

Aktenzeichen:
4 O 86/22



Landgericht Ulm

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:

gegen

Meta Platforms Ireland Limited Facebook Ireland Ltd., vertreten durch d. Geschäftsführer (Director) Gareth Lambe, ebenda, 4 Grand Canal Square, Dublin 2, Irland

- Beklagte -

Prozessbevollmächtigte:

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat das Landgericht Ulm - 4. Zivilkammer - durch die Richterin am Landgericht als Einzelrichterin aufgrund der mündlichen Verhandlung vom 02.02.2023 am 16.02.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 500 EUR zu zahlen nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 06.04.2022.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle künftigen Schäden zu ersetzen, die dem Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.
3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten des Klägers, namentlich Telefonnummer, Facebook-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern.
4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 367,23 EUR zu zahlen zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 06.04.2022.
5. Im Übrigen wird die Klage abgewiesen.
6. Von den Kosten des Rechtsstreits haben der Kläger 45 % und die Beklagte 55 % zu tragen.
7. Das Urteil ist hinsichtlich des Tenors zu Ziffer 1) und Ziffer 4) vorläufig vollstreckbar. Die Beklagte darf insoweit die Vollstreckung gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in gleicher Höhe leistet; im Übrigen ist das Urteil gegen Sicherheitsleistung in Höhe von 3.500 EUR vorläufig vollstreckbar.

Streitwert: Klageantrag zu 1: 500 EUR

Klageantrag zu 2: 1.500 EUR

Klageantrag zu 3: 2.000 EUR

Klageantrag zu 4: 1.500 EUR

Insgesamt 5.500 EUR

Tatbestand

Der Kläger macht Ansprüche wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (fortan: DSGVO) geltend.

Der Kläger nutzt die auf dem Gebiet der Europäischen Union von der Beklagten betriebene Social Media Plattform facebook, auf die sowohl über die Internetseite www.facebook.com als auch über Apps mittels Smartphone oder Tablet zugegriffen werden kann.

Wird ein Facebook-Konto eröffnet, müssen zur Erstellung eines Nutzerprofils verschiedene Daten angegeben werden (Bl. 8 ff. d.A.), wobei der angegebene Vor- und Nachname, das Geschlecht und die von der Beklagten erstellte Nutzer-ID als Teil des Nutzerprofils immer öffentlich einsehbar sind. Die Eingabe der Handynummer ist nicht zwingend erforderlich. Der Kläger fügte seine Handynummer jedoch den Nutzereinstellungen hinzu.

Hinsichtlich der weiteren Daten gibt es im Rahmen der Privatsphäre-Einstellungen Wahlmöglichkeiten für jeden Nutzer. Bei der sogenannten „Zielgruppenauswahl“ legt der Nutzer fest, wer einzelne Informationen auf seinem Profil, wie etwa Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse, einsehen kann. So kann der Nutzer anstelle der standardmäßigen Voreinstellung „öffentlich“ auswählen, dass nur „Freunde“ auf der Plattform, oder „Freunde von Freunden“ die jeweiligen Informationen einsehen können. Lediglich die Telefonnummer des Nutzers wird insoweit gesondert behandelt.

Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann. Wenn also ein Nutzer in seinem Smartphone eine Telefonnummer als Kontakt gespeichert hat, erlaubt es die Beklagte ihm, seine Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Dafür war nicht erforderlich, dass der andere Nutzer seine Telefonnummer nach der „Zielgruppenauswahl“ öffentlich gemacht hat. Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre „Suchbarkeits-Einstellung“ für Telefonnummern auf der Standard-Voreinstellung „Alle“ eingestellt war. Daneben waren die Einstellungen nur „Freunde von Freunden“ oder „Freunde“ auswählbar. Ab Mai 2019 stand Nutzern auch die Option

„Nur ich“ zur Verfügung. Streitig ist zwischen den Parteien, ob die „Suchbarkeits-Einstellung“ bei dem Kläger auf „Alle“ eingestellt war (Anlage B17; S. 3 d. Sitzungsniederschrift vom 02.02.2023; Bl. 421 d.A.).

Bei der Registrierung wird der Nutzer auf die Datenrichtlinie der Beklagten hingewiesen. Insoweit wird auf den in der Anlage B9 zur Akte gereichten Auszug Bezug genommen. Den Nutzern werden zudem im „Hilfereich“, 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 Hilfereich und in den Einstellungen wird auf die Abbildungen in der Klageschrift sowie auf die Anlagen B1 bis B8 Bezug genommen.

Im Zeitraum von Januar 2018 bis September 2019 sammelten Dritte mittels einem sogenannten „Datenscraping“, also dem massenhaften, automatisierten Sammeln, persönliche Daten von Facebook-Nutzern, die auf dem Facebook-Profil entweder „immer öffentlich“ oder aber zu diesem Zeitpunkt aufgrund der Privatsphäreneinstellungen der Nutzer öffentlich einsehbar waren. Dieses Sammeln von Daten mittels automatisierter Tools und Methoden war und ist nach den Nutzungsbedingungen der Beklagten untersagt.

Zusätzlich erbeuteten die Scraper Handy- bzw. Telefonnummern, die mit dem entsprechenden Nutzerprofil verknüpft waren, mittels sog. „Telefonnummernaufzählung“. Dabei machten sich die Scraper das „Contact-Import-Tool“ (fortan: CIT) der Beklagten zu Nutze. Mittels dieser Funktion war es Nutzern möglich, ihre Kontakte von ihren Mobilgeräten auf Facebook hochladen, um diese Kontakte auf der Facebook Plattform zu finden und mit ihnen in Verbindung zu treten, ohne dass die im Profil hinterlegte Nummer in der „Zielgruppenauswahl“ öffentlich gemacht worden wäre. Vor diesem Hintergrund luden die „Scraper“ mithilfe des „CIT“ Kontakte hoch, welche mögliche Telefonnummern von Nutzern enthielten, um festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit sie feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto verknüpft war, kopierten sie die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer den abgerufenen, öffentlich einsehbaren Daten hinzu.

Anfang April 2021 veröffentlichten Unbekannte nach Angaben eines Artikels des „Business Insider“ vom 03.04.2021 die Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet. Die Beklagte veröffentlichte daraufhin am 06.04.2021 den Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ (Anlage B10), in dem sie erläuterte, dass die Daten nicht durch ei-

nen Hackerangriff erlangt worden seien, sondern es sich um öffentlich einsehbare Informationen handele.

Die zuständige Datenschutzbehörde und auch der Kläger wurde von der Beklagte nicht über den Vorfall informiert.

Mit E-Mail des Prozessbevollmächtigten des Klägers vom 18.11.2021 forderte dieser die Beklagte zur Schadensersatzzahlung i.H.v. 500,00 EUR, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren (Anlage K1). Bereits mit Schreiben vom 23.08.2021 (Anlage K2) übermittelten die Prozessbevollmächtigten der Beklagten dem Prozessbevollmächtigten des Klägers eine Anleitung zur Einsichtnahme in die bei der Plattform der Beklagten hinterlegten Informationen und deren Verwendung.

Der Kläger behauptet.

seine persönlichen Daten wie Telefonnummer, Name, Wohnort und E-Mailadresse seien durch Scraping abgegriffen worden. Ob noch mehr Daten entwendet worden seien, lasse sich mangels ausreichender Auskunft durch die Beklagte noch nicht angeben. Die entsprechenden personenbezogenen Daten, wie auch diejenigen des Klägers, seien sodann im Internet auf Seiten, die illegale Aktivitäten begünstigen sollen, so z.B. in dem „Hacker-Forum“ raidforums.com., veröffentlicht worden. Sie würden insbesondere für gezielte Phishing Attacken genutzt. Infolge des erlittenen erheblichen Kontrollverlustes über seine Daten verbleibe bei ihm der Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekanntem Nummern und Adressen. Seit dem Vorfall erhalte er u.a. unregelmäßig unbekannt Kontaktversuche via SMS und E-Mail, versehen 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 der Kläger nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagiere und jedes Mal einen Betrug fürchte und Unsicherheit verspüre.

Die Telefonnummern der Benutzer hätten von den unbekanntem Dritten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden können. Durch die Eingabe einer Viel-

zahl von Kontakten in ein virtuelles Adressbuch sei es gelungen, die Telefonnummern konkreten Facebook-Profilen zuzuordnen, ohne dass die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die Telefonnummer jeweils zu korrelieren, sei mit Hilfe des CIT jede fiktive Nummer geprüft und der zugehörige Facebook-Nutzer angezeigt worden. Ein Programm habe unzählige Kombinationen von Telefonnummern getestet, um festzustellen, ob diese mit einem Facebook-Nutzer übereinstimmten bzw. ob diese bei Facebook hinterlegt worden sei. Wenn dies der Fall gewesen sei, sei es dem Programm möglich gewesen, sämtliche Daten des Nutzers abzufragen und zu exportieren. Das Scraping sei dadurch ermöglicht worden, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten CIT zu verhindern. So seien keine Sicherheitscapchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handle. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereit gehalten worden. Der massenhafte Zugriff auf die Facebook-Profile durch Dritte mit auffälligen Telefonnummerabfragen wäre durch einfachste IP-Logs erkennbar und blockierbar gewesen. Es sei eine Kombination mehrerer Maßnahmen erforderlich, angemessen und üblich. Die Einführung einer Begrenzung der abgleichbaren Rufnummern oder Nutzung des CIT für Freunde von Freunden sei möglich gewesen. Mindestens aber ein expliziter Hinweis auf die offenen Standard-Einstellungen für die Suchbarkeit per Telefonnummer fehle, insbesondere bei erstmaliger Erhebung der Telefonnummer des Nutzers. Wären derartigen Sicherheitsmaßnahmen vorgenommen worden, wäre es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich gewesen, mit einem automatisierten Verfahren Daten abzugreifen.

Die Einstellungen zur Sicherheit der Telefonnummer auf Facebook seien so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Beklagte handle aufgrund der datenschutzunfreundlichen Standard-Voreinstellungen entgegen des Prinzips der Datenminimierung und des „privacy by default“-Grundsatzes. Die versteckte Option, dass der Nutzer nicht anhand seiner Telefonnummer von der Öffentlichkeit gefunden werden möchte, sei aufgrund der vielschichtigen Einstellungsmöglichkeit nicht zu erreichen, wenn lediglich nach den Einstellungsmöglichkeiten für die Telefonnummer gesucht werde. Durch vielschichtige Einstellungsmöglichkeiten werde ein Gefühl der Sicherheit für den Nutzer erzeugt, was im Ergebnis zu einer erheblichen Datengefährdung führe, da mit hoher Wahrscheinlichkeit zu erwarten sei, dass ein Nutzer die voreingestellten Standardeinstellungen behalte und nicht selbständig ändere. Diese Undurchsichtigkeit setze sich bei der von der Beklagten betriebenen „Messenger“-App mit separaten Sicherheitseinstellungen fort, bei der die Nutzer mit ihren Facebook-Profilen zur Versendung von Mitteilungen angemeldet seien. Eine Information über etwaige

Risiken oder über die Verwendung der Telefonnummer erfolge nicht, obwohl ein Nutzer geradezu zur Verwendung des CIT gedrängt werde.

Der Kläger habe die Suchbarkeits-Einstellungen, ob sein Facebook-Profil auf der Facebook-Plattform mithilfe einer Telefonnummer gefunden werden könne, im relevanten Zeitraum nicht auf „alle“ eingestellt gehabt, sondern auf „Freunde“.

Der Kläger ist der Auffassung,

die Beklagte habe eine Persönlichkeitsrechtsverletzung begangen und mehrfach gegen die Datenschutzgrundverordnung verstoßen. Die Beklagte habe als Verantwortliche im Jahr 2019 die den Kläger betreffenden personenbezogene Daten ohne Rechtsgrundlage und ausreichende Informationen verarbeitet, diese Daten unbefugten Dritten zugänglich gemacht und Betroffenenrechte des Klägers verletzt. Dem Kläger stehe daher gegen die Beklagte nach Art. 82 Abs. 1 DSGVO ein Anspruch auf Schadensersatz in Höhe von mindestens 500 Euro nebst Rechtsanwaltskosten zu. Zudem bestehe ein Anspruch des Klägers auf Feststellung der Einstandspflicht der Beklagten für künftige Schäden, ein Unterlassungsanspruch sowie ein Auskunftsanspruch.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 500,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.
2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.
3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

- a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,
 - b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.
4. Die Beklagte wird verurteilt der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.
 5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt.

die Klage abzuweisen.

Die Beklagte behauptet.

soweit die durch Scraping abgerufenen Daten von der Facebook-Plattform stammten und Informationen über den Kläger enthielten, handle es sich dabei entweder um immer öffentliche Nutzerinformationen oder um Daten, die in dem Facebook-Profil der Klagepartei entsprechend der jeweiligen Zielgruppenauswahl öffentlich einsehbar gewesen seien. Der Kläger habe die Suchbar-

keits-Einstellungen, ob sein Facebook-Profil auf der Facebook-Plattform mithilfe einer Telefonnummer gefunden werden könne, im relevanten Zeitraum auf „alle“ eingestellt gehabt. Es werde bestritten, dass die Datenpunkte E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt und Beziehungsstatus des Klägers in den durch Scraping abgerufenen Daten enthalten seien. Der Missbrauch der klägerischen Daten werde mit Nichtwissen bestritten.

Hauptzweck der Facebook Plattform sei, andere Nutzer zu finden und mit diesen in Kontakt zu treten, woran sich auch die Standard-Voreinstellungen orientierten. Die Scraper hätten lediglich die diesem Zweck dienenden Funktionen ausgenutzt. Es sei daher grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung der Funktionen zu unterlaufen. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Da die Funktionen, welche Scraper ausnutzten, rechtmäßige, gewöhnliche Nutzerfunktionen darstellten, werde zur Begrenzung von Scraping regelmäßig nicht die gesamte zugrunde liegende Funktion beseitigt. Vielmehr würden in der Regel lediglich die Methoden, mit denen auf die maßgeblichen Funktionen zugegriffen werden könne, beschränkt. Zur Bekämpfung von Scraping beschäftige die Beklagte ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren. Eine der Maßnahmen der Beklagten zur Verringerung von Scraping seien die implementierten Übertragungsbeschränkungen, die die Anzahl von Anfragen von bestimmten Daten reduzierten, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden könnten. Ferner gehe die Beklagte grundsätzlich mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper und Hosting-Anbieter, also Unternehmen, auf deren Systemen die Daten zur Verfügung gestellt werden, vor. Die Beklagte nutze auch Captcha-Abfragen.

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

Die Beklagte halte keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalte.

Die Beklagte ist der Auffassung,

die Klage sei unzulässig. Klageantrag zu 1 bis 3 seien nicht hinreichend bestimmt. Der Kläger mache einen Zahlungsantrag geltend, stütze das Begehren jedoch auf zwei zeitlich auseinander-

fallende angebliche Verstöße und damit auf unterschiedliche Lebenssachverhalte. Es bestehe kein Feststellungsinteresse, auch der Unterlassungsantrag sei nicht hinreichend bestimmt.

Verstöße der Beklagten gegen datenschutzrechtliche Vorschriften lägen nicht vor. Der Datensatz, über den im Zusammenhang mit dem Scraping-Sachverhalt berichtet worden sei, beruhe nicht auf einem Datenschutzverstoß. Die Daten seien weder durch Hacking noch infolge eines Fehlers oder Sicherheitsverstoßes im System der Beklagten, sondern durch das automatisierte, massenhafte Sammeln von ohnehin öffentlich einsehbaren und damit nicht vertraulichen Daten erlangt und an anderer Stelle zugänglich gemacht worden.

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

Die Beklagte sei mangels Verletzung des Schutzes personenbezogener Daten auch nicht verpflichtet gewesen, die Nutzer über den Scraping-Sachverhalt zu informieren.

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die zwischen den Parteien gewechselten Schriftsätze der Parteien nebst Anlagen sowie auf die Sitzungsniederschrift vom 03.02.2023 (Bl. 419 ff. d.A.) Bezug genommen.

Entscheidungsgründe

Die zulässige Klage hat in dem aus dem Tenor ersichtlichen Umfang Erfolg; im Übrigen ist sie unbegründet.

I.

Die Klage ist zulässig.

1.

Klageantrag zu 1 ist - entgegen der Auffassung der Beklagten - hinreichend bestimmt im Sinne

des § 253 Abs. 2 Nr. 2 ZPO.

Grundsätzlich kann eine hinreichende Bestimmtheit des Antrags im Sinne des § 253 Abs. 2 Nr. 2 ZPO angenommen werden, wenn er den Anspruch konkret bezeichnet, den Rahmen der gerichtlichen Entscheidungsbefugnis erkennbar abgrenzt, den Inhalt und Umfang der materiellen Rechtskraft erkennen lässt, das Risiko des Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und wenn er die Zwangsvollstreckung aus dem beantragten Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 21. November 2017 - II ZR 180/15 -, juris, Rn. 8 m.w.N.). Der Klageantrag ist dabei der Auslegung zugänglich, wobei auch die Klagebegründung heranzuziehen ist (Zöller/Greger, ZPO, 33. Auflage 2022, § 253 Rn. 13 m.w.N.).

Aus Klageschrift ergibt sich vorliegend, dass der Zahlungsantrag in Klageantrag zu 1 sich auf einen zusammenhängenden, wenngleich über einen längeren Zeitraum erstreckenden, aber in sich abgeschlossenen Lebenssachverhalt stützt (LG Gießen, GRUR-RS 2022, 30480; LG Paderborn, GRUR-RS 2022, 39349). Von der Anmeldung des Klägers auf der Plattform der Beklagten bis zum Abgriff einiger persönlicher Daten des Klägers bzw. der möglicherweise nicht ausreichenden Benachrichtigung der Nutzer. Der Klageschrift lässt sich überdies entnehmen, dass der Schaden aufgrund eines kumulativen Zusammenwirkens der gerügten Datenschutzverstöße geltend gemacht wird, die Bezifferung des Schadens dabei indes in zulässiger Weise in das Ermessen des Gerichts gestellt wird (LG Paderborn, a.a.O.).

2.

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

Gemessen an vorstehenden Erwägungen genügt auch der Klageantrag zu 2 dem vorbenannten Bestimmtheitserfordernis des § 253 Abs. 2 Nr. 2 ZPO. Denn Klageantrag zu 2 lässt sich hinreichend bestimmt entnehmen, dass der Kläger festgestellt wissen will, dass die Beklagte verpflichtet ist, dem Kläger sämtliche künftige Schäden zu ersetzen, die dem Kläger aufgrund der missbräuchlichen Datenabgreifung entstanden sind bzw. noch entstehen werden (LG Paderborn, a.a.O.). Unter Berücksichtigung der Replik des Klägers lässt sich Klageantrag zu 2 zudem so auslegen, dass der Kläger lediglich den Ersatz künftiger materieller Schäden begehrt.

Auch das gemäß § 256 Abs. 1 ZPO erforderliche Feststellungsinteresse ist gegeben. Der Kläger

hat die Möglichkeit des Eintritts zukünftiger materieller Schäden hinreichend dargelegt. Denn das Feststellungsinteresse nach § 256 Abs. 1 ZPO liegt bei einer Verletzung eines absoluten Rechts oder eines vergleichbaren Rechtsguts bereits dann vor, wenn künftige Schadensfolgen möglich sind, auch wenn der Eintritt eines Schadens noch ungewiss ist. Dies wäre nur dann nicht der Fall, wenn aus Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (a.a.O.). Unter Berücksichtigung des Umstandes, dass die personenbezogenen Daten im Wege des Scrapings erlangt worden sind, erscheint es bei lebensnaher Betrachtung möglich, dass es bei dem Kläger zu künftigen materiellen Schäden, etwa durch betrügerische Anrufe, kommt. Dem Feststellungsinteresse steht bezogen auf bereits entstandene, dem Kläger aber noch nicht bekannte materielle Schäden auch nicht der Vorrang der Leistungsklage entgegen.

3.

Auch die Klageanträge zu 3a und 3b sind zulässig, insbesondere hinreichend bestimmt.

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

Zwar darf ein Unterlassungsantrag nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Absatz 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt. Doch ist eine auslegungsbedürftige Antragsformulierung dann hinzunehmen, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zu Gewährleistung eines effektiven Rechtsschutzes erforderlich ist (BGH GRUR 2017, 422).

Nach diesen Maßstäben ist auch Klageantrag zu 3a hinreichend bestimmt. Selbst bei einer Benennung derzeitiger möglicher Sicherheitsmaßnahmen würde dies in Anbetracht der technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen. Zudem wird aus der Klagebegründung deutlich, dass der Kläger Sicherheitsstandards verlangt, die möglichen (weiteren) Scraping-Angriffen vorbeugen. Die gesetzlich vorgeschriebenen Sicherheitsstandards

einzurichten ist jedoch zuvorderst die Aufgabe der Beklagten. Insoweit kann diese nicht von ihren Nutzern die konkrete Benennung der Sicherheitsmaßnahmen verlangen (vgl. hierzu LG Paderborn a.a.O.; LG Gießen a.a.O.; LG Bielefeld GRUR-RS 2022, 38375).

II.

Die Klage ist teilweise begründet.

1.

Dem Kläger steht gegen die Beklagte ein Anspruch auf Schadensersatz i.H.v. 500,00 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 oder den Auftragsverarbeiter.

a.

Die Beklagte hat als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO gegen mehrere Vorschriften aus der Datenschutzgrundverordnung verstoßen.

Im Einzelnen:

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

Gemäß Art. 13 DSGVO hat der Verantwortliche eines Datenverarbeitungsprozesses gegenüber dem Betroffenen, dessen personenbezogene Daten verarbeitet und bei diesem erhoben werden, umfangreiche Informations- und Aufklärungspflichten zu erfüllen. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen diese Informations- und Aufklärungspflichten bereits mit der Erhebung personenbezogener Daten. Teilt der Verantwortliche dem Betroffenen bereits bei Datenerhebung die in Art. 13 Abs. 1 und Abs. 2 DSGVO vorgesehenen Informationen nicht vollständig oder inhaltlich unrichtig mit, verletzt er seine Informationspflichten. Nach Art. 13 Abs. 1 lit. c) DSGVO besteht eine Informationspflicht insbesondere dahingehend, dass der Verantwortliche dem Betroffenen die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die

Verarbeitung mitteilt. Sinn und Zweck dieser Regelung ist, dass der Betroffene eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges, sondern darüber hinaus auch über die Zwecke der Verarbeitung unterrichtet wird (Ehmann/Selmayr/Knyrim, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1).

Gemessen hieran hat die Beklagte den Kläger bei Datenerhebung zwar hinreichend darüber aufgeklärt, dass dessen Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“, zu Werbezwecken sowie zum Zweck der Kommunikation mit Facebook verwendet wird. Denn die Information auf der Oberfläche „Handy-Einstellungen“ ist für einen Benutzer hinreichend verständlich und mit den Grundsätzen einer fairen und transparenten Verarbeitung von personenbezogenen Daten vereinbar (LG Paderborn a.a.O.). Auch kann eine Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO nicht schon darin gesehen werden, dass seitens der Beklagten kein Hinweis bei Erhebung der Daten der Mobilfunknummer des Klägers erfolgt ist, dass bei der voreingestellt für „Alle“ freigegebenen Mobilfunknummer die Möglichkeit einer missbräuchlichen Datenabgreifung besteht. Denn es besteht schon nicht eine dahingehende Informations- und Aufklärungspflicht auf Seiten der Beklagten. Diese Möglichkeit ist der Risikosphäre der betroffenen Person zuzuordnen, da dem Risiko einer missbräuchlichen Verwendung von persönlichen Daten zwangsläufig jede Person ausgesetzt ist, die ihre persönlichen Daten im Internet preisgibt bzw. diese in sozialen Netzwerken teilt (LG Paderborn a.a.O.).

Doch hat die Beklagte den Kläger bei Datenerhebung nicht hinreichend über die beabsichtigte Verwendung seiner Mobilfunknummer für das CIT informiert und aufgeklärt nach Art. 13 Abs. 1 lit. c) DSGVO. Durch die Verwendung des CIT ermöglicht die Beklagte einem Benutzer den Abgleich, der in seinem Smartphone gespeicherten Personenkontakte mit auf Facebook registrierten Benutzerprofilen, die ihr Benutzerprofil jeweils mit einer Mobilfunknummer verknüpft haben. Durch die Eingabe einer beliebigen Mobilfunknummer wird dem Benutzer ermöglicht, das mit der Mobilfunknummer verknüpfte Benutzerprofil als „Freunde“ hinzuzufügen. Weder der in der Anlage B9 vorgelegten Datenrichtlinie noch der Rubrik „Handy-Einstellungen“ sowie der Unterverlinkung durch einen Klick auf „Mehr dazu“ lässt sich eine Aufklärung über das von der Beklagte verwendete CIT entnehmen. Der mit der Anlage B9 überreichten Datenrichtlinie lässt sich auf den Seiten 3 und 4 unter der Überschrift „Wie verwenden wir diese Informationen?“ entnehmen, dass die von einem Benutzer bereitgestellten Informationen zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommuni-

kation mit dem die Informationen bereitstellenden Benutzer, zum Anzeigen und Messen von Werbeanzeigen und Diensten sowie zur Förderung der Sicherheit verwendet werden. Ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT erfolgt nicht. Auch den Hinweisen auf den Seiten 5 und 6 der Datenrichtlinie unter der Überschrift „Wie werden diese Informationen geteilt?“ lässt sich ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT nicht entnehmen. Auch der Rubrik „Handy-Einstellungen“ sowie der Unterverlinkung durch einen Klick auf „Mehr dazu“ ist keine Aufklärung über das durch die Beklagte verwendete CIT zu entnehmen. Dort findet sich zwar eine Aufklärung über die Verwendung der Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“ und ein Hinweis darauf, dass durch das Hinzufügen der Mobilfunknummer eben diese mit dem Benutzerkonto verknüpft ist und der jeweilige Benutzer festlegen kann, welche Personen dessen Mobilfunknummer sehen können und welche Personen auf Facebook nach der betroffenen Person suchen können. Ein weitergehender Hinweis, dass die betroffene Person durch das CIT der Beklagten im Wege eines Kontaktabgleichs durch Eingabe einer Mobilfunknummer gefunden werden kann, lässt sich den Einstellungen aber gerade nicht entnehmen. Auch den vorgelegten Anlagen B5 und B6 lässt sich kein Hinweis auf die Verwendung des CIT entnehmen.

Die Verletzung der nach Art. 13 DSGVO bestehenden Informations- und Aufklärungspflichten ist auch vom Anwendungsbereich des Schadensersatzanspruches des Art. 82 DSGVO erfasst. Ein Schadensersatzanspruch nach Art. 82 DSGVO kann nur dann begründet werden, wenn nach dessen Absatz 2 Satz 1 ein Schaden durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen die Informations- und Aufklärungspflichten des Art. 13 DSGVO bereits mit der Erhebung personenbezogener Daten. Bereits zu diesem Zeitpunkt hat der Verantwortliche gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen. Bildet - wie hier - die Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a) DSGVO die Grundlage des Datenerhebungs- und somit auch des Datenverarbeitungsvorganges, kann eine solche Einwilligung unter Berücksichtigung der in der DSGVO vorherrschenden Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten keinen Bestand haben, wenn dem Betroffenen nicht bereits bei Datenerhebung sämtliche nach Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden (LG Paderborn a.a.O.).

(1.2) Zudem hat die Beklagte als Verantwortliche aufgrund unzureichender Sicherheitsmaßnahmen bezüglich der Nutzung des CIT auch gegen Art. 32, 24, 5 Abs. 1 f) DSGVO verstoßen.

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

Diesen Anforderungen genügten die beklagenseits behaupteten Schutzmaßnahmen nicht. Dabei wird nicht verkannt, dass Art. 32 Abs. 1 DSGVO den Verantwortlichen und Auftragsverarbeiter nicht zu einem absoluten Schutz(niveau) der Daten verpflichtet, sondern das Schutzniveau vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein muss. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist. Doch sind die von der Beklagten behaupteten „Anti-Scraping-Maßnahmen“ selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO. Beim Zugang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34). So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf Facebook, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum Facebook-Profil, bei dem diese angegeben wurde, ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Facebook-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden (LG Paderborn a.a.O.). Die-

ses zu berücksichtigende Risiko führt dazu, dass der Maßstab für die Bestimmung der Angemessenheit des Schutzniveaus entsprechend hoch anzusetzen ist. Dies begründet sich unter anderem daraus, dass das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagten darstellt. Auch handelt es sich bei den Daten nicht um ohnehin öffentlich einsehbare Daten. Vielmehr wird Dritten ein Zugang zu diesen, insbesondere der Telefonnummer des Nutzers, gewährt. Es erfolgt eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren Daten des Nutzers auf der Facebook-Plattform der Beklagten. Die Gefahr einer Veröffentlichung aller zusammengetragenen Daten, darunter insbesondere die Verknüpfung von Telefonnummer und Name, ist, wie der vorliegende Datenscraping-Fall aufzeigt, besonders hoch. „Scraping“ ist weit verbreitet und entsprechende Versuche bei dem weltweit genutzten sozialen Netzwerk der Beklagten auch aus einer ex-ante-Sicht zu erwarten gewesen, was auch der Beklagten - wie sich der Anlage B10 entnehmen lässt - bekannt war (LG Paderborn a.a.O.). Soweit die Beklagte ausführt, dass sie gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorgehe, kommen diese Maßnahmen erst dann zu tragen, wenn ein Datenscraping tatsächlich eingetreten ist. Die Daten sind in diesem Stadium bereits entwendet worden. Eine Veröffentlichung oder anderweitiger Missbrauch kann in diesem Stadium praktisch nicht mehr verhindert werden. Die von Beklagtenseite behauptete teilweise Einschränkung des CIT wurde erst nach dem streitgegenständlichen Vorfall eingeführt. Auch die Beschäftigung eines Teams von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie CAPTCHA-Abfragen genügen den Anforderungen des Art. 32 DSGVO im vorliegenden Fall allein nicht (LG Paderborn a.a.O.). Die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den - aus ihrer Sicht im hiesigen Verfahren ausreichenden - Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Datenscraping kommen konnte. Wegen des hohen Risikopotenzials, das von einem Missbrauch des CIT ausgeht, waren weitergehende Maßnahmen für ein angemessenes Schutzniveau erforderlich, die beispielsweise so hätten ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind.

Der Verstoß gegen Art. 32 DSGVO ist auch vom Anwendungsbereich des Schadensersatzanspruches des Art. 82 DSGVO erfasst (Sydow/Marsch DS-GVO/BDSG/Mantz, 3. Aufl. 2022, DS GVO Art. 32 Rn. 31).

(1.3) Zudem hat die Beklagte gegen Art. 33 DSGVO verstoßen.

Gemäß Art. 33 Abs. 1 DSGVO meldet der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der gemäß Art. 55 DSGVO zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Der Mindestinhalt der Meldung ist in Art. 33 Abs. 3 DSGVO festgelegt.

Dem ist die Beklagte vorliegend nicht nachgekommen. Sie hat die zuständige Aufsichtsbehörde unstreitig nicht über den „Scraping“-Vorfall informiert.

Auch ist eine Verletzung des Schutzes personenbezogener Daten gegeben. Nach der Begriffsbestimmung in Art. 4 Nr. 12 DSGVO fällt darunter eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Erfasst ist damit im weitesten Sinn jede objektive Schutzverletzung, unabhängig davon, ob diese beabsichtigt war oder nicht, wie etwa Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 33 Rn. 5; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 33 Rn. 6 m.w.N.). Eine Verletzung liegt auch dann vor, wenn im Rahmen bestehender Zugriffsrechte Daten zweckentfremdet werden (Spindler/Schuster/Laue, DS-GVO Art. 33 Rn. 7). Solch eine Zweckentfremdung ist vorliegend unabhängig davon, dass Name, Nutzer-ID und Geschlecht des Klägers aufgrund seiner Privatsphäre-Einstellungen öffentlich waren und die Handynummer durch die freizugängliche Nutzung des CIT-Tools mit diesen Daten verknüpft werden konnte, vor dem Hintergrund des massenhaften „Scrapings“ gegeben. Der „Scraping“-Vorfall ist allein aufgrund seines Ausmaßes mit Datenpannen, -lecks, Hackerangriffe oder Datendiebstahl gleichzusetzen. Dies zeigt sich auch darin, dass ein solches Vorgehen nach den Nutzungsbedingungen untersagt ist und - so behauptet jedenfalls die Beklagte selbst - Sicherheitsmaßnahmen gegen derartige Vorfälle geschaffen wurden (LG Paderborn a.a.O.).

Eine Einschränkung der Meldepflicht nach Art. 33 Abs. 1 DSGVO ist nicht gegeben. Es ist nicht vorzusehen, dass die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten des Klägers führt. Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht gemäß Erwägungsgrund 85, wenn ihnen der

Verlust der Kontrolle über ihre Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen (BeckOK DatenschutzR/Brink, 42. Ed. 1.2.2022, DS-GVO Art. 33 Rn. 35). Ein solcher Kontrollverlust ist bereits eingetreten.

Der Verstoß gegen Art. 33 DSGVO, der auch dem Schutz des Betroffenen dient, ist auch geeignet eine Schadensersatzpflicht gemäß Art. 82 DSGVO zu begründen (Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 33 Rn. 24; Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 33 Rn. 27).

(1.4) Die Beklagte hat zudem auch gegen Art. 34 DSGVO verstoßen, da sie den Kläger nicht über den Scraping-Vorfall informiert hat.

Da die Beklagte keine geeigneten Sicherheitsvorkehrungen getroffen hat (s.o.), war eine Benachrichtigung auch nicht entbehrlich nach Art. 34 Abs. 3 a) DSGVO. Auch nach Art. 34 Abs. 3 c) DSGVO war die Benachrichtigung nicht entbehrlich. Zwar kann sich aus einer Vielzahl an betroffenen Personen - wie vorliegend - ein unverhältnismäßiger Zeit- bzw. Kostenaufwand ergeben. Allerdings kann von einem unverhältnismäßigen Aufwand nicht ausgegangen werden, wenn die betroffenen Personen bekannt sind und deren E-Mailadressen vorliegen. Im Übrigen setzt die öffentliche Bekanntmachung voraus, dass die Betroffenen vergleichbar wirksam informiert werden. Ob eine Publikation des Vorfalls auf der eigenen Homepage ausreicht, hängt davon ab, inwiefern der Internetauftritt vom betroffenen Personenkreis regelmäßig besucht wird. Jedenfalls darf die Bekanntmachung des Vorfalls auf der Website nicht versteckt werden. Es bedarf eines an herausragender Stelle platzierten Banners bzw. einer entsprechend deutlichen Meldung. Gegebenenfalls muss die Information sowohl über digitale, als auch über analoge Kanäle erfolgen. Demnach ist die ausschließliche Benachrichtigung durch eine Pressemitteilung oder in einem Unternehmensblog kein wirksames Mittel, um die betroffenen Personen von einer Datenschutzverletzung in Kenntnis zu setzen (LG Paderborn a.a.O.).

Vorliegend waren der Beklagten die betroffenen Personen und deren E-Mailadressen bekannt, so dass schon nicht von einem unverhältnismäßigen Aufwand in Bezug auf eine individuelle Benachrichtigung auszugehen ist. Die Mitteilung am 06.04.2021 in dem Artikel „Die Fakten zu Medienberichten über Facebook-Daten“ erfolgte weder rechtzeitig, noch auf einem probaten Weg, um den Anforderungen an eine öffentliche Bekanntmachung zu genü-

gen. Das Schreiben vom 23.08.2021 (Anlage K2) versandte die Beklagte jedenfalls nicht rechtzeitig.

(1.5) Da sich aus einem Verstoß gegen Art. 25 DSGVO wegen seines organisatorischen Charakters ein Anspruch auf Schadensersatz nach Art. 82 DSGVO nicht begründen lässt (Kühling/Buchner/Hartung, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 31; Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DS-GVO Art. 25 Rn. 25), kann dahinstehen, ob zudem noch ein Verstoß der Beklagten gegen Art. 25 DSGVO vorliegt.

b.

Die Beklagte kann sich auch nicht gemäß Art. 82 Abs. 3 DSGVO exkulpieren.

Danach wird der Verantwortliche von der Haftung nach Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Unabhängig davon, ob man den Begriff der Verantwortlichkeit mit Teilen der Rechtsprechung und der Literatur mit dem Begriff des Verschuldens gleichgesetzt (OLG Stuttgart, Urteil vom 31. März 2021 – 9 U 34/21 –, juris) oder Art. 82 DSGVO als Gefährdungshaftungstatbestand versteht (Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 19 ff.), kann die Beklagte sich vorliegend nicht entlasten. Denn der Beklagten gelingt weder der Nachweis fehlenden Verschuldens noch des Vorliegens ganz ungewöhnlicher Kausalverläufe, eines Falles höherer Gewalt oder weit überwiegenden eigenen Fehlverhaltens des Klägers.

Die Beklagte kann nicht nachweisen, dass sie kein Verschulden trifft. Das wäre nämlich nur dann der Fall, wenn sie sämtliche Sorgfaltsanforderungen erfüllt hätte und ihr nicht die geringste Fahrlässigkeit vorzuwerfen wäre (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54). Hält der Anspruchsgegner etwa sämtliche erforderlichen Sicherheitsmaßnahmen (Art. 32 DSGVO) ein und kommt es dennoch zu einem unbefugten Datenzugriff, fehlt es an einem Verschulden. War der Angriffsweg dagegen bekannt oder auch nur erkennbar, ist der Entlastungsbeweis nicht geführt (a.a.O.). Da vorliegend die nach Art. 32 DSGVO erforderlichen Sicherheitsmaßnahmen von der Beklagten nicht eingehalten wurden (s.o.), kann die Beklagte nicht nachweisen, dass sie kein Verschulden trifft.

c.

Dem Kläger ist auch ein kausaler immaterieller Schaden im Sinne des Art. 82 DSGVO entstanden.

(1.1) Die gemäß den vorstehenden Ausführungen festgestellten Gesetzesverletzungen sind auch kausal für den beim Kläger entstandenen Schaden.

Die Verletzung der Informations- und Aufklärungspflichten des Art. 13 Abs. 1 lit. c) DSGVO ist kausal für den bei dem Kläger entstandenen Schaden. Gemäß vorstehender Erwägungen hat die Beklagte den Kläger bereits bei Erhebung seiner Mobilfunknummer nur unzureichend über die Verwendung seiner Mobilfunknummer im Hinblick auf das CIT aufgeklärt, sodass bezogen auf die Mobilfunknummer eine rechtswidrige Verarbeitung vorliegt. Diese ist auch kausal für den beim Kläger entstandenen Schaden, da es durch die Verwendung des CIT zu einem Kontrollverlust auf Seiten des Klägers kam (LG Paderborn a.a.O.).

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

Der Schaden beruht zudem kausal auf einem Verstoß gegen Art. 33 und Art. 34 DSGVO. Zwar ist der geltend gemachte Kontrollverlust bereits durch das „Scraping“ der Daten erstmals eingetreten. Durch die unterlassene Benachrichtigung des Klägers wurde ihm jedoch die Möglichkeit genommen, geeignete Maßnahmen zu ergreifen, um das Risiko des Missbrauchs seiner Daten zu minimieren. Auch die zuständige Datenschutzbehörde konnte mangels rechtzeitiger Meldung keine Schritte zur Risikominimierung und Absicherung der Daten einleiten (a.a.O.).

(1.2) Auch ein Schaden ist gegeben. Zwar genügt ein bloßer Datenschutzverstoß als solcher nicht für das Entstehen des Schadensersatzanspruches (OLG Frankfurt GRUR 2022, 1252). Der Begriff des Schadens ist nach dem Erwägungsgrund 146 S. 3 im Lichte der Rechtsprechung des Europäischen Gerichtshofs allerdings weit und auf eine Art und Weise auszulegen, die den Zielen der Verordnung in vollem Umfang entspricht. Die Ziele der DSGVO bestehen dabei u.a. darin, den Risiken für die Rechte und Freiheit natürlicher Perso-

nen zu begegnen, die - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - aus einer Verarbeitung personenbezogener Daten hervorgehen und zu einem immateriellen Schaden führen können (LG Paderborn a.a.O.). In den Erwägungsgründen 75 und 85 wird der Kontrollverlust über die personenbezogenen Daten als ein Beispiel für das Vorliegen eines solchen Schadens aufgeführt (a.a.O.). Ein derartiger Kontrollverlust ist aus Sicht des Klägers eingetreten, da jedenfalls seine Telefonnummer, Nutzer-ID, sein Name und Geschlecht gescraped wurden. Unerheblich ist dabei, dass der Name, das Geschlecht und die Nutzer-ID nach den Nutzereinstellungen des Klägers öffentlich waren. Denn jedenfalls die Verknüpfung mit seiner Telefonnummer war bis dahin nicht hergestellt. Dabei handelt es sich vorliegend auch nicht um einen bloßen Bagatellschaden. Denn durch das Scrapen der klägerischen Daten ist grundsätzlich die Weiterverarbeitung durch einen unbegrenzten und unbestimmten Personenkreis, insbesondere auch für den gezielten Missbrauch etwa in Form von Betrugsanrufen, ermöglicht.

Dabei hält die erkennende Einzelrichterin im vorliegenden Einzelfall ein Schmerzensgeld in Höhe von 500 EUR angemessen, aber auch ausreichend, um einerseits der Ausgleichs- und Genugtuungsfunktion zu genügen, und andererseits der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung zu tragen. Vorliegend war zu berücksichtigen, dass sich die Beklagte mehrere Verstöße gegen die DSGVO vorwerfen lassen muss (s.o.), die einen sehr weitgehenden Kontrollverlust der personenbezogenen Daten des Klägers ermöglicht und begünstigt haben. Da jedoch - auch im Rahmen der informativischen Anhörung - keine besondere persönliche Betroffenheit des Klägers festgestellt werden konnte, sind 500 EUR auch ausreichend.

2.

Auch der mit dem Klageantrag zu 2 geltend gemachte Feststellungsantrag ist begründet. Gemäß vorstehender Ausführungen hat der Kläger gegenüber der Beklagten wegen Verletzung der DSGVO einen Anspruch auf Schadensersatz nach Art. 82 DSGVO. Die jeweiligen Gesetzesverletzungen sind - wie bereits erörtert - zudem kausal für den unkontrollierten Datenverlust des Klägers.

3.

Der Kläger kann gemäß Art. 17 DSGVO von der Beklagten auch die mit dem Antrag zu 3a) verlangte Unterlassung verlangen. Im Übrigen ist der begehrte Unterlassungsanspruch jedoch unbegründet.

a.

Der Kläger kann von der Beklagten die Unterlassung verlangen, seine personenbezogenen Daten unbefugten Dritten zugänglich zu machen, ohne dabei die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen.

Zwar sieht Art. 17 DSGVO i.V.m. Art. 6 DSGVO ein Recht auf Löschung und nicht auf Unterlassung vor, doch lässt sich aus dem in Art. 17 Abs. 1 DSGVO normierten Recht betroffener Personen, unter gewissen Umständen vom Verantwortlichen zu verlangen, sie betreffende personenbezogene Daten unverzüglich zu löschen, auch ein Anspruch auf Unterlassung ihrer Verarbeitung für die Zukunft ableiten (LG Frankfurt/M., Urteil vom 28.6.2019 – 2-03 O 315/17; BGH NJW 2022, 1098).

Die Beklagte hat gegen die DSGVO verstoßen (s.o.), indem sie u.a. ein nicht ausreichendes Sicherheitsniveau vorgehalten und damit unbefugten Dritten den Zugriff auf die personenbezogenen Daten des Klägers ermöglicht hat. Das Zugänglichmachen personenbezogener Daten stellt auch eine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO dar. Der Regelungsgehalt der Vorschrift ist weit gefasst und umfasst auch den Umgang mit personenbezogenen Daten unter dem Einsatz von Datenverarbeitungssystemen und deren Speicherung. Dies war auch unrechtmäßig, da eine entsprechende Rechtsgrundlage dafür nicht gegeben war (LG Paderborn, a.a.O.). Durch die Beeinträchtigung besteht eine tatsächliche Vermutung für die Wiederholungsgefahr, die die Beklagte nicht widerlegt hat.

b.

Dem Kläger steht jedoch gegen die Beklagte kein Anspruch zu, eine Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise des CIT und der Verwendung von Telefonnummern zu unterlassen.

Denn die Pflichtverletzung der Beklagten nach der DSGVO löst für die Zukunft keine Folgen mehr

aus, da der Kläger zumindest im Verlauf des Rechtsstreits sämtliche Informationen erhalten hat, die die fragliche Art und Weise der Datenverarbeitung betreffen (so auch LG Paderborn a.a.O.).

4.

Dem Kläger steht auch der mit Klageantrag zu 4 verfolgte Auskunftsanspruch nach Art. 15 DSGVO nicht zu, weil dieser durch den außergerichtlichen Schriftsatz der Beklagten vom 23.08.2021 bereits erfüllt wurde. Mit Schreiben vom 23.08.2021 hat die Beklagte in angemessener Weise mitgeteilt, welche personenbezogenen Daten verarbeitet werden, indem sie den Kläger auf die Selbstbedienungstools verwiesen hat. Weitergehende Auskunft kann der Kläger nicht verlangen. Ihm ist nämlich einerseits bekannt, welche Daten durch den Scraping-Vorfall erlangt wurden und zum anderen hat die Beklagte mehrfach versichert keine „Rohdaten“ des Scraping-Vorfalles zu halten.

5.

Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gemäß Art. 82 Abs. 1 DSGVO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche erforderlich und notwendig. Ausgehend von einem Wert des berechtigten Verlangens des Klägers von 3.000 EUR zum Zeitpunkt der außergerichtlichen Tätigkeit ergibt dies Kosten in Höhe von 367,23 EUR (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV RVG zzgl. 19% MwSt.).

III.

Die Kostenentscheidung beruht auf § 92 Abs. 1 Satz 1 ZPO; die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 11, 711, 709 ZPO.

Fetzer
Richterin am Landgericht