Abschrift

4 O 190/22

Landgericht Paderborn

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted],

Klägers,

Prozessbevollmächtigte:

gegen

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

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields u. a.,
Bockenheimer Anlage 44, 60322 Frankfurt,

hat die 4. Zivilkammer des Landgerichts Paderborn
auf die mündliche Verhandlung vom 30.01.2023
durch den Richter [redacted] als Einzelrichter

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 350,00 € zu zahlen nebst Zinsen seit dem 05.10.2022 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

2. Es wird festgestellt, dass die Beklagte dem Grunde nach verpflichtet ist, der Klägerseite auch 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 des Klägers, 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 des Klägers 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. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits tragen der Kläger 27 % und die Beklagte zu 73 %.

6. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich des Tenors zu Ziffer 1) aber nur gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages; im Übrigen gegen Sicherheitsleistung in Höhe von 5.000,00 €. 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.

Tatbestand:

Der Kläger macht Ansprüche wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung im Zusammenhang mit dem sog. „Datenleck“ der Beklagten geltend.

Der Kläger nutzt das von der Beklagten betriebene soziale Netzwerk Facebook, auf das sowohl über die Internetseite www.facebook.com als auch über eine gleichnamige App mittels Smartphone oder Tablet zugegriffen werden kann. Diese Plattform ermöglicht nach einer Anmeldung die Kommunikation mit anderen Nutzern, insbesondere können private Fotos und Informationen geteilt werden. 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 Facebook-Plattform, oder „Freunde von Freunden“ die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird insoweit gesondert behandelt, als dass diese standardmäßig nur der Nutzer selbst – so der Kläger – oder nur „Freunde“ – so die Beklagte – einsehen kann.

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 es die Beklagte ihm, 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. Ab Mai 2019 stand Nutzern auch die Option „Nur ich“ zur Verfügung. Die „Suchbarkeits-Einstellung“ war bei dem Kläger seit dem 01.03.2015 auf „Alle“ eingestellt (Anlage B17).

Bei der Registrierung wird der Nutzer auf die Datenrichtlinie der Beklagten hingewiesen. Insoweit wird auf die in der Anlage B9 und B10 zur Akte gereichten Auszüge Bezug genommen. Den Nutzern werden zudem im „Hilfebereich“, der unmittelbar auf der Facebook-Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift „Privatsphäre, Datenschutz und Sicherheit“ zugegriffen werden. Hinsichtlich der weiteren relevanten Inhalte im Hilfebereich und in den Einstellungen wird auf die Abbildungen in der Klageschrift sowie die Anlagen B1 bis B8 Bezug genommen.

Im Zeitraum von Januar 2018 bis September 2019 kam es zu einem sogenannten „Datenscraping“, also dem massenhaften, automatisierten Sammeln der persönlichen Daten von Facebook-Nutzern. „Scraping“ ist eine weitverbreitete Methode, um Daten, die typischerweise öffentlich einsehbar sind, von Internetseiten durch automatisierte Softwareprogramme abzurufen. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Der Abruf der Telefonnummern erfolgte hier jedoch nicht über die Facebook-Profile. Vielmehr wurden diese mit einem Prozess der sogenannten „Telefonnummernaufzählung“ bereitgestellt. So konnten die Nutzer ihre Kontakte von ihren Mobilgeräten mittels der sogenannten „Kontakt-Importer-Funktion“ bzw. dem Contact-Import-Tool“ (in Folge „CIT“) auf Facebook hochladen, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, ohne dass die im Profil hinterlegte Nummer in der „Zielgruppenauswahl“ öffentlich gemacht worden wäre. Vor diesem Hintergrund luden die „Scraper“ mithilfe des „CIT“ Kontakte hoch, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu. Die weiteren Einzelheiten hinsichtlich des Ablaufs des „Scrapings“ im vorliegenden Fall sind zwischen den Parteien streitig.

Anfang April 2021 veröffentlichten Unbekannte nach Angaben eines Artikels des „Business Insider“ vom 03.04.2021 die Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet. Die Beklagte veröffentlichte daraufhin am 06.04.2021 den Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ (Anlage B10), in dem sie erläuterte, dass die Daten nicht durch einen Hack erlangt worden seien, sondern es sich um öffentlich einsehbare Informationen handele. Die zuständige Datenschutzbehörde, Irish Data Protection Commission, informierte die Beklagte nicht über den Vorfall. Stattdessen ergriff die Beklagte als Reaktion auf die Medienberichterstattung Maßnahmen, um Nutzern Informationen über das „Scraping“ sowie die Möglichkeiten zur Änderung ihrer Privatsphäre-Einstellungen zur Verfügung zu stellen.

Mit einer E-Mail des Prozessbevollmächtigten des Klägers vom 11.08.2021 forderte dieser die Beklagte zur Schadensersatzzahlung i.H.v. 500,00 €, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren.

Der Kläger ist der Ansicht, die Beklagte habe eine Persönlichkeitsrechtsverletzung begangen und gegen die Datenschutzgrundverordnung verstoßen.

Hierzu behauptet er, dass seine persönlichen Daten wie Telefonnummer, Name, Wohnort und E-Mailadresse durch „Scraping“ abgegriffen worden seien. 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, FacebookID, 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“ raidforums.com, veröffentlicht worden. Sie würden insbesondere für gezielte Phishing Attacken genutzt. Auf einer im Darknet für jedermann abrufbaren Datenbank seien Telefonnummer, Name, Wohnort und Mailadresse des Klägers zugänglich gemacht worden. Zum jetzigen Zeitpunkt könne noch nicht abgesehen werden, welche Dritten Zugriff auf die Daten des Klägers erhalten hätten und für welche konkreten kriminellen Zwecke die Daten missbraucht würden.

Der Kläger behauptet, die Unbekannten hätten die Daten aus dem Datenbestand von Facebook mittels des „CIT“ aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert. Die Telefonnummern der Benutzer hätten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden können. Durch die Eingabe einer Vielzahl von Kontakten in ein virtuelles Adressbuch sei es gelungen, die Telefonnummern konkreten Facebook-Profilen zuzuordnen, ohne dass die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die Telefonnummer jeweils zu korrelieren, sei mit Hilfe des „CIT“ jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer angezeigt worden. Ein Programm habe unzählige Kombinationen von Telefonnummern getestet, um festzustellen, ob diese mit einem Facebook-Nutzer übereinstimmen bzw. ob diese bei Facebook hinterlegt worden ist. Wenn dies der Fall gewesen sei, sei es dem Programm möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren.

Der Kläger behauptet, dieses „Scraping“ sei dadurch ermöglicht worden, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten „CIT“ zu verhindern. So seien keine Sicherheitscapchas (Abkürzung für „Completely Automated Public Turing Test to tell Computers and Humans Apart“

– also ein vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden – verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handelt. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummerabfragen (z.B. 000001, 000002 usw.) wäre durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich, angemessen und üblich. Die Einführung einer Begrenzung der abgleichbaren Rufnummern oder Nutzung des „CIT“ für Freunde von Freunden sei möglich gewesen. Mindestens aber ein expliziter Hinweis auf die „offenen“ Standard-Einstellungen für die Suchbarkeit per Telefonnummer fehle, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers. Wären derartigen Sicherheitsmaßnahmen vorgenommen worden, sei es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen.

Der Kläger behauptet ferner, dass die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Plattform diene dazu, Kunden zu bewerben und Unternehmen die Möglichkeit für Werbung zu geben. Um diesen kommerziellen Interessen und Marketingzwecken der Beklagten zu dienen, finde eine intransparente Verarbeitung personenbezogener Daten von Milliarden Menschen statt. So handele die Beklagte aufgrund der datenschutz-unfreundlichen Standard-Voreinstellungen entgegen des Prinzips 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 Telefonnummer gesucht werde. Durch die vielschichtigen Einstellungsmöglichkeiten werde ein Gefühl der Sicherheit für den Nutzer erzeugt, was im Ergebnis zu einer erheblichen Datengefährdung führe, da mit hoher Wahrscheinlichkeit zu erwarten sei, dass ein Nutzer die voreingestellten Standardeinstellungen behalte und nicht selbständig ändere. Diese Undurchsichtigkeit setze sich bei der von der Beklagten betriebenen „Messenger“-App mit separaten Sicherheitseinstellungen fort, bei der die Nutzer mit ihren Facebook-Profilen zur Versendung von Mitteilungen angemeldet sind. Diese

Einstellungen seien unabhängig von denjenigen im sonstigen Facebook-Dienst und ermöglichen auch die Synchronisation der Telefonkontakte mit Facebook. So werde bereits bei Anmeldung in der Messenger-App angefragt, ob diese Synchronisierung vorgenommen werden solle. Eine Information über etwaige Risiken oder über die Verwendung der Telefonnummer erfolge nicht, obwohl ein Nutzer geradezu zur Verwendung des „CIT“ gedrängt werde.

Der Kläger behauptet, dass ihm durch das „Scraping“ ein kausaler Schaden entstanden sei. Hierzu trägt er vor, dass die Zuordnung von Telefonnummern zu weiteren Daten wie der E-Mail-Adresse oder Anschrift böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie z.B. Identitätsdiebstahl, die Übernahme von Accounts oder gezielte Phishing-Nachrichten ermögliche. Insbesondere sogenannte „Sim-Swap“-Angriffe würden durch die Verknüpfung von Telefonnummern zu weiteren Nutzer-Accounts eröffnet. Durch derartige Angriffe sei es Kriminellen möglich, Passwörter zu ändern, die durch telefonnummernbasierende Authentifizierung geschützt sind. Der Kläger habe deswegen einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch seiner Daten verblieben. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Darüber hinaus erhalte der Kläger seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese würden Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks enthalten. Oft würde auch bei bekannten Plattformen oder Zahlungsdienstleistern wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Das habe dazu geführt, dass der Kläger nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre.

Der Kläger behauptet schließlich, dass er seine Telefonnummer auf der Plattform nicht abgegeben hätte, wenn die Beklagte ausreichend und im angemessenen Umfang über die Folgen der Preisgabe der Telefonnummer informiert hätte.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, an ihn 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. nur für den Fall, dass dem Klageantrag zu 1. stattgegeben wird, festzustellen, dass die Beklagte verpflichtet ist, ihm alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden,

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

   a. personenbezogenen Daten des Klägers, 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 des Klägers 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, ihm Auskunft über die ihm betreffenden 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,

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, der Vortrag hinsichtlich der abgerufenen und veröffentlichten Daten sei bereits unzulässig, da die Behauptung zu weit gefasst sei und unklar bleibe, welche konkreten Daten des Klägers betroffen seien. Auch sei der Unterlassungsantrag nicht hinreichend bestimmt und ein Feststellungsinteresse sei nicht dargelegt.
Im Übrigen lägen keine Verstöße gegen datenschutzrechtliche Vorschriften vor. Hierzu behauptet die Beklagte, dass die Daten weder durch Hacking noch infolge eines Fehlers oder Sicherheitsverstoßes im System der Beklagten, sondern durch das automatisierte, massenhafte Sammeln von ohnehin öffentlich einsehbaren und damit nicht vertraulichen Daten erlangt und an anderer Stelle zugänglich gemacht worden seien. Die gesammelten Daten umfassten lediglich die immer öffentlichen Nutzerinformationen und diejenigen Daten, die entsprechend der jeweiligen „Zielgruppenauswahl“ öffentlich einsehbar seien. Bundesland, Geburtsort und „weitere korrelierende Daten“ seien nicht durch „Scraping“ erlangt, da diese schon nicht den Profilfeldern auf der Plattform entsprächen. Land und Telefonnummer seien durch die Telefonnummernaufzählung bereitgestellt worden.

Die Beklagte behauptet, dass es Hauptzweck der Facebook-Plattform sei, andere Nutzer zu finden und mit diesen in Kontakt zu treten, woran sich auch die Standard-Voreinstellungen orientierten. Die „Scraper“ hätten dementsprechend lediglich die diesem Zweck dienenden Funktionen ausgenutzt. Es sei daher grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung der Funktionen zu unterlaufen. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Da die Funktionen, welche Scraper ausnutzten, rechtmäßige, gewöhnliche Nutzerfunktionen darstellten, werde zur Begrenzung von Scraping regelmäßig nicht die gesamte zugrunde liegende Funktion beseitigt. Vielmehr würden in der Regel lediglich die Methoden, mit denen auf die maßgeblichen Funktionen zugegriffen werden könne, beschränkt. Zur Bekämpfung von „Scraping“ beschäftige die Beklagte ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping (das External

Data Misuse-Team, „EDM-Team“). Eine der Maßnahmen der Beklagten zur Verringerung von „Scraping“ seien die implementierten Übertragungsbeschränkungen, die die Anzahl von Anfragen von bestimmten Daten reduzierten, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden könnten. Ferner gehe die Beklagte grundsätzlich mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen „Scraper“ und Hosting-Anbieter, also Unternehmen, auf deren Systemen die Daten zur Verfügung gestellt werden, vor. Die Beklagte nutze auch Captcha-Abfragen und die Beklagte habe ihr System als Reaktion auf den Vorfall insofern angepasst, als dass das Verknüpfen von Telefonnummern mit bestimmten Facebook-Nutzern durch die Kontakt-Importer-Funktion nicht mehr möglich sei.

Zudem habe sie ihren Nutzern, wie auch dem Kläger, alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung gestellt und umfassend über die Möglichkeiten der Anpassung ihrer Einstellungen informiert. Die entsprechenden Einstellungen seien klar und leicht zu finden gewesen. Hinsichtlich der „Messenger“-App entsprächen die Sicherheitseinstellungen denjenigen im allgemeinen Facebook-Konto. Änderungen in den Privatsphäre-Einstellungen auf der Facebook-Plattform würden automatisch auch innerhalb der Messenger-App angewandt.

Schließlich behauptet die Beklagte, dass der Zugriff auf die Telefonnummer einer Person, selbst in Kombination mit den durch „Scraping“ erlangten Profildaten, das Risiko, dass diese Person Opfer von Betrug oder anderen schweren Internetverbrechen wird, nicht erhöhe, da diese Informationen häufig weitergegeben werden. Vielmehr würden solche Verbrechen in der Regel weitaus sensiblere Informationen wie Kredit- oder Bankkartennummern, nationale Ausweisnummern oder Kontopasswörter erfordern.

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

Entscheidungsgründe:

Die Klage ist zulässig und in dem aus dem Tenor ersichtlichen Umfang begründet; im Übrigen unbegründet.

I.

1.

Der Klageantrag zu 1) ist zulässig.

Entgegen der Auffassung der Beklagten ist er insbesondere hinreichend bestimmt. Eine hinreichende Bestimmtheit des Antrags i.S.d. § 253 Abs. 2 Nr. 2 ZPO kann grundsätzlich angenommen werden, wenn er den Anspruch konkret bezeichnet, den Rahmen der gerichtlichen Entscheidungsbefugnis erkennbar abgrenzt, den Inhalt und Umfang der materiellen Rechtskraft erkennen lässt, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und wenn er die Zwangsvollstreckung aus dem beantragten Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21. November 2017 – II ZR 180/15 –, juris, Rn. 8 m.w.N.). Der Klageantrag ist dabei der Auslegung zugänglich, wobei auch die Klagebegründung heranzuziehen ist (Zöller/Greger, 34. Auflage 2022, § 253 Rn. 13 m.w.N.).

Vorliegend ergibt sich aus der Klageschrift, dass dem Klageantrag zu 1) ein zusammenhängender, sich zwar auf einen längeren Zeitraum erstreckender, aber in sich abgeschlossener Lebenssachverhalt zu Grunde liegt (vgl. LG Gießen, GRUR-RS 2022, 30480). Denn der Schadensersatzanspruch bezieht sich nach dem Vortrag des Klägers auf die Vorgänge ab der Anmeldung des Klägers auf der Facebook Plattform über das „Scraping“ seiner Daten bis hin zu einer angeblich unzureichenden Information des Betroffenen. Der Klageschrift lässt sich überdies entnehmen, dass der Schaden aufgrund eines kumulativen Zusammenwirkens der gerügten Datenschutzverstöße geltend gemacht wird, die Bezifferung des Schadens dabei indes in zulässiger Weise in das Ermessen des Gerichts gestellt wird (vgl. Zöller/Greger, § 253 Rn. 14 f.). Für den Einwand der Beklagten, es handele sich um mehrere Streitgegenstände, die in einem unzulässigen Alternativverhältnis stünden, bleibt kein Raum.

2.

Auch der mit dem Antrag zu 2) geltend gemachte Feststellungsantrag ist zulässig.

a)

Dieser genügt dem Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO.

Der Klageantrag ist hinreichend bestimmt, wenn dieser Art und Umfang des begehrten Rechtsschutzes benennt, indem eine konkrete Bezeichnung des erhobenen Anspruches durch eine gegenständliche Beschreibung erfolgt (vgl. MüKoZPO/Becker-Eberhard, 6. Aufl. 2020, ZPO § 253 Rn. 88).

Dem Antrag zu 2) lässt sich hinreichend bestimmt entnehmen, dass der Kläger festgestellt wissen will, dass die Beklagte verpflichtet ist, dem Kläger sämtliche künftige Schäden zu ersetzen, die dem Kläger aufgrund der missbräuchlichen Datenabgreifung entstanden sind bzw. noch entstehen werden. Unter Berücksichtigung der Replik des Klägers vom 10.10.2022 lässt sich der Antrag zu 2) zudem so auslegen, dass der Kläger lediglich den Ersatz künftiger materieller Schäden begehrt.

b)
Daneben liegt auch das für den Antrag zu 2) erforderliche Feststellungsinteresse gemäß § 256 Abs. 1 ZPO vor. Der Kläger hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt.
Das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BeckOK ZPO/Bacher, 46. Ed. 1.9.2022, ZPO § 256 Rn. 24, Rn. 34).
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 der Name des Klägers im Internet zu künftigen materiellen 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.

3.

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

Soweit die Beklagte rügt, dass die Formulierung „*nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“* im Klageantrag zu 3. a.) zu unbestimmt sei, führt dieses nicht zur Unzulässigkeit des Antrags.

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. Etwas anderes kann dann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt.

Eine auslegungsbedürftige 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 = GRUR 2017, 422 m.w.N.). Unzulässigkeit liegt hingegen vor, wenn die Klägerseite seinen Antrag ohne weiteres konkreter fassen kann (vgl. BGH, Urteil vom 11.6.2015 – I ZR 226/13 = GRUR 2016, 88).

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.

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 zukünftige unrechtmäßige Datenverarbeitung zu verhindern, da der Kläger keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat.

Dass mit dem Klageantrag zu 3.b.) begehrte Anspruchsziel ist ebenfalls hinreichend bestimmt. Das Anspruchsziel wird jedenfalls durch die Klagbegründung hinreichend konkretisiert.

II.

1.
Dem Kläger steht gegen die Beklagte einen 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.

aa)

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.

(1)

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

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. 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.

(2)

Gemäß Art. 13 DSGVO hat der Verantwortliche eines Datenverarbeitungsprozesses gegenüber dem Betroffenen, dessen personenbezogene Daten verarbeitet und bei diesem erhoben werden, umfangreiche Informations- und Aufklärungspflichten zu erfüllen. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen diese Informations- und Aufklärungspflichten bereits mit der Erhebung personenbezogener Daten. Teilt der Verantwortliche dem Betroffenen bereits bei Datenerhebung die in Art. 13 Abs. 1 und Abs. 2 DSGVO vorgesehenen Informationen nicht vollständig oder inhaltlich unrichtig mit, verletzt er seine Informationspflichten.

Nach Art. 13 Abs. 1 lit. c) DSGVO besteht eine Informationspflicht insbesondere dahingehend, dass der Verantwortliche dem Betroffenen die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung mitteilt. Sinn und Zweck dieser Regelung ist, dass der Betroffene eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges, sondern darüber hinaus auch über die Zwecke der Verarbeitung unterrichtet wird (Ehmann/Selmayr/Knyrim, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1).

(a)

Die Beklagte hat den Kläger bei Datenerhebung hinreichend darüber aufgeklärt, dass dessen Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“, zu Werbezwecken sowie zum Zweck der Kommunikation mit Facebook verwendet wird. Dem steht bezogen auf die „Zwei-Faktor-Identifizierung“ nicht entgegen, dass der Benutzer im Rahmen der Rubrik „Handy-Einstellungen“ vorrangig darauf hingewiesen wird, dass dieser mit einer aktuellen Handynummer sein Passwort zurücksetzen kann, und erst per Unterverlinkung durch einen Klick auf „Mehr dazu“ auf die zweistufige Authentifizierung hingewiesen wird. Bereits die Information auf der Oberfläche „Handy-Einstellungen“ ist für einen Benutzer hinreichend verständlich und ist mit den Grundsätzen einer fairen und transparenten Verarbeitung von personenbezogenen Daten vereinbar.

(b)

Eine Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO kann nicht schon darin gesehen werden, dass seitens der Beklagten kein Hinweis bei Erhebung der Daten der Mobilfunknummer des Klägers erfolgt ist, dass bei der voreingestellt 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.

(c)

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.

Die Kammer vermochte nicht festzustellen, dass die Beklagte den Kläger bei Datenerhebung über den Zweck, seine Mobilfunknummer über die „Zwei-Faktor-Authentifizierung“ hinaus auch für das durch sie verwendete CIT zu verwenden, aufgeklärt hat. 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.

(aa)
Die Beklagte hatte gegenüber dem Kläger bei Datenerhebung eine Informations- und Aufklärungspflicht nach Art. 13 Abs. 1 lit. c) DSGVO dahingehend, diesen über die beabsichtigte Verwendung seiner Mobilfunknummer für das CIT aufzuklären.
Durch die Verwendung des CIT ermöglicht die Beklagte einem Benutzer den Abgleich, der in seinem Smartphone gespeicherten Personenkontakte mit auf Facebook registrierten Benutzerprofilen, die ihr Benutzerprofil jeweils mit einer Mobilfunknummer verknüpft haben. Durch die Eingabe einer beliebigen Mobilfunknummer wird dem Benutzer ermöglicht, das mit der Mobilfunknummer verknüpfte Benutzerprofil als „Freunde“ hinzuzufügen.

(bb)
Der Datenrichtlinie lässt sich eine Aufklärung über das von der Beklagte verwendete CIT nicht entnehmen.
Der mit der Anlage B9 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.

(cc)

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 – wie bereits ausgeführt – zum einen 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.

(dd)

Ein Hinweis auf die Verwendung des CIT lässt sich ferner nicht den auszugsweise dem Hilfebereich entnommenen Informationen, überreicht als 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.

bb)

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.

Denn 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.

Art. 32 DSGVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Er konkretisiert die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DSGVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 1).

Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Paal/Pauly/Martini, 3. Aufl. 2021, DSGVO Art. 32 Rn. 2; vgl auch Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DSGVO Art. 32 Rn. 2).

Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO sind dabei der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als Faktoren zu berücksichtigen. Dies bedeutet allerdings nur, dass sie in die Verhältnismäßigkeitsprüfung einzustellen, jedoch nicht notwendigerweise absolut zu befolgen sind (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 14).

Die DSGVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere weiter fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten müssen. Dabei kommt es letztlich darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4;

Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 41).

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen und Auftragsverarbeiter aber nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 3).

Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Diese sind zwingend in die Risikobetrachtung einzubeziehen (Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 5).

Ausweislich des Erwägungsgrunds 76 zur DSGVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten des betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklagte zumindest nicht ausreichend nachgekommen. Denn die von ihr behaupteten „Anti-Scraping-Maßnahmen“ sind selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO. Beim Zugang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses

Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34).

So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf Facebook sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum Facebook-Profil, bei dem diese angegeben wurde, ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Facebook-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden.

Dieses zwingend zu berücksichtigende Risiko bedingt bereits, dass der Maßstab für die Bestimmung der Angemessenheit des Schutzniveaus entsprechend hoch anzusetzen ist. Dies begründet sich unter anderem daraus, dass das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagten darstellt. Auch handelt es sich bei den Daten nicht um ohnehin öffentlich einsehbare Daten. Vielmehr wird Dritten ein Zugang zu diesen, insbesondere der Telefonnummer des Nutzers, gewährt. Es erfolgt eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren Daten des Nutzers auf der Facebook-Plattform der Beklagten.

Die Gefahr einer Veröffentlichung aller zusammengetragenen Daten, darunter insbesondere die Verknüpfung von Telefonnummer und Name, ist, wie der vorliegende Datenscraping-Fall aufzeigt, besonders hoch. „Scraping“ ist weit verbreitet und entsprechende Versuche bei dem weltweit genutzten sozialen Netzwerk der Beklagten auch aus einer ex-ante-Sicht zu erwarten gewesen. Dem ist sich auch die Beklagte bewusst. Für sie ist ausweislich ihres Artikels „Die Fakten zu Medienberichten über Facebook-Daten“ vom 06.04.2021 (Anlage B10) Scraping „eine gängige Taktik.“ Die Beklagte musste sich daher darüber bewusst sein, dass Maßnahmen für ein angemessenes Schutzniveau für die personenbezogenen Daten hinsichtlich des Risikos von Scraping zu treffen waren.

Soweit die Beklagte nun darauf abstellt, dass sie gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorgehe, kommt diese Maßnahme erst dann zu tragen, wenn ein Datenscraping tatsächlich

eingetreten ist. Die Daten sind in diesem Stadium bereits entwendet worden. Eine Veröffentlichung oder anderweitiger Missbrauch kann in diesem Stadium praktisch nicht mehr verhindert werden.

Des Weiteren ist die behauptete teilweise Einschränkung des CIT auch nach dem Beklagtenvorbringen erst nach dem streitgegenständlichen Vorfall eingeführt worden.

Auch die Beschäftigung eines Teams von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie CAPTCHA-Abfragen genügen den Anforderungen des Art. 32 DSGVO im vorliegenden Fall allein nicht. Die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den – aus ihrer Sicht im hiesigen Verfahren ausreichenden – Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Datenscraping kommen konnte.

Ungeachtet dessen, ist klarzustellen, dass dies nicht bedeutet, dass die genannten Maßnahmen nicht grundsätzlich den Schutz von personenbezogenen Daten fördern. Aufgrund des hohen Risikopotenzials, das von einem Missbrauch des CIT ausgeht, waren jedoch weitergehende Maßnahmen für ein angemessenes Schutzniveau erforderlich.

CAPTCHA-Abfragen werden z.B. bereits bei geringeren Risiken im Umgang mit personenbezogenen Daten eingesetzt. Die Arbeit des EDM-Teams entfaltet des Weiteren ausweislich des Vorbringens der Beklagten in der Regel erst während eines bereits begonnen Scraping-Prozesses ihre Wirkung, sodass Scraper in diesem Zeitpunkt bereits Datensätze erlangt haben. Außerdem ist es Scrapern möglich, Übertragungsbeschränkungen zu umgehen.

Daher wären weitergehende Maßnahmen notwendig gewesen. Diese hätten beispielsweise so ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind. Es kann ein Missbrauch des CIT in Form von Datenscraping dann zumindest erschwert werden, so z.B. durch die weitere Angabe eines Vornamens, der sich neben der Telefonnummer ebenfalls hochladen ließe. So würden weitere Variablen hinzutreten, die auf eine den Nutzungsbedingungen entsprechende Nutzung des CIT hindeuten. Datenscraper hingegen würden vor das Problem gestellt, dass neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren. Zudem wäre ein höherer Datenverkehr erforderlich, der ggf. den bereits behaupteten Maßnahmen der Übertragungsbeschränkungen und der Arbeit des EDM-Teams einen größeren Nutzen verleihen würde. Dies würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen. Denn laut der

Beklagten sei es Hauptzweck der Facebook-Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Das CIT ermöglicht dementsprechend Nutzern, ihre Kontakte ihrer Mobilgeräte auf Facebook hochzuladen und anhand der Telefonnummern die Facebook-Profile ihrer Kontakte zu finden. Weitergehende Angaben laufen diesen Absichten nicht zuwider, zumal diese ggf. ebenfalls über das CIT automatisch über die Kontaktliste des Mobilgeräts des Nutzers in Erfahrung gebracht werden könnten.

Diese oder andere Schutzmaßnahmen, wie die klägerseits angeführten Begrenzungen der abgleichbaren Rufnummern oder Nutzung nur für Freunde von Freunden, implementierte die Beklagte jedoch vor oder während des streitgegenständlichen Datenscrapings nicht. Erst im Nachgang implementierte die Beklagte eine vergleichbare Sicherheitsmaßnahme, der sog. „Social Connection Check“. Die Beklagte nahm damit vielmehr erst den Vorfall zum Anlass ihre Schutzmaßnahmen zu evaluieren und traf ausweislich ihres als Anlage B11 vorgelegten Artikel „Scraping nach Zahlen“ vom 19.05.2021 „eine Reihe von Verbesserungen“ im September 2019.

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

cc)

Die Beklagte hat zudem ihre Meldepflicht aus Art. 33 DSGVO verletzt. Gemäß Art. 33 Abs. 1 DSGVO meldet 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, 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 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, ob unbeabsichtigt oder unrechtmäßig 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 Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 33 Rn. 5; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 33 Rn. 6 m.w.N.). Eine Verletzung liegt auch dann vor, wenn im Rahmen bestehender Zugriffsrechte Daten zweckentfremdet werden (Spindler/Schuster/Laue, DS-GVO Art. 33 Rn. 7).
Nach der Stellungnahme 3/2014 der Artikel-29-Datenschutzgruppe erfolgt eine Kategorisierung in unterschiedliche Arten von Verletzungen der Sicherheit, namentlich der „Verletzung der Vertraulichkeit“, bei der es zu einer unbefugten oder unbeabsichtigten Offenlegung von oder zu einem Zugriff auf personenbezogene Daten kommt, der „Verletzung der Verfügbarkeit“, bei der es zu einem unbeabsichtigten oder unbefugten Verlust von, Zugriff auf, oder Vernichtung von personenbezogenen Daten kommt, sowie der „Verletzung der Integrität“, bei der es zu einer unbefugten oder unbeabsichtigten Veränderung von personenbezogenen Daten kommt. Eine Verletzung der Vertraulichkeit von Daten liegt auch immer dann vor, wenn die Ebene, auf der die Daten zur Verfügung stehen, geändert wurde (Artikel-29-Datenschutzgruppe, Stellungnahme 3/2014 on Personal Data Breach Notification, WP 213, S. 18).
Eine solche Verletzung der Vertraulichkeit ist festzustellen. Denn 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.
Dass die Leitlinien des Europäischen Datenschutzausschusses das „Scraping“ selbst nicht ausdrücklich als eines der Beispiele für eine Verletzung des Schutzes persönlicher Daten nennen, ist unbeachtlich, da diese ausdrücklich nicht abschließend sind (vgl. Guidelines 01/2021 on Examples regarding Data Breach Notification:
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf).

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 Recht 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, DS-GVO 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).

dd)
Auch ein Verstoß gegen Art 34 Abs. 1 DSGVO liegt vor. Nach dieser Vorschrift benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der

Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich ein hohes Risiko für seine persönlichen Rechte und Freiheiten zur Folge hat.

Auch ein Verstoß gegen diese Vorschrift ist geeignet, einen Schadensersatzanspruch zu begründen (OLG Frankfurt a.M. GRUR 2022, 1252; Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 34 Rn. 32; Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage 2019, § 11 Rn. 4).

Die Benachrichtigung muss grundsätzlich gegenüber der betroffenen Person i.S.v. Art. 4 Nr. 1 DSGVO erfolgen. Insofern bedarf es der Bestimmung der durch den Vorfall konkret betroffenen Personen. Der in Art. 34 Abs. 1 Hs. 2 DSGVO gewählte Singular „Person“ verdeutlicht, dass in den Fällen des Art. 34 regelmäßig eine individuelle Information bezüglich des Datenschutzvorfalls erfolgen muss (Gola/Heckmann/Reif DS-GVO Art. 34 Rn. 4). Eine solche individualisierte Information des Klägers ohne schuldhaftes Verzögern nach Offenbarung der Verletzung des Schutzes personenbezogener Daten im Jahr 2019 hat die Beklagte nicht vorgenommen.

Die hier vorliegende Verletzung des Schutzes personenbezogener Daten hat voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge. Ein solches Risiko besteht dann, wenn zu erwarten ist, dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten des Betroffenen eintritt. In einem solchen Fall ist es nicht maßgeblich, ob die Datenschutzverletzung auch zu einen besonders hohen Schadensumfang führt (vgl. BeckOK DatenschutzR/Brink, DS-GVO Art. 34 Rn. 25.). Ein solcher Schaden ist bereits eingetreten (s.u.).

Eine Ausnahme von der Benachrichtigungspflicht ist im hiesigen Fall nicht einschlägig.
Nach Art 34 Abs. 3 a) DSGVO ist eine Benachrichtigung nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt hat, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung. Entsprechend der Ausführungen zu dem Verstoß gegen Art. 32

DSGVO hat die Beklagte vorliegend keine geeigneten Sicherheitsvorkehrungen getroffen.

Ferner ist eine Benachrichtigung nicht gem. Art. 34 Abs. 3 c) DSGVO entbehrlich. Dafür müsste die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden sein. In diesem Fall hätte stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.
Zwar kann sich aus einer Vielzahl an betroffenen Personen ein unverhältnismäßiger Zeit- bzw. Kostenaufwand ergeben. Allerdings kann von einem unverhältnismäßigen Aufwand nicht ausgegangen werden, wenn die betroffenen Personen bekannt sind und deren Emailadressen vorliegen. Im Übrigen setzt die öffentliche Bekanntmachung voraus, dass die Betroffenen vergleichbar wirksam informiert werden. Ob eine Publikation des Vorfalls auf der eigenen Homepage ausreicht, hängt davon ab, inwiefern der Internetauftritt vom betroffenen Personenkreis regelmäßig besucht wird. Jedenfalls darf die Bekanntmachung des Vorfalls auf der Website nicht versteckt werden. Es bedarf eines an herausragender Stelle platzierten Banners bzw. einer entsprechend deutlichen Meldung. Gegebenenfalls muss die Information sowohl über digitale, als auch über analoge Kanäle erfolgen. Demnach ist die ausschließliche Benachrichtigung durch eine Pressemitteilung oder in einem Unternehmensblog kein wirksames Mittel, um die betroffenen Personen von einer Datenschutzverletzung in Kenntnis zu setzen (Gola/Heckmann/Reif DS-GVO Art. 34 Rn. 17 m.w.N.).
Nach dem Vortrag der Beklagten genügen ihre Maßnahmen nicht den Anforderungen des Art. 34 DSGVO. Zum einen sind die betroffenen Personen und ihre Emailadressen bekannt, sodass schon nicht von einem unverhältnismäßigen Aufwand in Bezug auf eine individuelle Benachrichtigung auszugehen ist. Im Übrigen hat die Beklagte lediglich darauf verwiesen, dass sie am 06.04.2021 in dem Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ erläutert habe, dass die Daten nicht durch einen Hack erlangt worden seien, sondern es sich um öffentlich einsehbare Informationen handele. Diese Mitteilung erfolgte weder rechtzeitig, noch auf einem probaten Weg, um den Anforderungen an eine öffentliche Bekanntmachung zu genügen. Die Informationen, die die Beklagte im Rahmen der Privatsphäre-Einstellungen zum Thema „Scraping“ zur Verfügung stellte, stellen schon keinen Bezug zu dem konkreten Vorfall her und sind im Übrigen nicht an einer herausragender Stelle platziert. Vielmehr hätte die Bekanntmachung auf der

Startseite eines jeden Nutzers erfolgen müssen. Das Schreiben vom 23.08.2021 versandte die Beklagte jedenfalls nicht rechtzeitig.

ee)
Die Beklagte verstößt mit ihren Grundeinstellungen zur Sichtbarkeit zumindest hinsichtlich der Emailadresse und zur Suchbarkeit über die Telefonnummer der Benutzer der Facebook-Plattform gegen Art. 25 DSGVO.

Dies verhilft der Klägerin indes jedoch nicht zu einem Anspruch gem. Art. 82 Abs. 1 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). „Datenschutz durch Voreinstellungen“ soll insbesondere diejenigen Nutzer schützen, welche die datenschutztechnischen Implikationen der Verarbeitungsvorgänge entweder nicht zu erfassen in der Lage sind oder sich darüber keine Gedanken machen und sich deshalb auch nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen, obwohl der Telemediendienst ihnen diese Möglichkeit prinzipiell eröffnet (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25 Rn. 13). 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. Abs. 2 verlangt aber nicht, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. Dem Wortlaut nach ist daher auch eine besonders datenintensive Voreinstellung mit Abs. 2 vereinbar, wenn der Zweck der Verarbeitung dies erfordert. Vor dem Hintergrund der Schutzrichtung des Abs. 2, den Nutzer vor einer Überrumpelung oder dem Ausnutzen seiner Unerfahrenheit zu schützen, muss der Verantwortliche aber stets sicherstellen, dass

die geplante Datennutzung auch für einen nicht-technikaffinen Nutzer hinreichend transparent ist. (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 18 f.).

Gegen diese Regelungen verstößt die Beklagte. Die Facebook-Plattform der Beklagten sah standardmäßig vor, dass neben den verpflichtenden öffentlichen Daten (Name, Geschlecht, Nutzer-ID) auch weitere Angaben des Nutzers öffentlich einsehbar waren. Hier gehörten einzelne Informationen auf seinem Facebook-Profil, wie etwa Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse. Allein die Telefonnummer war standardmäßig nur für einen selbst bzw. Freunde einsehbar. Die „Suchbarkeits-Einstellungen“ sahen jedoch in ihrer Standard-Voreinstellung unabhängig von der Einsehbarkeit der Telefonnummer vor, dass alle Personen mittels dieser die hinter den Nummern stehenden Facebook-Profile finden konnten. Die Nutzer mussten selbst aktiv werden, um ihre Daten Dritten weniger zugänglich zu machen.

Diese Voreinstellungen entsprechen nicht den Anforderungen, die insbesondere Art. 25 Abs. 2 S. 3 DSGVO normiert. Die Vorschrift ist insbesondere auf soziale Netzwerke ausgerichtet (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 20; Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 28, 31; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 25 Rn. 12). Demnach muss sichergestellt sein, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Der Nutzer muss demnach die Möglichkeit haben, die Veröffentlichung seiner personenbezogenen Daten aktiv zu steuern. Übertragen auf die sozialen Netzwerke folgt daraus, dass der Nutzer selbst festlegen können muss, ob und mit wem er Inhalte innerhalb eines Netzwerks teilt. Aus Abs. 2 S. 3 folgt in diesem Fall die Verpflichtung für den Betreiber des Netzwerks, die Default-Einstellungen so zu treffen, dass Inhalte der Nutzer nicht standardmäßig mit anderen Nutzern oder Dritten geteilt werden. Als Voreinstellung ist der kleinstmögliche Empfängerkreis vorzusehen (vgl. Ehmann/Selmayr/Baumgartner a.a.O.; Gola/Heckmann/Nolte/Werkmeister a.a.O; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 69). Entgegen der Ansicht der Beklagten darf es von den Nutzern nicht erforderlich sein, selbst aktiv individuelle Anpassungen vorzunehmen, die erst dann zu einer geringeren Zugänglichkeit ihrer Daten führen. Es sind vielmehr Voreinstellungen zu treffen, die entgegengesetzt zum Vorgehen der Beklagten den Nutzern die Möglichkeit verschaffen, ihre Angaben über den Personenkreis hinaus zugänglich zu

machen, der standardmäßig vorgesehen ist. Alternativ ist auch die Gestaltung denkbar, die den Nutzer zu einer Entscheidung für oder gegen die Einsehbarkeit bzw. Suchbarkeit zwingt (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 69).

Die Voreinstellungen auf „Alle“ in der Zielgruppenauswahl sowie für die Telefonnummer in den Suchbarkeits-Einstellungen lassen sich auch nicht für alle vom Nutzer angegebenen Daten mit dem von der Beklagten behaupteten Unternehmenszweck rechtfertigen. Der Unternehmenszweck der Beklagten besteht laut ihrer Angabe im hiesigen Verfahren darin, Menschen die Möglichkeit zu geben, Gemeinschaften zu bilden, und die Welt näher zusammenzubringen. Menschen würden die Facebook-Plattform nutzen, um mit Freunden und Familie in Verbindung zu bleiben, um zu erfahren, was in der Welt vor sich geht, sowie um sich mit bedeutsamen Gemeinschaften und Anliegen, die ihnen wichtig sind, zu verknüpfen. Eine öffentliche Einsehbarkeit der persönlichen Daten wie Name, Geburtsdatum, Wohnort, Interessen etc. ließe sich zwar anhand des o.g. Zwecks erklären. Denn Nutzer finden Kontakte in sozialen Netzwerken in der Regel über Namen, geographische Nähe, gemeinsame Lebensabschnitte, z.B. während der Ausbildung oder der Berufsausübung, oder über gemeinsame Interessen.

Dies gilt jedoch nicht hinsichtlich der E-Mail-Adresse sowie die Suchfunktion über die Handynummer. Eine Kontaktaufnahme anhand der öffentlich einsehbaren Emailadresse erscheint der Kammer nach allgemeiner Lebenserfahrung als zumindest untypisch. Dies gilt ebenfalls über die Suche über die Telefonnummer. Soweit eine Person die Telefonnummer einer anderen Person bereits hat, ist eine Vernetzung dieser durch telefonische Kontaktaufnahme durchführbar. In diesem Rahmen ist es auch möglich, sich gegenseitig auf der Facebook-Plattform zu finden. Eine Suchbarkeit über die Telefonnummer ist dann obsolet. Diese Einstellung sowie das „CIT“ unterliegen – wie das „Datenscraping“ aufzeigte – vielmehr einer Missbrauchsgefahr durch Dritte.

Nach alledem lässt sich zumindest für die Voreinstellungen der Beklagten über die Einsehbarkeit der Emailadresse und die Suchbarkeit über die Telefonnummer für „Alle“ ein Verstoß gegen Art. 25 DSGVO feststellen.

Allein aus einem Verstoß gegen Art. 25 DSGVO kann wegen seines organisatorischen Charakters ein Anspruch nach Art. 82 Abs. 1 DSGVO jedoch nicht begründet werden (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO

Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31). Die Vorschrift entfaltet bereits vor dem eigentlichen Beginn der Datenverarbeitung ihren Regelungscharakter. Zu diesem, einer tatsächlichen Datenverarbeitung vorgelagerten Zeitpunkt, entfaltet die DSGVO jedoch nach Art. 2 Abs. 1 DSGVO noch keine Wirkung. Die Anwendbarkeit der DSGVO setzt vielmehr eine tatsächliche Verarbeitung personenbezogener Daten voraus (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DSGVO setzt daher darüber hinaus voraus, dass weitere Verstöße gegen die DSGVO vorliegen (vgl. Gola/Heckmann/Nolte/Werkmeister a.a.O.).

ff)

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)

Der Beklagten gelingt zur Abwendung des Anspruchs auch nicht die Exkulpation gem. Art. 82 Abs. 3 DSGVO. Demnach gelingt eine Befreiung nur, wenn der Verantwortliche oder der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Damit wird die Verantwortlichkeit der Beklagten widerleglich vermutet.

Zwar ist der Begriff der Verantwortlichkeit i.S.d. § 82 Abs. 3 DSGVO nicht näher definiert. So wird dieser vorwiegend mit dem Begriff des Verschuldens gleichgesetzt (vgl. OLG Stuttgart 31.3.2021 – 9 U 34/21; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 24; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 49). Teilweise wird dies hingegen nicht angenommen mit der Folge, dass Art. 82 DSGVO möglicherweise als Gefährdungshaftungstatbestand zu begreifen sei, sodass dem Verantwortlichen oder Auftragsverarbeiter unabhängig von jedwedem Verschulden lediglich ganz ungewöhnliche Kausalverläufe, die jeder Lebenserfahrung widersprechen, sowie Fälle höherer Gewalt und weit überwiegenden eigenen Fehlverhaltens der betroffenen Person nicht anzulasten seien (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 18). Hierauf kommt es vorliegend jedoch nicht an. Denn der Beklagten gelingt weder der Nachweis fehlenden Verschuldens noch des Vorliegens ganz ungewöhnlicher Kausalverläufe, eines Falles höherer Gewalt oder weit überwiegenden eigenen Fehlverhaltens des Klägers.

Die Beklagte kann nicht nachweisen, dass sie im vorliegenden Fall kein Verschulden trifft. Das wäre nur dann der Fall, wenn sie sämtliche Sorgfaltsanforderungen erfüllt hat und ihm nicht die geringste Fahrlässigkeit vorzuwerfen ist (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54 m.w.N.; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 82 Rn. 11). Das Verschulden wird vorliegend bereits allein dadurch indiziert, dass sich ein Verstoß der Beklagte gegen Art. 25 DSGVO feststellen lässt. Denn jedenfalls wohnt einem Verstoß gegen Art. 25 DSGVO praktisch immer eine Erhöhung der Gefahr eines Schadens inne. Eine Exkulpation ist dann nicht bzw. nur unter erschwerten Bedingungen möglich (Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31; Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 25 Rn. 77).

Soweit die Beklagte hierzu vorträgt, dass sie ihre Pflichten aus der DSGVO nicht verletzt hat, verfängt dies aufgrund der obigen Ausführungen bereits nicht. Auch der Verweis der Beklagten auf fehlende Rechtsprechung, aufsichtsbehördliche Leitlinien oder Literatur hinsichtlich des Umgangs mit Scraping-Sachverhalten verhilft dieser nicht zu einer Exkulpation. Es lässt sich hieraus schon nicht entnehmen, dass die Beklagte sämtliche Sorgfaltsanforderungen erfüllt hat oder ihr nicht die geringste Fahrlässigkeit vorzuwerfen ist. Vielmehr nutzten Dritte bereits erkannte oder erkennbare Angriffswege, um auf Daten zuzugreifen, sodass die Nichtverantwortlichkeit des Verantwortlichen nicht nachgewiesen werden kann (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 15; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54). Scraping ist ausweislich des Beklagtenvorbringens „eine gängige Taktik“. Es war jedenfalls erkennbar, dass das CIT durch Scraping ausgenutzt werden kann. Dies begründet sich bereits aus dem Umstand, dass die Beklagte selbst Schutzmaßnahmen behauptet und somit von der Notwendigkeit dieser ausgeht. Im Übrigen behauptet die Beklagte das Vorliegen ganz ungewöhnlicher Kausalverläufe, einen Fall höherer Gewalt oder ein weit überwiegendes eigenes Fehlverhalten des Klägers nicht.

c)

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

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.). So stellt auch der Generalanwalt in seinen Schlussanträgen im Rahmen des Vorabentscheidungsersuchens des österreichischen Obersten Gerichtshofs vom 12.05.2021 auf das Erfordernis eines konkreten Schadens ab (Generalanwalt beim EuGH Schlussantrag v. 6.10.2022 – C-300/21, BeckRS 2022, 26562).

Der Begriff des Schadens ist nach dem Erwägungsgrund 146 S. 3 im Lichte der Rechtsprechung des Europäischen Gerichtshofs weit und auf eine Art und Weise auszulegen, die den Zielen der Verordnung in vollem Umfang entspricht. Die Ziele der DSGVO bestehen dabei u.a. darin, den Risiken für die Rechte und Freiheit natürlicher Personen zu begegnen, die – mit unterschiedlicher

Eintrittswahrscheinlichkeit und Schwere – aus einer Verarbeitung personenbezogener Daten hervorgehen und zu einem immateriellen Schaden führen können (LAG Hamm, BeckRS 2021, 21866). In den Erwägungsgründen 75 und 85 wird der Kontrollverlust über die personenbezogenen Daten gerade als ein Beispiel für das Vorliegen eines solchen Schadens aufgeführt.

Ein derartiger Kontrollverlust ist aus Sicht des Klägers eingetreten, da jedenfalls seine Telefonnummer, Facebook-ID, sein Name und Geschlecht im sog. „Darknet“ auf einer für jedermann abrufbaren Datenbank veröffentlicht wurden. Soweit die Beklagte die Veröffentlichung der Daten im Darknet mit Nichtwissen bestreitet, kann sie damit nicht gehört werden. Im Übrigen tritt der Kontrollverlust– unabhängig von der Veröffentlichung im „Darknet“ – bereits durch den „Scraping“-Vorfall und das damit verbundene Abschöpfen der Daten ein.

Unerheblich ist, dass der Name, das Geschlecht und die Facebook-ID nach den Nutzereinstellungen des Klägers öffentlich waren. Denn jedenfalls die Verknüpfung mit seiner Telefonnummer war bis dahin nicht hergestellt. Darüber hinaus sieht Erwägungsgrund 75 vor, dass ein immaterieller Schaden auch dann anzunehmen ist, wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von Personen betrifft. Auch dies ist aufgrund der Tatsache, dass im Rahmen des „Scraping“-Vorfall die Daten von Millionen von Facebook-Nutzern veröffentlicht wurden, anzunehmen.

Ob eine erhebliche Beeinträchtigung etwa in Form eines schwerwiegenden Persönlichkeitseingriffs vorliegen muss ist umstritten (pro: OLG Dresden NJW-RR 2020, 1370; LG München I GRUR-RS 2021, 33318; LG Karlsruhe BeckRS 2021, 20347; contra: OLG Frankfurt GRUR 2022, 1252 Rn. 63; LAG Hannover, ZD 2022, 61; LG München I GRUR-RS 2021, 41707; LG Lüneburg BeckRS 2020, 36932; Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 18), kann aber im Ergebnis dahinstehen. Zwar geht auch der Generalanwalt in seinen Schlussanträgen davon aus, dass es den nationalen Gerichten obliegt herauszuarbeiten, wann ein subjektives Unmutsgefühl die Grenze zwischen bloßem nicht ersatzfähigem Ärger und echtem ersatzfähigen immateriellen Schaden überschreitet (Generalanwalt beim EuGH Schlussantrag v. 6.10.2022 – C-300/21, BeckRS 2022, 26562). Vorliegend handelt es jedoch nicht um einen bloßen Bagatellschaden. Denn durch die Veröffentlichung der personenbezogenen Daten des Klägers im „Darknet“ ist die Weiterverarbeitung durch einen unbegrenzten und unbestimmten Personenkreis, insbesondere auch für den gezielten Missbrauch etwa in Form von Betrugsanrufen, ermöglicht.

d)

Die Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO ist kausal für den bei dem Kläger entstandenen Schaden.
Der Verantwortliche haftet lediglich für kausal durch die rechtswidrige Verarbeitung verursachte Schäden (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 41). Gemäß vorstehender Erwägungen hat die Beklagte den Kläger bereits bei Erhebung seiner Mobilfunknummer nur unzureichend über die Verwendung seiner Mobilfunknummer im Hinblick auf das CIT aufgeklärt, sodass bezogen auf die Mobilfunknummer eine rechtswidrige Verarbeitung vorliegt. Diese ist auch kausal für den beim Kläger entstandenen Schaden, da es durch die Verwendung des CIT zu einem Kontrollverlust auf Seiten des Klägers kam.

Auch der Verstoß gegen Art. 32, 24, 5 Abs. 1 f) DSGVO ist für den eingetretenen Schaden kausal, denn durch die unzureichenden Schutzmaßnahmen ermöglichte bzw. erleichterte die Beklagte ein Ausnutzen des CIT durch Scraping. Dieses hat einen Kontrollverlust über die personenbezogenen Daten zur Folge.

Der Schaden beruht zudem kausal auf einem Verstoß gegen Art. 33 und Art 34 DSGVO. Dabei ist zu beachten, dass bei der Auslegung europarechtlicher Regelungen eine effektive Anwendung des Europarechts zu gewährleisten ist (BeckOK DatenschutzR/Quaas, 41. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 26a). Eine Mitursächlichkeit des Verstoßes genügt (OLG Stuttgart ZD 2021, 375; LG Köln ZD 2022, 52 Rn. 21). Zwar ist der geltend gemachte Kontrollverlust bereits durch das „Scraping“ der Daten erstmals eingetreten. Durch die unterlassene Benachrichtigung des Klägers wurde ihm jedoch die Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren. Auch die zuständige Datenschutzbehörde konnte mangels rechtzeitiger Meldung keine Schritte zur Risikominimierung und Absicherung der Daten einleiten.

e)

Die Kammer hält ein Schmerzensgeld von 350,00 € für angemessen, aber auch ausreichend, um einerseits der Ausgleichs- und Genugtuungsfunktion zu genügen, und andererseits der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung zu tragen. Dabei hat das Gericht von dem ihm gem. § 287

Abs. 1 ZPO eingeräumten Ermessen Gebrauch gemacht (vgl. BAG NJW 2022, 2779 Rn. 14 ff.).

Unter Berücksichtigung des Erwägungsgrundes 146 S. 6 soll die betroffene Person einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden erhalten. Zur Bemessung der Höhe des immateriellen Schadensersatzes können die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden (so LAG Hamm BeckRS 2021, 21866; BeckOK DatenschutzR/Quaas, 41. Ed. 1.8.2022, DS-GVO Art. 82 Rn. 31; Wybitul/Haß/Albrecht NJW 2018, 113, 115; LG Saarbrücken, ZD 2022, 163 hat die Frage dem EuGH vorgelegt; dahinstehen lassend: BAG NJW 2022, 2779 Rn. 17). Nach dieser Vorschrift sind für die Ermittlung der Höhe einer Geldbuße u.a. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens, frühere einschlägige Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten zu betrachten. Je intimer, finanziell bedrohlicher, potentiell ehrverletzender oder kränkender und persönlich wichtiger die abgeflossenen Daten sind, desto höher muss der immaterielle Schaden ausfallen (Dickmann r+s 2018, 345, 353).

Darüber hinaus ist zu berücksichtigen, dass dem Schadensersatzanspruch unter Berücksichtigung der Erwägungsgründe 75 und 85 eine abschreckende Wirkung zukommen und der Datenschutzgrundverordnung durch eine empfindliche Anspruchshöhe zu einer effektiven Geltung verhelfen soll (EuGH NJW 2016, 1080; Wybitul/Haß/Albrecht NJW 2018, 113, 115; BeckOK DatenschutzR/Quaas, DS-GVO Art. 82 Rn. 32). Wenn es zu vielen Fällen von Rechtsverstößen durch den gleichen Verantwortlichen kommt, kann die Abschreckung allerdings auch in der Breite der Schadensersatzpflicht, d.h. in der Summe aller immateriellen Ersatzansprüche gesehen werden (OLG Koblenz VuR 2022, 347, 353).

Wesentlich sind am Ende allerdings die konkreten Umstände des Einzelfalles (so auch BAG v. 26.8.2021 – 8 AZR 253/20).

Vorliegend hat das Gericht seiner Entscheidung zugrunde gelegt, dass sich die Beklagte mehrere Verstöße gegen die DSGVO vorwerfen lassen muss, die einen sehr weitgehenden Kontrollverlust der personenbezogenen Daten des Klägers ermöglicht und begünstigt haben. Hinzu kommt, dass der Kläger plausibel und glaubhaft den Erhalt von Spam-Anrufen und Phishing-SMS mit vermögensschädigenden Inhalten geschildert hat. Im Rahmen seiner persönlichen

Anhörung hat der Kläger erklärt, dass er derzeit zwei bis drei Nachrichten pro Woche erhalte. Vor dem Scraping-Vorfall habe er zwar auch schon gelegentlich Phishing-Nachrichten erhalten, jedoch habe die Häufigkeit deutlich zugenommen.
Eine Reduzierung des klägerseits angegebenen Mindestbetrages war indes gerechtfertigt, da das Gericht im Rahmen der persönlichen Anhörung des Klägers keine besondere persönliche Betroffenheit feststellen konnte. So hat der Kläger keine besonderen Maßnahmen ergriffen, um seine Daten zu schützen. Zwar hat der Kläger im Rahmen seiner persönlichen Anhörung erklärt, dass er seine Passwörter geändert und seine Einstellungen auf möglichst privat eingestellt habe, er nutze Facebook jedoch weiterhin sowohl privat als auch im Rahmen seines Gewerbes. Generell wurde bei der Anhörung deutlich, dass der Kläger keine besonders hohe Sorgfalt auf den Schutz seiner privaten Daten zu verwenden scheint. So nutzt er sowohl für den privaten, als auch für den gewerblichen Bereich eine einheitliche Handynummer. Diese ist zudem auf der Internetseite seines Gewerbebetriebes veröffentlicht. Daneben besitzt der Kläger noch immer einen Account bei Instagram. Er ist also in einem weiteren sozialen Netzwerk aktiv, welches gewerbsmäßig Daten seiner Nutzer verarbeitet und verwertet.

Der geltend gemachte Anspruch auf Rechtshängigkeitszinsen folgt aus §§ 288, 291 BGB.

2.
Der mit dem Antrag zu 2) geltend gemachte Feststellungsantrag ist auch begründet. Da der Antrag zu 1) begründet ist, ist mit Blick auf die vom Kläger gesetzte innerprozessuale Bedingung auch über den Antrag zu 2) zu entscheiden.

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.

3.
Der Kläger kann von der Beklagten in der Sache auch die Unterlassung im beantragten Umfang (vgl. Klageanträge 3. a.) u. 3. b.)) verlangen. Dies folgt aus Art. 17 DSGVO.

Art. 17 DSGVO iVm Art. 6 DSGVO sieht in der Rechtsfolge ein Recht auf Löschung („Recht auf Vergessenwerden“) vor; nicht hingegen einen Anspruch auf Unterlassung.

Nach Art. 17 Abs. 1 DSGVO hat die betroffene Person unter bestimmten Voraussetzungen das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Die DSGVO definiert hingegen nicht, was unter Löschung zu verstehen ist. Jedoch lässt sich aus dem in Art. 17 Abs.1 DSGVO normierten Recht betroffener Personen, unter gewissen Umständen vom Verantwortlichen zu verlangen, sie betreffende personenbezogene Daten unverzüglich zu löschen, auch ein Anspruch auf Unterlassung ihrer Verarbeitung für die Zukunft ableiten (Argumentum a maiore ad minus). Dies folgt grundsätzlich auch aus Art. 79 DSGVO, der der betroffenen Person einen „wirksamen gerichtlichen Rechtsbehelf“ zugesteht (vgl. so auch im Ergebnis OLG Frankfurt/M., Urteil vom 06.9.2018 – 16 U 193/17 = ZD 2019, 78; LG Frankfurt/M., Urteil vom 28.6.2019 – 2-03 O 315/17 = ZD 2019, 410).

Dieses Rechtsverständnis wird auch – wenn auch ohne nähere Begründung - von der höchstrichterlichen Rechtsprechung (vgl. BGH, Urteil vom 12.10.2021 – VI ZR 488/19 = NJW 2022, 1098) geteilt, dem sich die Kammer anschließt. Dem steht auch nicht die beklagtenseits zitierte Entscheidung des VI. Senats des Bundesgerichtshofs (VI ZR 832/20 = GRUR 2022, 1009) entgegen. Vielmehr ist der Senat von einem Unterlassungsanspruch ausgegangen, der sich direkt aus Art. 17 DSGVO ergibt.

Die klägerischen Unterlassungsansprüche sind auch nicht gemäß Art. 79 DSGVO gesperrt. Die Vorschrift soll garantieren, dass eine betroffene Person einen materiell-rechtlichen Anspruch gerichtlich durchsetzen kann; verhält sich jedoch nicht dazu, ob und unter welchen Voraussetzungen ein Unterlassungsanspruch in materiell-rechtlicher Hinsicht besteht. Besteht ein solcher Unterlassungsanspruch – wovon die Kammer nach dem Vorgesagten ausgeht – steht der betroffenen Person über Art. 79 DSGVO auch der gerichtliche Eilrechtsschutz zur Verfügung.

Bei der Aufzählung des „verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs“, der unbeschadet des Art. 79 DSGVO gelten soll, handelt es sich nicht um eine abschließende Aufzählung der weiteren verfügbaren Rechtsbehelfe. Dies folgt auch nicht aus den Erwägungsgründen 9, 11 und 13 DSGVO, in denen von einem „einheitlichen Schutzniveau“ die Rede ist; jedenfalls lässt sich daraus nicht ableiten, dass strengere Regelungen im nationalen Recht keine Gültigkeit haben sollen. Es würde auch dem Effektivitätsgrundsatz des Europarechts sowie

dem Recht auf einen „wirksamen“ gerichtlichen Rechtsbehelf nach Art. 79 DSGVO widersprechen, der betroffenen Person den Rechtsschutz im gerichtlichen Verfahren zu verweigern und sie stattdessen auf eine Beschwerde bei der Aufsichtsbehörde nach Art. 77 DSGVO zu verweisen. Die Formulierung in Art. 79 DSGVO „aufgrund dieser Verordnung zustehenden Rechte“ stellt keinen Verweis (allein) auf Kapitel 3 DSGVO („Rechte der betroffenen Person“) dar. Verletzte Rechte könnten neben solchen, die dem Betroffenen „durch“ die DSGVO zustehen, auch die „aufgrund“ der Verordnung zustehenden Rechte sein, mithin auch solche, die durch andere Rechtsakte gewährt werden. (vgl. VG Wiesbaden, Beschluss vom 01.12.2021 – 6 L 738/21.WI = ZD 2022, 177).

Mit den geltend gemachten Anträgen (vgl. Klageanträge zu 3.a.) u. 3.b.) verfolgt der Kläger auch unzweifelhaft ein Unterlassen, nämlich das Unterlassen personenbezogene Daten ohne ausreichende Sicherheitsvorkehrungen zu verarbeiten bzw. die Verarbeitung der Telefonnummer ohne Erfüllung der Informationspflichten gemäß Art. 13, 14 DSGVO.

Tatbestandsvoraussetzung ist insoweit eine Verletzung der betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nicht im Einklang mit materiellem Datenschutzrecht erfolgte.
Demnach kann der Kläger inhaltlich von der Beklagten die Unterlassung verlangen, seine personenbezogenen Daten unbefugten Dritten zugänglich zu machen.
Die Beklagte hat auch gegen die DSGVO verstoßen, indem sie u.a. ein nicht ausreichendes Sicherheitsniveau vorgehalten hat und damit unbefugten Dritten den Zugriff auf die personenbezogenen Daten des Klägers ermöglicht hat.
Das Zugänglichmachen personenbezogener Daten stellt auch eine Verarbeitung iSd Art. 4 Nr. 2 DSGVO dar. Der Regelungsgehalt der Vorschrift ist weit gefasst und umfasst auch den Umgang mit personenbezogenen Daten unter dem Einsatz von Datenverarbeitungssystemen und deren Speicherung. (vgl. *Schild* in: BeckOK Datenschutzrecht, 41 Edition, Stand: 01.08.2022, DSGVO, Art. 4, Rn. 34).
Die Verarbeitung personenbezogener Daten ist gem. Art. 6 DSGVO nur dann rechtmäßig, wenn eine der in Art. 6 Abs. 1 S. 1 lit. a - f DSGVO genannten Voraussetzungen gegeben sind. Im Streitfall erfolgte das Zugänglichmachen der personenbezogenen Daten der Klägerseite ohne eine der in Art. Art. 6 Abs. 1 S. 1 lit. a - f DSGVO aufgeführten Rechtsgrundlagen.

Dass der Klägerseite zum Zugänglichmachen seine personenbezogenen Daten für Unbefugte eine in informierter Art und Weise erteilte Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO erklärt hat, behauptet die Beklagte schon nicht.
Soweit die Beklagte vorträgt, dass die Datenverarbeitung für die Erfüllung eines Vertrages in Bezug auf die Bereitstellung eines sozialen Netzwerks erforderlich nach Art. 6 Abs. 1 S. 1 lit. b DSGVO gewesen sei, kann dem nicht gefolgt werden. Die Datenverarbeitung für die Erfüllung eines Vertrages setzt immanent voraus, dass technisch ausreichend und gesetzgeberisch geschuldete Sicherheitsmaßnahmen vorgehalten werden, um wie im Streitfall Unbefugten das Zugänglichmachen personenbezogener Daten zu verhindern. Diesen Anforderungen hat die Beklagte jedoch gerade nicht genügt.
Weiterhin besteht auch kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO am Zugänglichmachen der personenbezogenen Daten der Klägerseite für Unbefugte.
Mangels Rechtsgrundlage erfolgte die Verarbeitung der Daten des Klägers deshalb in rechtswidriger Weise. Für den Kläger bestand auch keine Duldungspflicht. Zwar hat die Klägerseite ihre personenbezogenen Daten selbst bei Erstellung ihres Nutzerprofiles angegeben, hierdurch liegt allerdings keine Veröffentlichung dieser vor. Denn diese Angaben wurden ausschließlich der Beklagten gegenüber zum Zwecke der Registrierung gemacht.
Da die personenbezogenen Daten der Klägerseite unrechtmäßig Dritten zugänglich gemacht wurden, können diese Daten unbefugt verwendet werden. Hierdurch wird der Kläger in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt. Weitere Beeinträchtigungen durch eine unrechtmäßige Verwendung personenbezogenen Daten drohen und können nicht ausgeschlossen werden.
Durch die Beeinträchtigung besteht eine tatsächliche Vermutung für die Wiederholungsgefahr, die die Beklagte nicht widerlegt hat.

Dem Kläger steht gegen die Beklagte auch ein Unterlassungsanspruch gem. Art. 17 DSGVO dahingehend zu, eine Datenverarbeitung ohne Erfüllung der Informationspflichten zu unterlassen.
Die Beklagte hat gegen die DSGVO verstoßen, indem sie nicht ausreichend nach Art. 13, 14 DSGVO über die Nutzung der mitgeteilten Mobilfunknummer informiert und den Kläger damit in seinen Rechten verletzt hat. Insoweit wird auf die Begründung im vorangegangen Teil der Entscheidungsgründe Bezug genommen.

Der Kläger musste den Verstoß gegen die Informationspflichten der DSGVO auch nicht dulden.
Da der Kläger nicht den Anforderungen der Art. 13, 14 DSGVO entsprechend aufgeklärt und informiert wurde, ist er in seinen Rechten verletzt worden. Diese Beeinträchtigung besteht sowohl gegenwärtig als auch zukünftig.
Durch die Beeinträchtigung besteht eine tatsächliche Vermutung für die Wiederholungsgefahr, die die Beklagte nicht widerlegt hat.

4.
Dem Kläger steht jedoch der mit dem Klageantrag zu 4.) verfolgte Auskunftsanspruch ggü. der Beklagten nicht zu.

Der Anspruch folgt nicht aus Art. 15 DSGVO. Nach dieser Vorschrift kann die betroffene Person Auskunft über personenbezogenen Daten verlangen, wenn der Verantwortliche sie betreffende personenbezogene Daten verarbeitet hat.
Art. 15 Abs. 1 1 Hs. 1, 2 DSGVO enthält zunächst einen Anspruch der betroffenen Person gegen den Verantwortlichen, ihm zu bestätigen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Verarbeitet der Verantwortliche personenbezogene Daten der betroffenen Person, so hat die betroffene Person gem. Art. 15 Abs. 1 1 Hs. 1, 2 DSGVO ein Recht auf Auskunft über diese personenbezogenen Daten (vgl. BGH, Urteil vom 15.06.2021 – VI ZR 576/19 = NJW 2021, 1381). Im Ausgangspunkt steht dem Kläger nach dieser Vorschrift grundsätzlich ein Auskunftsanspruch über die bei der Beklagten als Verantwortlicher im Sinne des Art. 4 Nr. 7 Hs. 1 DSGVO verarbeiteten ihn betreffenden personenbezogenen Daten zu.

Der Anspruch ist jedoch durch Erfüllung untergegangen, § 362 Abs. 1 BGB.
Den Auskunftsanspruch erfüllt der Verantwortliche dann, indem er die verlangten Informationen nach Maßgabe des Art. 15 erteilt. Außerdem muss der Verantwortliche eine Kopie der personenbezogenen Daten, die er verarbeitet, zur Verfügung stellen. 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 (vgl. BGH, Urteil vom 03.09.2020 - III ZR 136/18 = GRUR 2021,110). Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll.

So liegt es auch im Streitfall. Mit Schreiben vom 23.08.2021 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie den Kläger auf die Selbstbedienungstools verwiesen hat. Diese Erfüllungshandlung war ausreichend um den Erfüllungserfolg zu gewährleisten. Dem ist der Kläger in der Replik auch nicht mehr entgegen getreten, sodass das Auskunftsbegehren hinsichtlich dieses Teilaspekts des Auskunftsanspruchs durch Erfüllung untergegangen ist.

Soweit der Kläger darüber hinaus Auskunft verlangt, *„welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten“* besteht ein Anspruch nicht.
Der Anspruch ist (ebenfalls) durch Erfüllung untergegangen, § 362 BGB. Die Beklagte hat mit der Klageerwiderung vorgetragen, über die Verarbeitungstätigkeiten Dritter (hier: „Scraper“), keine Angaben machen zu können. Unabhängig davon, ob die erteilte Auskunft unrichtig oder unvollständig ist, begründet die erteilte Auskunft jedenfalls keinen (weiteren) Auskunftsanspruch, da die Beklagte zum Ausdruck gebracht hat, das Auskunftsbegehren des Kläger vollständig erfüllt zu haben.

Weitere Anspruchsgrundlagen zur Erreichung des Klageziels sind weder ersichtlich noch von der Gegenseite vorgetragen worden.

6.
Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO, die Entscheidung zur vorläufigen Vollstreckbarkeit auf den §§ 709, 708 Nr. 11, 711 ZPO.

7.
Der Gegenstandswert wird auf 6.000,00 € festgesetzt. Der Wert setzt sich dabei aus dem Wert des Klageantrags zu 1.) in Höhe von 1.000,00 €, dem Wert des

Klageantrags zu 2.) und 3.) in Höhe von jeweils 2.000,00 € sowie dem Wert des Klageantrags zu 4.) in Höhe von 1.000,00 € zusammen.

Rechtsbehelfsbelehrung:

Gegen dieses Urteil ist das Rechtsmittel der Berufung für jeden zulässig, der durch dieses Urteil in seinen Rechten benachteiligt ist,

1. wenn der Wert des Beschwerdegegenstandes 600,00 EUR übersteigt oder

2. wenn die Berufung in dem Urteil durch das Landgericht zugelassen worden ist.

Die Berufung muss **innerhalb einer Notfrist von einem Monat nach Zustellung** dieses Urteils schriftlich bei dem Oberlandesgericht Hamm, Heßlerstr. 53, 59065 Hamm, eingegangen sein. Die Berufungsschrift muss die Bezeichnung des Urteils (Datum des Urteils, Geschäftsnummer und Parteien) gegen das die Berufung gerichtet wird, sowie die Erklärung, dass gegen dieses Urteil Berufung eingelegt werde, enthalten.

Die Berufung ist, sofern nicht bereits in der Berufungsschrift erfolgt, binnen zwei Monaten nach Zustellung dieses Urteils schriftlich gegenüber dem Oberlandesgericht Hamm zu begründen.

Die Parteien müssen sich vor dem Oberlandesgericht Hamm durch einen Rechtsanwalt vertreten lassen, insbesondere müssen die Berufungs- und die Berufungsbegründungsschrift von einem solchen unterzeichnet sein.

Mit der Berufungsschrift soll eine Ausfertigung oder beglaubigte Abschrift des angefochtenen Urteils vorgelegt werden.

Hinweis zum elektronischen Rechtsverkehr:
Die Einlegung ist auch durch Übertragung eines elektronischen Dokuments an die elektronische Poststelle des Gerichts möglich. Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet und mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg gemäß § 130a ZPO nach näherer Maßgabe der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (BGBl. 2017 I, S. 3803) eingereicht werden. Auf die Pflicht zur elektronischen Einreichung durch professionelle Einreicher/innen ab dem 01.01.2022 durch das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013, das Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017 und das Gesetz zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften vom 05.10.2021 wird hingewiesen.
Weitere Informationen erhalten Sie auf der Internetseite www.justiz.de.