Abschrift

5 O 188/22

Landgericht Siegen

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

[redacted],

Klägers,

Prozessbevollmächtigte: Rechtsanwälte WBS.LEGAL,
Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln,

gegen

die Meta Platforms Ireland Limited, vertreten durch den Geschäftsführer, 4 Grand Canal Square, Dublin 2, Irland,

Beklagte,

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

hat die 5. Zivilkammer des Landgerichts Siegen
auf die mündliche Verhandlung vom [redacted]

für Recht erkannt:

I. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 500 Euro nebst Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 7. Oktober 2022.

II. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen materiellen 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, noch entstehen werden.

III. Die Beklagte wird weiter verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000 Euro, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) personenbezogene Daten des Klägers, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Stadt, 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 Sichtbarkeitseinstellung 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.

IV. Die Beklagte wird weiter verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 280,60 Euro zu zahlen, zuzüglich Zinsen in Höhe von fünf Prozentpunkten über dem Basiszinssatz seit dem 7. Oktober 2022.

V. Im Übrigen wird die Klage abgewiesen.

VI. Von den Kosten des Verfahrens tragen der Kläger 25 Prozent und die Beklagte 75 Prozent.

VII. Das Urteil ist vorläufig vollstreckbar, für den Kläger wegen der Ziffer III gegen Sicherheitsleistung in Höhe von 11.000 Euro. Im Übrigen kann jede Partei die Vollstreckung durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrages abwenden, wenn nicht die andere Partei vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Tatbestand:

Die Parteien streiten um Ansprüche des Klägers wegen behaupteter Verstöße der Beklagten gegen die Datenschutzgrundverordnung (DSGVO).

Der Kläger nutzt die von der Beklagten betriebene Social-Media-Plattform facebook.com. Die Plattform ermöglicht es Nutzern, persönliche Profile und Informationen zu erstellen und diese in einem digitalen Freundeskreis und darüber hinaus zu teilen. Im Rahmen der Registrierung gab der Kläger seinen Vornamen, Nachnamen, sein Geschlecht, seinen Wohnort und seinen Arbeitgeber an. Außerdem gab der Kläger auch seine Mobiltelefonnummer an. Die Daten „Bundesland“ und „Geburtsort“ werden von der Beklagten nicht vom Nutzer abgefragt. Bei der Registrierung auf der Plattform wurde der Kläger darauf hingewiesen, dass er damit den hinterlegten Nutzungsbedingungen der Beklagten zustimmte. Auf der Registrierungsseite war außerdem die Datenrichtlinie der Beklagten hinterlegt, die Informationen zum Erfassen, Verwenden und Teilen der Daten enthält. Diese Datenrichtlinie enthält u. a. Angaben dazu, welche der vom Nutzer erteilten Informationen immer öffentlich zugänglich sind, nämlich Name, Profil- und Titelbilder, Netzwerke, Geschlecht, Nutzername und Nutzer-ID, und die Angabe, dass öffentlich zugängliche Informationen jeder sehen kann, also auch Personen außerhalb der Plattform der Beklagten. Die Beklagte stellt den Nutzern ihrer Plattform auch Erklärungen darüber zur Verfügung, wie der Nutzer festlegen kann, wer die von ihm über die öffentlichen Informationen hinaus bereitgestellten Informationen sehen kann (Zielgruppenauswahl) und wer ihn anhand seiner E-Mail-Adresse oder seiner Telefonnummer, sofern überhaupt bereitgestellt, finden kann (Suchbarkeits- und Kontaktierungseinstellungen). Ohne Änderung durch den Nutzer sind die Zielgruppenauswahl von der Beklagten standardmäßig auf „Freunde“ und die „Suchbarkeits- und Kontaktierungseinstellung“ standardmäßig auf „alle“ eingestellt. Diese Voreinstellungen für die von ihm eingegebene Mobilfunknummer hatte der Kläger nicht geändert. Durch Nutzung des von der Beklagten zur Verfügung gestellten „Contact-Import-Tools“ (CIT) war es anderen Personen daher möglich, über die Eingabe der Telefonnummer des Klägers in das CIT sich dessen facebook-Profil anzeigen zu lassen und die öffentlich einsehbaren Informationen über den Kläger anzusehen. Wegen Inkrafttretens der DSGVO am 25. Mai 2018 aktualisierte die Beklagte im April 2018 ihre Nutzungsbedingungen und die Datenrichtlinie und forderte ihre Nutzer zur Überprüfung ihrer Privatsphäreeinstellungen auf.

Zu einem nicht näher bekannten Zeitpunkt im Zeitraum zwischen Januar 2018 und September 2019 sammelten Dritte unter Nutzung automatisierter IT-Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Das genaue Vorgehen ist bis heute nicht öffentlich bekannt. Allerdings wird allseits von folgendem Vorgehen ausgegangen: Die Dritten (sog. Scraper) erstellten Listen mit möglichen Telefonnummern und luden diese in das CIT der Plattform hoch, um so festzustellen, ob über die hochgeladenen Telefonnummern Nutzerkonten gefunden werden konnten. Wenn dies der Fall war, griffen die Scraper auf alle auf diesem Nutzerkonto öffentlich zugänglichen Informationen zu und fügten diesen die Telefonnummer hinzu, über die sie das Nutzerkonto gefunden hatten. Zu einem ebenso nicht näher bekannten Zeitpunkt vor April 2021 wurden die so erlangten Datensätze von über 500 Mio. Nutzern aus mehreren Ländern im Darknet frei zum Download bereitgestellt. Hierzu gehörten auch die immer öffentlich

zugänglichen Informationen des Profils des Klägers und die mit seinem Konto verknüpfte Telefonnummer.

Mit Schreiben vom 15. Juli 2021 (siehe Anlage K1, Bl. 53ff. der Akte) forderte der Kläger die Beklagte über seine Prozessbevollmächtigten zur Zahlung von 500 Euro Schadenersatz, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft über den im April 2021 bekannt gewordenen Datenabgriff auf. Mit Schreiben vom 7. Oktober 2021 (Anlage B16, Bl. 116ff. der Akte) teilte die Beklagte dem Kläger mit, dass unter den abgegriffenen Daten auch diejenigen des Klägers enthalten waren, und lehnte die Erfüllung weiterer Ansprüche ab. Die Prozessbevollmächtigten der Beklagten übermittelten dem Prozessbevollmächtigten des Klägers eine dezidierte Anleitung zur Einsichtnahme in seine bei der Plattform der Beklagten hinterlegten Informationen und deren Verwendung.

Die irische Datenschutzbehörde DPC verhängte gegen die Beklagte am 28. November 2022 eine Geldbuße in Höhe von 265 Mio. Euro, weil die Beklagte es nicht ausreichend verhindert habe, dass etwa 533 Mio. Datensätze mit persönlichen Informationen von Facebook-Nutzern und -Nutzerinnen abgegriffen und veröffentlicht wurden. Die vorbezeichnete Entscheidung ist nicht rechtskräftig; die Beklagte hat hiergegen Rechtsmittel eingelegt.

Der Kläger behauptet, dass seine Daten für gezielte Phishing-Attacken genutzt worden seien. Der Kläger habe einen erheblichen Kontrollverlust über seine Daten erlitten und mache sich Sorgen über deren Missbrauch. E-Mails und Anrufen von unbekannten Absendern oder Nummern begegne er mit verstärktem Misstrauen. Seit dem Scraping-Vorfall erhalte der Kläger seit April 2021 unregelmäßig Kontaktversuche per SMS und E-Mail, die offensichtliche Betrugsversuche und potentielle Virenlinks beinhalteten. Die Beklagte habe keine ausreichenden Sicherheitsmaßnahmen vorgehalten, um die Ausnutzung des von ihr zur Verfügung gestellten CIT zu verhindern, weder Sicherheitscaptchas, um automatische Suchläufe abzuwehren, noch einen Mechanismus zur Überprüfung der Plausibilität von Anfragen. Durch die fehlenden Sicherheitsvorkehrungen sei der „Datenklau“ überhaupt erst möglich geworden. Erst im Jahr 2019 habe die Beklagte nach Bekanntwerden des Datenlecks die bestehende Sicherheitslücke geschlossen. Der Kläger behauptet, dass er seine Telefonnummer nicht angegeben hätte, wenn er ausreichend über die möglichen Folgen dieser Preisgabe informiert worden wäre.

Der Kläger meint, die Beklagte als Verantwortliche nach Art. 4 Nr. 7 DSGVO habe seine personenbezogenen Daten ohne Rechtsgrundlage (Art. 6, 7 DSGVO) und ohne ausreichende Information (Art. 13, 14 DSGVO) verarbeitet, Art. 4 Nr. 2 DSGVO, diese unbefugten Dritten zugänglich gemacht und dabei Pflichten aus Art. 5, 25, 32 und 34 DSGVO sowie Betroffenenrechte des Klägers aus Art. 15, 17, 18 DSGVO verletzt. Die Einstellungsmöglichkeiten zur Sicherheit der Telefonnummer auf facebook seien so undurchsichtig und kompliziert gestaltet, dass ein Nutzer rein tatsächlich keine sicheren Einstellungen erreichen könne. Durch die DSGVO sei das Prinzip der Datenminimierung und der datenschutz- und nutzerfreundlichen Voreinstellungen vorgegeben. Der Nutzer solle aktiv entscheiden, für welche Fälle er seine Daten freigeben will, was zu den Voreinstellungen der Beklagten insbesondere

im Hinblick auf die Suchbarkeitseinstellungen in Widerspruch stehe. Die Beklagte habe beim Nutzer durch die vielschichtigen Einstellungsmöglichkeiten ein Gefühl der Sicherheit erzeugt und damit im Ergebnis eine erhebliche Datengefährdung verursacht. Für eine effektive digitale Sicherheit müsse der Nutzer mehrere von der Beklagten aufgedrängte Einstellungen ändern, um die Verwendung seiner Telefonnummer zu verhindern. Aufgrund der nutzerunfreundlichen Voreinstellungen fehle eine wirksame Einwilligung des Klägers zur Verarbeitung seiner Daten. Nach dem Vorfall habe die Beklagte weder den Kläger noch die zuständige Irische Datenschutzbehörde rechtzeitig und ausreichend über die Entwendung und Veröffentlichung der gescrapten Daten informiert. Das Auskunftsschreiben der Beklagten an den Kläger werde Art. 15 DSGVO nicht gerecht. Für das Bestehen eines Schadensersatzanspruchs reiche schon der hier eingetretene Kontrollverlust über die eigenen Daten.

Der Kläger beantragt,

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

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

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

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

   b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat" noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung

verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird;

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

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

Die Beklagte beantragt,

die Klage abzuweisen.

Sie behauptet, sie habe alle Nutzer umfassend und transparent über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppen-Auswahl informiert, auch der Kläger habe diese jederzeit nach seinen Wünschen anpassen können. Die Suchbarkeits-Einstellungen seien im Abschnitt „Privatsphäre“ des Haupteinstellungsmenüs im Nutzerkonto leicht zu finden gewesen. Die Daten des Klägers seien weder durch Hacking noch durch Ausnutzen einer Sicherheitslücke aus den Systemen der Beklagten erlangt worden. Die Beklagte habe Maßnahmen getroffen, um das Risiko von Scraping zu unterbinden, und diese Maßnahmen kontinuierlich weiterentwickelt. Maßnahmen zur Verringerung des Scraping-Risikos bestünden in der Regel aus Übertragungsbegrenzungen und Bot-Erkennung; beides habe Beklagte im relevanten Zeitraum eingesetzt. Nachdem die Beklagte festgestellt habe, dass das CIT von Scrapern genutzt wurde, habe sie ihre Systeme angepasst. Es habe auch keine Sicherheitsverletzung gegeben; sämtliche abgeschöpften Daten seien öffentlich gewesen.

Die Beklagte meint, sie habe nicht gegen ihre Pflichten aus der DSGVO verstoßen. Für den Zweck ihrer facebook-Plattform, dass Menschen sich verbinden könnten, sei es erforderlich, dass die Suchbarkeits-Einstellung über die Telefonnummer standardmäßig auf „alle“ eingestellt sei. Die dem Kläger erteilte Auskunft über den mutmaßlichen Ablauf des Scraping-Vorfalls sei ausreichend gewesen, weitere Informationen könne sie mangels eigener Kenntnis nicht erteilen. Das – bestrittene – Bestehen eines Kontrollverlusts über die eigenen Daten reiche für die Bejahung eines ersatzfähigen Schadens nicht aus. Ein Unterlassungsanspruch scheitere jedenfalls an der fehlenden Wiederholungsgefahr.

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

Das Gericht hat den Kläger im Termin am 9. Juni 2023 persönlich angehört. Insoweit wird auf das Protokoll vom 9. Juni 2023 verwiesen (Bl. 918ff. der Akte).

Entscheidungsgründe:

I.

Die weitgehend zulässige Klage ist teilweise begründet.

A.

Die Klage ist überwiegend zulässig.

1.

Das Landgericht Siegen ist international, sachlich und örtlich zuständig. Die internationale und örtliche Zuständigkeit ergibt sich für die Verbraucherklage des Klägers aus Art. 6 Abs. 1, Art. 18 Abs. 1 Var. 2 EuGVVO (Brüssel Ia-VO) und Art. 79 Abs. 2 DSGVO. Das Landgericht Siegen ist wegen der rügelosen Einlassung der Beklagten gem. § 39 Satz 1 ZPO trotz des niedrigen Streitwerts auch sachlich zuständig.

2.

Der Kläger hat auch ein hinreichendes Feststellungsinteresse im Sinne von § 256 ZPO dargelegt. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. BGH, Beschluss vom 9. Januar 2007, Az. VI ZR 133/06; BGH, Urteil vom 16. Januar 2001, Az. VI ZR 381/99; Saarländisches Oberlandesgericht Saarbrücken, Urteil vom 20. Februar 2014, Az. 4 U 411/12). Bei den behaupteten Verstößen gegen die DSGVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte. Es ist insbesondere nicht völlig ausgeschlossen, dass der Kläger infolge der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Namen sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleidet. Allerdings ist im Hinblick auf zukünftige immaterielle Schäden der Vorrang der Leistungsklage zu berücksichtigen, da diese bereits bei der Bemessung des beantragten Schmerzensgeldes zu berücksichtigen sind und die Möglichkeit des Auftretens künftiger weiterer, bisher noch nicht erkennbarer immaterieller Schäden nicht vorgetragen ist (vgl. BGH, Urteil vom 10. Juli 2018, Az. VI ZR 259/15, NJW-RR 2018, 1426).

3.

Die Klageanträge sind auch ausreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO. Insbesondere ist der Kläger nicht gehalten, für seinen Unterlassungsantrag die nach dem aktuellen Stand der Technik möglichen und notwendigen Sicherheitsmaßnahmen selbst zu ermitteln. Zur Gewährleistung eines effektiven Rechtsschutzes ist dabei eine gewisse Auslegungsbedürftigkeit hinzunehmen (BGH, Urteil vom 21. Mai 2015, Az. I ZR 183/13).

B.

Die Klage ist im tenorierten Umfang auch begründet.

1.

Dem Kläger steht gegen die Beklagte aus Art. 82 DSGVO ein Anspruch auf Ersatz seines immateriellen Schadens in Höhe von 500 Euro zu.

a)

Die Beklagte als Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO hat gegen ihr nach der DSGVO obliegende Pflichten verstoßen. Sie hat zum einen im Hinblick auf die Suchbarkeit des Klägers über dessen Telefonnummer datenschutzunfreundliche Voreinstellungen getroffen und damit gegen Art. 25 DSGVO verstoßen. Zum anderen hat sie den Kläger nicht ausreichend darüber aufgeklärt, dass die Angabe seiner Telefonnummer zunächst automatisch zur Folge hat, dass sein Facebook-Profil von jedermann nach Eingabe dieser Telefonnummer gefunden werden kann, und damit gegen Art. 13 DSGVO verstoßen. Schließlich hat sie nicht schlüssig dargelegt, dass sie im Zeitpunkt des Abschöpfens der klägerischen Daten bei dem Scraping-Vorfall ausreichende Sicherheitsvorkehrungen getroffen hätte, um den nach ihren Nutzungsbedingungen untersagten Scraping-Vorfall zu verhindern und die ihr von den Nutzern anvertrauten Daten hinreichend zu schützen, sodass sie auch gegen Art. 24 und 32 DSGVO verstoßen hat.

aa)

Gemäß Art. 25 Abs. 2 Satz 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen ist zu gewährleisten, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben. Das hat zur Folge, dass alle für die Nutzung nicht erforderlichen personenbezogenen Daten anderen Nutzern nicht zugänglich gemacht werden dürfen, es sei denn, die betroffene Person nimmt entsprechende Änderungen in den Voreinstellungen selbst vor (vgl. Gola/Heckmann,

DS-GVO BDSG, 3. Auflage, Art. 25 DS-GVO Rn. 28; Kühling/Buchner, DS-GVO BDSG, 3. Auflage, Art. 25 DS-GVO Rn. 26).

Der von der Beklagten angegebene Zweck, dass die Plattform die Vernetzung von Menschen ermöglichen solle, ist kein solcher Verarbeitungszweck, der eine grundsätzlich für jedermann gewährleistete Suchbarkeit des Klägers über seine Telefonnummer erfordern würde. Der Zweck der Plattform ist vielmehr auch dann zu erreichen, wenn der Nutzer sich hierfür bewusst entscheiden kann. Der zu ermöglichende Vernetzung der Plattform-Nutzer führt nicht dazu, dass der Kläger ohne seinen ausdrücklichen Willen über seine Telefonnummer für jedermann auffindbar sein muss. Dass dies auch der Beklagten bewusst war, zeigt sich auch schon daran, dass die Voreinstellung, ohne Weiteres geändert werden konnte, ohne dass dies der weiteren Vertragsdurchführung entgegenstehen würde (vgl. KG, Urteil vom 20. Dezember 2019, Az. 5 U 9/18, BeckRS 2019, 35233 Rn. 39). Allein der Hinweis auf die Möglichkeit der Änderung dieser Voreinstellung genügt nicht, um einen Verstoß gegen Art. 25 Abs. 2 DSGVO zu verneinen.

Ein Verstoß gegen Art. 25 Abs. 2 DSGVO ist auch ein Pflichtverstoß im Sinne von Art. 82 DSGVO (vgl. Gola/Heckmann, a. a. O., Art. 25 DS-GVO Rn. 3, 34). Wie sich gerade im vorliegenden Fall zeigt, hat gerade die datenschutzunfreundliche Voreinstellung der Suchbarkeitseinstellung über die Telefonnummer dazu geführt, dass die Daten des Klägers abgeschöpft werden konnten. Bei Beachtung der Vorgaben von Art. 25 Abs. 2 DSGVO wäre das Nutzerprofil des Klägers ohne dessen bewusste Entscheidung für eine Suchbarkeit für „alle“ nicht bei dem automatischen Telefonnummernsuchlauf gefunden worden.

bb)

Gemäß Art. 13 Abs. 1 lit. c DSGVO hat die Beklagte die Zwecke, für die personenbezogene Daten verarbeitet werden sollen, zum Zeitpunkt der Erhebung der Daten mitzuteilen. Dem ist die Beklagte jedenfalls insofern nicht nachgekommen, als sie den Kläger bei der Datenerhebung seiner Mobilfunknummer nicht ausreichend über die Zwecke der Verarbeitung dieser Nummer aufgeklärt hat, nämlich insbesondere nicht auf die Verwendungsmöglichkeit für das von ihr zur Verfügung gestellte CIT und die daraus folgenden möglichen Konsequenzen hingewiesen hat.

Aus den vorgelegten Unterlagen ist hierzu keine ausreichende Aufklärung durch die Beklagte ersichtlich. Im Gegenteil wird durch die Information „Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke: … um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf facebook verbinden kannst“ gerade ein gegenteiliger Eindruck erweckt. 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. Diese Information ist selektiv und damit unvollständig. Auch an anderer Stelle finden sich in den Nutzungsbedingungen oder der Datenrichtlinie der Beklagten hierzu keine ausreichenden Informationen.

Daher kann nicht von einer wirksamen Einwilligung des Klägers im Sinne von Art. 6 Abs. 1 lit. a DSGVO ausgegangen werden, ebenso wenig ist das Auffinden über das CIT im Sinne von Art. 6 Abs. 1 Satz 1 lit. d DS-GVO für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich (siehe oben unter aa).

Auch ein Verstoß gegen Art. 13 DSGVO kann einen Schadensersatzanspruch nach Art. 82 DSGVO auslösen (vgl. Gola/Heckmann, a. a. O, Art. 13 DS-GVO Rn. 64; Kühling/Buchner/Bergt, 3. Auflage 2020, Art. 82 DSGVO Rn. 23; BeckOK DatenschutzR, 42. Edition 1.8.2022, Art. 82 DSGVO Rn. 14).

cc)

Die Beklagte hat auch gegen Art. 24 und 32 DSGVO verstoßen. Zwar ist zwischen den Parteien streitig, inwieweit fehlende Sicherheitsmaßnahmen kausal zu dem Scraping-Vorfall geführt haben. Unstreitig ist allerdings, dass die Beklagte zwar Datenscraping in ihren Nutzungsbedingungen untersagt hat, hiergegen aber vor dem Vorfall keine ausreichenden Vorkehrungen getroffen hat, um den Scraping-Vorfall zu verhindern. Jedenfalls hat die Beklagte zu solchen ausreichenden Sicherheitsmaßnahmen vor dem Vorfall nicht substantiiert vorgetragen. Die Behauptung, im „relevanten Zeitraum“ Übertragungsbegrenzungen und Bot-Erkennung eingesetzt und Captchas genutzt zu haben, reicht hierfür nicht. Konkreter Vortrag dazu, was für Übertragungsbegrenzungen das im Einzelnen waren, wie die Bot-Erkennung beschaffen war, welche Sicherheits-Captchas verwendet wurden und in welchen Zeitpunkten welche konkreten Maßnahmen getroffen wurden, fehlt. Vielmehr ist dem Vortrag der Beklagten zu entnehmen, dass sie nach eingetretenen Vorfällen jeweils auf diese reagiert hat, ohne jedoch zu spezifizieren, was jeweils konkret geändert wurde.

Damit hat die Beklagte gegen Art. 24, 32 DSGVO verstoßen, was ebenfalls einen Schadensersatzanspruch nach Art. 82 DSGVO auslösen kann (vgl. Kühling/Buchner/Bergt, a. a. O.; BeckOK DatenschutzR, a. a. O).

dd)

Soweit der Kläger zuletzt bestritten hat, dass nur die öffentlichen Daten von Nutzern abgeschöpft und schließlich mit deren zur Suche benutzten Telefonnummer verknüpft wurden, wenn deren Suchbarkeits-Einstellung im Abschöpfungszeitpunkt auf „alle“ eingestellt war, ist dieses Bestreiten zum einen unsubstantiiert und zum anderen für den streitgegenständlichen Fall irrelevant, da das Nutzerprofil des Klägers im „relevanten Zeitraum“ (von Januar 2018 bis September 2019) für alle über seine Telefonnummer auffindbar war. Allein die Vorlage von drei Beispielen aus Parallelprozessen, bei denen die jeweiligen Nutzer ihre Suchbarkeits-Einstellungen über die Telefonnummer jeweils ab September 2018 während des relevanten Zeitraumes geändert hatten, genügt noch nicht, um den bisher unstreitigen Vortrag der Beklagten zum Hergang des Scraping-Vorfalls erfolgreich anzugreifen. Denn

insbesondere das beim abgeschöpften Datensatz des Klägers angegebene Datum „8/14/2018 12,00,00 AM“ (Bl. 247 der Akte) spricht dafür, dass die Daten bereits vorher abgeschöpft wurden. Substantiierter Vortrag für einen weitergehenden DSGVO-Verstoß der Beklagten ist hieraus nicht ableitbar.

ee)

Ob die Beklagte im Zusammenhang mit dem Daten-Scraping-Vorfall weitere Pflichtverletzungen in Ansehung der DSGVO begangenen hat, kann dahinstehen, da sich daraus weitere Konsequenzen für den dem Kläger insofern zuzubilligenden Schadensersatzanspruch nicht ergeben können. Denn es besteht hinsichtlich der vom Kläger der Beklagten vorgeworfenen Verstöße letztlich kein weitergehender Unrechtsgehalt als derjenige, der bereits aus den Verstößen gegen Art. 25 Abs. 2 DSGVO, Art. 24, 32 DSGVO und aus Art. 13 DSGVO folgt.

b)

Dem Kläger ist hierdurch auch ein kausaler Schaden entstanden. Seine persönlichen Daten Vorname, Nachname und NutzerID wurden unstreitig abgeschöpft und sie wurden danach unstreitig mit der zum Auffinden des Profils benutzten Telefonnummer verknüpft. Die Kombination dieser Daten wurde anschließend veröffentlicht, sodass sie so in dieser Kombination für jedermann zur Verfügung standen. Die Kombination wäre allein über das Facebook-Profil des Klägers so nicht zusammenstellbar, insbesondere nicht die Verknüpfung zur Telefonnummer, da diese im Profil des Klägers nicht angezeigt wurde.

Gerade die Kombination von Name und Telefonnummer gibt Kriminellen ausreichend Informationen für Phishing-Attacken an die Hand. Die Veröffentlichung dieser Kombination hat zu einem Kontrollverlust des Klägers über seine Daten geführt.

Dieser Kontrollverlust ist bereits ausreichend, um einen Schaden des Klägers im Sinne der Vorschrift anzunehmen. Auch die Entscheidung des EuGH vom 4. Mai 2023 (Rechtssache C-300/21), wonach für einen Schadensersatzanspruch nach Art. 82 DSGVO zwar ein Schaden erforderlich sei, für diesen aber gerade keine Erheblichkeitsschwelle gelte, steht dieser Auslegung nicht entgegen. Dafür, dass darin ein immaterieller Schaden im Sinne von Art. 82 Abs. 1 DSGVO liegen kann, spricht auch der Erwägungsgrund 75 der DSGVO, wo dem Schadensbegriff auch der Verlust der Kontrolle über personenbezogene Daten zugeordnet wird. Daher kommt es auf die Frage, ob der unregelmäßige Erhalt von SMS und Anrufen unbekannter Nummern auf seinem Mobiltelefon auf die Veröffentlichung der beim Scraping-Vorfall abgeschöpften persönlichen Daten des Klägers zurückzuführen ist, nicht an.

Wenn die Beklagte ihren Pflichten aus Art. 25, 13 und 24, 32 DSGVO nachgekommen wäre, wäre der Schaden in Form des Kontrollverlusts nicht eingetreten. Für eine Enthaftung der Beklagten nach Art. 82 Abs. 2 DSGVO ist weder ein Umstand vorgetragen noch sonst ersichtlich.

Für die Frage des kausalen Schadens spielt es auch keine Rolle, dass der Kläger inzwischen seine Telefonnummer geändert hat. Der Kontrollverlust ist dennoch zunächst eingetreten und hat gerade dazu geführt, dass der Kläger – zur Vermeidung weitergehender Schäden – eigene Maßnahmen ergriffen hat.

c)

Zum Ausgleich des erlittenen immateriellen Schadens hält das Gericht einen Betrag in Höhe von 500 Euro für angemessen, aber auch ausreichend.

Für die Bemessung von Schadensersatzansprüchen nach Art. 82 Abs. 1 DSGVO enthält die DSGVO nur wenige Vorgaben. Aus dem Nebeneinander von materiellem und immateriellem Schaden folgt, dass auch solche Schäden auszugleichen sind, die sich nicht unmittelbar in Geld bemessen lassen. Nach Erwägungsgrund 146 sollen die Auslegung des Schadensbegriffs den Zielen der Verordnung in vollem Umfang entsprechen und die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für erlittene Schäden erhalten.

Hiernach hat sich der Schadensersatz auch bei immateriellen Schäden zuerst am Ziel des Schadensausgleichs zu orientieren, darüber hinaus spielt auch die Genugtuungsfunktion eine Rolle (Eichelberger, WRP 2021, 159, 162 ff). Maßgeblich sind die Umstände des konkreten Einzelfalls, etwa Art, Schwere und Dauer des Datenschutzverstoßes, das Verhalten des Verantwortlichen sowie die Auswirkungen des Verstoßes für den Betroffenen (siehe EuGH, Urteil vom 30. Mai 2017, Rechtssache C-45/15 P, juris, Rn. 52, zu Art. 340 Abs. 2 AEUV). Hier war vor allem entscheidend, dass der Beklagten mehrere DSGVO-Verstöße zur Last fielen, von denen die Befolgung jeder einzelnen verletzten DSGVO-Vorschrift höchstwahrscheinlich dazu geführt hätte, dass der Schaden nicht eingetreten wäre. Der Kläger hat durch die Veröffentlichung seiner Daten im Darknet einen weitgehenden Kontrollverlust erlitten, den die Beklagte begünstigt hat und den der Kläger nur durch Änderung seiner Telefonnummer wieder einfangen konnte. Angesichts der dennoch relativ geringen persönlichen Betroffenheit des Klägers erschien ein Betrag von 500 Euro als ausreichend.

2.

Der Feststellungsantrag ist im tenorierten Umfang begründet. Ein Schadensersatzanspruch des Klägers besteht dem Grunde nach aus Art. 82 DSGVO (vgl. oben 1). Es ist nicht ausgeschlossen, dass dem Kläger infolge des Kontrollverlusts über seine Daten konkrete materielle Schäden entstehen, die die Beklagte zu ersetzen hat.

3.

Der Kläger hat gegen die Beklagte auch einen Anspruch auf zukünftige Unterlassung der bereits erfolgten Verstöße gegen die DSGVO aus §§ 823 Abs. 2, 1004 Abs. 1 Satz 2 BGB analog i. V. m. Art. 6 Abs. 1 DSGVO bzw. aus Art. 17 Abs. 1 lit. d DSGVO (vgl. BGH, Urteil vom 12. Oktober 2021, Az. VI ZR 488/19, NJW 2022, 1098).

a)

Dabei kann der Kläger zum einen verlangen, dass die Beklagte es zukünftig unterlässt, seine personenbezogenen Daten Telefonnummer, Facebook-ID, Familienname, Vorname, Geschlecht und Wohnort unbefugten Dritten über die CIT-Software zugänglich zu machen. Ausgenommen davon sind jedoch die Daten „Bundesland“ und „Land“, die nach dem vom Kläger unbestritten gebliebenen Vorbringen der Beklagten nicht Gegenstand der Angaben auf der Facebook-Plattform sind. Auch seinen Beziehungsstatus hat der Kläger nicht für sein Nutzerprofil angegeben.

Für den Unterlassungsanspruch ist es auch unerheblich, dass der Kläger durch eine Änderung der Einstellungen auf der Facebook-Plattform selbst erreichen kann, dass sein von unbekannten Dritten über das CIT unter Angabe seiner Telefonnummer gefunden werden kann, nämlich durch einfache Änderung seiner Suchbarkeitseinstellungen. Auch die inzwischen erfolgte Änderung seiner Telefonnummer wirkt sich nicht auf die Wiederholungsgefahr aus. Denn dadurch entfällt die Wiederholungsgefahr nicht, denn auch wenn er seine Suchbarkeitseinstellungen nicht ändert, seine Telefonnummer aber schon, hat er gegen die Beklagte einen Anspruch darauf, dass diese seine Daten durch ausreichende Sicherheitsvorkehrungen gegen unbefugte Zugriffe schützt, Art. 24, 32 DSGVO. Der Kläger kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen.

b)

Der Kläger hat auch einen Unterlassungsanspruch im Hinblick auf die Verarbeitung seiner Telefonnummer, die die Beklagte ohne ausreichende Erfüllung ihrer Informationspflichten erlangt hat (siehe oben 1. a) bb). Die Vermutung einer Wiederholungsgefahr ergibt sich dabei grundsätzlich bereits aus der Rechtsverletzung. Auch die Umstände sprechen nicht für ein Entfallen der Wiederholungsgefahr. Die Beklagte hat keine Unterlassungserklärung abgeben. Zwar hat die Beklagte dem Kläger im Nachhinein Auskunft über die Funktionsweise des CIT und die Konsequenzen der Suchbarkeitseinstellungen erteilt. Dies lässt aber die Wiederholungsgefahr nicht entfallen, denn eine Verletzungshandlung begründet die Vermutung der Wiederholungsgefahr nicht nur für identische Verletzungsformen, sondern für alle im Kern gleichartigen Verletzungshandlungen, in denen das Charakteristische der konkreten Verletzungsform zum Ausdruck kommt (vgl. BGH, Urteil vom 22. September 2021, Az. I ZR 83/20).

c)

Die Ordnungsmittelandrohung beruht auf § 890 Absatz 2 ZPO.

4.

Der Kläger hat gegen die Beklagte keinen Anspruch auf weitere Auskunftserteilung aus Art. 15 Abs. 1 lit. a und c DSGVO.

Die Beklagte hat den Anspruch bereits erfüllt, soweit ihr dies möglich war, sodass er gemäß § 362 Abs. 1 BGB erloschen ist (vgl. BGH, Urteil vom 3. September 2020, Az. III ZR 136/18, GRUR 2021,110). Anhaltspunkte dafür, dass die Beklagte dem Kläger nicht sämtliche ihr zu dem Scraping-Vorfall bekannten Umstände mitgeteilt hat, liegen nicht vor.

5.

Die vorgerichtlichen Rechtsanwaltskosten sind in Höhe von 280,60 Euro als Teil des Schadens gemäß Art. 82 Abs. 1 DSGVO zu ersetzen. Im Umfang seines berechtigten Verlangens kann der Kläger gemäß §§ 280 Abs. 1, 2, 286 Abs. 2 BGB die vorgerichtlichen Rechtsanwaltskosten nach einem Gegenstandswert von 2.000 Euro erstattet verlangen.

Gemäß § 291 BGB hat der Kläger hinsichtlich der zugesprochenen Beträge ab dem 7. Oktober 2022 Anspruch auf Rechtshängigkeitszinsen, nachdem die Klage am 6. Oktober 2022 zugestellt worden ist (Bl. 150 der Akte).

II.

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

Die Entscheidung über die vorläufige Vollstreckbarkeit ergibt sich für den Kläger hinsichtlich der Zahlungsverurteilung und der durch ihn vollstreckbaren Kosten aus § 708 Nr. 11, 711 ZPO und hinsichtlich der Unterlassungsverurteilung aus § 709 Satz 1 und 2 ZPO; für die Beklagte, die nur Kosten von nicht mehr als 1.500 Euro vollstrecken kann, aus den §§ 708 Nr. 11, 711 ZPO. Für die Bemessung der Sicherheitsleistung hinsichtlich Ziffer III des Tenors war nicht auf den entsprechenden Streitwert abzustellen, sondern auf den drohenden Vollstreckungsschaden (vgl. Zöller, ZPO, 34. Auflage 2022, § 709 Rn. 5).

III.

Der Streitwert wird auf 2.600 Euro festgesetzt.

Heerwig