Abschrift

6 O 65/22

Landgericht Hagen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted]

Klägers,

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

gegen

Meta Platforms Ireland LimitedFacebook Ireland Ltd., vertr. d. d. Gf. (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields und Partner,
Bockenheimer Anlage 44, 60322 Frankfurt,

hat die 6. Zivilkammer des Landgerichts Hagen
auf die mündliche Verhandlung vom 27.04.2023
durch die Vorsitzende Richterin am Landgericht Dr. [redacted], die Richterin am Landgericht [redacted] und die Richterin [redacted]

für Recht erkannt:

1. **Die Beklagte wird verurteilt, an den Kläger 350,00 € nebst Zinsen seit dem 30.09. 2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen.**

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 an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene 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 zur Sicherung eines angemessenen Schutzniveaus geeigneten, erforderlichen und angemessenen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der individuellen Kontaktaufnahme zu verhindern.**

4. **Die Beklagte wird verurteilt, dem Kläger Auskunft darüber zu erteilen, durch welche Empfänger personenbezogene Daten des Klägers bei der Beklagten durch den Scraping-Vorfall im Jahr 2019 erlangt wurden.**

5. **Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 367,23 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 26.07.2022 zu zahlen.**

   Im Übrigen wird die Klage abgewiesen.

6. **Von den Kosten des Rechtsstreits tragen der Kläger 53 % und die Beklagte 47 % Prozent.**

7. **Das Urteil ist vorläufig vollstreckbar. Hinsichtlich des Tenors zu Ziffer 3 und 4 aber nur gegen Sicherheitsleistung der Klägers in Höhe von 2.500,00 €. Im Übrigen wird der Beklagten nachgelassen, die Vollstreckung durch den Kläger gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.**

8. **Der Streitwert wird auf 6.500,00 € festgesetzt.**

Tatbestand:

Die Parteien streiten über Ansprüche auf Schadensersatz, Unterlassung, Auskunft und Nebenforderungen aufgrund behaupteter Verstöße der Beklagten gegen die Datenschutzgrundverordnung (DS-GVO) im Zusammenhang mit einem sog. „Scraping-Vorfall" bei der Beklagten.

Der Kläger nutzt das soziale Netzwerk Facebook, das auf dem Gebiet der Europäischen Union von der Beklagten betrieben wird und auf das sowohl über die Website www.facebook.com als auch über die gleichnamige App zugegriffen werden kann. Die Plattform ermöglicht es Nutzern, persönliche Profile für sich zu erstellen, auf denen diese Angaben zu ihrer Person machen und diese mit Freunden teilen können.

Auf ihren persönlichen Profilen können die Nutzer Angaben zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Die Beklagte stellt dabei Tools und Informationen zur Verfügung, damit Nutzer ihre Privatsphäre auf der

Facebook-Plattform verwalten können. Damit Nutzer leichter mit anderen Nutzern in Kontakt treten können, müssen sie bestimmte Informationen bei der Registrierung angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und Nutzer-ID. Eine Eingabe der Handynummer ist nicht zwingend erforderlich. Hinsichtlich der weiteren Daten gibt es im Rahmen der Privatsphäre-Einstellungen Wahlmöglichkeiten für jeden Nutzer. Bei der sogenannten "Zielgruppenauswahl" legt der Nutzer fest, wer einzelne Informationen auf seinem Facebook-Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann. So kann der Nutzer anstelle der standardmäßigen Voreinstellung "öffentlich" auswählen, dass nur "Freunde" auf der Plattform, oder "Freunde von Freunden" die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird insoweit gesondert behandelt, als dass die Standard-Einstellung auf „Freunde“ voreingestellt ist.

Die "Suchbarkeits-Einstellungen" legen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann. Wenn also ein Nutzer in seinem Smartphone eine Telefonnummer als Kontakt eingespeichert hat, erlaubt ihm die Beklagte, seine Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Dafür war nicht erforderlich, dass der andere Nutzer seine Telefonnummer nach der "Zielgruppenauswahl" öffentlich gemacht hat. 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. Die "Suchbarkeits-Einstellung" war bei dem Kläger seit dem 12.01.2010 auf "Alle" eingestellt (Anl. B17).

Auf der Anmeldeseite findet sich eine Verlinkung auf die „Datenrichtlinie“ der Beklagten. Hinsichtlich der konkreten Inhalte wird auf Anlage B9 (Bl. 232 ff. d. A.) Bezug genommen. Im Hilfebereich der Website der Beklagten finden sich zu den „öffentlichen Informationen“ die in Anl. B 1 (Bl. 221 ff. d. A.) niedergelegten Informationen, die für weitere Einzelheiten in Bezug genommen werden. Die Handhabung der Privatsphäre-Einstellungen ergibt sich aus den Abbildungen in der Klageschrift (Bl. 10 ff. d.A.).

In der Facebook-Messenger-App bestand für die Nutzer die Möglichkeit, mithilfe eines „Contact-Import-Tools" (im Folgenden: „CIT") ihre auf dem Handy befindlichen Telefonkontakte auf Facebook hochzuladen, um diese automatisch auf der

Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, ohne dass deren im Profil hinterlegte Nummer in der "Zielgruppenauswahl" öffentlich gemacht worden wäre.

Anfang April 2021 wurden Daten von diversen Facebook-Nutzern im Internet veröffentlicht. Bei diesem Vorfall nutzten Dritte die o.g. Importfunktion dergestalt, dass sie eine Vielzahl von (massenhaft selbst generierten) Kontakten in ein virtuelles Adressbuch mit Nummer eingaben, um sodann mittels der Importfunktion das Vorhandensein eines Nutzers mit entsprechender Telefonnummer zu beproben und die Nummer mit den weiteren vorhandenen Daten des Nutzers zu korrelieren (sog. Scraping). Die Beklagte informierte die zuständige Datenschutzbehörde, die Irish Data Protection Commission (DPC), nicht unverzüglich über den Vorfall.

Vorgerichtlich forderte der Kläger die Beklagte mit Email seiner Prozessbevollmächtigten vom 13.10.2021 zur Zahlung von 500,00 € Schadenersatz, Unterlassung der zukünftigen Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunftserteilung auf (Anl. K1). Mit Schreiben vom 04.11.2021 (Anl. B16) wies die Beklagte die Schadenersatz- und Unterlassungsansprüche zurück und teilte mit, dass sich unter den abgegriffenen und veröffentlichten Daten auch jene des Klägers befunden hätten und wo der Kläger seine Daten finde.

Am 28.11.2022 verhängte die irische Datenschutzbehörde (DPC) mit Blick auf den Vorfall gegen die Beklagte eine Geldbuße in Höhe von 265 Mio. Euro und begründete dies insbesondere mit einem Verstoß gegen Art. 25 Abs. 1 und 2 DSGVO.

Der Kläger behauptet, seine persönlichen Daten wie Telefonnummer, Name, Wohnort, und E-Mailadresse seien durch "Scraping" abgegriffen worden. Ob noch mehr Daten entwendet worden seien, lasse sich mangels ausreichender Auskunft durch die Beklagte noch nicht angeben. Grundsätzlich seien von dem Vorfall Nutzerdaten wie Telefonnummer Facebook-ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten betroffen. Die entsprechenden personenbezogenen Daten, wie auch diejenigen des Klägers, seien sodann im Internet auf Seiten, die illegale Aktivitäten wie Internetbetrug begünstigen sollen, so z.B. in dem " Hacker-Forum" raid.com, veröffentlicht worden. Sie würden insbesondere für gezielte Phishing-Attacken

genutzt. Auf einer im Darknet für jedermann abrufbaren Datenbank seien Telefonnummer, Facebook-ID, Name, Geschlecht, Wohnort und Arbeitsstätte des Klägers zugänglich gemacht worden. Zum jetzigen Zeitpunkt könne noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten des Klägers erhalten hätten.

Die Unbekannten hätten die Daten mittels des "CIT" aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert. Die Telefonnummern der Nutzer hätten wegen einer Sicherheitslücke massenhaft mit den restlichen Personendaten korreliert werden können, ohne dass die hinterlegten Telefonnummern öffentlich freigegeben gewesen seien. Den Scrapern sei es möglich gewesen, die Daten des Nutzers abzufragen und zu exportieren.

Das „Scraping" sei dadurch ermöglicht worden, dass die Beklagte keinerlei bzw. unzureichende Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Contact-Import-Tools z.B. durch Bots zu verhindern. So seien keine Sicherheitscaptchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die individuelle Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage im Rahmen eines massenhaften Geschehens handelt. Ein Mechanismus zur Überprüfung der Plausibilität der Anfragen sei nicht bereitgehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummernabfragen (z.B. 000001, 000002 usw.) sei durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich, angemessen und üblich. Die Beklagte hätte die maximale Anzahl mit dem CIT abgleichbarer Rufnummern begrenzen können. Die Voreinstellung (default) für die Suchbarkeit nach Rufnummern hätte auf „ Freunde-Freunde" stehen müssen. Ein Monitoring- und Alarmierungssystem habe gefehlt, das bei Upload von sehr großen Adressbuchchargen eine Information zum Einleiten von Maßnahmen gegeben habe. Mindestens aber ein expliziter Hinweis auf die "offenen" Standard-Einstellungen für die Suchbarkeit per Telefonnummer habe gefehlt, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers.

Überdies seien die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich kaum sichere Einstellungen erreichen könne.

Die Beklagte handele aufgrund der datenschutzunfreundlichen Standard-Voreinstellungen entgegen dem Prinzip der Datenminimierung und des "privacy by

default"-Grundsatzes. Die versteckte Option, dass der Nutzer nicht anhand seiner Telefonnummer von der Öffentlichkeit gefunden werden möchte, sei aufgrund der vielschichtigen Einstellungsmöglichkeit nicht zu erreichen, wenn lediglich nach den Einstellungsmöglichkeiten für die Sichtbarkeit der Telefonnummer gesucht werde.

Die Einstellungen der Messenger-App seien unabhängig von denjenigen im sonstigen Facebook-Dienst. Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolge nicht.

Die Beklagte habe ihre Nutzer nicht hinreichend über die ihr bekannten Gefahren informiert, insbesondere fehle der Hinweis, dass unberechtigte Dritte öffentlich zugängliche Daten leicht mit Hilfe von „Facebook-Tools" anreichern und diese im Darknet veröffentlichen könnten und dass die Beklagte die betroffenen Personen nicht über solche Vorfälle informiere.

Der Kläger behauptet, die Veröffentlichung ihrer Daten habe weitreichende Folgen für ihn. Er habe einen erheblichen Kontrollverlust über seine Daten erlitten, welcher großes Unwohlsein und große Sorge über einen möglichen Missbrauch der sie betreffenden Daten ausgelöst habe. Er habe ein verstärktes Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen entwickelt und seit April 2021 vermehrt dubiose Nachrichten erhalten. Er könne nur noch mit äußerster Vorsicht auf E-Mails und Nachrichten reagieren.

Es könne zudem zum jetzigen Zeitpunkt noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten der klagenden Partei erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden. Folgen von Datenschutzverletzungen würden sich ihrem Wesen nach erst spät zeigen und lange unerkannt bleiben. Es erscheine auf Grund der Veröffentlichung der Telefonnummern möglich, dass der Kläger auch künftig durch eine Vielzahl betrügerischer Anrufe belästigt werde.

Die Beklagte habe ihre Auskunftsverpflichtung nicht erfüllt.

Ferner habe die Beklagte als Verantwortliche i.S.d. DSGVO die Klägerseite betreffende personenbezogene Daten ohne Rechtsgrundlage verarbeitet.

Die Beklagte habe weder die Klägerseite noch die Aufsichtsbehörde in ausreichendem Maße und rechtzeitig über die Verarbeitung sie betreffender personenbezogener Daten informiert bzw. aufgeklärt.

Ursprünglich hat der Kläger unter Ziff 3 a.) unter anderem beantragt, die Beklagte zu verurteilen, es zu unterlassen, personenbezogenen Daten des Klägers 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.

Nach Hinweis des Gerichts zu Antrag Ziff. 3 a.) beantragt der Kläger nunmehr,

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

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

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, 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, Facebook-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die zur Sicherung eines angemessenen Schutzniveaus geeigneten, erforderlichen und angemessenen 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 zu verurteilen, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte behauptet, sie stelle ihren Nutzern alle in der DS-GVO festgelegten Informationen hinsichtlich der Datenverarbeitung zur Verfügung, daher sei ein Verstoß gegen Transparenzpflichten bereits im Grundsatz zu verneinen.

Zur Bekämpfung von „Scraping" habe sie Übertragungsbegrenzungen /-beschränkungen und eine Bot-Erkennung eingerichtet, diese auch fortlaufend weiterentwickelt und ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren beschäftigt. Im April 2018 habe sie die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion deaktiviert. Zudem habe sie die Übertragungsbeschränkungen innerhalb der Kontakt-Importer-Funktion gesenkt, auch wenn sie zu diesem Zeitpunkt keine Scraping-Aktivität über diese Funktion festgestellt habe. Sie habe Captcha-Abfragen genutzt. Ferner gehe die Beklagte mittels Unterlassungsaufforderungen, Kontosperrungen und

Gerichtsverfahren gegen „Scraper" und Hosting-Anbieter, also Unternehmen, auf deren Systemen die Daten zur Verfügung gestellt werden, vor.

Die im Internet erfolgte Veröffentlichung von Daten des Klägers habe sich nicht signifikant auf das ohnehin bestehende Risiko der Cyber-Kriminalität ausgewirkt. Es sei Teil des allgemeinen Lebensrisikos, Opfer von Internetkriminalität beziehungsweise Identitätsdiebstahl zu werden. Beim Kläger seien lediglich NutzerID, Vorname, Land und Geschlecht betroffen gewesen, wobei das Land wohl eher der Telefonnummer entnommen worden sei.

Hinsichtlich der Standardeinstellungen sei außerdem der Zweck der Facebook-Plattform maßgebend. Dieser liege gerade darin, Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden. Daher seien die Funktionen gezielt so konzipiert, dass sie den Nutzern helfen, andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Melde- oder Benachrichtigungspflichten hätten die Beklagte nicht getroffen, da es bereits an einer Verletzung der Sicherheit bzw. an einer unbefugten Offenlegung von Daten fehle, welche eine derartige Verpflichtung auslösen könnten.

Die Beklagte ist der Auffassung, Auskunft sei schon hinreichend erteilt worden. Zur Beantwortung von Fragen betreffend die Verarbeitungstätigkeiten Dritter sei die Beklagte nach Art. 15 DSGVO rechtlich nicht verpflichtet.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze der Parteien nebst Anlagen Bezug genommen.

Die Kammer hat den Kläger persönlich angehört. Wegen des Ergebnisses der Parteianhörung wird auf das Protokoll der mündlichen Verhandlung vom 27.04.2023 Bezug genommen.

Entscheidungsgründe:

Die Klage ist zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet.

I.

Die Klage ist — mit Ausnahme des Antrags Ziffer 3 b), dem das Rechtsschutzbedürfnis fehlt — zulässig.

1.

Das Landgericht Hagen ist für sämtliche Anträge international, örtlich sowie sachlich zuständig.

a)

Die internationale und örtliche Zuständigkeit deutscher Gerichte folgt aus Art. 79 Abs. 2 S. 2 DS-GVO, der die Vorschriften der EuGVVO verdrängt (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, Art. 79 DS GVO Rn. 33). Danach können Klagen gegen einen Verantwortlichen — von einiegen hier nicht relevanten Ausnahmen abgesehen — wahlweise auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat. Der Kläger hat seinen Wohnsitz im Bezirk des Landgerichts Hagen, mithin in der Bundesrepublik Deutschland.

b)

Das Landgericht Hagen ist auch gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG für die Klagen sachlich zuständig. Der Streitwert liegt nach Bewertung der hinter den Anträgen stehenden Interessen bei 6.500,00 €, mithin über 5.000,00 €.

Der Streitwert für den Klageantrag Ziffer 1 ergibt sich aus dem vom Kläger vorgestellten (Mindest-)Schadensersatzbetrag in Höhe von 1.000,00 €. Der auf Feststellung gerichtete Klageantrag Ziffer 2 ist ebenso wie der auf Auskunft gerichtete Klageantrag Ziffer 4 mit 500,00 € anzusetzen. Beides erscheint mit Blick auf das bisher verfolgte Leistungsinteresse in Höhe von 1000,00 € Schadensersatz angemessen. Schließlich beträgt der Streitwert für die Unterlassungsanträge in Ziffer 3 im Gesamten 4.500,00 €. Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist letztlich anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen (vgl. Musielak/Voit/Heinrich, 19. Aufl. 2022, ZPO § 3 Rn. 36). Bei der Beklagten handelt es sich um einen multinationalen Konzern mit hohen Umsätzen, die Bedeutung der Sache ist auf Grund der Vielzahl der vom Scraping betroffenen Personen für die Beklagte erheblich.

2.

Die Klageanträge zu Ziffer 1 und 3 sind hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

a)

Die Bemessung des immateriellen Schadenersatzes unter Ziffer 1 stellt der Kläger zulässig in das Ermessen des Gerichts. Der unbezifferte Klageantrag ist zulässig, wenn statt der Bezifferung mindestens die Größenordnung des Betrags, den der Kläger sich vorstellt, angegeben wird (h.M., vgl. MüKoZPO/Becker-Eberhard, 6. Aufl. 2020, ZPO § 253 Rn. 121). Dem ist der Kläger nachgekommen, indem er einen Mindestbetrag in Höhe von 1.000,00 € genannt hat.

Entgegen der Auffassung der Beklagten liegt auch keine unzulässige alternative Klagehäufung vor. Eine solche ist gegeben, wenn der Kläger mehrere Streitgegenstände mit der Maßgabe geltend macht, dass das Gericht wahlweise einem dieser Begehren stattgeben soll und das jeweils andere Begehren dann nicht mehr beschieden werden muss, wobei die Prüfungsreihenfolge nicht vom Kläger vorgegeben wird (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 260 Rn. 12; MüKoZPO/Becker-Eberhard, 6. Aufl. 2020, ZPO § 260 Rn. 22).

Eine solche Konstellation liegt hier indessen nicht vor. Die Kammer hatte hier nur einen Lebenssachverhalt zu beurteilen, nämlich denenigen, ob die Beklagte vor dem Scraping durch Dritte im April 2021 mangelhafte Datenschutzvorkehrungen getroffen hatte bzw. ihre Nutzer unzureichend bzw. intransparent informiert hat. Hierbei mag es sich mit Blick auf die Eingabe von Daten zum Zeitpunkt der Anmeldung und die erforderlichen Belehrungen und Voreinstellungen über den streitgegenständlichen Scraping-Vorfall bis hin zu einer etwaig pflichtwidrigen Unterlassung um einen längeren Zeitraum handeln, verknüpft sind sämtliche Einzelaspekte dieses Vorgangs aber durch die Daten, die der Kläger bei der Registrierung hinterlegt hat. Eine Aufspaltung in mehrere Abschnitte stellte eine unnatürliche Trennung eines einheitlichen Sachverhaltes dar.

b)

Auch der Klageantrag zu 3.a.) weist die erforderliche Bestimmtheit auf, § 253 Abs. 2 Nr. 2 ZPO.

Nach der ständigen höchstrichterlichen Rechtsprechung darf ein Verbotsantrag im Hinblick auf § 253 Abs. 2 Nr. 2 ZPO nicht derart undeutlich gefasst sein, dass

Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts (§ 308 ZPO) nicht erkennbar abgegrenzt sind, sich die Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was der Beklagten verboten ist, dem Vollstreckungsgericht überlassen bleibt. Aus diesem Grund sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen.

Eine ausreichend bestimmte Antragsformulierung ist jedoch dann hinzunehmen, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urt. v. 26.1.2017 – I ZR 207/14).

Daran gemessen weist der Klageantrag zu 3. a.) eine ausreichende Bestimmtheit auf.

Selbst bei einer Benennung derzeitiger möglicher Sicherheitsmaßnahmen würde dies in Anbetracht der technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping – Angriffen vorbeugen. Die gesetzlich vorgeschrieben Sicherheitsstandards einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen.

3.

Auch das für den Klageantrag Ziffer 2 erforderliche Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt vor.

Ein Feststellungsantrag ist bereits dann zulässig, wenn die Schadensentwicklung noch nicht gänzlich abgeschlossen und der Kläger aus diesem Grund nicht im Stande ist, seinen Anspruch ganz oder teilweise zu beziffern (OLG Hamm, Urteil vom 21.05.2019 — 9 U 56/18). Das Feststellungsinteresse ist daher nur dann zu verneinen, wenn aus der Sicht des Geschädigten keinerlei Besorgnis besteht, zumindest mit dem Eintritt eines Schadens zu rechnen (vgl. BGH, Beschluss vom 09. Januar 2007 - VI ZR 133/06 -, juris; BGH, Urteil vom 16. Januar 2001 - VI ZR 381/99 -, juris; Saarländisches Oberlandesgericht Saarbrücken, Urteil vom 20. Februar 2014 - 4 U 411/12, Rn. 46, juris, m.w.N.).

Unter Berücksichtigung des Umstandes, dass die im Wege des „Scrapings“ erlangten personenbezogenen Daten im Internet veröffentlicht worden sind, erscheint es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger aufgrund der Veröffentlichung der Telefonnummer und weiterer persönlicher Daten wie seinem Namen im Internet zu künftigen Schäden, etwa durch betrügerische Anrufe, kommt.

Dem Feststellungsinteresse steht bezogen auf bereits entstandene, dem Kläger aber noch nicht bekannte materielle Schäden nicht der Vorrang der Leistungsklage entgegen. Aufgrund der Veröffentlichung der personenbezogenen Daten des Klägers im Internet ist nicht auszuschließen, dass dessen Daten bereits zu illegalen Zwecken verwendet worden sind, dies dem Kläger allerdings derzeit noch unbekannt geblieben ist.

4.

a)

Dem Klageantrag zu 3.a.) fehlt auch nicht das Rechtsschutzbedürfnis. Das Rechtschutzbedürfnis ist gegeben, wenn der Rechtssuchende ein berechtigtes Interesse daran hat, gerichtliche Hilfe in Anspruch zu nehmen, d.h. sein Ziel nicht auf einem einfacheren, billigeren Weg erreichen kann.

Zwar kann der Kläger durch die Anpassung der Privacy-Einstellungen die Suchbarkeit über die Telefonnummer deaktivieren. Dieses genügt aber nicht, um eine zukünftige unrechtmäßige Datenverarbeitung zu verhindern, da der Kläger keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat.

b)

Anders stellt sich dies aber im Hinblick auf den Antrag zu 3.b.) dar.

Soweit der Kläger von der Beklagten fordert, seine Telefonnummer nicht mehr auf der Grundlage einer unaufgeklärt erteilten Einwilligung zu verarbeiten, fehlt ihm dafür zum jetzigen Zeitpunkt das Rechtsschutzbedürfnis (Klagantrag zu 3.b.).

Selbst wenn der Kläger grundsätzlich an der weiteren Verarbeitung seiner Telefonnummer durch die Beklagte interessiert ist, diese also nicht aus seinem Profil löschen möchte, was wiederum ein einfacherer Weg zur Rechtsdurchsetzung wäre, verlangt er von der Beklagten eine Aufklärung über die Art und Weise der

Verarbeitung seiner Nummer, obwohl ihm diese mittlerweile bekannt ist und er diese selbst in seinem Klageantrag beschreibt. Mit dem Begehren, dass ihn die Beklagte nochmals über etwas informieren soll, das er selbst beschreibt, vermag der Kläger keinerlei schutzwürdigen Vorteil zu erlangen. Ihm ist spätestens aus dem hiesigen Verfahren bekannt, wie seine Telefonnummer verarbeitet wird (so auch LG Heidelberg, Urteil vom 31.03.2023 – 7 O 142/22). Damit verfügt er über eine hinreichende Grundlage, zu entscheiden, ob er mit deren Weiterverarbeitung durch die Beklagte einverstanden ist oder nicht. Eine Klage auf Unterlassung führt ihn nicht weiter.

II.

Die Klage ist — soweit sie zulässig ist — in der Sache nur teilweise erfolgreich. Der Kläger hat Anspruch gegen die Beklagte auf Ersatz immateriellen Schadens in Höhe von 350,00 € nebst Zinsen (1. und 2.), auf Feststellung der Erstzpflicht bzgl. etwaigen zukünftigen materiellen Schadens (3.), auf Unterlassen im tenorierten Umfang (4.), auf Auskunft in beschränktem Umfang (5.) sowie auf Zahlung außergerichtlicher Rechtsanwaltskosten nebst Zinsen (6.). Hinsichtlich der weitergehenden Ansprüche ist die Klage abzuweisen.

1.

Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz i.H.v. 350,00 € aus Art. 82 Abs. 1 DSGVO zu. Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

a)

Zur Überzeugung der Kammer hat die Beklagte als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO gegen mehrere Vorschriften aus der Datenschutzgrundverordnung verstoßen.

(1)

Die Beklagte ist der ihr nach Art. 13 DSGVO auferlegten Informations- und Aufklärungspflicht nicht in vollständigem Umfang nachgekommen. Die Kammer vermochte nicht festzustellen, dass die Beklagte den Kläger zum Zeitpunkt der Datenerhebung seiner Mobilfunknummer hinreichend über die Zwecke der Verarbeitung seiner Mobilfunknummer aufgeklärt hat.

Die Verletzung der nach Art. 13 DSGVO bestehenden Informations- und Aufklärungspflichten ist vom Anwendungsbereich des Schadensersatzanspruches des Art. 82 DSGVO erfasst.

aa)

Ein Schadensersatzanspruch nach Art. 82 DSGVO kann nur dann begründet werden, wenn nach dessen Absatz 2 Satz 1 ein Schaden durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde, auch wenn Art. 82 Abs. 1 DSGVO vom Wortlaut her jeden Verstoß gegen die Verordnung ausreichen lässt. Dass nur Verstöße relevant sein sollten, die bei der Datenverarbeitung unterlaufen, ergibt sich aus dem Umstand, dass ansonsten die Verordnung einen umfassenden Schadensersatzanspruch konstatieren würde, für den allerdings niemand voll umfänglich einzutreten hätte. Dies ergibt sich zudem aus der Systematik, wonach Abs. 3 der Regelung eine Exkulpation für die Haftung nach Abs. 2 der Norm vorsieht (hierfür auch Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 8; Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 7).

Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen die Informations- und Aufklärungspflichten des Art. 13 DSGVO bereits mit der Erhebung personenbezogener Daten. Bereits zu diesem Zeitpunkt hat der Verantwortliche – wie noch auszuführen sein wird – gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen. Bildet – wie hier – die Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a) DSGVO die Grundlage des Datenerhebungs- und somit auch des Datenverarbeitungsvorganges, kann eine solche Einwilligung unter Berücksichtigung der in der DSGVO vorherrschenden Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten keinen Bestand haben, wenn dem Betroffenen nicht bereits bei Datenerhebung sämtliche nach Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden.

bb)

Art. 13 Abs. 1 c) DSGVO verlangt bei der Erhebung personenbezogener Daten bei der betroffenen Person, dass der Verantwortliche der Person zum Zeitpunkt der Erhebung der Daten die Zwecke mitteilt, für die die personenbezogenen Daten verarbeitet werden sollen. Dabei sind alle Zwecke anzugeben, welche die verantwortliche Stelle im Zeitpunkt der Erhebung verfolgt (Cola/Heckmann/Franck, 3. Aufl. 2022, DS-GVO Art. 13 Rn. 12). Die Informationspflicht aus Art. 13 DS-GVO soll die betroffenen Personen von Beginn an in die Lage versetzen, bestimmen und einschätzen zu können, wer was wann über sie weiß (Sydow/Marsch DS-GVO/BDSG/Ingold, 3. Aufl. 2022, DS GVO Art. 13 Rn. 8). Nach ihrem Zweck müssen die Informationspflichten (ggf. unmittelbar) vor Beginn der Datenerhebung erfüllt werden. Denn die Informationen sollen der betroffenen Person auch ermöglichen, darüber zu entscheiden, ob sie in die Verarbeitung ihrer Daten einwilligt bzw. ob sie hiergegen Einwände erhebt.

Eine Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO kann nicht bereits darin gesehen werden, dass seitens der Beklagten kein Hinweis bei Erhebung der Daten der Mobilfunknummer des Klägers erfolgt ist, dass bei der gemäß der Voreinstellung für „alle“ freigegebenen Mobilfunknummer die Möglichkeit einer missbräuchlichen Datenabgreifung besteht. Es besteht schon nicht eine dahingehende Informations- und Aufklärungspflicht auf Seiten der Beklagten. Diese Möglichkeit ist der Risikosphäre der betroffenen Person zuzuordnen, da dem Risiko einer missbräuchlichen Verwendung von persönlichen Daten zwangsläufig jede Person ausgesetzt ist, die ihre persönlichen Daten im Internet preisgibt bzw. diese in sozialen Netzwerken teilt.

Die Beklagte hat den Kläger allerdings bei Erhebung der Daten seiner Mobilfunknummer unzureichend über den Zweck der Verwendung seiner Mobilfunknummer für das seitens der Beklagten verwendete Contact-Import-Tool (kurz: CIT) aufgeklärt. Hierdurch hat sie ihre Informations- und Aufklärungspflichten nach Art. 13 Abs. 1 lit. c) DSGVO verletzt.

Eine solche Aufklärung kann weder bei Hinzufügen der Mobilfunknummer im Rahmen der Registrierung unter Bezugnahme der Datenrichtlinie noch bei späterem Hinzufügen der Mobilfunknummer in der Rubrik „Handy-Einstellungen“ festgestellt werden.

Der Datenrichtlinie lässt sich eine Aufklärung über das von der Beklagte verwendete CIT nicht entnehmen.

Der mit der Anlage B9 (Bl. 234 ff. d.A.) überreichten Datenrichtlinie aus dem Jahr 2018 lässt sich auf den Seiten 3 und 4 unter der Überschrift „Wie verwenden wir diese Informationen“ entnehmen, dass die von einem Benutzer bereitgestellten Informationen zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommunikation mit dem die Informationen bereitstellenden Benutzer, zum Anzeigen und Messen von Werbeanzeigen und Diensten sowie zur Förderung der Sicherheit verwendet werden. Ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT erfolgt nicht.

Auch den Hinweisen auf den Seiten 5 und 6 der Datenrichtlinie unter der Überschrift „Wie werden diese Informationen geteilt“ lässt sich ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT nicht entnehmen.

Dass die Beklagte den Kläger über das durch sie verwendete CIT aufgeklärt hat, lässt sich auch nicht der Rubrik „Handy-Einstellungen“ sowie der Unterverlinkung durch einen Klick auf „Mehr dazu“ entnehmen.

Dort findet sich die Aufklärung seitens der Beklagten über die Verwendung der Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“. Zum anderen erfolgt der Hinweis, dass durch das Hinzufügen der Mobilfunknummer eben diese mit dem Benutzerkonto verknüpft ist und der jeweilige Benutzer festlegen kann, welche Personen dessen Mobilfunknummer sehen können und welche Personen auf Facebook nach der betroffenen Person suchen können. Ein weitergehender Hinweis, dass die betroffene Person durch das CIT der Beklagten im Wege eines Kontaktabgleichs durch Eingabe einer Mobilfunknummer gefunden werden kann, lässt sich den Einstellungen gerade nicht entnehmen.

Ein Hinweis auf die Verwendung des CIT lässt sich ferner nicht den auszugsweise dem Hilfebereich entnommenen Informationen (Anlagen B5 und B6), entnehmen.

Ungeachtet dessen, dass es auf die Informationen im Hilfebereich schon nicht ankommen dürfte, da die Datenerhebung – entweder durch Hinzufügen der Mobilfunknummer bei der Registrierung oder bei den „Handy-Einstellungen“ – bereits erfolgt ist und eine Aufklärung wie bereits ausgeführt unterblieben ist, findet sich auch in diesem Bereich kein Hinweis auf die Verwendung des CIT.

(2)

Die Beklagte als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO verstieß aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des CIT auch gegen Art. 32, 24, 5 Abs. 1 f) DSGVO.

Gem. Art. 32 Abs. 1 Hs. 1 DSGVO haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diesen Anforderungen genügten die beklagtenseits behaupteten Schutzmaßnahmen nicht.

Ziel von Art. 32 DSGVO ist die Gewährleistung eines dem Risiko angemessenen Schutzniveaus. Es sind daher nicht alle theoretisch möglichen Maßnahmen zur Gewährleistung von Datensicherheit zu ergreifen, sondern nur solche, die als verhältnismäßig anzusehen sind. Denn die DSGVO verlangt keine Datensicherheit um jeden Preis, sondern es muss eine Abwägung zwischen Schutzzweck und Aufwand vorgenommen werden (OLG Stuttgart, Urteil vom 31. März 2021 — 9 U 34/21 —, Rn. 54, juris; Dr. Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DSGVO) / Bundesdatenschutz-gesetz (BDSG), Artikel 32 Sicherheit der Verarbeitung, Rn. 3; BeckOK DatenschutzR/Paulus, 42. Ed. 1.11.2021, DSGVO Art. 32 Rn. 7). Dem Adressaten bleibt daher unter Berücksichtigung der in Abs. 1 vorgegebenen Abwägungskriterien ein Ermessensspielraum (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 10)

Angesichts des Umstands, dass das Risiko unbefugten Zugangs zu personenbezogenen Daten durch Scraping-Aktionen schon nach dem eigenen Vorbringen der Beklagten vergleichsweise hoch lag, da es sich um „gängige“ Techniken unbefugter Dritter zur Datenabgreifung im Internet handelte, und die Nutzung des Kontaktimporttools einen simplen Mechanismus zur Auslesung durch automatisierte Verfahren darstellte, mussten die organisatorischen Verhinderungsmaßnahmen relativ stark ausgeprägt sein; denn grundsätzlich gilt, dass je höher das Risiko und drohende Schäden sind, desto wirksamer die Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO ausfallen müssen (vgl. VG Mainz, Urteil v. 17.12.2020 – 1 K 778/19) .

Den Anforderungen des Art. 32 Abs. 1 und 2 DSGVO ist die Beklagte nicht hinreichend nachgekommen. Dies hat der Kläger unter Aufzeigung verschiedener technischer Möglichkeiten substantiiert vorgetragen. Die Beklagte trifft insoweit eine sekundäre Darlegungslast, zu den getroffenen Schutzmaßnahmen im Übrigen vorzutragen, da es sich insoweit um Sachverhalte handelt, auf die nur sie Zugriff hat (vgl. OLG Stuttgart, Urteil v. 31.03.2021 – 9 U 34/21). Der hierzu getätigte Sachvortrag vermag nicht zu belegen, dass hinreichende Maßnahmen zur Vermeidung des unbefugten Zugriffs Dritter auf Daten getroffen wurden.

Soweit die Beklagte auf Unterlassungsverfügungen oder gerichtliche Verfahren gegenüber Scrapern hinweist, betrifft auch dies ersichtlich keine präventiven Schutzmaßnahmen zur Verhinderung eines Vorfalls wie dem streitgegenständlichen, sondern es stellen Reaktionen auf bereits eingetretene Vorfälle dar. Das unbefugte Abgreifen von persönlichen Daten ist zu diesem Zeitpunkt bereits erfolgt. Soweit die Beklagte weiter vorträgt, sie habe die Suche von Nutzern anhand der Telefonnummer in der Facebook-Suchfunktion beschränkt, hat dies mit den technischen Vorkehrungen beim Kontaktimporttool nichts zu tun. Auch der Vortrag zu dem Expertenteam der Beklagten, welches sich um die technischen Vorkehrungen kümmere und diese weiterentwickle, ist zu abstrakt und losgelöst von konkreten Schutzvorkehrungen zur Verhinderung von Scraping-Attacken über die Kontaktimportfunktion im streitgegenständlichen Zeitpunkt.

Zwar hat die Beklagte auch vorgetragen, dass schon zum Zeitpunkt des hiesigen Scraping-Vorfalls alle seinerzeit technisch erforderlichen und möglichen Maßnahmen ergriffen worden seien, darunter insbesondere die vom Kläger monierten Mechanismen der Captcha-Anfragen oder Bot-Erkennungen sowie Übertragungsbeschränkungen. Auch dieses Vorbringen war jedoch zur Anspruchsverteidigung unzureichend, da es zu abstrakt war und keinen Vortrag dazu enthält, weshalb es trotz der angeblich implementierten Mechanismen dennoch zu dem streitgegenständlichen Scraping-Vorfall gekommen ist. Hiermit hätte sich die Beklagte jedoch konkret auseinandersetzen müssen und anhand der seinerzeit angeblich vorhandenen Techniken detailliert darlegen müssen, warum und inwieweit diese gleichwohl umgangen werden konnten bzw. womöglich umgangen worden sind. Ohne eine solche detaillierte Beschreibung bleibt die Behauptung, man habe seinerzeit alle technisch erforderlichen Maßnahmen ergriffen, substanzlos, da sie die Eignung, Erforderlichkeit und Angemessenheit der ergriffenen Maßnahmen eben nicht überprüfbar macht.

Dabei mag es zutreffen, dass ein Scraping-Vorgang nicht schlechterdings zu vermeiden ist. Jedoch hätte die Beklagte die seinerzeit technisch realisierbaren und zumutbaren Möglichkeiten aufzeigen und deren Unfähigkeit, gerade den hiesigen Vorfall zu verhindern, darlegen müssen. Auch an einer hinreichenden Auseinandersetzung mit der Möglichkeit der Kombination verschiedener einzelner technischer Maßnahmen fehlt es.

Etwas anderes ergibt sich auch nicht daraus, dass die Daten des Klägers aufgrund der Voreinstellungen öffentlich zugänglich waren, woraus die Beklagte ableitet, dass sie insoweit gar keine Schutzmaßnahmen habe treffen müssen (so auch LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 54). Aus dem Regelungsgefüge der DSGVO lässt sich im Anschluss an die vorangehenden Ausführungen keine Beschränkung des Grundsatzes der Datenminimierung entnehmen. Insbesondere ergibt sich kein Ausschlussverhältnis zwischen dem Grundsatz der Datenminimierung und dem auch von Art. 5 Abs. 1 lit. f) geforderten Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Demgemäß lässt sich auch keine Einschränkung des Anwendungsbereichs des Art. 32 Abs. 1 DSGVO auf den Tatbestand der Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO entnehmen, der u.a. eine unbefugte Offenlegung oder einen unbefugten Zugang fordert. Dies lässt sich auch Art. 32 Abs. 2 DSGVO nicht entnehmen. Die Regelung nimmt zwar auch auf unbefugte Offenlegung bzw. unbefugten Zugang Bezug, nennt diese Modalitäten indes nur Beispielhaft („insbesondere“) und ist daher nicht abschließend.

Ein Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DSGVO hat, bei Vorliegen der übrigen Anspruchsvoraussetzungen, auch einen Anspruch nach Art. 82 DSGVO zur Folge (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 40a; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 31).

(3)

Die Beklagte hat zudem ihre Meldepflicht aus Art. 33 DSGVO verletzt. Gemäß Art. 33 Abs. 1 DSGVO muss der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gem. Art. 55 DSGVO zuständigen Aufsichtsbehörde melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde

nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Der Mindestinhalt der Meldung ist in Art 33 Abs. 3 DSGVO festgelegt.

Dem ist die Beklagte vorliegend nicht nachgekommen. Dass sie die Irish Data Protection Commission als zuständige Aufsichtsbehörde i.S.d. Art 55 DSGVO über den „Scraping“-Vorfall nicht zeitnah informiert hat, ist unstreitig.

Zudem liegt eine Verletzung des Schutzes personenbezogener Daten vor. Nach der Begriffsbestimmung in Art. 4 Nr. 12 DSGVO fällt darunter eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Erfasst ist damit im weitesten Sinn jede objektive Schutzverletzung, unabhängig davon, ob diese beabsichtigt war oder nicht, wie etwa infolge von Datenpannen, Datenlecks, Hackerangriffen oder Datendiebstahl (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 33 Rn. 5; Spindler/Schuster/Laue, 4. Aufl. 2019, DSGVO Art. 33 Rn. 6 m.w.N.). Eine Verletzung liegt auch dann vor, wenn im Rahmen bestehender Zugriffsrechte Daten zweckentfremdet werden (Spindler/Schuster/Laue, DSGVO Art. 33 Rn. 7).

Es ist zu einem unbefugten Zugang zu personenbezogenen Daten gekommen, der in der zweckwidrigen Ausnutzung des – nicht hinreichend erklärten und nicht hinreichend abgesicherten – Contact-Import-Tools zur Verknüpfung von nicht veröffentlichter Mobilnummer und Facebookprofil zu erkennen ist. Unabhängig davon, dass Name, Facebook ID und Geschlecht des Klägers aufgrund seiner Privatsphäre-Einstellungen öffentlich waren und die Handynummer durch die frei zugängliche Nutzung des CIT-Tools mit diesen Daten verknüpft werden konnte, liegt vor dem Hintergrund des massenhaften „Scrapings“ und der Veröffentlichung der Daten in „Darknet“ eine Zweckentfremdung im Rahmen der grundsätzlich gewährten Zugriffsrechte vor. Der „Scraping“-Vorfall ist allein aufgrund seines Ausmaßes mit Datenpannen, -lecks, Hackerangriffen oder Datendiebstahl gleichzusetzen. Dies zeigt sich auch darin, dass ein solches Vorgehen nach den Nutzungsbedingungen untersagt ist und – so behauptet jedenfalls die Beklagte selbst – Sicherheitsmaßnahmen gegen derartige Vorfälle geschaffen wurden. Durch die Veröffentlichung der Daten im „Darknet“ wurde zudem die Ebene, auf denen die Daten zur Verfügung stehen, geändert.

Eine Einschränkung der Meldepflicht nach Art. 33 Abs. 1 DSGVO ist nicht gegeben. Es ist nicht vorauszusehen, dass die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten des Klägers führt. Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht gemäß des Erwägungsgrunds 85, wenn ihnen der Verlust der Kontrolle über ihre Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen. Ein solcher Kontrollverlust ist bereits eingetreten (s.u.).

Schließlich ist ein Verstoß gegen die Meldepflicht geeignet, für den Verantwortlichen eine Haftung und eine Schadensersatzpflicht gem. Art. 82 DSGVO zu begründen (LG Essen ZD 2022, 50; Kühling/Buchner/Jandt, 3. Aufl. 2020, DSGVO Art. 33 Rn. 27; Spindler/Schuster/Laue DS-GVO Art. 33 Rn. 24). Denn die Vorschrift dient sowohl dem Schutz des Betroffenen, als auch der Ermöglichung von Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung durch die Aufsichtsbehörde. Insofern genügt bereits ein solch formeller Verstoß gegen die DSGVO zur Begründung eines Schadensersatzanspruchs dem Grunde nach (vgl. LG Essen ZD 2022, 50; BeckOK DatenschutzR/Quaas, 41. Edition Stand: 01.08.2022, DS-GVO Art. 82 Rn. 14).

(4)

Das vorstehend Gesagte gilt auch hinsichtlich eines Verstoßes gegen Art. 34 Abs. 1 DSGVO, nachdem die Beklagte auch den Kläger als betroffene Person unverzüglich hätte benachrichtigen müssen. Ein hohes Risiko für die Rechte des Betroffenen im Normsinne lag nach dem Vorgesagten vor. Die von der Beklagten insoweit herausgegebene Information vom 6.4.2021 stellte dabei keine hinreichende individuelle Information des Klägers dar. Der Beklagten wäre es wegen der ihr bekannten E-Mail-Adresse des Klägers und sämtlicher weiterer betroffener Nutzer ohne weiteres möglich gewesen, individuelle Benachrichtigungen per E-Mail oder jedenfalls solche auf der individuellen Profilseite eines jeden Nutzers zu versenden. Das Schreiben der Beklagten vom 23.08.2021 war sodann nicht mehr unverzüglich im Sinne des Art. 34 Abs. 1 DSGVO.

Ein Ausschlussgrund nach Art. 34 Abs. 3 DSGVO liegt nicht vor. Insbesondere ist ein Risiko für die Zukunft nach dem eigenen Beklagtenvorbringen im Sinne von Art. 34

Abs. 3 lit. b) DSGVO im Hinblick auf Scraping-Attacken weiterhin nicht ausgeschlossen.

(5)

Die Beklagte verstößt mit ihren Voreinstellungen zur Sichtbarkeit zumindest hinsichtlich der E-Mail-Adresse und zur Suchbarkeit über die Telefonnummer der Benutzer der Facebook-Plattform auch gegen Art. 25 DSGVO.

Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden („Privacy by Design“). Abs. 2 konkretisiert diese allgemeine Verpflichtung und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten“ Voreinstellungen („Privacy by default“) zu setzen (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 3).

Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst „datensparsame“ Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Voreinstellungen erst durch ein aktives „Eingreifen“ der Nutzer möglich werden. Die Regelung soll die Verfügungshoheit der Nutzer über ihre Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen.

Das ist aber durch die Beklagte nicht gewährleistet. Aus ihrem eigenen Vortrag in der Klageerwiderung ergibt sich, dass der Umstand, dass die Telefonnummer des Klägers „öffentlich“ war, darauf beruhte, dass er dies in den Voreinstellungen nicht geändert hat, nachdem - wie die Beklagte zugesteht - die Standard-Einstellung für die Suchbarkeit von Telefonnummern während des relevanten Zeitraums „alle“ gewesen ist. Nicht ausreichen kann insoweit sein, dass - worauf die Beklagte abstellt - etwaige Einstellungen vom Nutzer geändert werden können. Dasselbe gilt für den von der Beklagten angeführten „Privatsphäre-Check“.

Diese durch die Voreinstellungen ermöglichte Datenerhebung ist nicht für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich (Art. 6 Abs. 1 Satz 1 lit. b DS-GVO), ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO).

Die Beklagte kann sich nicht darauf berufen, dass eine entsprechende Einstellung erforderlich gewesen sei, um den Zweck des sozialen Netzwerks, der unabhängig von der Frage, ob die Beklagte mit dem Betrieb Werbeeinnahmen erzielt, ersichtlich auf die Knüpfung von Kontakten angelegt ist, nicht zu konterkarieren. Im Ausgangspunkt ist der Beklagten beizupflichten, dass ein soziales Netzwerk darauf ausgerichtet ist, als Kontakt- und Kommunikationsplattform für eine Vielzahl von Menschen zu dienen. Eine entsprechende Funktionalität ist ersichtlich nicht (effektiv) gegeben, wenn sich die Möglichkeit der Kontaktaufnahme und des Findens/Knüpfens von Kontakten darauf beschränkt, quasi zufällig über öffentliche Kommentare etwa auf Unternehmensseiten etc. auf andere Nutzer zu stoßen. Dementsprechend ist grundsätzlich ein valides Interesse des Betreibers zu konstatieren, eine Suchfunktion vorzuhalten, mit der sich die Nutzer des Netzwerks anhand bestimmter Parameter finden können. Dieser Funktion dürfte aber mit weitaus weniger sensiblen Informationen wie dem Namen entsprochen werden können, der erster „Anlaufparameter“ für diejenigen sein wird, die nach einer Person suchen, die sie interessiert und mit der sie über das Netzwerk in Kontakt treten möchten. Diese Erwägung liegt dabei offenbar auch den für „immer öffentlich“ vorbestimmten Informationen eines Nutzers in Gestalt von Name, Geschlecht und Nutzer-ID zugrunde. Die Telefonnummer befindet sich gerade nicht darunter.

(6)

Ob die Beklagte dem Auskunftsersuchen der Klägerseite über ihre personenbezogenen Daten nicht in ausreichendem Maße nachgekommen ist und dadurch gegen Art. 15 DSGVO verstoßen hat - worauf die Kammer im Klageantrag zu 4) noch näher eingehen wird - kann dahinstehen, da ein etwaiger Verstoß keinen Schadensersatzanspruch nach Art. 82 DSGVO auslöst.

Die Norm spricht zwar demjenigen einen Schadensersatzanspruch zu, der wegen eines Verstoßes gegen diese DSGVO einen Schaden erlitten hat. Gemäß Art. 82 Abs. 2 DSGVO haften die Verantwortlichen – insoweit konkretisierend – jedoch nur für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung entstanden ist. Dies steht im Einklang mit Erwägungsgrund 146 S. 1, in dem es lautet „Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person auf Grund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen.“ Daher kommt nur ein Verstoß durch die Verarbeitung selbst in Betracht, die verordnungswidrig sein muss, um einen Schadensersatzanspruch auszulösen. Auf Grund von anderen Verstößen, die nicht durch eine der DSGVO

zuwiderlaufende Verarbeitung verursacht worden sind, kommt eine Haftung nach Art. 82 Abs. 1 DSGVO nicht in Betracht (vgl. Nemitz in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Rn. 8).

Datenverarbeitung bezeichnet gem. Art. 4 Nr. 2 DSGVO nur jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Daran gemessen stellt eine - nach Auffassung des Klägers – nicht ausreichende Auskunftserteilung keine Verarbeitung personenbezogener Daten i.S.d. DSGVO dar.

b)

Die Beklagte kann sich nicht gemäß Art. 82 Abs. 3 DSGVO, der das Verschulden widerleglich vermutet, exkulpieren.

Soweit in der Vorschrift von der Verantwortlichkeit für den Schaden die Rede ist, ist dies im Sinne von Verschulden aufzufassen (vgl. OLG Stuttgart, Urteil vom 31. März 2021 — 9 U 34/21 —, Rn. 45, 51, juris; BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DSGVO Art. 82 Rn. 17.2, Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DSGVO Art. 82 Rn. 14; Gola/Heckmann/Cola/Piltz, 3. Aufl. 2022, DSGVO Art. 82 Rn. 24; Spindler/Schuster/Spindler/Horvâth, 4. Aufl. 2019, DSGVO Art. 82 Rn. 11; a.A. Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DSGVO Art. 82 Rn. 19: fehlendes Verschulden für Entlastung nicht ausreichend). Art. 82 Abs. 3 DS-GVO ordnet eine Beweislastumkehr hinsichtlich des Verschuldens an (Oberster Gerichtshof Wien, Urteil vom 27. November 2019 — 6 Ob 217/19h —, juris). Der Anspruchsverpflichtete kann sich daher nur entlasten, indem er beweist, dass er die am Maßstab des Stands der Technik und im Verkehr, d.h. am allgemeinen Schutzinteresse orientierte erforderliche Sorgfalt im Sinne von § 276 Abs. 2 BGB angewendet hat (BeckOK DatenschutzR/Quaas, 42. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 18).

Die Beklagte hat keinerlei Umstände angeführt, die sie hinsichtlich der unzureichend erteilten Informationen in Bezug auf die Verarbeitung der Telefonnummer, die fehlenden Sicherheitsmaßnahmen zur Vermeidung des automatisierten Abgreifens von Daten über das CIT mittels Telefonnummern, die nicht möglichst datenschützenden Voreinstellungen und den Verstoß gegen die ihr obliegenden Melde- und Benachrichtigungspflicht entlasten könnte.

c)

Dem Kläger ist nach Auffassung des Gerichts ein immaterieller Schaden i.S.d. Art. 82 DSGVO entstanden.

(1)

Ein bloßer Datenschutzverstoß als solcher genügt für das Entstehen des Schadensersatzanspruches nicht (a.A. BAG ZD 2022, 56 Rn.33; OLG München NJW 2020, 779; Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 11 ff.). Vielmehr folgt bereits aus dem Wortlaut der Vorschrift, dass der Verordnungsgeber keine allein an den Rechtsverstoß anknüpfende Zahlungspflicht begründen wollte (OLG Frankfurt GRUR 2022, 1252 Rn. 61 m.w.N.). Auch der EuGH stellt auf das Erfordernis eines konkreten Schadens ab (EuGH 4.5.2023 – C-300/21).

Allerdings können – abweichend von anderen Bereichen des Rechts - auch Bagatellschäden eine Ersatzpflicht hervorrufen. Denn eine Erheblichkeitsschwelle ist Art. 82 DS-GVO nicht zu entnehmen. Eine solche Beschränkung stünde zu dem vom Unionsgesetzgeber gewählten weiten Verständnis des Begriffs "Schaden" im Widerspruch. Eine Erheblichkeitsschwelle könnte auch die Kohärenz der mit der DSGVO eingeführten Regelung beeinträchtigen. Denn die graduelle Abstufung, von der die Möglichkeit, Schadenersatz zu erhalten, abhinge, könnte je nach Beurteilung durch die angerufenen Gerichte unterschiedlich hoch ausfallen (EuGH 4.5.2023 – C-300/21).

Deshalb kann ein Schaden auch bereits in einem unguten Gefühl, in der Angst und Besorgnis liegen, dass personenbezogene Daten Unbefugten bekannt geworden sind, wenn die Gefahr besteht, dass die Daten unbefugt weiterverwendet werden (vgl. Landesarbeitsgericht Baden-Württemberg, Urteil vom 25. Februar 2021 — 17

Sa 37/20). So führen die Erwägungsgründe 75 und 85 als möglichen Schaden unter anderem den Verlust, die personenbezogenen Daten kontrollieren zu können, auf.

(2)

Eine spürbare Beeinträchtigung ist durch den Kläger nachvollziehbar in der mündlichen Verhandlung geschildert worden. Er konnte sowohl das ungute Gefühl als auch den zusätzlichen Aufwand schildern, den er durch eine Vielzahl von unseriösen Anrufen und Kontaktaufnahmen via SMS durch unbekannte Nummern seit dem Scrapingvorfall hat. Um Spamkontakte zu identifizieren und Betrugsmaschen auszuschließen, sieht sich der Kläger veranlasst, vermehrt Kontaktversuche auf ihre Seriosität überprüfen. Dies nehme Zeit in Anspruch. Er sei sogar kurz davor gewesen, seine Nummer zu ändern, und habe dies bisher auch nur unterlassen, da er seine Nummer schon mehrfach im Rahmen von geschäftlichen Kontakten abgegeben habe, und Angst habe, hierdurch Job- und Geschäftschancen zu verpassen. Hinzu kommt, dass der Kläger plausibel und glaubhaft den Erhalt von Anrufen und Phishing-SMS mit potentiell vermögensschädigendem Inhalt geschildert hat, die in einem kausalen Zusammenhang mit der Veröffentlichung der personenbezogenen Daten im Internet stehen können. Hierbei konnte er in zeitlicher Hinsicht passend schildern, dass er vor dem streitgegenständlichen Scraping-Vorfall deutlich weniger derartige Anrufe und SMS erhielt.

Soweit die Beklagte meint, ein Schaden könne schon deshalb nicht entstanden sein, weil es keinen Schutz vor der (erneuten) Veröffentlichung bereits öffentlicher Daten gebe, verfängt dies nicht. Denn gerade die Verknüpfung der gescrapten Daten mit der Telefonnummer des Klägers in einem Datensatz führt zu einer höheren Dimension des Kontrollverlustes des Klägers hinsichtlich seiner Daten. Dabei spielt es insbesondere keine Rolle, dass die Scraper überhaupt erst durch Eingabe einer selbst generierten, mit der Nr. des Klägers identischen Telefonnummer zu einem „Match" mit seinem Facebook-Profil kamen und seine Nr. nicht originär dem Profil entnahmen.

Die erforderliche Kausalität zwischen den Verstößen der Beklagten gegen die DSGVO und dem Schaden des Klägers liegt vor. Wäre der Kläger ohne Verstoß gegen die Informationspflichten nach Art. 13 Abs. 1 c) DS-GVO ordnungsgemäß darüber aufgeklärt worden, dass seine Telefonnummer, die er in der Zielgruppenauswahl als nicht öffentlich eingestellt hatte, im Rahmen des Einsatzes des CIT ohne Veränderungen der Einstellungen angesichts der

Standardvoreinstellung für die Suchbarkeit über die Telefonnummer auf „für alle" dazu verwendet wird, um ihn auf Facebook zu finden, hätte er nach seinem glaubhften Bekunden seine Telefonnummer nicht eingetragen oder die Standardeinstellungen verändert. Schließlich ist der Schaden auch kausal auf den Verstoß der Beklagten gegen Art. 24, 32, 5 Abs. 1 f) DS-GVO zurückzuführen, denn durch die unzureichenden Schutzmaßnahmen ermöglichte die Beklagte das missbräuchliche Abgreifen der Daten des Klägers.

(3)

Im streitgegenständlichen Fall hält das Gericht unter Berücksichtigung der Ausgleichs- und Genugtuungsfunktion sowie der generalpräventiven Funktion des immateriellen Schadenersatzes einen Betrag in Höhe von 350,00 € erforderlich, aber auch ausreichend.

Bei der Bestimmung des vom Kläger in das Ermessen des Gerichts gestellten Höhe des Schadenersatzes gemäß § 287 Abs. 1 S. 1 ZPO sind alle Umstände des Einzelfalls zu würdigen (vgl. BAG, Urteil vom 5. Mai 2022 — 2 AZR 363/21 —, Rn. 12 f., juris). Die Kriterien des Art. 83 Abs. 2 DSGVO, die Anhaltspunkte für die Höhe der von der Aufsichtsbehörde zu verhängenden Geldbuße geben sollen, können auch für die Bemessung des immateriellen Schadenersatzes herangezogen werden (vgl. Hans-Jürgen Schaffland, Gabriele Holthaus iw Schaffland/Wiltfang, Datenschutz-Grundverordnung (DSGVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz, Rn. 10; Kühling/Buchner/Bergt, 3. Aufl. 2020, DSGVO Art. 82 Rn. 18d; BeckOK DatenschutzR/Quaas, 43. Ed. 1.2.2023, DSGVO Art. 82 Rn. 31). Danach sind unter anderem Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens sowie die Kategorien der personenbezogenen Daten zu betrachten. Gemäß Erwägungsgrund 146 S. 6 DSGVO sollen die betroffenen Personen einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. Schadensersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17; Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 10).

Dabei fließt anspruchserhöhend ein, dass der Beklagten mehrere schadensursächliche Verstöße gegen die DSGVO zur Last zu legen sind, wobei die den Zweck von Facebook fördernde Art der Datenerhebung die Regeln der DSGVO

nicht nur im Einzelfall, sondern systematisch und über einen längeren Zeitraum missachtet hat. Überdies sind Aufwand und investierte Zeit, die der Kläger in die Prüfung von Spam-SMS investiert, zu berücksichtigen. Dies beschäftigte den Kläger und beeinträchtigte ihn in gewissem Umfang in seiner Lebensführung.

Eine Reduzierung des klägerseits angegebenen Mindestbetrages war indes gerechtfertigt, da die Kammer im Rahmen der persönlichen Anhörung des Klägers festgestellt hat, dass das Ausmaß der Sorge des Klägers vor zukünftigen negativen Auswirkungen des Ausspähens seiner Daten - wenngleich er über einen Wechsel der Telefonnummer immerhin nachgedacht hat - letztlich doch nicht so groß ist, dass er sich veranlasst gesehen hätte, seinen Facebook-Account aufzulösen, die dortigen Einstellungen jeweils auf die größtmögliche Privatsphäre hin abzuändern oder seine Telefonnummer zu wechseln. Bei den gescrapten Daten handelt es sich zudem nicht um hochsensible Informationen wie Gesundheits- oder Kontodaten.

2.

Der Zinsanspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB.

3.

Der mit dem Antrag zu 2) geltend gemachte Feststellungsantrag ist auch begründet. Gemäß vorstehender Ausführungen hat der Kläger gegenüber der Beklagten wegen Verletzung der DSGVO einen Anspruch auf Schadensersatz nach Art. 82 DSGVO. Die jeweiligen Gesetzesverletzungen sind – wie bereits erörtert – zudem kausal für den unkontrollierten Datenverlust des Klägers. Die Gefahr auch künftiger Schäden besteht, da die gescrapten Daten nicht rückholbar sind.

4.

Der Kläger kann von der Beklagten in der Sache auch die Unterlassung in tenoriertem Umfang verlangen.

Aus Art. 32 Abs. 1 und 2 DSGVO folgt, dass der Verantwortliche ein dem Risiko eines unbefugten Zugangs zu personenbezogenen Daten angemessenes

Schutzniveau zu gewährleisten hat. Dabei liegt es im Ermessen des Verantwortlichen, aus der Vielzahl möglicher Maßnahmen, die das Risiko der Datenverarbeitung reduzieren können, konkrete Maßnahmen auszuwählen, durch die nach seiner Einschätzung ein angemessenes Schutzniveau erreicht wird (Kühling/Buchner/Jandt, 3. Aufl. 2020, DSGVO Art. 32 Rn. 8).

Allerdings ist wesentlich, dass nicht alle möglichen Maßnahmen zur Gewährleistung von Datensicherheit zu ergreifen sind, sondern nur solche, die unter Abwägung zwischen Schutzzweck und Aufwand unter Berücksichtigung der Art der Daten, dem Stand der Technik und den anfallenden Kosten als verhältnismäßig anzusehen sind (vgl. Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 10). Denn die DSGVO verlangt keine Datensicherheit um jeden Preis und verpflichtet den Verantwortlichen nicht zu einem absoluten Schutz der personenbezogenen Daten, vielmehr muss das Schutzniveau dem jeweiligen Einzelfall angemessen sein, wobei Risiken nicht gänzlich ausgeschlossen werden können (Cola/Heckmann/Piltz, DSGVO 3. Aufl., Art. 32 Rn. 11; Paal/Pauly/Martini, DSGVO 3. Aufl., Art. 32 Rn. 46; Dr. Hans-Jürgen Schaffland; Gabriele Holthaus in. Schaffland/Wiltfang, Datenschutz-Grundverordnung (DSGVO)/Bundesdatenschutzgesetz (BDSG), Artikel 32 Sicherheit der Verarbeitung, Rn. 3).

Der Kläger kann daher lediglich ein angemessenes Schutzniveau bzw. die Unterlassung einer Datenverarbeitung ohne dieses verlangen. Darauf, dass eines der Abwägungskriterien in den Vordergrund gestellt wird, hat der Kläger ebenso wenig Anspruch wie auf konkrete Maßnahmen (vgl. dazu auch BGH, Urteil vom 22. Oktober 1976 — V ZR 36/75 —, BGHZ 67, 252-254, Rn. 11; Urteil vom 17. Dezember 1982 — V ZR 55/82 —, Rn. 17, juris, jeweils zu Unterlassungsansprüchen gegen Immissionen).

Nachdem das Gericht auf diesen Aspekt hingewiesen hat, beantragt der Kläger auch nicht länger mehr. Es sollen lediglich Sicherheitsmaßnahmen vorgesehen werden, die ein angemessenes Schutzniveau einhalten.

5.

Der auf Auskunft gerichtete Antrag des Klägers ist nur zum Teil begründet. Der Kläger kann von der Beklagten verlangen, ihm Auskunft darüber zu erteilen, durch welche Empfänger welche Daten des Klägers durch Scraping erlangt wurden. Der

Anspruch ist aber in dem darüberhinausgehenden Umfang durch Erfüllung erloschen und daher abzuweisen.

(1)

Der Kläger hat gegen die Beklagte einen Anspruch auf Mitteilung der Empfänger der durch Scraping erlangten Daten des Klägers aus Art. 15 Abs. 1 c) DS-GVO und Art. 33 Abs. 2 DS-GVO.

a)

aa)

Gemäß Art. 15 Abs. 1 c) DS-GVO hat der Betroffene insbesondere das Recht auf Informationen über die Empfänger der personenbezogene Daten. Art. 34 Abs. 2 DS-GVO statuiert die Pflicht des Verantwortlichen nach einer Verletzung des Schutzes personenbezogener Daten mit einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, die betroffene Person über die „Art der Verletzung des Schutzes personenbezogener Daten" zu informieren. Die Voraussetzungen dieser Vorschrift sind erfüllt. Insbesondere ist von einem hohen Risiko auszugehen. Dies ist etwa anzunehmen, wenn ein Kontrollverlust der betroffenen Person im Hinblick auf ihre personenbezogenen Daten eingetreten ist (vgl. Erwägungsgrund 85; so auch Gola/Heckmann/Reif, a.a.O., Art. 34 Rn. 8).

Beide Vorschriften sind so zu verstehen, dass dem von einem unbefugten Zugriff auf seine Daten Betroffenen vom Verantwortlichen, soweit diesem bekannt, auch die Identität des unbefugt Zugreifenden mitzuteilen ist.

Der Wortlaut der Regelungen lässt dies zu. Als Empfänger im Sinne des Art. 15 Abs. 1 c) DSGVO, dem gegenüber Daten offengelegt wurden, kann zwanglos auch noch derjenige verstanden werden, der diese unbefugt erhalten hat. Auch der Begriff „Offenlegen" umfasst die unbeabsichtigte Preisgabe. Sinn und Zweck der Auskunfts- und Informationsrechte legen eine weite Auslegung nahe. Gerade unter dem Gesichtspunkt der in der DSGVO mehrfach betonten Transparenz sowie der Kontrolle der Betroffenen über ihre eigenen Daten wäre es widersinnig, einen solchen Anspruch zu verneinen. Denn erst mit der Kenntnis der unbefugten Dritten wird der Betroffene in die Lage versetzt, diesen gegenüber Ansprüche, wie etwa das Recht auf Löschung gemäß Art. 17 DSGVO, effektiv geltend zu machen, und die Möglichkeit zu haben, die Kontrolle über seine Daten wiederzuerlangen (vgl. dazu

auch die Schlussanträge des Generalanwalts vom 15.12.2022, C-579/21, Celex-Nr. 62021CC0579).

bb)

Der Anspruch ist nicht durch Erfüllung untergegangen. Dafür genügt nicht etwa der Hinweis der Beklagten in ihrem Schriftsatz vom 23.05.23, über die Verarbeitungstätigkeiten Dritter keine Angaben machen zu können und keine Kenntnis über die Identität der ihr „unbekannte[n] Dritte[n]“ zu haben.

Außer Frage steht, dass bei tatsächlicher Unkenntnis jegliche Anhaltspunkte für die Identität der Scraper auch diese Angabe zur Erfüllung des Anspruchs führt.

Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die - gegebenenfalls konkludente - Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist (BGH, Urteil vom 15. Juni 2021 — VI ZR 576/19 —, Rn. 19, juris). Sollte der Auskunftsersuchende trotz dessen an der Richtigkeit der Angaben zweifeln, steht ihm der Weg zur eidesstattlichen Versicherung der Angaben offen.

Im vorliegenden Fall hat die Beklagte jedoch noch nicht einmal im Ansatz erkennen lassen, dass sie alle Quellen zur Informationsgewinnung ausgeschöpft und die Angaben getätigt hat, welche ihr möglich und zumutbar gewesen sind. Es hätte erwartet werden können, dass sie nicht nur kurz und knapp jede Kenntnis ablehnt, sondern zusätzlich etwa erklärt, was sie zur Identifizierung des bzw. der Scraper unternommen hat und weswegen sie, auch in Anbetracht des Umstandes, dass der oder die „Scraper“ selbst zur missbräuchlichen Nutzung des „CIT“ Inhaber eines Facebook-Accounts bzw. Nutzer der entsprechenden App gewesen sein mussten, nicht z.B. einen Nutzernamen, eine IP-Adresse, oder ähnliche Anknüpfungsumstände nennen kann. Hierzu wurde aber, trotz Hinweises des Gerichts in der mündlichen Verhandlung und einem dazu gewährten Schriftsatznachlass, nicht in der gebotenen Tiefe Auskunft erteilt. Indem die Beklagte lediglich darauf verweist, zu „Verarbeitungstätigkeiten Dritter“ keine Auskünfte geben

zu können, verkennt sie, dass sie nicht zu deren Verarbeitungstätigkeiten, sondern zu deren Identität so weit wie möglich Auskunft erteilen soll.

b)

Anderes gilt für den Anspruch auf Mitteilung, welche Daten durch Scraping erlangt werden konnten.

Dieser ergibt sich zwar nicht aus Art. 15 Abs. 1 DSGVO, denn diese Vorschrift sieht eine entsprechende Information nicht vor. Allerdings ist Art. 34 Abs. 2 DSGVO funktional dahingehend auszulegen, dass, soweit möglich, auch Angaben zu den von der Verletzung des Schutzes konkret betroffenen Daten bzw. Datenkategorien zu machen sind (Gola/Heckmann/Reif, 3. Aufl. 2022, DSGVO Art. 34 Rn. 22). Denn geeignete Schutzmaßnahmen der betroffenen Person dürften ohne diese Kenntnis gegebenenfalls nicht möglich sein (ebenda).

Der genannte Anspruch ist jedoch gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen.

Ob Art. 34 Abs. 2 DSGVO auch einen Anspruch auf Mitteilung des Zeitpunktes der Verletzung des Schutzes der Daten beinhaltet, kann dahinstehen.

Die Beklagte hat dem Kläger mit Schreiben vom 04.11.2021 (Anl. B16), S. 7, genau beschrieben, wie er die von ihm gespeicherten Daten auf Facebook herunterladen kann. Damit ist sie ihrer Auskunftsverpflichtung gemäß Art. 15 Abs. 1 b) DS-GVO nachgekommen. Insbesondere genügt vorliegend auch der Verweis auf die Selbstbedienungstools „Access Your Information" und „Deine Informationen herunterladen", mit dem sich der Kläger eine Kopie seiner Daten herunterladen kann.

In dem genannten Schriftsatz hat die Beklagte dem Kläger zudem auch mitteilen lassen, über eine Kopie der gescrapten Rohdaten zwar nicht zu verfügen, aber auf der Grundlage der bisherigen Analysen von im Einzelnen genannten durch Scraping abgerufenen Datenkategorien auszugehen. Damit hat die Beklagte zu erkennen gegeben, insoweit keine weiteren Auskünfte erteilen zu können. Ungeachtet einer etwaigen Unrichtigkeit der genannten Informationen ist dem Auskunftsanspruch des Klägers damit Genüge getan.

Auch der Zeitpunkt des Scraping-Vorfalls wurde dem Kläger von der Beklagten näher bestimmt. Dass er insoweit informiert wurde, lässt er etwa in der Formulierung des

Antrages Ziffer 2 (,,...der nach Aussage der Beklagten im Jahr 2019 erfolgte ... ") erkennen.

6.

Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DS-GVO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche erforderlich und notwendig. Unter Zugrundelegung des Wertes des berechtigten Verlangens des Klägers von 2850,00 € zum Zeitpunkt der außergerichtlichen Tätigkeit (350,00 € immaterieller Schadenersatz + 2.250,00 € Unterlassen + mit 250,00 € zu bemessender Anteil des Auskunftsbegehrens) führt dies zu berechtigten außergerichtlichen Kosten in Höhe von 367,23 € (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV RVG zzgl. 19% MwSt.).

Der Zinsanspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB.

II.

Die Entscheidung über die Kosten beruht auf § 92 Abs. 1 ZPO. Der Kläger hat in Höhe eines Anteils von 3025,00 € (350,00 € immaterieller Schadenersatz + 175,00 € Feststellung + 2.250,00 € Unterlassen + mit 250,00 € zu bemessender Anteil des Auskunftsbegehrens) am Streitwert obsiegt.

III.

Die Entscheidung zur vorläufigen Vollstreckbarkeit folgt aus §§ 708 Nr. 11, § 711 S. 1 und 2 und § 709 S. 1 und 2 ZPO.

IV.

Zur Begründung der Streitwertentscheidung, die auf § 48 GKG i.V.m. §§ 3, 4, 5 ZPO beruht, wird auf die Ausführungen zur sachlichen Zuständigkeit (oben A. I. 2.) verwiesen.

Dr. [redacted] [redacted]

Richterin am Landgericht
[redacted] ist aufgrund ihres
Erholungsurlaubs an der
Unterschriftsleistung
gehindert.
Dr. [redacted]