Beglaubigte Abschrift

12 O 100/23

Landgericht Aachen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted]

Klägers,

Prozessbevollmächtigte: Rechtsanwälte WBS.Legal,
Eupener Str. 67, 50933 Köln,

gegen

Meta Platforms Ireland Limited (zuvor: Facebook Ireland Ltd), vertr. d. d. GF (Director) Gareth Lambe, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

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

hat die 12. Zivilkammer des Landgerichts Aachen
auf die mündliche Verhandlung vom 02.11.2023
durch die Richterin am Landgericht [redacted] als Einzelrichterin

für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 150,00 EUR nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 25.4.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger 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 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 bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat' noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits tragen der Kläger zu 37 % und die Beklagte zu 63 %.

6. Das Urteil ist vorläufig vollstreckbar, hinsichtlich Ziff. 1 und wegen der Kosten nur gegen Sicherheitsleistung i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages, hinsichtlich Ziff. 3 gegen Sicherheitsleistung i.H.v. 3.000,00 EUR.

Tatbestand:

Die Parteien streiten um Ansprüche auf Schadensersatz, Auskunft, Unterlassung und Erstattung der Rechtsverfolgungskosten begründet durch Verletzungen von Datenschutzbestimmungen im Zusammenhang mit einem sog. „*Scraping-Sachverhalt*“.

Die Beklagte betreibt für Nutzer in der Europäischen Union die Facebook-Plattform, auf der sie es registrierten Nutzern ermöglicht, auf die Facebook-Dienste über die Webseite www.facebook.com oder über Apps für Mobiltelefone und Tablett-PCs zuzugreifen. Die Facebook-Plattform soll Menschen dazu dienen, mit Familie und Freunden in Kontakt zu bleiben, neue Menschen kennenzulernen, Gemeinschaften und Gruppen beizutreten und ganz allgemeine Vorgänge in der Welt zu beobachten. Dazu ermöglicht die Plattform deren Nutzern, persönliche Profile für und über sich zu erstellen und diese mit anderen Nutzern der Plattform zu teilen. Die Nutzer können auf den persönlichen Profilen Angaben zu verschiedenen Daten ihrer Person machen. Dabei ist die Angabe der Daten Name, Geschlecht und eine von der Beklagten generierten Nutzer-ID zwingende Voraussetzung für die Registrierung bei Facebook. Diese Daten können nicht nur die Facebook-Nutzer, sondern auch alle im Internetverkehr aktiven User („alle“) einsehen. Weiter für die Registrierung erforderlich ist die Angabe entweder einer E-Mail-Adresse oder einer Telefonnummer. Dem Nutzer wird darüber hinaus die Möglichkeit eingeräumt, im Rahmen des Registrierungsprozesses oder auch nach der Registrierung weitere Daten einzugeben.

Die Beklagte stellt ihren Nutzern bezüglich der Daten, welche freiwillig zusätzlich eingegeben werden können, jederzeit abänderbare Einstellungsmöglichkeiten unter anderem in Form einer Zielgruppenauswahl und in Form von Suchbarkeits-Einstellungen zur Verfügung. Der Nutzer kann hierbei im Rahmen der Zielgruppenauswahl festlegen, wer ein bestimmtes Datenelement im Facebook-Profil des Nutzers sehen kann. Mit der Suchbarkeits-Einstellung bestimmt der Nutzer, ob

sein Nutzerkonto auf der Facebook-Plattform anhand bestimmter Daten, beispielsweise Telefonnummern gefunden werden kann. Die Suchbarkeits-Einstellungen stellen die Optionen „alle“, „Freunde von Freunden“, „Freunde“ und die Option „nur ich" zur Verfügung. Die von der Beklagten für die Telefonnummer zur Verfügung gestellte Voreinstellung lautet „alle“. Das bedeutet, dass standardmäßig jeder Facebook-User ein Facebook-Profil anhand der dort hinterlegten Telefonnummer ausfindig machen konnte.

Die Suchbarkeits-Einstellungen befinden sich im Abschnitt "Privatsphäre" des Haupteinstellungsmenüs im Konto eines Nutzers. Zu diesem Menü kann der Nutzer direkt von der Facebook-Startseite aus gelangen, nachdem er sich in seinem Konto angemeldet hat. Die Beklagte stellt dem Eigennutzer eine Vielzahl von Möglichkeiten unter anderem über die Bereiche „Privatsphäre“ und „Hilfe“ auf der Facebook Startseite zur Verfügung, um zu den jeweils maßgeblichen Einstellungen zu gelangen. Hinsichtlich der Handynummer stellt die Beklagte den Nutzern gesonderte Hinweise zur Verfügung. Auf die Darstellung der Klageschrift vom 22.08.2022 (Bl. 9 ff. d. A.) wird Bezug genommen.

Die Beklagte bot den Nutzern im streitgegenständlichen Zeitraum die Funktion an, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf Facebook zu synchronisieren. Der Nutzer konnte über das sogenannte Contact-Importer-Tool (kurz CIT) seine Kontakte mit Telefonnummern hochladen, um diese mit den auf den Facebook-Konten hinterlegten Telefonnummern abzugleichen und so zu den Facebook-Konten zu gelangen, bei denen Telefonnummern hinterlegt waren, die sich auch in seinen Kontakten befanden.

Der Kläger ist bei der Beklagten als Nutzer registriert und gab neben den zwingend für die Registrierung erforderlichen und stets öffentlich einsehbaren Daten Name, Geschlecht und Nutzer-ID u.a. auch seine Telefonnummer an. Die „Suchbarkeits-Einstellung“ bezüglich dieser Telefonnummer war auf „Alle“ eingestellt. Die Telefonnummer selbst war zu keinem Zeitpunkt öffentlich auf dem Facebook-Profil des Klägers einsehbar. Er nutzte die Facebook-Dienste insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

Bei der Registrierung wurde der Kläger auf die Datenschutz- und Cookie-Richtlinie der Beklagten hingewiesen. Facebook-Nutzern werden seitens der Beklagten 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 Bezug genommen.

Zwischen Januar 2018 und September 2019 lasen unbekannt gebliebene Dritte - deren genaues Vorgehen ist zwischen den Parteien streitig - die von auf Facebook als „öffentlich“ hinterlegten Daten von Millionen von Facebook-Nutzern in Form des so genannten „*Scrapings*“ aus. Indem - vermutlich über das Contact-Importer-Tool - eine Vielzahl von Kontakten mit automatisch erzeugten Telefonnummern in ein virtuelles Adressbuch eingegeben wurden, gelang es den unbekannten Dritten, diese - selbst generierten - Telefonnummern konkreten Facebook-Profilen zuzuordnen. Wurde mit einer der automatisch generierten „fiktiven“ Telefonnummer eine Übereinstimmung mit einer bei Facebook hinterlegten „realen“ Telefonnummer erzielt, wurde sodann, ohne dass in den entsprechenden Profilen bei den Sichtbarkeitseinstellungen die hinterlegten Telefonnummern öffentlich freigegeben waren, mit Hilfe des Contact-Importer-Tools der jeweils zugehörige Facebook-Nutzer angezeigt. Auf diese Weise konnten die öffentlich einsehbaren Daten des jeweiligen Nutzers abgegriffen und mit dessen Telefonnummer verbunden werden. Der konkrete Ablauf des „*Scraping-Vorfalls*“ steht zwischen den Parteien im Streit; insbesondere wie die mittels des „CIT“ abgerufenen Telefonnummern in die Hände der Dritten gelangt sind.

Scraping“ war und ist nach den Nutzungsbedingungen der Beklagten untersagt. Das Phänomen war bereits vor dem hier streitgegenständlichen Vorfall bekannt und fand und findet im Internet bekanntermaßen statt. 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 in einer ungesicherten Datenbank im Internet. Die Beklagte veröffentlichte als Reaktion darauf am 06.04.2021 den Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ (Bl. 319 ff. d. A.). Sie informierte nicht die Datenschutzbehörde *Irish Data Protection Commission* 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. Die irische Datenschutzbehörde DPC verhängte gegen die Beklagte am 28.11.2022 eine Geldbuße in Höhe von 265 Mio. Euro. Die DPC sah einen Verstoß der Beklagten insbesondere gegen Art. 25 Abs. 1 und 2 DSGVO.

Mit der als Anlage K1 (Bl. 52 ff. d. A.) vorgelegten E-Mail vom 30.11.2022 forderte der Prozessbevollmächtigte des Klägers die Beklagte vorgerichtlich zur Zahlung von 500,00 EUR, Unterlassung künftiger Zugänglichmachung der Daten des Klägers sowie zur Erteilung einer Auskunft, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht wurden, auf. Die Beklagte wies die von dem Kläger geltend gemachten Ansprüche auf Schadensersatz und Unterlassung zurück und teilte jedenfalls mit, welche Arten von Daten des Klägers verarbeitet.

Der Kläger behauptet, dass resultierend aus dem „*Scraping-Vorfall*“ seine persönlichen Daten wie Telefonnummer, Vorname, Nachname, E-Mail-Adresse, Geschlecht und Geburtsdatum abgegriffen worden seien. Insbesondere sei seine Telefonnummer nirgendwo öffentlich Diese Daten würden insbesondere für gezielte Phishing Attacken genutzt. Es könne noch nicht abgesehen werden, welche Dritte Zugriff auf die Daten des Klägers erhalten hätten und für welche konkreten strafbaren Handlungen die Daten missbraucht würden. Unbekannten Dritten seien wegen des nicht hinreichend gesicherten Contact Import Tools zur Korrelation zwischen Facebook-Profilen und deren Telefonnummern befähigt gewesen. Dabei hätten die Unbekannten in ein Programm unzählige zufällige Zahlenfolgen und jede fiktive Nummer in das „CIT“ eingegeben, um festzustellen, ob hinter dieser wahllosen Zahlenfolge eine mit einem Facebook-Konto verknüpfte Telefonnummer darstelle. Sei dies der Fall gewesen, habe das Programm sämtliche Daten des Nutzers abgefragt und in eine Liste exportiert.

Weiter behauptet der Kläger, dass das „*Scraping*“ nur möglich gewesen sei, weil die Beklagte keine ausreichenden Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Contact Import Tools zu verhindern. Wären derartige Sicherheitsmaßnahmen vorgenommen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen. Es habe zudem ein ausdrücklicher Hinweis der

Beklagten gefehlt, dass standardmäßig die Telefonnummer eines Nutzers von jedermann mit dessen Profil verknüpft werden kann.

Der Kläger behauptet darüber hinaus, dass die gesamte Facebook-Plattform datenschutzunfreundlich ausgerichtet sei. Der Registrierungsvorgang auf der Plattform sei bewusst undurchsichtig und verwirrend gestaltet. Dies diene dazu, dass Nutzer im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern preisgäben. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht ändere.

Der Kläger behauptet, er erhalte seit vermehrt „dubiose“ Nachrichten und E-Mails. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks. Oft würden auch bekannte Plattformen oder Zahlungsdienstleister wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Das habe dazu geführt, dass er nur noch mit äußerster Vorsicht auf jegliche Emails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte und Unsicherheit verspüre.

Der Kläger ist der Ansicht, dass die Beklagte gegen Art. 13, 14, 15, 24, 25, 32, 33 und 34 DSGVO verstoßen habe und ihm dadurch ein kausaler immaterieller Schaden entstanden sei, der nach Art. 82 Abs. 1 DSGVO zu ersetzen sei. Dabei sei die Vielzahl der Verstöße der Beklagten und deren datenfeindliches Agieren im Rahmen der Bemessung der Höhe des Schadensersatzes ebenso zu berücksichtigen wie das in Art. 83 DSGVO enthaltene Bußgeldregime. Der geltend gemachte Feststellungsantrag auf Ersatz künftiger Schäden sei dadurch gerechtfertigt, dass die Wahrscheinlichkeit eines Schadenseintritts durch zukünftige erhebliche Belästigungen und die Gefahr einer missbräuchlichen Nutzung der erworbenen Daten mit einer entsprechenden Schadensverursachung besteht. Er ist darüber hinaus der Ansicht, dem geltend gemachten Unterlassungsanspruch könne weder die fehlende Bestimmtheit noch ein Entfall der Wiederholungsgefahr entgegengehalten werden. Der Kläger meint schließlich, der ihm zustehende Auskunftsanspruch sei durch die außergerichtlich erteilte Auskunft jedenfalls nicht vollständig erfüllt.

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

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

   a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

   b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat' noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung

4. die Beklagte zu verurteilen, ihm Auskunft über ihn betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

Die Beklagte beantragt,

die Klage abzuweisen.

Sie behauptet, dass die Daten weder durch Hacking noch durch mangelnde Sicherheitssysteme der Beklagten in die Hände der Dritten gefallen seien. Vielmehr liege lediglich ein automatisiertes massenhaftes Sammeln ohnehin öffentlicher, und damit nicht vertraulicher Daten vor (sog. „Datenscrapings“). Die so abgegriffenen Daten seien im Einklang mit den jeweiligen Privatsphäre-Einstellungen der Nutzer für jedermann öffentlich auf deren Profil einsehbar gewesen. Der Kläger habe zudem ein fehlerhaftes Verständnis für den „*Scraping*-Vorfall“. Der Vorfall sei nicht nur durch das CIT der Beklagten, insbesondere nicht durch das wahllose Eingeben zufälliger Nummernfolgen erfolgt. Vielmehr hätten den Scrapern bereits konkrete Telefonnummern zur Verfügung gestanden, die sie nur in das CIT eingegeben hätten. Das Contact-Im- port-Tool ermöglicht den Nutzern lediglich, ihre Kontakte von ihren Mobilgeräten auf Facebook hochzuladen, um diese Kontakte auf der Facebook-Plattform zu finden und mit ihnen in Verbindung zu treten, nicht dagegen einen Export von Nutzerdaten.

Sie behauptet ferner, dass es grundsätzlich nicht möglich sei, das 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 zugrundeliegende Funktion beseitigt. Vielmehr würden in der Regel lediglich die Methoden beschränkt, mit denen auf die maßgeblichen Funktionen zugegriffen werden könne. Die Beklagte habe angemessene technische und organisatorische Maßnahmen ergriffen, das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen. Der Kläger habe unsubstantiiert dazu vorgetragen, welche Maßnahmen die Beklagte konkret hätte erbringen müssen.

Sie behauptet weiter, dass der Kläger sowohl über die Einstellungsmöglichkeiten als auch über mögliche Konsequenzen seiner Einstellungen hinreichend durch die Beklagte informiert worden. Er habe sich, in Kenntnis der Datenschutzbestimmung der Beklagten, dazu entschieden bestimmte Daten öffentlich einsehbar auf seinem Facebook-Profil zu teilen. Es habe eine umfassende und verständliche Information über die Möglichkeit der Anpassung der „Suchbarkeits-Einstellungen“ und

„Zielgruppenauswahl“ gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem Profil hinterlegt habe, einsehen könne.

Ferner behauptet die Beklagte, dass es dem allgemeinen Lebensrisiko entspringe, dass Daten abgegriffen werden und Spam Mails und Anrufe eingehen. Sie bestreitet, dass die persönlichen Daten und insbesondere die Telefonnummer des Klägers nicht bereits vor dem streitgegenständlichen Vorfall öffentlich bekannt war.

Zur Sache selbst vertritt die Beklagte die Ansicht, dass die Klage bereits unzulässig sei, da die Klageanträge Ziffern 1 und 2 nicht hinreichend bestimmt i.S.d. § 253 Abs.2 Nr. 2 ZPO seien. Dem klägerischen Antrag zu 2) fehle bereits das notwendige Feststellungsinteresse. Weiter sei der mit dem Antrag zu 4) geltend gemachte Auskunftsanspruch bereits außergerichtlich, nämlich mit Schreiben vom 23.8.2022, erfüllt worden.

Die Klage ist der Beklagten am 24.4.2023 zugestellt worden.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf das Protokoll der mündlichen Verhandlung vom 2.11.2023 sowie auf die zu den Akten gereichten Schriftsätze der Parteien nebst Anlagen Bezug genommen.

Entscheidungsgründe

I.

Die zulässige Klage ist teilweise begründet.

A

B 1. Die Klage ist zulässig.

a) Das Landgericht Aachen ist international, sachlich und örtlich zuständig (vgl. hierzu LG Aachen, Urt. v. 10.2.2023 - 8 O 177/22, GRUR-RS 2023, 2621)

Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2. EuGVVO (Brüssel Ia - VO). Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat.

Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO Verbraucher. Er gibt an, einen Nutzungsvertrag mit der Beklagten geschlossen zu haben über die Nutzung der Social-Media-Plattform Facebook mittels eines Benutzerkontos zu privaten Zwecken. Der Kläger hat seinen Wohnort in Stolberg, woraus sich die internationale Zuständigkeit der deutschen Gerichte ergibt.

Die sachliche Zuständigkeit des Landgerichts Aachen folgt aus § 1 ZPO i.V.m. §§ 23 Nr. 1, 71 Abs. 1 GVG, wobei das Gericht einen Streitwert von mehr als 5000 EUR zugrunde legt.

Das Landgericht Aachen ist nach Art. 18 Abs. 1 Alt. 2 EuGVVO sowie Art. 79 Abs. 2 Satz 2 DS-GVO örtlich zuständig.

b) Die von der Klägerseite gestellten Anträge sind hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO.

aa) Der Klageantrag zu 1) ist zulässig und insbesondere hinreichend bestimmt.

Der Kläger stellt die Bemessung des Schmerzensgeldes, hinsichtlich dessen er eine Größenordnung seiner Vorstellungen angegeben hat, zulässigerweise in das Ermessen des Gerichts. Ferner hat er mitgeteilt, worauf sich sein Begehren bezieht und dass Schmerzensgeld sowohl für das Verhalten der Beklagten vor dem Daten-Scraping-Vorfall als auch für das nachfolgende Verhalten begehrt wird, so dass eine alternative Klagebegründung nicht angenommen werden kann. Soweit die Beklagte ihre Auffassung, es lägen mehrere Lebenssachverhalte vor, auf die von der Klägerseite behauptete Verletzung mehrerer Vorschriften der DSGVO stützt, handelt es sich um rechtliche Qualifizierungen, die nicht zum Lebenssachverhalt gehören. Entgegen der Auffassung der Beklagtenseite wird von der Klägerseite lediglich ein Lebenssachverhalt beschrieben, der den Zeitraum von der Registrierung bis hin zur behaupteten Schädigung in der Gegenwart mit umfasst und durch die bestehenden vertraglichen Beziehungen betreffend die Nutzung der von der Beklagten zur Verfügung gestellten Dienste verbunden wird.

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

Der Klageantrag muss aus sich heraus verständlich sein, den Umfang des begehrten Rechtsschutzes nennen und den Antrag so konkret bezeichnen, dass der Inhalt und Umfang der begehrten Entscheidung ersichtlich ist (MüKo ZPO/Becker-Eberhard, 6. Aufl. 2020, § 253 Rn. 88). Diesen Voraussetzungen wird der Antrag zu 2) gerecht. Soweit die Beklagte darauf abstellt, dass der Antrag unverständlich sei, da nicht erkenntlich sein soll, ob damit lediglich zukünftige oder bereits in der Vergangenheit entstandene Schäden erfasst werden sollen, kann dieser Ansicht nicht gefolgt werden. Aus dem Wortlaut des Antrags ergibt sich eindeutig, dass der Kläger damit den Ersatz zukünftiger (also momentan noch nicht entstandener) Schäden begehrt, die auf dem bereits vergangenen Ereignis des Datenschutzvorfalles beruhen. Durch den Bezug auf den „Scraping-Vorfall“ findet gerade eine Konkretisierung des Antrags statt. Eine andere Deutung verbietet sich hier.

Der Kläger hat auch sein Feststellungsinteresse nach § 256 Abs. 2 ZPO hinreichend dargelegt. Ein Feststellungsantrag ist bereits dann zulässig, wenn die

Schadensentwicklung noch nicht gänzlich abgeschlossen und der Kläger aus diesem Grund nicht im Stande ist, seinen Anspruch deshalb ganz oder teilweise zu beziffern (OLG Hamm, Urteil vom 21.05.2019 – 9 U 56/18). Das Feststellungsinteresse ist daher nur dann zu verneinen, wenn aus der Sicht des Geschädigten keinerlei Besorgnis besteht, zumindest mit dem Eintritt eines Schadens zu rechnen (BGH, Beschluss vom 09.01.2007 –VI ZR 133/06). 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. Weiter ist auch nicht davon auszugehen, dass die Schadensentwicklung ein Ende gefunden hat. Dies insbesondere vor dem Hintergrund, dass zwischen dem „Scraping“ und der Publizierung der daraus gewonnenen Daten ein Zeitraum von etwa zwei Jahren lag. Daraus wird ersichtlich, dass diesem Vorfall ein Gefährdungspotential inne liegt, welches weder in zeitlicher noch in inhaltlicher Hinsicht vollständig ausgeschlossen werden kann.

2. Die Klage ist teilweise begründet.

a) Dem Kläger steht gegen die Beklagte einen Anspruch auf Schadensersatz i.H.v. 150,00 EUR 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.

Die Beklagte hat als Verantwortliche i.S.d. Art. 4 Nr. 7 DSGVO gegen mehrere Vorschriften aus der DSGVO verstoßen. Konkret verstieß die Beklagte gegen Art. 25 Abs. 2 DSGVO, gegen Art. 13 Abs. 1 lit. c) DSGVO, gegen Art. 32, 24, 5 Abs. 1 lit. f) DSGVO, gegen Art. 33 DSGVO (und gegen Art. 34 Abs. 1 DSGVO. Durch diese Verstöße ist dem Kläger ein immaterieller Schaden entstanden. Die Verstöße gegen die DSGVO sind auch kausal für den bei dem Kläger entstandenen Schaden. Die Beklagte handelte auch schuldhaft. Der Kläger hat sich auch kein Mitverschulden nach § 254 Abs. 1 BGB anrechnen zu lassen.

aa) Nach Art. 82 Abs. 1 DSGVO ist für eine Schadensersatzpflicht ein Verstoß gegen die DSGVO erforderlich. Da der sachliche Anwendungsbereich der DSGVO nach deren Art. 2 Abs. 1 jedoch nur für die Datenverarbeitung eröffnet ist, ist ein Verstoß in Form einer gegen die Vorschriften der DSGVO erfolgten Datenverarbeitung erforderlich. Art. 82 Abs. 1, Abs. 2 S. 1 und S. 2 DSGVO beinhalten daher lediglich die Klarstellung, dass der Verantwortliche für alle - durch entsprechende Verstöße verursachte - Schäden haftet, während der Auftragsverwalter nur unter weiteren Voraussetzungen für Schäden haftet. Eine Einschränkung hinsichtlich der - eine Haftung nach Art. 82 Abs. 1 DSGVO begründenden - Verstöße liegt hierin jedoch nicht.

bb) Die Beklagte hat durch die Ausgestaltung ihrer standardmäßigen Voreinstellungen gegen ihre obliegenden Verpflichtungen aus Art. 25 Abs. 2 DSGVO verstoßen.

Nach Art. 25 Abs. 2 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, um den Anforderungen der DSGVO gerecht zu werden. Durch standardmäßige Voreinstellungen („privacy by default“) soll sichergestellt werden, dass nur diejenigen personenbezogenen Daten von dem Verarbeiter erhoben werden, die für den jeweiligen Verarbeitungszweck notwendig sind (Sydow/Marsch/Mantz, DS-GVO/BDSG 3. Aufl., DS GVO Art. 25 Rn. 3,7). Dadurch sollen die Nutzer geschützt werden, die sich nicht von selbst dazu veranlasst sehen, datenschutzfreundliche Einstellungen einzurichten, obwohl ihnen prinzipiell die Möglichkeit dazu vom Diensteanbieter eröffnet wird (Paal/Pauly/Martini, DS-GVO 3. Aufl., Art. 25 Rn. 13). Der Nutzer soll selbst aktiv werden, um von datenschutzfreundlichen Voreinstellungen abzurücken. So soll der Nutzer vor ihm unbewussten Datenerhebungen geschützt und eine Verfügungshoheit über seine Daten möglichst erhalten werden. Durch Art. 25 Abs. 2 DSGVO soll kein genereller Zwang zur standardmäßigen Einrichtung einer datenschutzfreundlichsten Voreinstellung statuiert werden. Vielmehr sollen datenschutzfeindliche Voreinstellungen unterbunden werden. Welche Erhebung datenschutzfreundlich ist, bestimmt sich dabei maßgeblich nach dem Zweck der Erhebung und Verarbeitung der betroffenen personenbezogenen Daten. Demnach sind nur Voreinstellungen für solche Verarbeitungen zulässig, die für den Verarbeitungszweck erforderlich sind (Paal/Pauly/Martini, DS-GVO 3. Aufl., Art. 25 Rn. 45). Nach Art. 25 Abs. 2, S. 2

DSGVO gilt der Grundsatz „privacy by default“ für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Gegen diese Anforderungen hat die Beklagte verstoßen, indem die standardmäßigen Voreinstellungen für die „Suchbarkeits-Einstellung“ der vom Kläger hinterlegten Telefonnummer auf „Alle“ eingestellt waren. Diese Voreinstellung war nicht für den Verarbeitungszweck der Beklagten erforderlich ist.

Art. 25 Abs. 3 S. 2 DSGVO adressiert insbesondere soziale Netzwerke. Der Verantwortliche – hier die Beklagte – soll durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass personenbezogene Daten eines Nutzers – hier des Klägers – nicht ohne dessen Eingreifen einer unbestimmten Anzahl von Personen zugänglich gemacht wird (Ehmann/Selmayr/Baumgartner, DS-GVO 2. Aufl., Art. 25 Rn. 20). Dem Nutzer muss die Möglichkeit verbleiben, die Hoheit über seine Daten und deren Veröffentlichung bzw. Verarbeitung aktiv zu gestalten. Konkret bezogen auf soziale Netzwerke folgt daraus, dass ein Nutzer selbst in die Lage versetzt werden muss, darüber zu entscheiden, ob und mit wem er diese inner- und außerhalb des Netzwerkes teilt (LG Paderborn, Urteil vom 19.12.2022 – 3 O 99/22). Aus Art. 25 Abs. 2 S. 3 DSGVO folgt, dass Inhalte und Daten eines Nutzers nicht standardmäßig mit anderen geteilt werden bzw. für diese verfügbar sind. Als Voreinstellung ist somit der kleinstmögliche Adressatenkreis zu wählen (Gola/Heckmann/Nolte /Werkmeister, DS-GVO 3. Aufl., Art. 25, Rn. 31).

Dem widerspricht die fragliche Gestaltung der Beklagten diametral. Durch die Voreinstellung der „Suchbarkeits-Einstellung“ hinsichtlich der Telefonnummer des Klägers auf „Alle“ war es einer unbegrenzten Anzahl von natürlichen Personen möglich, das Facebook-Profil des Klägers mittels des von der Beklagten vorgehaltenen CIT aufzufinden, wodurch weitere persönliche Daten, die zwingend öffentlich sind, einsehbar werden.

Die von der Beklagten standardmäßig getroffene „Suchbarkeits-Einstellung“ hinsichtlich der der von dem Kläger hinterlegten Telefonnummer war nicht zur Erreichung ihres Verarbeitungszweckes erforderlich. Erforderlichkeit im Sinne des Art. 25 Abs. 2 S. 1 DSGVO besteht dann, wenn sich der Verarbeitungszweck ohne die standardmäßig erhobenen Daten nicht erreichen lässt (vgl. ErwGr 39, S. 8). Nach

dem eigenen Vortrag der Beklagten dient die von ihr betriebene Facebook-Plattform dazu, Menschen miteinander zu verbinden und Kommunikation zwischen ihnen zu ermöglichen. Zwar ist der Verarbeiter in der Wahl seines Verarbeitungszweckes frei (Paal/Pauly/Martini, DS-GVO 3. Aufl., Art. 25 Rn. 45c). Für die Erreichung dieses kommunikativen und verbindenden Verarbeitungszweckes war es nach Ansicht des Einzelrichters jedoch nicht erforderlich, dass die „Suchbarkeits-Einstellung“ der bei Facebook hinterlegten Telefonnummer „Alle“ war. Zwar mag es dem Verarbeitungszweck der Beklagten nützlich sein, wenn die Nutzer der Facebook-Plattform auch über ihre hinterlegte Telefonnummer aufgefunden werden können. Für die Kammer erscheint es aber fernliegend, dass sich der kommunikative und verbindende Zweck der Facebook-Plattform ohne die Auffindbarkeit eines Facebook-Users über seine Telefonnummer nicht erreichen lässt. Das Wissen um eine Mobilfunknummer einer anderen Person spricht bereits deutlich dafür, dass sich diejenigen Personen bereits kennen. Selbst wenn dies nicht namentlich der Fall sein sollte, ließe sich eine Kontaktaufnahme unter Zuhilfenahme ebendieser Telefonnummer bewerkstelligen, ohne dass dafür auf die Facebook-Plattform und deren CIT zugegriffen werden müsste. Eine Suche über Facebook erübrigt sich in diesem Fall. Die Möglichkeit der Suche eines anderen Facebook-Nutzers mittels dessen Telefonnummer stellt somit lediglich einen zusätzlichen Nutzer-Service dar, der zur Erreichung der selbst deklarierten Zwecke der Beklagten nicht erforderlich ist und darüber hinaus auch Datenmissbrauch mittels Scraping ermöglicht. Die Nichterforderlichkeit der fraglichen Voreinstellung ist auch daran erkennbar, dass die „Suchbarkeits-Einstellung“ der Telefonnummer restriktiv geändert werden kann, ohne dass dies ersichtlich dem kommunikativen Aspekt der Plattform der Beklagten entgegensteht (vgl. KG Berlin, Urteil vom 20.12.2019 - 5 U 9/18, Rn. 39).

Eine andere Bewertung wird auch nicht dadurch gerechtfertigt, dass der Kläger die Suchbarkeitseinstellungen nachträglich ändern oder einen „Privatsphäre-Check“ durchführen konnte. Art. 25 Abs. 2 DSGVO stellt auf datenschutzfreundliche Voreinstellungen und nicht auf nachträgliche Änderungsmöglichkeiten ab. Entgegen der Ansicht der Beklagten sind vielmehr Voreinstellungen zu treffen, die dem Nutzer mittels eines „Opt-In-Verfahrens“ ermöglichen, seine personenbezogenen Daten über den voreingestellten Adressatenkreis hinaus zugänglich zu machen (Sydow/Marsch/Mantz, DS-GVO/BDSG 3. Aufl., DSGVO Art. 25 Rn. 69).

cc) Darüber hinaus ist die Beklagte auch ihrer Informations- und Aufklärungspflicht gemäß Art. 13 DSGVO jedenfalls nicht in vollem Umfang nachgekommen. Die Kammer ist zu der Überzeugung gelangt, dass die Beklagte den Kläger im Zeitpunkt der Datenerhebung ihrer Handynummer nicht ausreichend über die Zwecke der Verarbeitung besagter Handynummer aufgeklärt hat. Ein Verstoß gegen Art. 13 DSGVO kann einen Schadensersatzanspruch nach Art. 82 DSGVO begründen, auch Art. 13 DSGVO fällt unter den Schutzbereich des Art. 82 DSGVO (Franck in: Gola/Heckmann, DSGVO, BDSG, Art. 13 DSGVO, Rn. 64; Schmidt-Wudy in: BeckOK Datenschutzrecht, Art. 13 DSGVO, Rn. 18; LG Stuttgart, Urteil vom 26.01.2023 - 53 O 95/22, Rn. 72, juris; a.A. LG Essen, Urteil vom 10.11.2022 - 6 O 111/22, Rn. 62, 65, 72, juris).

Art. 13 Abs. 1 lit. c DSGVO legt die Verpflichtung fest, die betroffene Person über die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung anzugeben. Entsprechend der Legaldefinition der (Daten-) Verarbeitung in Art. 4 Nr. 2 DSGVO entstehen die Informations- und Aufklärungspflichten des Art. 13 DSGVO bereits mit der Erhebung personenbezogener Daten. Bereits zu diesem Zeitpunkt hat der Verantwortliche gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen.

Der Kläger gab im Rahmen seiner Registrierung auf der Facebook-Plattform seine Mobilfunknummer an. Die vorstehende Verpflichtung hat die Beklagte jedenfalls in Bezug auf die Verwendung der Handynummer im Rahmen des „Contact-Import-Tool“ nicht genügt. Bei der Mobilfunknummer des Klägers handelt es sich um ein personenbezogenes Datum gemäß Art. 4 Nr. 1 DSGVO. Bei der Hinterlegung der Telefonnummer in seinem Facebook-Profil wurde der Kläger durch die Beklagte darüber informiert, dass diese für verschiedene Zwecke benutzt wird.

Der Kläger wurde jedoch durch die Beklagte nicht hinreichend über den Zweck der Verwendung seiner Mobilfunknummer für das seitens der Beklagten bereitgestellte Contact-Im- port-Tool aufgeklärt, obwohl eine solche Information vorliegend notwendig war. Es wird nicht darüber informiert, dass andere den Kläger als Nutzer finden können, sondern darüber, dass dem Kläger seine Telefonnummer nützlich sein kann, andere Facebook-Nutzer zu finden. Das eine mag zwar mit dem anderen unmittelbar zusammenhängen, indes gestaltet sich die Information der Beklagten selektiv und damit unvollständig. Das wird auch nicht durch den anschließenden

Hinweis, dass man kontrollieren könne, wer die eigene Telefonnummer sehen könne, geheilt. Eine Aufklärung lässt sich ferner auch nicht aus der Datenschutzrichtlinie der Beklagten (Anlage B9) entnehmen. Weder ein konkreter noch ein abstrakter Hinweis auf die Benutzung der angegebenen Mobilfunknummer für das CIT sind enthalten. Solche Hinweise finden sich auch nicht unter der Überschrift „Wie werden diese Informationen geteilt“ derselben Datenrichtlinie. Angesichts des Vorstehenden kann hier auch nicht von einer wirksamen Einwilligung des Klägers i.S.d. Art. 6 Abs. 1 lit. a DSGVO ausgegangen werden.

Eine Einwilligung kann mithin keinen Bestand haben, wenn dem Betroffenen nicht schon bei der Datenerhebung sämtliche gemäß Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden. Ebenso wenig ist das Auffinden über das „Contact-Import-Tool“ für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich (Art. 6 Abs. 1 Satz 1 lit. c DSGVO).

dd) Die Beklagte hat weiter keine hinreichenden Sicherheitsmaßnahmen zur Verhinderung des streitgegenständlichen „Scraping-Vorfalls“ mittels des CIT vorgehalten und somit gegen Art. 32, 24, 5 Abs. 1 lit. f) DSGVO verstoßen.

Nach Art. 32 Abs. 1 DSGVO hat der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zielrichtung dieser Norm ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Mantz in: Sydow/Marsch DSGVO/BDSG, Art. 32 DSGVO 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 (Martini in: Paal/Pauly, DSGVO, BDSG, Art. 32 DSGVO Rn. 2). Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO 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 DS-GVO 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. Ausweislich des Erwägungsgrundes 76 zur DSGVO sollten dabei die Eintrittswahrscheinlichkeit und Schwere des Risikos anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt (so auch LG Lübeck, Urteil vom 25.05.2023 - 15 O 74/22, Rn. 84, juris).

Im vorliegenden Fall ist dabei zur Überzeugung der Kammer an die vorzunehmenden Maßnahmen und das damit verbundene notwendige Schutzniveau ein hoher Maßstab anzusetzen. Das folgt daraus, dass im Falle von Scraping nicht lediglich Daten erhoben werden, die ohnehin öffentlich zugänglich sind. Vielmehr wird durch die Scraping-Angriffe eine Verknüpfung zu dem Konto des Betroffenen und der darin erhaltenen Daten erstellt und somit ein ganzes Datenpaket einschließlich der zuvor nicht öffentlich einsehbaren Telefonnummer zusammengestellt. Die Gefahr, dass diese Daten sodann einschließlich der Telefonnummer massenhaft durch Dritte veröffentlicht werden, ist – wie auch der vorliegende Fall zeigt – besonders hoch (vgl. auch LG Paderborn, Urteil vom 19. Dezember 2022 - 3 O 99/22 -, juris). Zum anderen ist gerade bei einem Unternehmen in der Größenordnung der Beklagten davon auszugehen, dass sie grundsätzlich die Möglichkeit hat, geeignete technische Maßnahmen zum Schutz gegen Scraping zu ergreifen.

Die von der Beklagten hinsichtlich des CIT behaupteten Schutzmaßnahmen werden diesen Anforderungen nicht gerecht. Die Beklagte trifft insoweit eine sekundäre Darlegungslast, zu den von ihr aufgeführten Schutzmaßnahmen konkret vorzutragen (OLG Stuttgart, Urteil vom 31.03.2021 – 9 U 34/21 –, juris). Eine sekundäre Darlegungslast trifft den Prozessgegner der primär darlegungsbelasteten Partei, wenn diese keine nähere Kenntnis der maßgeblichen Umstände und auch keine Möglichkeit zur weiteren Sachaufklärung hat, während der Bestreitende alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen (BGH, Urteil vom 10.02.2015 – VI ZR 343/13 –, juris). So liegt die Dinge hier, da es der Beklagten ohne weiteres möglich ist, darzulegen, welche konkreten Maßnahmen zum Schutz der Daten ergriffen wurden. Demgegenüber hat der Kläger als Außenstehende keine Kenntnis über die konkret implementierten Maßnahmen.

Die Beklagte hat zu den notwendigen und ergriffenen Maßnahmen jedoch nicht ausreichend vorgetragen. Sie hat nicht hinreichend dargelegt, welche konkreten Maßnahmen sie überhaupt angewandt hat und wie genau diese ausgestaltet gewesen sein sollen. Insbesondere der pauschale Vortrag, es seien Übertragungsbeschränkungen eingeführt und Captcha-Anfragen genutzt worden, ist einer konkreten Prüfung, ob diese Maßnahmen auch dem erhöhten Maßstab der Sicherungsmaßnahmen genügen, nicht zugänglich, da weder hinreichend zu der Funktionsweise noch zu der konkreten Ausgestaltung vorgetragen wurde. Soweit die Beklagte darüber hinaus vorträgt, auf andere Art gegen Scraper vorzugehen, handelt es sich bei diesen Maßnahmen augenscheinlich um solche, die erst nach dem erfolgten Scraping-Vorfall ergriffen wurden und die demnach zum hier streitgegenständlichen Zeitpunkt noch nicht im Einsatz waren.

ee) Der Beklagten fällt zudem eine Verletzung ihrer Meldepflicht nach Art. 33 DSGVO zur Last.

Nach Art. 33 Abs. 1 S. 1 DSGVO meldet der Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gemäß Art. 55 DSGVO zuständigen Aufsichtsbehörde. Diese Pflicht zur Meldung entfällt dann, wenn die eingetretene Verletzung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen

führt. Der Mindestinhalt der Meldung wird in Art. 33 Abs. 3 DSGVO normiert. Dem ist die Beklagte vorliegend nicht nachgekommen. Unstreitig hat die Beklagte die zuständige Aufsichtsbehörde im Sinne des Art. 55 DSGVO nicht über den "Scraping"-Vorfall informiert. Zudem liegt eine Verletzung des Schutzes personenbezogener Daten vor. Darunter ist 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, zu verstehen. Es genügt dabei eine objektive Schutzverletzung. Ob der Verantwortliche die Datenschutzverletzung als solche erkennt und einstuft, ist im Rahmen des Art. 33 DSGVO unbeachtlich (BeckOK DatenschutzR/Brink, DSGVO Stand 01.02.2022, Art. 33 Rn. 27, 29). Umfasst sind davon also unbeabsichtigte Verletzungen wie Datenlecks, Hackerangriffe, Datendiebstähle oder das Abgreifen von Daten sowie die Zweckentfremdung von Daten bei bestehenden Zugriffsrechten (Ehmann/Selmayr/Hladjk, DSGVO 2. Aufl., Art. 33 Rn. 5; Schaffland/Wiltfang/Schafflang/Holthaus, Datenschutz-Grundverordnung Werkstand: 1. Ergänzungslieferung 2023, Art. 33 Rn. 9; Spindler/Schuster/Laue, DSGVO 4. Aufl., Art. 33 Rn. 7).

Eine solche Schutzverletzung ist durch das „Scrapen“ mittels des CIT bei der Beklagten zu sehen. Durch diesen Vorfall wurden, entgegen der Nutzungsbedingung der Beklagten, eine immense Anzahl an Daten abgegriffen und anschließend in einer nicht gesicherten Datenbank im Internet veröffentlicht. Damit wurden Daten, die auf den jeweiligen persönlichen Profilen der Facebook-Nutzer angegeben wurden, zweckentfremdet, um damit kriminellen Aktivitäten Vorschub zu leisten. Zwar waren die Daten Name, Facebook-ID und Geschlecht des Klägers vorliegend aufgrund seiner Privatsphäreeinstellungen auf seinem Profil öffentlich einsehbar. Jedoch liegt in der Verknüpfung dieser öffentlichen Daten mit der nicht öffentlich einsehbaren Mobilfunknummer des Klägers mittels des CIT und der anschließenden Veröffentlichung dieses Datensatzes im Internet ohne den Willen des Klägers ein Vorfall, der mit einem Datenleck oder Hackerangriff vergleichbar ist und somit eine Verletzung des Schutzes personenbezogener Daten darstellt (so auch LG Paderborn, Urteil vom 19.12.2022 - 2 O 236/22).

Die Meldepflicht der Beklagten nach Art. 33 Abs. 1 DSGVO war vorliegend auch nicht einzuschränken. Die Verletzung des Schutzes personenbezogener Daten führt

vorliegend zu einem Risiko für die Rechte und Freiheiten des Klägers. Dieses Risiko ist anzunehmen, wenn der betroffenen Person der Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, 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. Hier ist bereits beim Kläger ein Kontrollverlust über seine abgegriffenen Daten eingetreten.

ff) Weiter hat die Beklagte gegen Art. 34 Abs. 1 DSGVO verstoßen, indem sie als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO den Kläger als betroffene Person nicht unverzüglich von der Verletzung des Schutzes seiner personenbezogenen Daten benachrichtigt hat, obwohl die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten des Klägers zur Folge hatte.

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. Für die Beklagte streitet auch keine Ausnahme nach Art. 34 Abs. 3 DSGVO. Die Benachrichtigungspflicht entfällt vorliegend nicht schon nach Art. 34 Abs. 3 lit. a DSGVO, da die Beklagte keine geeigneten Sicherheitsvorkehrungen zum Schutz des CIT vor dessen missbräuchlicher Verwendung getroffen hat. Als geeignet kann eine Sicherheitsvorkehrung nur dann angesehen werden, wenn die Vorkehrungen ein hohes Risiko einer Sicherheitsverletzung ausschließen (Paal/Pauly/Martini, DSGVO 3. Aufl., Art. 34 Rn. 38). Dies war hier aber gerade nicht der Fall, vgl. oben.

Weiter war auch eine Benachrichtigung durch die Beklagte nicht nach Art. 34 Abs. 3 lit. c DS- GVO entbehrlich. Dies wäre nur dann der Fall gewesen, wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand für die Beklagte verbunden gewesen wäre. Grundsätzlich kann sich bei einer Vielzahl von betroffenen Personen ein unverhältnismäßig hoher Kosten- und Zeitaufwand des Benachrichtigungsverpflichteten ergeben. Sind jedoch die betroffenen Personen und deren E-Mail-Adressen dem zur Benachrichtigung Verpflichteten, wie vorliegend bekannt, kann nicht von einem unverhältnismäßigen Aufwand ausgegangen werden (Gola/Heckmann/Reif, DSGVO 3. Aufl., Art. 34 Rn. 17).

gg) Der Beklagten fällt allerdings kein Verstoß gegen Art. 15 DSGVO zur Last. Einen entsprechenden Verstoß hat der Kläger nicht dargelegt.

Der Kläger hat ausgeführt, er habe sich mithilfe seiner Prozessbevollmächtigten mit Schreiben vom 30.11.2022 an die Beklagte gewandt und Auskunft hinsichtlich konkret formulierter Fragen wegen des „im April 2021 bekannt gewordenen Datenschutzvorfall“ verlangt. Die Fragen betreffen dabei die Verarbeitung personenbezogener Daten des Klägers durch die Beklagte und inwieweit Daten des Klägers vom streitgegenständlichen „Scraping-Vorfall“ betroffen waren. Auf dieses Auskunftsverlangen, das sich aus Art. 15 DSGVO ableiten lässt, soll die Beklagte nach insoweit übereinstimmendem Vortrag reagiert haben. Vorgelegt hat der Kläger indes lediglich ein Schreiben der Prozessbevollmächtigten der Beklagten vom 23.8.2021, das sich datumsbedingt nicht auf den hier streitgegenständlichen Fall bezogen haben kann. Insofern kann nicht beurteilt werden, ob die – unstreitig erfolgte – Auskunft seitens der Beklagten erschöpfend war oder nicht. Dies geht zu Lasten des Klägers.

hh) Dem Kläger ist nach Auffassung der Kammer ein immaterieller Schaden in Höhe von 150,00 EUR gemäß Art. 82 Abs. 1 DSGVO entstanden.

Der Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO dient nicht nur dem Ausgleich erlittenen Schadens, sondern auch repressiven und präventiven Zwecken, indem er Verstöße sanktioniert, weiteren Verstößen präventiv vorbeugt und vor zukünftigen Verstößen abschreckt (BeckOK DatenschutzR/Quaas, DS-GVO Stand: 01.08.2022, Art. 82 Rn. 1). Der Erwägungsgrund 75 zur DSGVO benennt den Kontrollverlust ausdrücklich als zu erwartendes Risiko der Verarbeitung personenbezogener Daten, das zu einem Schaden bei den Betroffenen führt, indem es dort heißt: „Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere (...) wenn die betroffenen Personen (...) daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren“. Würde ein Schaden erst dann angenommen werden, wenn es durch das Abgreifen der Daten zu einer vertieften vermögens- oder persönlichkeitsrechtlichen Verletzung des Betroffenen kommt, würde das dem weit auszulegenden Schadensbegriff und dem damit verbundenen

individuellen Ausgleichsanspruch entgegenstehen (vgl. OLG Koblenz Urteil vom 18.05.2022 – 5 U 2141/21). Als weitere Schäden in diesem Zusammenhang kommen zudem Angst, Stress und Zeiteinbußen in Betracht.

Es kann vorliegend dahinstehen, ob für eine Ersatzpflicht nach Art. 82 Abs. 1 DSGVO bereits ein Verstoß gegen eine Norm der DSGVO genügt (so: BAG, Beschluss vom 26.08.2021 – 8 AZR 253/20 (A)), oder ein konkreter Schaden des Klägers vorliegen muss (EuGH, Urteil vom 04.05.2023 – C 300/21; zum Ganzen auch: OLG Frankfurt a.M., Urteil vom 02.03.2022 – 13 U 206/20).

Unter Anwendung der vorstehenden Grundsätze, geht die Kammer davon aus, dass auf Seiten des Klägers ein Schaden vorliegt. Die Kammer geht – auch im Hinblick auf die Erfahren aus zahlreichen Parallelfällen – davon aus, dass der Vortrag des Klägers zutrifft, wonach er seit April 2021 vermehrt „dubiose“ Nachrichten und E-Mails erhalten hat. Dass der hierin und durch das Bekanntwerden des Sachverhalts zutage tretende Kontrollverlust über eigene Daten (in psychischer Hinsicht) belastende Wirkung aufweist, liegt nach Auffassung der Kammer auf der Hand.

ii) Die Verstöße gegen die DSGVO durch die Beklagte können nicht hinweg gedacht werden, ohne dass der Schaden des Klägers entfiele. Erst durch diese Verstöße war es den unbekannten Scrapern möglich, personenbezogene Daten des Klägers abzugreifen.

jj) Die Beklagte handelte hinsichtlich der festgestellten Verstöße auch schuldhaft. Sie kann sich hinsichtlich der einzelnen Verstöße nicht nach Art. 82 Abs. 3 DS-GVO entlasten (vgl. auch LG Stuttgart, Urteil vom 26. Januar 2023 – 53 O 95/22 –, juris).

Danach 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. Hier ist der Beklagten weder der Nachweis fehlenden Verschuldens noch des Vorliegens ganz ungewöhnlicher Kausalverläufe, eines Falles höherer Gewalt oder weit überwiegenden eigenen Fehlverhaltens des Klägers.

Der Kläger hat sich auch kein Mitverschulden nach § 254 Abs. 1 BGB anrechnen zu lassen. Ein mögliches und etwaiges Mitverschulden des Klägers (§ 254 BGB), weil er die Datenschutzeinstellungen seines Facebook-Profils nicht geändert hat und dadurch auch den Zugriff der Daten-Scraper mit ermöglicht hat, tritt hinter die Verstöße der Beklagten vollkommen zurück.

jj) Der vom Kläger erlittene immaterielle Schaden war vorliegend auf 150,00 EUR zu bemessen. Diese Summe erachtet des Gerichts im Rahmen des von ihm ausgeübten Ermessens nach § 287 Abs. 1 ZPO (vgl. BAG NJW 2022, 2779) als ausreichend, um sowohl der Ausgleichs- und Genugtuungsfunktion des Schadensersatzes gerecht zu werden und außerdem als hinreichend, um dem präventiven Charakter der Norm zu genügen.

Der Schadensersatz der DSVGO soll dem Betroffenen einen vollständigen und zugleich wirksamen Ersatz für den von ihm erlittenen Schaden bringen. Bei der Bemessungshöhe des immateriellen Schadensersatzes nach Art. 82 Abs. 1 DSGVO können dabei die Grundlagen des Art. 83 Abs. 2 DSGVO herangezogen werden. Demnach sind u.a. Art, Schwere und Dauer des Verstoßes und die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind, zu berücksichtigen. Unter Berücksichtigung der Erwägungsgründe 75 und 85 der DSGVO muss weiter beachtet werden, dass dem Schadenersatzanspruch auch eine abschreckende Wirkung gegenüber dem Verantwortlichen zukommen soll, um somit eine effektive Durchsetzung der DSGVO sicherzustellen. Schließlich sind auch die konkreten Umstände des maßgeblichen Einzelfalls zu berücksichtigen.

Hier war einerseits zu berücksichtigen, dass der Kläger keine Anhaltspunkte vorgetragen hat, dass die Geschehnisse für ihn Belastungen verursacht hätten, die über das psychische Unwohlsein aufgrund eines Kontrollverlusts über eigene Daten hinausgehen, also etwa – wie aus anderen Fällen bekannt – Anrufe zur Nachtzeit mit entsprechenden Störungen der Nachtruhe o.ä. Andererseits sind der Beklagten mehrere schadensursächliche Verstöße gegen die DSGVO vorzuwerfen, welche einen sehr weitgehenden Kontrollverlust der personenbezogenen Daten des Klägers ermöglicht und begünstigt haben.

Ein den Betrag in Höhe von 150,00 EUR übersteigender Ansatz erscheint vor diesem Hintergrund nicht angemessen.

kk) Der geltend gemachte Zinsanspruch folgt aus §§ 288, 291 BGB.

b) Der klägerische Antrag zu 2) ist begründet. Es ist vorliegend nicht ausgeschlossen, dass der Kläger in Zukunft durch die Verstöße der Beklagten gegen die DSGVO weitere – auch materielle – Schäden erleidet. Dies auch nicht deshalb, weil der Kläger nunmehr eine andere Mobilfunknummer besitzt. Es ist derzeit nach Ansicht des Gerichts nicht absehbar, wie die Veröffentlichung der abgegriffenen Daten auf den Kläger zurückfallen kann.

c) Darüber hinaus kann der Kläger die mit dem Klageantrag zu Ziff. 3 beanspruchte Unterlassung erfolgreich gegenüber der Beklagten geltend machen.

Die Beklagte hat gegen Art. 25 Abs. 2 DSGVO, Art. 13 Abs. 1 lit. c) DSGVO, gegen Art. 32, 24, 5 Abs. 1 lit. f) DSGVO, gegen Art. 33 DSGVO und gegen Art. 34 Abs. 1 DSGVO verstoßen. Diese Rechtsverstöße geben dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung. Daher kann der Kläger verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten, insbesondere Telefonnummer unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen. In gleicher Weise kann der Kläger beanspruchen, dass die Beklagte es unterlässt, personenbezogenen Daten, insbesondere Telefonnummer ohne Einholung einer Einwilligung oder Erfüllung sonstiger gesetzlicher Erlaubnistatbestände zu verarbeiten. Soweit die Beklagte darauf verweist, dass der Kläger durch eine Änderung der Einstellungen auf der Facebook-Plattform die von ihm gewünschte Rechtsfolge erreichen kann, steht dies Unterlassungsansprüchen des Klägers nicht entgegen. Durch mögliche, vom Kläger selbst vorzunehmende Änderungen von Einstellungen in seinem Facebook-Profil ist eine Wiederholungsgefahr nicht entfallen, und der Kläger kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen. Die Ordnungsmittelandrohung folgt aus § 890 ZPO.

d) Der Antrag zu Ziff. 4 ist unbegründet.

Der Kläger hat nicht dargelegt, dass die Beklagte den grundsätzlich bestehenden Anspruch nach Art. 15 DSGVO nicht bereits erfüllt hätte, vgl. die obigen Ausführungen.

II.

Die Kostenentscheidung beruht auf § 92 Abs. 1 S. 1 ZPO, die Entscheidung über die vorläufige Vollstreckbarkeit auf §§ 709 S. 1 und S. 2 ZPO.

Streitwert:
Antrag zu 1): 2.000 EUR
Antrag zu 2): 500,00 EUR
Antrag zu 3): 3.000 EUR
Antrag zu 4): 250,00 EUR

= 5.750,00 EUR

[redacted]

Beglaubigt
Urkundsbeamter/in der Geschäftsstelle
Landgericht Aachen

Verkündet am 30.11.2023

Doschat, Justizsekretärin
als Urkundsbeamtin der Geschäftsstelle