hierzu vertretenen Auffassungen wird auf die ausführliche Darstellung im Urteil des OLG Stuttgart vom 22.11.2023 - 4 U 20/23 - verwiesen (vgl. juris Rn. 558 ff.).

Das Gericht folgt der u.a. vom Bundesgerichtshof und dem OLG Stuttgart vertretenen differenzierenden Ansicht, wonach aus Art. 17 DSGVO zwar ein Anspruch auf Unterlassung der Speicherung von Daten hergeleitet werden kann, nicht hingegen ein Anspruch auf Unterlassung einer Übermittlung, und Schadensersatzansprüche und Unterlassungsansprüche des nationalen Rechts – soweit diese auf Verstöße gegen Regeln zur Verarbeitung personenbezogener Daten und anderer Regelungen der DSGVO gestützt sind – keine Anwendung finden, weil die Vorschriften der DSGVO eine abschließende, weil voll harmonisierende europäische Regelung bilden (vgl. *BGH,* Urt. v. 13.12.2022 - VI ZR 60/21 -, juris Rn. 13; Urt. v. 12.10.2021 - VI ZR 489/19 -, juris Rn. 10; Urt. v. 27.07.2020 - VI ZR 405/18 -, juris Rn. 20, 23; *OLG Stuttgart*, a.a.O., Rn. 559 f., 562 f.; *OLG Frankfurt*, Urt. v. 30.03.2023 - 16 U 22/22 -, juris Rn. 50 ff. mit ausführlicher Begründung).

4.2.

Dem Kläger geht es mit dem geltend gemachten Unterlassungsanspruch in der Sache nicht um die Unterlassung einer (erneuten) Speicherung, sondern der Unterlassungsanspruch zielt unmittelbar darauf ab, dass die Beklagte nach dem Stand der Technik bestimmte Sicherheitsmaßnahmen vorzusehen hat, damit die Telefonnummer bei bestimmten Voreinstellungen nicht zugänglich gemacht wird. Gefordert wird also neben der Unterlassung auch ein bestimmtes Verhalten der Beklagten. Unabhängig davon, ob damit nicht verdeckt eine (nicht näher bestimmte) Leistung verlangt wird, zielt der Antrag auf Unterlassung bestimmter Datenverarbeitungsvorgänge und ist daher nicht mehr vom Schutzumfang des Art. 17 DSGVO erfasst, da es nicht um die Unterlassung einer erneuten Speicherung geht.

Da Art. 17 DSGVO lediglich ein Löschungsrecht bezüglich personenbezogener Daten einräumt, jedoch gerade keine weitergehenden Rechte bezüglich der Datenverarbeitungsvorgänge an sich normiert worden sind, können keine Unterlassungsansprüche geltend gemacht werden, die im Ergebnis die Verarbeitungsvorgänge des Verantwortlichen reglementieren können (vgl. *OLG Stutt-*

gart, a.a.O., Rn. 576).

5.

Auch der mit Klageantrag Ziff. 4 geltend gemachte Auskunftsanspruch ist nicht begründet.

5.1.

Ausweislich seiner Ausführungen in der Replik vom 03.02.2023 (S. 67, Bl. 234 d. e.A.) fordert der Kläger mit Klageantrag Ziff. 4 keine allgemeine/umfassende Auskunft über seine bei der Beklagten gespeicherten personenbezogenen Daten, sondern darüber, welche Daten welche konkreten Empfänger durch Srcaping oder durch Anwendung des Kontaktimporttools erlangen konnten.

Art. 15 Abs. 1 lit. c) DSGVO gibt der betroffenen Person einen Anspruch, vom Verantwortlichen eine Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf Informationen über die Empfänger oder Kategorien von Empfängern, gegenüber denen diese personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (vgl. *EuGH*, Urt. v. 12.01.2023 - C-154/21 -, juris Rn. 30).

Nach der genannten Entscheidung des EuGH ist Art. 15 Abs. 1 lit. c) DSGVO dahin auszulegen, dass das in dieser Bestimmung vorgesehene Recht der betroffenen Person auf Auskunft über die sie betreffenden personenbezogenen Daten bedingt, dass der Verantwortliche, wenn diese Daten gegenüber Empfängern offengelegt worden sind oder noch offengelegt werden, verpflichtet ist, der betroffenen Person die Identität der Empfänger mitzuteilen, es sei denn, dass es nicht möglich ist, die Empfänger zu identifizieren, oder dass der Verantwortliche nachweist, dass die Anträge auf Auskunft der betroffenen Person offenkundig unbegründet oder exzessiv im Sinne von Art. 12 Abs. 5 DSGVO sind; in diesem Fall kann der Verantwortliche der betroffenen Person lediglich die Kategorien der betreffenden Empfänger mitteilen (vgl. juris Rn. 51).

5.2.

Wie bereits zu Art. 32 DSGVO ausgeführt wurde, hat die Beklagte durch die automatisierte Verarbeitung der Such- und Kontaktimportfunktionsabfragen die Daten des Klägers, insbesondere dessen Mobilfunktelefonnummer offengelegt (Art. 4 Nr. 2 DSGVO), so dass sie gemäß Art. 15 Abs. 1 Hs. 2 lit. c DSGVO grundsätzlich zur gewünschten Auskunft verpflichtet war.

5.3.

Die Beklagte hat den Auskunftsanspruch des Klägers indes mit Schreiben vom 14.04.2022 (Anl. B16) erfüllt.

Erfüllt im Sinne von § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist allein 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 (vgl. *BGH*, Urt. v. 15.06.2021 - VI ZR 576/19 -, juris Rn. 19 f.)

Nach diesen Maßstäben ist vorliegend von einer Erfüllung des klägerischen datenschutzrechtlichen Auskunftsanspruchs auszugehen.

Mit Schreiben vom 14.04.2022 (Anl. B16) haben die Beklagtenvertreter den Vorfall und die (vermutete) Ursache des Abrufs von persönlichen Daten des Klägers erläutert und einen Link zur einer Internetseite der Beklagten mitgeteilt, auf der die über einen individuellen Nutzer gespeicherten Daten eingesehen werden können.

Die Auskunftserteilung mittels Fernzugriffs auf ein elektronisches Auskunftssystem des Datenverantwortlichen genügt den an die Auskunftserteilung zu stellenden formellen Anforderungen (vgl. *OLG Dresden,* a.a.O., Rn. 65 m.w.N.).

Ferner hat die Beklagte hinreichend deutlich gemacht, dass sie keine weiteren Auskünfte zur Identität der Scraper und zum genauen, den Kläger betreffenden Scraping-Zeitpunkt machen könne (vgl. Anl. B16; S. 87/88 der Klageerwiderung, Bl. 158/159 d. e.A.).

5.4.

Soweit der Kläger 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 seinem Anspruch § 275 Abs. 1 BGB entgegen (vgl. *OLG Köln*, a.a.O., Rn. 85; *OLG Dresden*, a.a.O., Rn. 66; *OLG Stuttgart*, a.a.O. Rn. 585).

Die Voraussetzungen einer Unmöglichkeit und des deshalb bestehenden Leistungsverweigerungsrechts sind von dem Schuldner darzulegen und zu beweisen, der das Recht zur Leistungsverweigerung in Anspruch nimmt (vgl. *BGH*, Urt. v. 21.05.2010 – V ZR 244/09 –, juris Rn. 9; *OLG Stuttgart,* a.a.O., Rn. 581).

Die Beklagte hat sich bzgl. der Empfänger darauf berufen, dass ihr diese nicht bekannt seien. Dieser Vortrag wurde von der Klägerseite nur insoweit bestritten, als auf den Beklagtenvortrag hingewiesen wurde, die Beklagte gehe gegen Scraper per Unterlassungsverfügung vor. Hieraus lässt sich indes nicht schließen, dass der Beklagten technische und organisatorische Maßnahmen zur Verfügung standen, um die Dritten, welche persönliche Daten des Klägers abgegriffen haben, zu ermitteln.

6.

Dem Kläger steht schließlich - unabhängig von der Aktivlegitimation (§ 86 VVG) kein Anspruch auf Erstattung vorgerichtlich entstandener Rechtsanwaltskosten zu.

Grundsätzlich können die Rechtsverfolgungskosten als Teil des nach Art. 82 DSGVO zu ersetzenden Schadens angesehen werden (vgl. *OLG Stuttgart,* a.a.O., Rn. 592; *OLG Köln*, a.a.O., Rn. 92), so dass es für die Erstattungsfähigkeit nicht darauf ankommt ob die Beklagte sich im Zeitpunkt der Beauftragung der Klägervertreter in Verzug befand.

Die Ersatzfähigkeit vorgerichtlicher Rechtsanwaltskosten setzt u.a. voraus, dass die vom Kläger mit Klageantrag Ziff. 5 geltend gemachte Gebühr Nr. 2300 VV RVG entstanden ist, was wiederum von Art und Umfang des im Einzelfall erteilten Mandats abhängt (vgl. *BGH,* Urt. v. 24.02.2022 – VII ZR 320/21 –, juris.Rn. 23).

Erteilt der Mandant den unbedingten Auftrag, im gerichtlichen Verfahren tätig zu werden (vgl. Vorbemerkung 3 Abs. 1 Satz 1 VV RVG), lösen bereits Vorbereitungshandlungen die Gebühren für das gerichtliche Verfahren aus, und zwar auch dann, wenn der Anwalt zunächst nur außergerichtlich tätig wird. Für das Entstehen der Geschäftsgebühr nach Nr. 2300 VV RVG ist dann kein Raum mehr. Anders liegt es, wenn sich der Auftrag nur auf die außergerichtliche Tätigkeit des Anwalts beschränkt oder der Prozessauftrag jedenfalls unter der aufschiebenden Bedingung erteilt wird, dass zunächst vorzunehmende außergerichtliche Einigungsversuche erfolglos bleiben. Ein lediglich (aufschiebend) bedingt für den Fall des Scheiterns des vorgerichtlichen Mandats erteilter Prozessauftrag steht der Gebühr aus Nr. 2300 VV RVG nicht entgegen (vgl. *BGH,* a.a.O., Rn. 24 m.w.N.).

Der Kläger hat hinsichtlich seines Anspruchs auf Erstattung vorgerichtlich entstandener Rechtsanwaltskosten lediglich auf die E-Mail seiner Prozessbevollmächtigten vom 14.12.2021 Bezug genommen (Anl. K1), mit welcher u.a. ein entsprechender Anspruch geltend gemacht wurde. Er hat indes inhaltlich keinen weitergehenden Vortrag zu den Anspruchsvoraussetzungen gehalten.

Die vom Kläger mit Anlage K1 vorgelegte, von ihm am 03.03.2022 unterzeichnete Vollmacht, erstreckt sich nicht nur auf die in Ziff. 1 aufgeführte

> *„Außergerichtlicher Vertretung, Geltendmachung von Ansprüchen gegen Schädiger, Fahrzeughalter und deren Versicherer und Akteneinsicht.“,*

sondern auch auf die in Ziff. 5 aufgeführte

> *„Prozessführung (u. a. nach §§ 81 ff. ZPO).“*

Mangels anderweitigen klägerischen Sachvortrages ist daher davon auszugehen, dass das Mandat der Klägervertreter vom Kläger unbedingt und umfassend erteilt war und die E-Mail vom 18.03.2022 als zur Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 Satz 2 Nr. 1 RVG zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 RVG VV abgegolten ist (vgl. *OLG Stuttgart*, a.a.O. Rn. 604).

Ein Hinweis hierauf war gem. § 139 Abs. 2 S. 1 ZPO entbehrlich, da nur eine Nebenforderung betroffen ist.

III.

Die Kostenentscheidung beruht auf § 92 Abs. 1 Satz 1 ZPO.

Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 708, 709, 711 ZPO.

Rechtsbehelfsbelehrung:

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

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

Landgericht Ulm
Olgastraße 106
89073 Ulm

einzulegen.

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

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

Rechtsbehelfe können auch als elektronisches Dokument eingelegt werden. Eine Einlegung per E-Mail ist nicht zulässig. Wie Sie bei Gericht elektronisch einreichen können, wird auf www.ejustice-bw.de beschrieben.

Schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zu Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

Vorsitzende Richterin am Landgericht