I.

10 O 11/23

Landgericht Düsseldorf

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

Klägers,

Prozessbevollmächtigte: Rechtsanwälte Wilde Beuger Solmecke,
Kaiser-Wilhelm-Ring 27-29, 50672 Köln,

gegen

die Meta Platforms Ireland Ltd., vertreten durch den Geschäftsführer (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

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

hat die 10. Zivilkammer des Landgerichts Düsseldorf
auf die mündliche Verhandlung vom 15.01.2024
durch die Richterin als Einzelrichterin

für Recht erkannt:

Die Beklagte wird verurteilt, an den Kläger einen Betrag in Höhe von 300,00 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 13.04.2023 sowie außergerichtliche Anwaltskosten in Höhe von 90,96 EUR nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 13.04.2023 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Rechtsstreits trägt der Kläger.

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

Tatbestand:

Die Parteien streiten über Ansprüche im Zusammenhang mit Datenschutzrecht und Persönlichkeitsrechtsverletzungen vor dem Hintergrund eines Vorfalls, der zur Veröffentlichung von Daten von Nutzern, die diese auf der von den Beklagten betriebenen sozialen Plattform „Facebook“ eingestellt hatten, im Darknet durch dritte Täter im Frühjahr 2021 führte.

Der Kläger war Nutzer der Plattform Facebook. Er unterhielt auf dieser insgesamt zwei Profile, nämlich einerseits ein unter der E-Mail-Adresse
errichtetes Profil, andererseits ein unter Verwendung der E-Mail-Adresse
errichtetes Profil mit der Nutzer-ID
Erstmals registrierte der Kläger sich im Jahr 2008. Ein Versuch im Jahr 2013 sein Nutzerprofil zu löschen scheiterte.

Zwischenzeitlich änderten sich die Nutzungsbedingungen der Beklagten zum 19.04.2018, 31. Juli 2019 und 20.12.2020 geringfügig. Informationen zur Datenerhebung und Verarbeitung erteilte die Beklagte in dem gesonderten Dokument der Datenrichtlinie, die Verwendung von Cookies wurde den Nutzern in dem dritten Dokument der Cookie-Richtlinie erläutert.

Die Einstellung zur Sichtbarkeit der vom Kläger auf der Webseite eingefügten Informationen, ferner zur Privatsphäre generell und zur Sicherheit der Daten waren im Zeitraum der streitgegenständlichen Vorgänge von der Startseite aus abrufbar über den Reiter „Privatsphäre auf einen Blick“. Hierüber gelangte ein Nutzer auf die Einstellungsübersicht mit Haupt- und Unterkategorien wie auf dem auf Seite 10 der Klageschrift eingefügten Screenshot ersichtlich (Bl. 11 d.A.). Die Unterkategorie „Privatsphäre-Check“ ist auch über einen direkten Link von der Startseite aus zu erreichen und führt zu einem Einstellungsmenü, in dem bei einer tabellarischen Auflistung, wie auf dem weiteren Screenshot (s. 12 der Klageschrift, Bl. 13 d.A.) ersichtlich, zu der Fragestellung “Wer kann dich anhand der angegebenen Telefonnummer finden“ entweder „Alle“, „Freunde von Freunden“, „Freunde“ oder „nur ich“ angewählt werden kann.

Durch Eingabe einer Telefonnummer im Suchfeld der Plattform konnte durch Dritte ein Nutzungsprofil ausfindig gemacht werden, auch, wenn der Nutzer hinsichtlich seiner Telefonnummer nicht die Einstellung „öffentlich“ gewählt hatte. Die Plattform der Beklagten verfügte zudem über eine sogenannte Kontaktimportfunktion (engl. „Contact import tool“, im Folgenden auch als „KIF“ und „CIT“ bezeichnet). Nutzer konnten hiermit, sofern sie ihre Kontakte auf die Plattform und auch von ihren Mobilgeräten in den sogenannten Messenger von Facebook hochgeladen hatten, die Facebook-Profile derjenigen Kontakte, die ebenfalls auf der Facebook-Plattform registriert waren, finden und mit ihnen in Verbindung zu treten.

Das galt jedenfalls, soweit die entsprechenden Kontakte ihre Einstellungen nicht aktiv dahingehend angepasst hatten, dass eine Auffindbarkeit des zu ihrer Telefonnummer zugehörigen Nutzerprofils nicht mehr möglich war. Um eine Suchbarkeit über die Suchfunktion auf der Plattform und über die Kontaktimportfunktionen auszuschließen oder einzuschränken, war es erforderlich, die Einstellung auf „Freunde“ oder auch „Freunde von Freunden“ sowie seit Mai 2019 auch auf „nur ich“ umzustellen. Die

standardmäßige Voreinstellung für die Suchbarkeit über die Suchfenstereingabe oder das CIT war die Einstellung „alle“ / „everyone“.

Für die Dauer der streitgegenständlichen Vorgänge, auf die sich das Schadensersatzverlangen bezieht, waren jedenfalls die Angaben des Klägers seines Namens sowie seines Geschlechts, die aufgrund der Gestaltungsweise der Plattform Facebook stets öffentlich angezeigt werden, für jedermann sichtbar. Ebenso war die Suchbarkeit über die Telefonnummer durch einen jeden („alle“) entsprechend der Voreinstellung eingestellt. Hinsichtlich des Informationspunktes der Telefonnummer selbst waren die Einstellung so gewählt, dass weder Freunde, noch die Öffentlichkeit diese auf dem Profil einsehen konnten.

Im Januar 2018 bis September 2019 kam es auf der Plattform Facebook zu einem Datenscraping in erheblichem Umfang. Dabei bezeichnet der Begriff des „Scrapings“ das Auslesen und Sammeln von Daten durch Dritte in großer Zahl über Computerprogramme (Bots/ Scrapring-Tools). Betroffen waren zunächst öffentliche Nutzerdaten.

Darüber hinaus machten sich die Täter die Telefonnummersuchfunktionen sowie das CIT zunutze, um die Angabe der Telefonnummer mit den öffentlichen Daten eines Nutzerprofils in Verbindung zu bringen und hieraus Datensätze zusammenzustellen. Konkret verwendeten die Täter den Mechanismus der Telefonnummeraufzählung. Die Täter registrierten sich (unter Vorgabe fremder oder nicht existenter Identitäten) bei der Beklagten als Nutzer und generierten unter Verwendung der gängigen Rufnummernformate fiktive Telefonnummern und suchten über die Suchfunktionen nach passenden Nutzern. Wurde eine Telefonnummer einem Nutzer zugeordnet („one-to-one“), wurden dessen öffentliche Nutzerinformationen zugeordnet und abgerufen. Die Kontaktimportfunktionen machten sich Dritte zunutze, um unter Einhaltung seitens der Beklagten eingeführter Übertragungsbeschränkungen durch Telefonnummernaufzählung generierte Telefonnummern als ihre vermeintlichen Kontakte hochzuladen, die passenden individuell angezeigten Nutzer allein aufgrund dieser Telefonnummern zu identifizieren („one-to-one“) und ihnen ihre öffentlichen Nutzerinformationen zuzuordnen.

Die so erlangten Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern wurden Anfang April 2021 von den unbekannten Dritten im Internet, hier im Darknet

auf einer Hacker-Plattform, veröffentlicht. Auch der Kläger war bezüglich eines seiner Profile, nämlich hinsichtlich des unter der Nutzer ID und unter Verwendung der E-Mail-Adresse errichteten Nutzerkontos, hiervon betroffen. Es wurden die aus dem Facebook-Profil entnommenen Angaben des Namens, Nutzer ID, Geschlechts und die über die Telefonnummeraufzählung erlangte Telefonnummer, ferner das Land des Klägers als gemeinsamer Datensatz veröffentlicht.

Die Beklagte informierte von dem Vorgang weder den Kläger noch die „Irish Data Protection Commission“ als Datenschutzbehörde am Sitz der Beklagten.

Mit vorgerichtlichem Schreiben vom 11.06.2021 forderte der Kläger die Beklagte durch anwaltliches Schreiben zur Auskunft und zur Zahlung von 500 EUR Schadensersatz auf. Zur Begründung verwiesen die Rechtsanwälte des Klägers darauf, es seien von dem vom Kläger unter Verwendung der E-Mail-Adresse genutzten Facebook-Profil Daten entnommen worden, die Gegenstand einer Veröffentlichung im April 2021 gewesen seien.

Die Beklagte wies das Schadensersatzverlangen zurück mit Schreiben vom 9. September 2021. Hierin führte sie aus, dass eine Betroffenheit des Klägers bezüglich des unter der E-Mail-Adresse eröffneten Accounts von einem Datenschutzvorfall nicht zu erkennen sei und insbesondere Daten des Klägers aus diesem Profil nicht unter den im April 2021 veröffentlichten Datensätzen aufzufinden seien (s. Kopie des Schreibens der Beklagten vom 09. September 2021, s. Anlage B 15, Bl. 48 ff. Anl. KV)

Der Kläger behauptet, seit dem Facebook Datenleck und der nachfolgenden Datenveröffentlichung durch Dritte Spam-Anrufe und SMS-Nachrichten erhalten zu haben. Die Zahl derselben sei im Nachgang zu dem Vorfall vom April 2021 rapide angestiegen und sei derart auffallend gewesen, dass er Recherchen zu möglichen Ursachen für den ihm unerklärlichen Vorgang angestellt habe. Er habe einen Kontrollverlust über seine Daten erlitten und sei durch lästige Spam-Anrufe und Nachrichten nicht nur gestört, sondern auch in seiner Erreichbarkeit eingeschränkt gewesen mit schwerwiegenden Folgen. So sei er während der zwei „Wellen“ vermehrter Kontaktaufnahmen im Schlaf gestört worden bzw. habe, um diese Störungen abzuschalten, schließlich nachts sein Handy auf lautlos stellen müssen

und nicht mehr erreicht werden können. Auf Kontaktversuche Angehöriger, die ihn über eine Notfalloperation seines Vaters hätten in Kenntnis setzten wollen, habe er nicht reagiert, da er angenommen habe, es handele sich erneut um Spamanrufe. Hierdurch sei ihm mittelbar aufgrund des Datenschutzvorfalls die Möglichkeit genommen worden, sich von seinem anschließend verstorbenen Vater zu verabschieden. Dies sei ihm später, im Rahmen einer zweiten „Belästigungswelle“ hinsichtlich eines weiteren Familienmitglieds ähnlich passiert.

Der Kläger behauptet, bei ihm sein ein immaterieller Schaden eingetreten, er habe unter anderem einen Kontrollverlust erlitten. Ferner habe er unter den vorgenannten Umständen gelitten, insbesondere in Bezug auf die fehlende Verabschiedung von seinem Vater.

Über die unstreitig aus seinem Profil entnommenen Daten hinaus sei auch eine Berufsbezeichnung , der Beziehungsstatus sein Geschlecht sowie die vom Kläger nicht näher erläuterten Angaben von Dritten aus seinem Profil ausgelesen und veröffentlicht worden. Die unstreitig betroffene Facebook-ID sei, anders als von der Beklagten behauptet, nicht verpflichtend öffentlich auf dem Profil eingestellt gewesen und sei auch bei dem Kläger verdeckt gewesen.

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 627,13 € € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, sie habe gegen Scraping umfangreiche Sicherungsmaßnahmen getroffen, insbesondere, aber nicht ausschließlich, auch über Captcha-Abfragen.

Sie rügt im Übrigen die unzureichende Substantiiertheit und fehlende Individualisierung eines immateriellen Schadens des Klägers, den sie bestreitet.

Die Klage ist der Beklagten jedenfalls spätestens am 12.04.2023 zugestellt worden ausweislich der Vertretungsanzeige vom selben Tag.

Hinsichtlich des weiteren Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 15.01.2024 (Bl. 452 ff. d.A.) verwiesen.

Entscheidungsgründe:

Die überwiegend zulässige Klage ist in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Die Klage ist weitgehend zulässig.

1.

Das Landgericht ist sachlich und örtlich zuständig gem. § 39 ZPO, Art. 79 Abs. 2 S. 1 DSGVO. Aus Art. 79 Abs. 2 S. 1 DSGVO folgt vorliegend auch die internationale Zuständigkeit deutscher Gerichte.

2.

Der Leistungsanträge zu Ziffer 1.) sowie der Unterlassungsantrag zu Ziffer 3.) a. sind hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

Es liegt keine unzulässige alternative Klagehäufung vor. Das Vorbringen des Klägers zu unterschiedlichen datenschutzrechtlichen Normen, auf die der Antrag zu 1.) gestützt wird, führt nicht zu dem Vorliegen unterschiedlicher Streitgegenstände im Sinne des prozessualen zweigliedrigen Streitgegenstandsbegriffs. Das Stützen eines Klagebegehrens auf mehrere rechtliche Grundlagen beseitigt die Einheitlichkeit nicht. Hierdurch wird weder zwangsläufig ein neuer Grund noch Antrag eingebracht, aus denen sich der Streitgegenstand zusammensetzt. Der Antrag ist hier einheitlich die Zahlung eines bestimmten Betrages. Dieser ist auf denselben Grund, also einen einheitlichen tatsächlichen Lebenssachverhalt, gestützt. Der Kläger verlangt Ersatz für das immaterielle, psychische Leid, welches durch den Daten-Leak unter Zuordnung seiner Telefonnummer zu öffentlichen Profildaten bei ihm entstanden sein soll. Sämtliche Verstöße sind in Bezug gesetzt zur Begünstigung dieser einheitlichen Folgewirkung, die als Schaden geltend gemacht wird. Sowohl hinsichtlich der laut Kläger unzureichenden Information, unzureichend eingeholten Einwilligung als auch hinsichtlich der unterbliebenen Offenlegung geht es dem Kläger um Schadensersatz hierfür insoweit, als diese das potentiell für ihn schädigende Verhalten der dritten Personen nach sich gezogen und dessen Folgen vertieft haben.

Selbst wenn man dieser Auffassung nicht folgen würde, würde dies vorliegend nichts an der Zulässigkeit ändern. Teilt man diese Auffassung nicht, so liegt jedenfalls eine im Hinblick auf § 260 ZPO zulässige Klagehäufung vor. Mehrere Streitgegenstände wären dann in einem Antrag unter Angabe eines einheitlichen Zahlbetrages zusammengefasst. Da der Kläger vorliegend mit dem Antrag zu 1.) einen unbezifferten Antrag auf Ersatz immaterieller Schäden stellt, führt dies auch nicht zur unzureichenden Bestimmtheit des Antrages zu 1.). Die Stellung eines unbezifferten Antrages unter Angabe lediglich einer Rahmenvorstellung ist bei solchen Anträgen mit Blick auf die Bestimmung der Schadenshöhe durch das Gericht nach billigem Ermessen ausnahmsweise zulässig. Die fehlende Zuordnung bestimmter Zahlbeträge zu den einzelnen Gegenständen ist danach entbehrlich (so auch OLG Hamm, Urt. v. 18.05.2023 – 7 U 19/23, veröffentlicht im Rechtsprechungsportal der Justiz NRW, abrufbar unter https://www.justiz.nrw/BS/nrwe2/index.php, Rn. 54 - 56).

3.
Unzulässig ist indessen der Unterlassungsantrag zu 3.) b, da dieser bereits nicht hinreichend bestimmt ist, § 253 Abs. 2 Nr. 2 ZPO.

Das Bestimmtheitsgebot setzt im Interesse der Schaffung einer sicheren Rechtslage nach Rechtskraft sowie mit Blick auf das im Vollstreckungsrecht geltende Gebot der Formalisierung der Zwangsvollstreckung voraus, dass sich aus dem Inhalt eines Antrages, der die Grundlage des späteren Tenors bildet, der Inhalt des Gebotes klar und eindeutig entnehmen lässt. Eine Verurteilung, die mehr als einen Deutungsgehalt zulässt und spezifisch in Bezug auf einen Unterlassungsantrag nicht zweifelsfrei bestimmen lässt, ob ein bestimmtes Verhalten hierunter fällt oder nicht, genügt diesen Anforderungen nicht. Es darf nicht dem Vollstreckungsgericht die Entscheidung darüber überlassen werden, was dem Beklagten verboten ist (vgl. BGH, Urt. v. 20.06.2013 – I ZR 55/12, Rn. 12).

Durch die Anknüpfung des Klägers an eine Verarbeitung ohne Einwilligung bezeichnet dieser keine konkrete Verhaltensweise. Die Unterlassungsaufforderung gibt den Inhalt eines gesetzlichen Handlungsverbotes wieder, unter welches aufgrund der Abstraktheit einer Rechtsnorm und der Vielgestaltigkeit der Anwendungsfälle, eine in Umfang und Art unbeherrschbare Zahl von Haftungsfällen auf die Beklagte zukommen würde, die sich im Zweifelsfall nicht einwandfrei bestimmen lassen würden. Dem Vollstreckungsorgan wäre die Rechtsprüfung, die im Erkenntnisverfahren stattfinden soll, vollumfänglich auferlegt, was mit den Grundsätzen des Zivilprozesses nicht vereinbar ist. Der von dem Kläger formulierte Unterlassungstatbestand stellt keinen tatsächlichen Sachverhalt, sondern ein Rechtskriterium dar. Der Kläger umschreibt im Wesentlichen den Wortlaut des Art. 6 DSGVO. Ein lediglich durch Wiedergabe eines unbestimmten gesetzlichen Tatbestandsmerkmals umgrenzter Unterlassungsantrag ist unzulässig (vgl. *Greger*, in: Zöller, § 253, Rn. 13b).

4.
Es kann dahinstehen, ob das erforderliche Feststellungsinteresse nach § 256 ZPO besteht. Ist die Klage unbegründet, unterliegt sie unabhängig von einem bestehenden Feststellungsinteresse der Abweisung (vgl. Greger, in: Zöller, § 256, Rn. 7).

II.
Die Klage, soweit sie zulässig ist, ist lediglich hinsichtlich des Antrages zu Ziffer 1.) teilweise begründet. Im Übrigen ist sie unbegründet.

1.

Der Antrag zu 1.) gerichtet auf Zahlung eines in das Ermessen des Gerichts gestellten immateriellen Schadensersatz ist begründet, jedoch lediglich in Höhe von 300,00 EUR, durch die das von dem Kläger aufgrund des streitgegenständlichen Vorfalls erlittene Leid angemessen, aber auch ausreichend abgegolten ist.

a)

Ein Anspruch in dieser Höhe folgt aus Art. 82 Abs. 1 DSGVO.

Nach Art. 82 Abs. 1 DSGVO steht jeder Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, ein Anspruch auf Schadenersatz gegen den Verantwortlichen zu. Im Streitfall macht der Kläger Ersatz eines behaupteten immateriellen Schadens geltend.

aa)

Die haftungsbegründenden Voraussetzungen eines Anspruchs nach Art. 82 DSGVO gegen die Beklagte liegen vor.

(1)

Der persönliche und sachliche Anwendungsbereich der DSGVO ist eröffnet. Die Beklagte als verantwortliches Unternehmen hat ihren Sitz in Irland, sie betreibt die streitgegenständliche Tätigkeit der Datenverarbeitung innerhalb der Union. Der Betrieb eines sozialen Netzwerkes durch Sammlung/Speicherung jedenfalls des Namens und Geschlechts von Mitgliedern und die automatisierte Vernetzung der Mitglieder sowie deren Beschickung mit individualisierter Werbung fällt in den sachlichen Anwendungsbereich nach Art. 2 Abs. 2 DSGVO. Ein Ausnahmetatbestand iSv Art. 2 Abs. 2 - 4 DSGVO oder der Öffnungsklausel nach Art. 85 Abs. 2 DSGVO ist nicht einschlägig. Bei den hier in Rede stehenden Daten handelt es sich um personenbezogene Daten iSd Art. 5 Abs. 1 Buchst. a Var. 1 DSGVO, Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO, Art. 7 DSGVO, Art. 2 Abs. 1 DSGVO iVm Art. 4 Nr. 1 DSGVO.

(2)

Es muss ein Verstoß gegen Vorschriften der DSGVO vorliegen. Insoweit umfasst der Schutzbereich des Art. 82 Abs. 1 DSGVO sämtliche Vorschriften der DSGVO (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 9). Soweit diese zur

Verursachung eines Schadens nicht geeignet erscheinen, wird ebendem durch das ausdrückliche weitere Tatbestandsmerkmal eines Schadens, der „wegen eines Verstoßes“ entstanden sein muss, Rechnung getragen. Für eine Eingrenzung auf bestimmte datenschutzrechtliche Vorschriften der DSGVO bietet der Wortlaut keinerlei Anhaltspunkte. Gemessen an den Zielen der Norm, wie diese im Erwägungsgrund 146 S. 5 der DSGVO zum Ausdruck kommen, würde eine solche Auslegung auch Sinn und Zweck nach der Vorstellung des Unionsgesetzgebers zuwiderlaufen.

Vorliegend steht fest, dass Verstöße gegen mehrere Vorschriften der DSGVO vorliegen, nämlich gegen Art. 5 Abs. 1, 6 Abs. 1 DSGVO wegen einer Verarbeitung der Daten des Klägers ohne Berechtigung, gegen Art. 5 Abs. 1. 25 Abs. 2 S. 1 DSGVO wegen der datenschutzunfreundlichen Voreinstellungen in Bezug auf das CIT und gegen Art. 32 DSGVO aufgrund unzureichender Sicherheitsvorkehrungen. Dies ergibt sich bereits aufgrund des unstreitigen Sachverhalts, weshalb eine Beweisaufnahme insoweit entbehrlich ist.

Zunächst liegt ein Verstoß der Beklagten gegen Art. 5 Abs. 1, Art. 6 Abs. 1 UAbs. 1 Buchst. a) – f) DSGVO iVm Art. 7 DSGVO vor. Die Beklagte hat Daten des Klägers verarbeitet, wobei keine der Parteien vorgetragen hat, dass sie sich die für die Rechtmäßigkeit der Datenverarbeitung erforderliche Einwilligung des Klägers zur Datenverarbeitung eingeholt hat. Eine solche ist vorliegend zwingend erforderlich, da die Verarbeitung auch nicht nach einer der übrigen Tatbestandsvarianten des Art. 6 UAbs. 1 Buchst. b) – f) entbehrlich war. Insoweit führt das OLG Hamm in seinem Urteil vom 15.08.2023 (7 U 19/23, GRUR 2023, 1791, 1795, Rn.82 -98) aus:

„Zunächst war die Datenverarbeitung mit Blick auf die Suchbarkeit eines Nutzerprofils über die Mobilfunktelefonnummer per Such- und Kontaktimportfunktion und insbesondere die diesbezügliche Voreinstellung der Suchbarkeit für „alle“ – entgegen der Ansicht der Bekl. – nicht zur Vertragszweckerfüllung erforderlich und damit nicht gem. Art. 6 I UAbs. 1 Buchst. b DSGVO gerechtfertigt.

Soweit die Bekl. die streitgegenständliche, mittlerweile deaktivierte Suchbarkeit des Nutzerprofils über die Telefonnummer für „alle“ unter Nutzung der Such- oder Kontaktimportfunktion als für die Vertragserfüllung essentiell, da zur Vernetzung der

Nutzer untereinander erforderlich, erachtet, vermag sich der Senat dem nicht anzuschließen:

(aa) Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich iSd Art. 6 I UAbs. 1 Buchst. b DSGVO angesehen werden kann, muss sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte (EuGH GRUR 2023, 1131 Rn. 98 – Metaplatforms u. a.).

Der etwaige Umstand, dass eine solche Verarbeitung im Vertrag erwähnt wird oder für dessen Erfüllung lediglich von Nutzen ist, ist insoweit für sich genommen unerheblich. Entscheidend für die Anwendung des in Art. 6 I UAbs. 1 Buchst. b DSGVO genannten Rechtfertigungsgrundes ist nämlich, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen (EuGH GRUR 2023, 1131 Rn. 99 – Meta Platforms u. a.).

Dabei ist im Fall eines Vertrags, der mehrere Dienstleistungen oder mehrere eigenständige Elemente einer Dienstleistung umfasst, die unabhängig voneinander erbracht werden können, die Anwendbarkeit von Art. 6 I UAbs. 1 Buchst. b DSGVO für jede dieser Dienstleistungen gesondert zu beurteilen (EuGH GRUR 2023, 1131 Rn. 100 – Meta Platforms u. a., mwN).

(bb) Demzufolge ergibt sich schon allein aus dem Umstand, dass die Bekl. nur hinsichtlich bestimmter personenbezogener Daten vorgab und -gibt, 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, dass diese Daten nicht objektiv unerlässlich waren und sind, um eine (hinreichende) Verknüpfung der Nutzer der Bekl. zu ermöglichen. Dass dies (unter Umständen) für die Nutzer (und vor allem im Hinblick auf die Werbezweckrichtung und damit das Geschäftsmodell der Bekl.) wünschenswert gewesen sein mag, reicht gerade nicht. Ob der einzelne

Nutzer (sich) diesen Wunsch erfüllen mochte, musste ihm vielmehr im Rahmen einer informierten Einwilligung selbst überlassen bleiben.

(cc) Ohne Erfolg beruft sich die Bekl. in rechtlicher Hinsicht darauf, die vorgenannten Vorgaben des EuGH, die der Senat zugrunde legt, bezögen sich nur auf die vom Vorabentscheidungsersuchen betroffenen Off-Facebook-Daten und beträfen einen anderen Verarbeitungszweck und ließen sich deshalb auf den vorliegenden Fall nicht übertragen. Wenn auch der Kontext, zu dem sich der EuGH zur Auslegung der geforderten Erforderlichkeit für die Vertragserfüllung geäußert hat, ein anderer war, so besteht jedoch keinerlei Zweifel daran, dass diese Aussagen des EuGH allgemeingültig sind (vgl. explizit EuGH GRUR 2023, 1131 Rn. 98 – Meta Platforms u. a.). Dafür, dass der EuGH insoweit eine differenzierende Begriffsbestimmung für geboten hielte, besteht keinerlei Anhaltspunkt.

(dd) Ebenso wenig lässt sich – entgegen der im Senatstermin ins Feld geführten Argumentation der Bekl. – in Anwendung der Begriffsbestimmung durch den EuGH eine Erforderlichkeit der streitgegenständlichen Suchbarkeit des Profils per Suchbarkeits- oder Kontaktimportfunktion über eine künstliche Aufspaltung des einheitlichen Nutzungsvertrags in mehrere gesonderte Verträge oder eigenständige Elemente, jeweils in sich geschlossen auf bestimmte Funktionen des Online-Netzwerkes, annehmen.

Zwar sind mehrere Dienstleistungen oder mehrere eigenständige Elemente einer Dienstleistung, die unabhängig voneinander erbracht werden können, im Hinblick auf die Anwendbarkeit von Art. 6 I UAbs. 1 Buchst. b DSGVO für jede dieser Dienstleistungen gesondert zu beurteilen (vgl. EuGH GRUR 2023, 1131 Rn. 100 – Meta Platforms u. a., mwN).

Jedoch können vorliegend die Such- oder die Kontaktimportfunktion gerade nicht als eigenständige Elemente einer Dienstleistung betrachtet werden; denn sie dienen schlicht dem von der Bekl. beschriebenen Hauptnutzungszweck der Plattform einer möglichst einfachen Vernetzung der Nutzer untereinander. Ihnen fehlt folglich jeglicher eigenständige Charakter, sie sind Mittel zum Zweck, aber eben kein unerlässliches mit Blick auf die Vernetzung der Nutzer.

(b) Auch wenn sich die Bekl. im vorliegenden Rechtsstreit nicht explizit auf eine Rechtfertigung über Art. 6 I UAbs. 1 Buchst. f DSGVO beruft, so hat sie doch zugleich als Anlage einen Auszug von ihrer Webseite zur Akte gereicht, in dem dieser Rechtfertigungsgrund behandelt wird. Aus Rechtsgründen sah sich der Senat deshalb gehalten, eine mögliche Rechtfertigung über Art. 6 I UAbs. 1 Buchst. f DSGVO in den Blick zu nehmen; denn Art. 6 I UAbs. 1 DSGVO enthält eine erschöpfende und abschließende Liste der Fälle, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann (EuGH GRUR 2023, 1131 Rn. 90 – Meta Platforms u. a., mwN; EuGH NJW 2021, 841 Rn. 34). Die dort genannten Möglichkeiten einer Rechtfertigung bestehen dabei grundsätzlich alternativ nebeneinander (EuGH GRUR 2023, 1131 Rn. 92 – Meta Platforms u. a., mwN).

Eine Rechtfertigung über Art. 6 I UAbs. 1 Buchst. f DSGVO scheidet vorliegend jedoch aus:

(aa) Verarbeitungen personenbezogener Daten sind nach Art. 6 I UAbs. 1 Buchst. f DSGVO unter drei kumulativen Voraussetzungen rechtmäßig: Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen (EuGH GRUR 2023, 1131 Rn. 106 – Meta Platforms u. a., mwN).

(bb) Jedenfalls das Vorliegen der zweiten Voraussetzung der Erforderlichkeit lässt sich nicht feststellen.

Entscheidend hierfür ist, ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Art. 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen (EuGH GRUR 2023, 1131 Rn. 108 – Meta Platforms u. a., mwN).

Zudem ist die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem sog. Grundsatz der „Datenminimierung“ zu prüfen, der in Art. 5 I Buchst. 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 (EuGH GRUR 2023, 1131 Rn. 109 – Meta Platforms u. a.).

Dass die Suchbarkeit über die Telefonnummer auf den verschiedenen Ebenen, insbesondere per Kontaktimportfunktion von Facebook oder im Facebook-Messenger, nicht erforderlich ist und war, wird dadurch belegt, dass diese Funktion zum 6.9.2019 endgültig und vollständig aus allen Anwendungsbereichen eliminiert wurde.“

Diesen ausführlichen und zutreffenden Erwägungen, die sich das Gericht vollumfänglich zu Eigen macht, ist nichts hinzuzufügen. Die Tatbestandsvarianten des Art. 6 UAbs. 1 Buchstabe c) bis e) DSGVO sind vorliegend offensichtlich nicht einschlägig.

Dass der Kläger den geänderten Nutzungsbedingungen und der anlässlich des Inkrafttretens der DSGVO neu eingeführtem Daten- sowie Cookie-Richtlinie zugestimmt hätte, hat die Beklagte nicht vorgetragen. Sie trifft indes für das Vorliegen einer Einwilligung und zur Ausräumung eines Verstoßes nach Art. 5 Abs. 1, 6 UAbs. 1 DSGVO kraft der besonderen Vorschriften der Art. 5 Abs. 2, 7 Abs. 1 DSGVO auch im Rahmen des Schadensersatzverlangens eine primäre Darlegungs- und Beweislast (OLG Hamm, Urt. v. 15.08.2023 - 7 U 19/23 - , GRUR 2023, 1791, 1794, Rn. 75, 76).

Die Beklagte hat gegen Art. 5 Abs. 1, 25 Abs. 2 DSGVO, also den Grundsatz datenschutzfreundlicher Grundeinstellung verstoßen, indem die Voreinstellung bezüglich der Suchbarkeit auf „alle“ gesetzt war. Dies hätte zum Zeitpunkt des Inkrafttretens der DSGVO, zu dem der Kläger bereits registrierter Nutzer bei Facebook war, dahingehend angepasst werden müssen, das statt einem Abstellen des Klägers dieser Funktion („Opt out“) ein aktives Anwählen des Klägers („Opt in“) der Funktion zu deren Aktivierung erforderlich ist.

Es liegt ferner ein Verstoß gegen Art. 32 DSGVO vor. Das OLG Hamm führt im Urteil vom 15.08.2023 (Az. 7 U 19/23 , GRUR 2023, 1791, 1797, Rn. 114 ff.) hierzu aus:

„(e) Weiterhin hat die Bekl. nicht dargelegt, dass ihre Datenverarbeitung den Anforderungen der Art. 5 I Buchst. f DSGVO, Art. 32 DSGVO entsprach.

Die Bekl. hat trotz der sie treffenden Darlegungs- und Beweislast konkret weder substanziiert dargelegt noch bewiesen, dass sie den Vorgaben des Art. 32 DSGVO zur Sicherheit der Verarbeitung genügt hätte, worauf sie bereits unter dem 30.6.2023 hingewiesen worden ist.

(aa) Die Argumentation der Bekl. verfängt zunächst insoweit nicht, als sie sich auf den Rechtsstandpunkt einer als solchen schon fehlenden, aber jedenfalls rechtmäßigen Datenverarbeitung durch sie stellt – mit der Begründung, die Daten gar nicht unbefugt Dritten, den Scrapern, offengelegt zu haben, weil unter Verstoß gegen die Meta-Nutzungsbedingungen nur die Art des Abrufs der Daten durch die Scraper, nicht aber der Zugang zu den abgerufenen, ohnehin öffentlichen Daten unberechtigt gewesen sei.

Entgegen ihrer Rechtsansicht hat die Bekl. die geleakten Daten den Scrapern offengelegt; denn in der (seitens der Bekl. automatisierten) Ausführung des Abrufs über die Such- oder Kontaktimportfunktionen liegt unzweifelhaft eine Datenverarbeitung iSd Art. 4 Nr. 2 DSGVO in Form der Offenlegung durch Übermittlung. Der Begriff „Verarbeitung“, wie er in Art. 4 Nr. 2 DSGVO definiert wird, ist nach dem Willen des Unionsgesetzgebers mit der Formulierung „jede(r) Vorgang“ weit zu fassen und stellt keine erschöpfende Aufzählung von Vorgängen im Zusammenhang mit personenbezogenen Daten oder Sätzen solcher Daten – wie etwa Erheben, Erfassen, Speicherung und Abfragen – dar (vgl. EuGH NJW 2023, 2555 Rn. 46 ff. mwN zu Abfragen von Mitarbeitern des datenverarbeitenden Unternehmens; EuGH NJW 2023, 2253 = GRUR-RS 2023, 8971 Rn. 27 mwN).

Ohne die automatisierte Datenverarbeitung der Bekl. hätten die Scraper die Nutzerinformationen nicht zusammenstellen und veröffentlichen können.

Offenlegung und Zugangsgewährung geschahen auch unbefugt. Das ergibt sich schon – unabhängig von deren genauer rechtlicher Einordnung – aus den

Nutzungsbedingungen der Bekl., die ein Vorgehen wie das der Scraper, die als Nutzer registriert sein mussten, explizit untersagen:

„Du darfst (ohne unsere vorherige Genehmigung) nicht mittels automatisierter Methoden auf Daten unserer Produkte zugreifen, solche Daten erfassen oder versuchen, auf Daten zuzugreifen, für die du keine Zugriffsberechtigung hast."

Das galt erst recht für Personen, die sich – wie die Scraper unter Vorgabe fremder oder nicht existierender Identitäten – bereits unrechtmäßig im Netzwerk der Bekl. angemeldet hatten.

(bb) Auch die weitere Argumentation der Bekl. verfängt nicht, soweit sie sich nämlich im Wesentlichen schlicht auf den Standpunkt stellt, ihre Pflichten zur Implementierung angemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DGVO, Art. 24 DSGVO, Art. 5 I Buchst. f DSGVO im Zusammenhang mit der Kontaktimportfunktion nicht verletzt zu haben, weil sie ihre Anti-Scraping-Maßnahmen im relevanten Zeitraum regelmäßig überprüft und gegebenenfalls entsprechend den Marktgepflogenheiten zu den Sicherheitsstandards sukzessive aus der maßgeblichen ex-ante-Betrachtung in angemessener Weise angepasst habe, zB durch Übertragungsbegrenzungen, Boterkennung, Captchas („Completely Automated Public Turing Test to tell Computers and Humans Apart" (auf Deutsch: Vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden)) und den „Social Connection Check" (Anzeige von Personen, nur wenn diese sich zu kennen schienen).

Tatsächlich waren die im Zeitpunkt des Scraping-Vorfalls bestehenden Maßnahmen unter Zugrundelegung des unstreitigen und streitigen Vortrags der Bekl. technisch und organisatorisch ungeeignet iSd Art. 32 I 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.

[1] Der Senat verkennt insoweit zunächst nicht, dass allein die Tatsache, dass es zum Scraping-Vorfall gekommen ist, kein Beweis dafür ist, dass die Bekl. im Vorfeld

ungeeignete Maßnahmen ergriffen hätte (vgl. GA Pitruzzella GRUR-RS 2023, 8707 Rn. 29–37).

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 GRUR-RS 2023, 8707 Rn. 38–44).

[2] Vorliegend hat die Bekl. 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.

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 GRUR-RS 2023, 8707 Rn. 20).

Es ist weder von der Bekl. 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 Bekl., 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 30.6.2023 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 sechszehn Monate dauerte oder warum nicht wenigstens andere weniger einschneidende, aber wirkungsvolle Maßnahmen getroffen wurden.

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 Bekl. 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 Bekl. ihre Standardeinstellung „alle" für die Suchbarkeit über die Telefonnummer nicht – wie geboten – geändert hatte.

Soweit die Bekl. vorträgt, sie habe für die Kontaktimportfunktion der Plattform zu einem – im vorliegenden Verfahren trotz Hinweises vom 30.6.2023 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 Ähnlichkeitskontrolle 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."

Auch insoweit schließt sich die Richterin dem OLG Hamm an und macht sich die diesbezüglichen Ausführungen zu Eigen. Insbesondere verteidigt sich die Beklagte auch in dem vorliegenden Verfahren nur durch Darlegung einzelner Maßnahmen zur Bekämpfung und Verringerung von Scraping. Dass sie Vorkehrungen traf, um zu

unterbinden, dass Dritte unter Ausnutzung des CIT die gescrapten Daten mit der Telefonnummer zusammenführen, hat sie nicht vorgetragen. Weder hat sie vorgetragen, obwohl ihr die naheliegende Gefahr eines solchen Missbrauchs bewusst sein musste und ab April 2018 bewusst war, dass die betroffenen Funktionen in einer Weise technisch absicherte, dass der Missbrauch nicht mehr möglich war, noch, dass sie diese in der Folge abstellte. Dies wäre aber, angesichts des massiven Eingriffs in Datenschutzrechte der Nutzer, geboten gewesen.

(3)
Die Beklagte ist hinsichtlich der Verstöße Verantwortliche im Sinne des Art. 82 Abs. 1 DSGVO gem. Art. 4 Nr. 7 DSGVO.

(4)
Schließlich kann sich die Beklagte nicht gem. § 82 Abs. 3 DSGVO durch den Nachweis fehlenden Verschuldens exkulpieren. Die Beklagte kann sich, wie bereits aufgezeigt, weder durch den Verweis auf das Verschulden dritter Täter, noch durch die behaupteten allgemeinen Anti-Scraping-Maßnahmen entlasten.

bb)
Dem Kläger ist durch die vorgenannten Verstöße ein kausaler immaterieller Schaden entstanden, der nach Einzelfallabwägung einen Anspruch auf Schmerzensgeldzahlung in Höhe von 300,00 € begründet.

Nicht zu berücksichtigen bei der Bemessung ist ein etwaiger Verstoß gegen Art. 15 DSGVO im Zusammenhang mit der vorgerichtlichen Auskunft. Es ist nicht ersichtlich, dass die inzwischen nachgeholte fehlende Auskunft über von dem Vorfall vom April 2021 betroffene Daten des Klägers irgendeinen immateriellen Schaden nach sich ziehen könnte. Materielle aus der fehlenden Auskunft resultierende Schäden sind ebenso wenig vorgetragen.

Der Anspruch nach Art. 82 Abs. 1 DSGVO ist nicht schlechthin begründet, weil ein zu verantwortender Verstoß gegen die Vorschriften der DSGVO vorliegt. Der in der Norm benannte kausale Schaden ist als eigenständiges Tatbestandsmerkmal zu verstehen. Wenn immaterieller Schadensersatz verlangt wird, ist darzutun, im Bestreitensfall zu beweisen, dass ein solcher in Form irgendeines psychischen Leides, Angst, Furcht oder aber eines vom Kläger erlebten Kontrollverlusts, der sich

bei ihm in einer konkreten Form als Leid niedergeschlagen hat, entstanden ist. Der Eingrenzung durch eine „Erheblichkeitsschwelle“ unterliegt der Schadensersatzanspruch nach Art. 82 DSGVO nicht, wie der EuGH in seinem Urteil vom 04.05.2023, C-300/21 („Österreichische Post“) festgestellt hat. Gleichwohl hebt auch der EuGH in der Entscheidung klar hervor, was sich ebenfalls unzweifelhaft aus dem Wortlaut des Art. 82 DSGVO ergibt, dass an dem Kriterium eines irgendwie gearteten materiellen oder immateriellen Schadens als eigenständige Anspruchsvoraussetzung festzuhalten ist. (s. OLG Hamm, Urt. v. 15.08.2023 – 7 U 19/23, GRUR 2023, 1791, 1799 Rn. 139; EuGH, Urt. v. 04.05.2023, C-300/21, „Österreichische Post“, Rn. 50). Nach ständiger Rechtsprechung des EuGH setzt die Annahme eines konkreten Schadens iSd Art. 82 DSGVO nach unionsautonomer Auslegung voraus, dass ein solcher „tatsächlich und sicher“ besteht (OLG Hamm, Urt. v. 15.08.2023 – 7 U 19/23, GRUR 2023, 1791, 1799 Rn. 140).

Der Begriff des Schadens soll zur Gewährung eines wirksamen Ersatzes nach dem Erwägungsgrund 146 S. 3 weit ausgelegt werden. Beispielhaft aufgezählt werden im Erwägungsgrund 75 der DSGVO folgende Nichtvermögensschäden, die einen immateriellen Schaden darstellen können: Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugte Aufhebung der Pseudonymisierung oder andere gesellschaftliche Nachteile, die an sich schon ein immaterieller Schaden sind, wenn die betroffene Person um ihre Rechte und Freiheiten gebracht oder daran gehindert wird, die sie betreffenden personenbezogenen Daten zu kontrollieren. Der Schaden muss auch wirklich „erlitten“ sein (ErwGr. 146 S. 6). Es muss ein realer und sicherer emotionaler Schaden eingetreten sein. Empirisch führt nämlich jeder Verstoß gegen eine Datenschutzvorschrift zu einer negativen Reaktion der betroffenen Person. Nicht jeder Datenschutzverstoß soll jedoch einen Schadensersatzanspruch auslösen. Ein immaterieller Schadensersatz für ein bloßes Gefühl des Unwohlseins käme einer Entschädigung ohne Schaden gleich (GA Pitruzzella, Schlussantrag vom 27.04.2023 – C-340/21, Rn. 81 f). Auch soweit der Erwägungsgrund 75 den Kontrollverlust als beispielhafte Auswirkung, die zu einem immateriellen Schaden führen „könnte“, in Bezug nimmt, entbindet dies den betroffenen nicht von der Einzelfalldarlegung, worin der durch den Kontrollverlust erlittene immaterielle Schaden bei ihm konkret liegt.

Vorliegend ist das Gericht nach durchgeführter persönlicher Anhörung des Klägers davon überzeugt, dass kausal verursacht durch das Bekanntwerden der Telefonnummer des Klägers in einem gemeinsamen Datensatz mit weiteren Angaben ein sprunghafter Anstieg von SPAM-Nachrichten und –Anrufen zu verzeichnen war, der dem Kläger auch emotional zu einem gewissen Grad zusetzte. So ist das Gericht davon überzeugt, dass der Kläger den Anstieg als störend und lästig empfand, illustriert durch das Anstellen von Recherchen zu möglichen Ursachen anlassbezogen durch die Nachrichten. Ferner ist das Gericht davon überzeugt, dass der Kläger diese als empfindliche Einschränkung seiner Erreichbarkeit empfand, da die SPAM-Nachrichten und -Anrufe – nachvollziehbarer Weise, da eine Vielzahl der Benachrichtigungen auf seinem Mobiltelefon während der zwei „Spam-Wellen“ tatsächlich keinem Kontaktverlangen sozialer Bekanntschaften entsprach – abstrakt zu einem veränderten Nutzungsverhalten in diesen Zeiträumen führte.

Die Beklagte hat die Zunahme von SPAM-Nachrichten kausal bedingt durch die Veröffentlichung im April 2021 bestritten. Darlegungs.- und beweisbelastet hinsichtlich des Vorliegens eines kausalen Schadens ist der Kläger. Diesem ist der Beweis der behaupteten Folgen und Schäden überwiegend gelungen.

Wenngleich die persönliche Anhörung nicht zu den Strengbeweismitteln zählt, kann sie dennoch im Einzelfall im Rahmen umfassender freier Würdigung des gesamten Akteninhalts, s. § 286 ZPO, zur vollen Überzeugung des Gerichts von einer Tatsache führen. Dies ist hier hinsichtlich des Umstandes der Zunahme von SPAM-Inhalten der Fall. Der Kläger verwendet insoweit den Begriff von „Wellen“. Dieser sehr plastische Begriff spricht dafür, dass der Kläger einen zweimaligen ungewöhnlichen Anstieg tatsächlich erlebt hat. Auch schildert der Kläger die chronologischen Abläufe detailreich und präzise. Dass er sich an die Zeitpunkte derart genau erinnern kann, ist plausibel, da diese sich jeweils mit Todesfällen in seiner Familie zeitlich überschnitten. Dass der Kläger auch zugesteht, dass er nicht nach dem plötzlichen Anstieg von SPAM-Kontaktierung von dem Vorfall vom April 2021 erfuhr, sondern zuvor bereits vereinzelt Informationen am Rande zu Kenntnis nahm, zeugt von der Glaubhaftigkeit. Der Kläger sucht nicht durch Aussparung ihm ungünstiger Informationen seine Behauptung, erst durch den plötzlichen Anstieg auf die Idee gekommen zu sein, dass er Betroffener ist, glaubhaft zu machen.

Das Gericht ist davon überzeugt, dass der nachgewiesene SPAM-Anstieg kausal darauf zurückgeht, dass es Dritten aufgrund der Datenschutzverstöße der Beklagten gelang, ein Datenpaket mit dem auf dem Nutzerprofil angegebenen Namen, Facebook-ID, Geschlecht, Land und Telefonnummer zusammenzustellen und dieses durch Veröffentlichung im Darknet dem Zugriff eines unbegrenzten Personenkreises auszusetzten. Es steht zur Überzeugung des Gerichts fest, dass, wenngleich bereits der Kläger auch zuvor von SPAM-Nachrichten betroffen war, was er auch zugibt, und die Erlangung der Telefonnummer allein auch über eine Rufnummeraufzählung möglich ist, eine spürbare Zunahme nach der streitgegenständlichen Datensatzveröffentlichung zu vermerken war, die hierauf kausal zurückgeht. Denn die Steigerung fand in unmittelbarem zeitlichen Zusammenhang statt. Im April 2021 kam es zu der Datenveröffentlichung. Die erste Belästigungswelle datiert der Kläger auf den Juli 2021. Dass auf andere Weise ein Anlass für diesen plötzlichen Anstieg des Missbrauchs der Nummer geschaffen wurde, ist auszuschließen. Denn der Kläger hat geschildert, dass er nicht nur einen Telefonnummereintrag unterbunden hat, sondern auch sonst hinsichtlich dieses Datenpunktes eine Vorsicht walten lässt, die zu einer möglichst geringen Verbreitung führt. Er gebe die Nummer nie öffentlich an, bei Nutzung von Angeboten im Internet nur dort, wo es Pflicht sei und auch dann versuche er nach Möglichkeit, durch Eingabe lediglich der Ziffer „0“ die Angabe der wahren Telefonnummer zu umgehen. Webshops oder Essenslieferanten seien Angebote, bei denen er von vorne herein keine Nummer angebe. Die so veranschaulichte restriktive Datenangabe ist durch die glaubhaften Ausführungen zur Überzeugung des Gerichts bewiesen.

Dass darüber hinaus die Datensatzveröffentlichung sogar kausal dafür war, dass dem Kläger die Gelegenheit zur Verabschiedung von seinem im Juli 2021 verstorbenen Vater genommen wurde bzw. hinsichtlich seiner Großmutter dazu führte, dass er von ihrem Versterben in der Nacht erst am nächsten Morgen erfuhr, was er andernfalls unmittelbar erfahren hätte, ist dagegen nicht zur Überzeugung des Gerichts belegt.

Ersatzfähig sind im Rahmen des Art. 82 DSGVO nur solche Schäden, die kausal sind, wobei nach der Rechtsprechung des EuGH die jeweiligen nationalrechtlichen Kausalitätsbegriffe dieses Tatbestandsmerkmal konkretisieren, solange der Effektivitätsgrundsatz bei der Auslegung beachtet ist (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 11; OLG Hamm, Urt. v. 15.08.2023 – 7 U 19/23, GRUR

2023, 1791, 1802 Rn. 173). Auch das Unionsrecht kennt schadensrechtliche Eingrenzungen und steht einer uferlosen Haftung entgegen (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 11)

Dass abstrakt die SPAM-Belästigung während der Wellen zu einem geänderten Nutzungsverhalten führen kann, liegt für das Gericht auf der Hand und kann ohne Weiteres nachvollzogen werden. Dass aber auch konkret zu den streitgegenständlichen Zeitpunkten der Kontaktierungsversuche durch Angehörige sein Nutzungsverhalten gerade in der Weise verändert war, dass er wegen diesem die zeitnahe Kenntnisnahme von den Notfällen und die Abschiedsnahme versäumte, während ohne den Datenschutzvorfall in jedem Fall sein Verhalten so gewesen wäre, dass dies ermöglicht worden wäre, ist nicht hinreichend belegt. So lag zwischen dem ersten versäumten Anruf seiner Mutter um 9:00 Uhr und dem Operationsbeginn um 11:00 Uhr lediglich eine Spanne von drei Stunden, wobei laut Kläger die Fahrt zum Krankenhaus weitere zwei Stunden in Anspruch genommen hätte. Es liegt nahe, dass auch ohne die Vorgänge rund um die Datenveröffentlichung der Kläger nicht rechtzeitig von dem Anruf seiner Mutter Kenntnis genommen hätte, um seinen Vater noch im Krankenhaus anzutreffen. Ebenso wenig ist ersichtlich, dass der Kläger bei zeitlich knapper kurzfristiger Kenntnisnahme sich überhaupt noch zum Krankenhaus begeben hätte, da nicht ersichtlich ist, dass der Operationsbeginn von 11:00 Uhr von Anfang an feststand. Angesichts des erlittenen Herzinfarkts ist denkbar, dass das Krankenhaus eine Operation schnellstmöglich avisierte, sodass auch ein früherer Termin im Vorhinein möglich erschien. Eine zweistündige Anreise hätte dies obsolet gemacht. Es ist nicht vorgetragen, dass der Vater des Klägers, wäre dieser in der Zeit zwischen 9 bis 11:00 Uhr kontaktiert worden, für die Führung eines Telefongesprächs verfügbar und in der Lage gewesen wäre. Nahe liegt, dass Mutter und Schwester den Kläger angesichts dieser Gesamtumstände bewusst nicht nachdrücklich kontaktierten, etwa nach der erkannten Unerreichbarkeit über das Mobiltelefon über das Arbeitstelefon, Mitbewohner oder Ehefrau versuchten, den Kläger zu kontaktieren. Denn die Einflussmöglichkeiten des Klägers in Bezug auf den medizinischen Notfall waren naturgemäß wegen der örtlichen Entfernung beschränkt. Auch ergibt sich aus dem Vortrag des Klägers, wonach ursächlich für den Tod ein Operationsfehler war, nicht, dass die Familienmitglieder vor Beginn der Operation von einem derart unglücklichen Verlauf ausgingen.

Letztlich ist das Gericht auch nicht davon überzeugt, dass der Kläger unter gewöhnlichen Umständen stets unmittelbar erreichbar war und bei telefonischen Kontaktaufnahmen stets zeitnah reagierte. Denn auch unter Berücksichtigung einer Vielzahl von SPAM ist die Dauer von acht Stunden, nach denen der Kläger seine Schwester erst anrief, eine überaus lange Reaktionszeit. Diese Zeitdauer wartete der Kläger zu, obwohl er selbst angab, auch von dem Krankenhaus, also einer Festnetznummer mit zuzuordnender Ortswahl, und nur teilweise unter unbekannter Nummer angerufen worden zu sein. Es liegt nahe, dass der Kläger generell sein Handy restriktiv nutzte, es also auch ohne die SPAM-Welle vorkam, dass er sein Handy für Zeitblöcke von einer bis drei Stunden nicht nutzte. Ebenso wenig ist das Gericht davon überzeugt, dass der Kläger nachts stets telefonisch erreichbar gewesen wäre ohne den streitgegenständlichen Datenschutzvorfall und sein Handy nie auf lautlos gestellt hätte. Es finden sich in den Darstellungen des Klägers nicht genügend Anhaltspunkte, aufgrund derer das Gericht von einem solchen untypischen Verhalten überzeugt ist. Zudem führt der Kläger aus, dass an dem Tag des Versterbens seines Vaters er durchaus SPAM-Nachrichten erhalten habe, dies aber zu diesem Zeitpunkt noch nicht durch Abspeichern dokumentiert hätte, da er sich hier noch nicht genug dabei gedacht hätte. Er datiert den Vorfall auf den 19. oder 20. Juli 2021. Es ist fernliegend, dass das Nutzungsverhalten des Klägers sich zum Zeitpunkt des 19./20. Julis maßgebend in einer Weise verändert hatte, die ein Versäumen der Anrufe bedingte, wenn die SPAM-Welle zu diesem Zeitpunkt noch nicht einmal seine besondere Aufmerksamkeit weckte.

Kausal ist demgemäß nur ein immaterieller Schaden aufgrund empfundener Belästigung durch SPAM. Insoweit stellt sich der Kontrollverlust hier als immaterieller Schaden dar, da der Kläger sich einem Rückgriff zahlreicher Unbekannter auf den von ihm zuvor sorgsam gehüteten Datenpunkt seiner Telefonnummer ausgesetzt sieht. Aufgrund dieser äußeren Umstände nachvollziehbar ist, dass der Kläger innerlich ein Ärgernis in der Form empfand, solche Nachrichten „wegklicken“ zu müssen. Während der SPAM-Wellen ist er in seinem Nutzungsverhalten des Mobiltelefons und in der Erreichbarkeit beeinträchtigt. Hierdurch hat sich bei dem Kläger eine gewisse Sorge gebildet, bei etwa medizinischen Notfällen schlechter erreichbar zu sein, als er es sonst wäre. Für diese Folgen erscheint ein Schmerzensgeld in Höhe von 300,00 EUR angemessen. Dieses gilt das etwaige Ärgernis darüber, dass der Kläger seine seit langer Zeit gehaltene Mobilfunknummer ändern muss oder abstrakt befürchten muss, dass eine weitere SPAM-Welle auf ihn

zukommt und von ihm inzwischen vorgesehene Gegenmaßnahmen erforderlich macht, mit ab. Das Schmerzensgeld ist in dieser Höhe aber auch ausreichend. Ausweislich des Beibehaltens der Telefonnummer, die der Kläger laut eigener Angaben in der mündlichen Verhandlung auch zukünftig nicht ändern will, hält sich die Furcht des Klägers, allein wegen SPAM sich von weiteren Familienmitgliedern nicht verabschieden zu können oder wichtige Informationen nicht zu erhalten, in Grenzen. Die SPAM-Belästigungen beschränkten sich auf die zwei Wellen, wobei die letzte hiervon mittlerweile etwa zwei Jahre zurückliegt.

Keine Erhöhung des Schmerzensgeldes rechtfertigt sich dadurch, dass der Kläger Furcht vor Straftaten aufgrund des Datenschutzvorfalls mit etwa materiellen Folgen leidet. Eine solche wäre, selbst unterstellt, dass sämtliche weiteren Datenpunkte, die laut Kläger veröffentlicht worden seien, tatsächlich betroffen sind, schlechthin nicht nachvollziehbar. Selbst mit dem bürgerlichen Namen des Klägers ist nicht ersichtlich, wie Betrüger hieraus Vorteile für entsprechende Straftaten ziehen können. Im Übrigen ist in dem von dem Kläger vorgelegten Datensatz nur die Angabe
vorhanden. Es ist davon auszugehen, dass dies das Pseudonym ist, zu dem er ausweislich seiner Angaben in der persönlichen Anhörung seinen Namen in dem Nutzerprofil geändert hat. Eine Beweiserhebung darüber, ob die weiteren, von der Beklagten bestrittenen Datenpunkte öffentlich wurden, kann unterbleiben.

Im Übrigen hat der Kläger selbst in der persönlichen Anhörung (anders als von seinen Prozessbevollmächtigten angeführt) verneint, dass er unter irgendeiner Furcht leidet.

b)
Ein weitergehender Zahlungsanspruch folgt aus keiner erdenklichen Rechtsgrundlage. Auch ein nationalrechtlicher Anspruch, etwa nach § 823 Abs. 1 BGB iVm Art. 2 Abs. 1, 1 Abs. 21 GG, wäre der Höhe nach auf ein angemessenes Schmerzensgeld begrenzt, das mit maximal 300,00 EUR zu bemessen ist.

c)
Die Zinsforderung wie tenoriert ab dem auf den 12.04.2023 folgenden Tag folgt aus §§ 291, 288 Abs. 1, analog 187 Abs. 1 BGB. Es kann ein früherer Tag der Zustellung mangels eines zur Akte gelangten Rückscheins nicht festgestellt werden.

2.

Der Antrag zu Ziffer 2.) ist unbegründet. Der Kläger hat keinen Anspruch auf die begehrte Feststellung, da die Entstehung zukünftiger materieller oder immaterieller Schäden kausal verursacht durch den streitgegenständlichen Vorfall ausgeschlossen ist. Es ist schlechthin undenkbar, dass Vermögensschäden durch Ausnutzung der bekannt gewordenen Daten, auch unterstellt, hierunter habe sich der Beziehungsstatus und Beruf „Eventer“ zusätzlich befunden, zu Vermögensstraftaten genutzt werden können bzw. hierfür in irgendeiner Weise Vorteile verschaffen. Das gilt umso mehr, als potentielle Täter nicht einmal über die Information des Namens des Klägers verfügen, das Pseudonym gibt hier wenig Aufschluss und dürfte den Kläger (bei dessen Angabe durch Täter) kaum zu Vermögensverfügungen bewegen. Derlei Schädigungen sind bei dem Kläger auch deshalb ausgeschlossen, da er selbst angibt, keine Furcht hiervor zu haben, mithin einräumt, dass für eine solche Selbstschädigung bei ihm keine Gefährdung besteht.

Zukünftige Kosten des Telefonnummerwechsels aufgrund des Vorfalls werden ebenfalls nicht entstehen, da der Kläger in der persönlichen Anhörung angegeben hat, diese nicht aufgrund desselben wechseln zu wollen.

Die Befürchtung des möglichen zukünftigen Eintritts weiterer SPAM-Wellen kann bei dem bereits zugesprochenen Schmerzensgeld berücksichtigt werden, was entsprechend geschehen ist. Sofern sich bei etwaigen zukünftigen Wellen ein anderweitiges, aktuell noch unvorhersehbares immaterielles Leid verwirklicht, führt dieses jedenfalls wegen eines den Verstoß der Beklagten vollständig zurückdrängenden Eigenverschuldens nicht zu einem Schmerzensgeldanspruch, § 254 BGB. Denn der Kläger hat sich bewusst dazu entschieden, den überschaubaren Aufwand eines Rufnummerwechsels nicht auf sich zu nehmen und durch diesen ein immaterielles Leid für die Zukunft mit Sicherheit zu unterbinden.

3.

Der Antrag zu Ziffer 3.) a. ist ebenfalls unbegründet.

Es besteht kein Rechtsschutzbedürfnis, insbesondere aber auch nicht die für einen Anspruch nach § 1004 Abs. 1 S. 2 BGB erforderliche Wiederholungsgefahr, das Vorliegen der übrigen Anspruchsvoraussetzungen unterstellt, da der Kläger die begehrte Sachlage, in dem er die Suchbarkeitsfunktion schlicht abstellt (bzw. die

Einstellung „nur ich“ anwählt) selbst herstellen kann. Der Kläger hat über dieses Instrument einen ausschließlichen Einfluss darauf, dass seine Telefonnummer in dem CIT und über die Suchfunktion nicht mehr in der hier beanstandeten Weise, weder aktuell, noch zukünftig, verwendet werden kann.

4.
Der Antrag zu Ziffer 4.) ist unbegründet. Der Kläger hat keinen Anspruch gegen die Beklagte auf Erteilung der Auskunft gem. Art. 15 Abs. 1 DSGVO.

Nach Art. 15 Abs. 1 lit. a) und c) hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und über die a.) Verarbeitungszwecke und über c.) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen.

Erfüllt ist der Auskunftsanspruch, 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 (vgl. BGH, Urteil vom 03.09.2020 – III ZR 136/18, juris, Rn. 43).

Hinsichtlich der im Schriftsatz vom 02.04.2024 nunmehr angegebenen Datenpunkte ist der Anspruch durch Erfüllung erloschen (vgl. § 362 Abs. 1 BGB). In diesem teilte die Beklagte nämlich mit, welche Datenpunkte nach ihrer Kenntnis und welche Datenpunkte nicht abgegriffen worden seien. Dadurch sollte auch erkennbar die gewünschte Auskunft erteilt werden. Im Übrigen behauptet der Kläger selbst eine weitergehende Betroffenheit unter Bezeichnung bestimmter Daten, worauf er bereits eine Leistungsklage stützte, ohne etwa das Auskunftsverlangen im Wege der Stufenklage voranzustellen. Über die begehrten Informationen verfügte er offensichtlich bereits, potentiell sogar umfassender, als die Beklagte selbst. Diesbezüglich bestand kein Rechtsschutzbedürfnis für ein Auskunftsverlangen.

Insoweit der Kläger verlangt, dass ihm Auskunft auch im Hinblick auf Zeit und Orte der Veröffentlichung durch Dritte und Anzahl der Empfänger und Zeit des Abgreifens im Hinblick auf den Empfänger sowie den Zeitpunkt des Zugriffs auf die Daten nach Art. 15 Abs. 1 lit.c DSGVO nicht erfüllt wurde, so ist der Beklagte die Beantwortung dieser Auskunft unmöglich i.S.d. § 275 Abs. 1 BGB. Dies liegt in der Natur des Scraping als unbefugtes „Sammeln“ der Daten von außen begründet. Selbiges gilt für die konkretere Auskunftserteilung hinsichtlich des zeitlichen Abrufens der Datenpunkte. Die Nachfrage nach zukünftig beabsichtigten Maßnahmen der Beklagten zum Datenschutz ist bereits tatbestandlich nicht von Art. 15 DSGVO erfasst.

5.
Ein Anspruch auf Ersatz vorgerichtlicher Anwaltskosten steht dem Kläger in Höhe von 90,96 EUR errechnet aus dem Gegenstandswert der begründeten Hauptforderung zu. Ein Anspruch folgt hier unmittelbar aus Art. 82 DSGVO iVm §§ 249 ff. BGB. Der Verstoß gegen Art. 82 DSGVO, der hier gegeben ist (s.o.), führt zu einem Ersatzanspruch hinsichtlich materieller Schäden, wozu insbesondere die Kosten der Rechtsverfolgung gehören (Paal, MMR 2020, 14, 16). In der Höhe, in der die Schadensfolgen bei dem Kläger einen Schmerzensgeldanspruch rechtfertigten, ist die Aufwendung der Kosten auch erforderlich gewesen im Sinne des § 249 Abs. 1 BGB. Hinsichtlich der überschießenden Kosten besteht ein Anspruch aus keiner erdenklichen Rechtsgrundlage.

Aus der Position der Anwaltskosten, soweit der Anspruch besteht, kann der Kläger Ersatz von Rechtshängigkeitszinsen wie tenoriert verlangen, §§ 291, 288 Abs. 1, analog 187 Abs. 1 BGB.

III.
Die prozessualen Nebenentscheidungen folgen aus §§ 92 Abs. 2 Nr. 1, 708 Nr. 11, 711 ZPO.

IV.
Der Streitwert wird festgesetzt auf 4.050,00 EUR.

Der Streitwert setzt sich wie folgt zusammen:

Antrag zu Ziffer 1.): 1.000,00 EUR

Antrag zu Ziffer 2.) (Feststellungsantrag): 800,00 EUR

Anträge zu Ziffer 3.) a. und b (Unterlassungsanträge).: 1.500,00 EUR (750,00 EUR je Unterlassungsantrag)

Antrag zu Ziffer 4.) (Auskunftsantrag): 750,00 EUR

Der Antrag zu Ziffer 5.) wirkt sich nicht streitwerterhöhend aus, § 43 Abs. 1 GKG.