Aktenzeichen:
4 O 380/22

Landgericht Ulm

Im Namen des Volkes

Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde, Beuger, Solmecke**, Kaiser-Wilhelm-Ring 27 - 29, 50672 Köln, Gz.: [redacted]

gegen

Meta Platform Ireland Limited (zuvor Facebook Ireland Ltd.), vertreten durch d. Geschäftsführer, 4 Grand Canal Square, Dublin 2, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater Partnergesellschaft mbB**, Bockenheimer Anlage 44, 60322 Frankfurt, Gz.: [redacted]

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung (nachfolgend: DSGVO)

hat das Landgericht Ulm - 4. Zivilkammer - durch die Richterin [redacted] als Einzelrichterin aufgrund der mündlichen Verhandlung vom 17.05.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 500,00 EUR immateriellen Schadensersatz nebst Zinsen seit 11.01.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu

zahlen.

2. 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, durch die Verknüpfung der Mobilfunknummer des Klägers mit seiner Facebook ID und/oder seinem Vor- und Nachnamen und/oder seinem Geschlecht 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.

   die Telefonnummer der Klägerseite durch Kontaktvorschläge für Dritte, welche diese Telefonnummer abfragen, mit dem Facebookprofil des Klägers zu verknüpfen, solange der Kläger hierzu nicht ausdrücklich einwilligt.

   b.

   bei Vorliegen einer Einwilligung des Klägers, die es der Beklagten erlaubt, Kontakte aufgrund eines Abgleichs mittels der Telefonnummer und des Facebookprofils vorzuschlagen, keine ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern.

4. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 367,23 EUR zu zahlen zuzüglich Zinsen seit 11.01.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits haben der Kläger 22 % und die Beklagte 78 % zu tragen.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich Ziff. 1, Ziff. 4 und wegen der Kosten nur gegen Sicherheitsleistung i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages, ansonsten hinsichtlich Ziff. 2 gegen Sicherheitsleistung i.H.v. 600,00 EUR und

hinsichtlich Ziff. 3 gegen Sicherheitsleistung i.H.v. 6.000,00 EUR. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung i.H.v. 110 Prozent des aufgrund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit i.H.v. 110 Prozent des jeweils zu vollstreckenden Betrages leistet.

Beschluss

Der Streitwert wird auf bis zu 7.000,00 EUR festgesetzt.

Tatbestand

Der Kläger macht Ansprüche gegen die Beklagte 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.

Bei der Eröffnung eines Facebook-Kontos müssen die Nutzer Informationen über sich angeben. Durch entsprechende Einstellungen des Facebook-Kontos können die Nutzer bestimmen, welche Informationen für welche Personenkreise einsehbar sind. Die Nutzer-ID, der Vor- und Nachname und das Geschlecht sind jedoch immer öffentlich einsehbar. Die Angabe der Handynummer ist nicht zwingend, der Kläger hinterlegte seine Handynummer jedoch in seinem Facebook-Konto.

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. Dem Nutzer ist es möglich, die standardmäßige Voreinstellung „öffentlich“ abzuändern und die einzelnen Informationen nur einem eingeschränkten Personenkreis wie „Freunde“ auf der Plattform, oder „Freunde von Freunden“ einsehen zulassen. Lediglich die Telefonnummer des Nutzers wird gesondert behandelt.

In den „Suchbarkeits-Einstellungen“ wird festgelegt, wer das Profil eines Nutzers durch die Telefonnummer finden kann. In der App für Mobiltelefone ist eine Software namens Contact-Import-Tool (CIT) integriert. Das CIT gleicht die bei Facebook hinterlegten Telefonnummern mit Telefonnummern ab, die bei einem Nutzer in seinem Smartphone als Kontakte gespeichert sind. Dann werden dem Nutzer die entsprechenden Facebook-Profile angeboten, die zu seinen im Smartphone abgespeicherten Telefonnummern passen. Der Nutzer kann dann diesen Profilen z.B. eine „Freundschaftsanfrage“ stellen. Maßgeblich für diese Funktion sind allein die Angaben unter der „Suchbarkeits-Einstellung“, nicht die der Zielgruppenauswahl. Demnach war es möglich, Nutzer anhand einer Telefonnummer zu finden, solange ihre „Suchbarkeits-Einstellung“ für Telefonnummern auf der Standard-Voreinstellung „Alle“ eingestellt war. Daneben waren die Einstellungen nur „Freunde von Freunden“ oder „Freunde“ auswählbar. Ab Mai 2019 stand Nutzern auch die Option „Nur ich“ zur Verfügung. Die Suchbarkeits-Einstellung des Klägers war vor 2019 und ist zum Schluss der mündlichen Verhandlung so eingestellt gewesen, dass durch das CIT ein Abgleich der Telefonnummer für „Alle“ Nutzer der Facebook-Plattform erfolgte.

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 „Hilfebereich“, der unmittelbar auf der Facebook Homepage verlinkt ist, Informationen über die Privatsphäre-Einstellungen zur Verfügung gestellt. Auf diese Einstellungen kann unter der Überschrift „Privatsphäre, Datenschutz und Sicherheit“ zugegriffen werden. Hinsichtlich der weiteren relevanten Inhalte im Hilfebereich und in den Einstellungen wird auf die Abbildungen in der Klageschrift sowie auf die Anlagen B1 bis B8 Bezug genommen.

Nach der Anmeldung konnten die Nutzer im Hilfebereich folgende Information zur Mobilfunknummer finden:

„*Möglicherweise verwenden wir deine Mobilnummer für diese Zwecke:*

Um dir bei der Anmeldung zu helfen: Wenn du dein Passwort oder deine E-Mail-Adresse vergessen hast, über die du dich bei Facebook anmeldest, kannst [du] diese erfragen, indem du die mit deinem Konto verbundene Mobilnummer eingibst.

Um dein Konto mit Opt-in Funktionen wie die zweistufige Authentifizierung oder SMS-Nachrichten bei Logins über unbekannte Geräte zu schützen.

Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst.

Beachte, dass du kontrollieren kannst, wer deine Telefonnummer sehen kann. Mehr dazu erfährst du in unserer Datenrichtlinie.“

Durch einen „Privatsphärencheck“ ermöglichte es die Beklagte den Nutzern die Einstellungen zu den persönlichen Daten aktiv zu überprüfen.

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.

Hierbei wurde die Funktion des CITs genutzt, indem durch systematische Eingaben von Zahlenabfolgen bzw. Telefonnummer (sogenannte „Telefonnummernaufzählung“) Nutzerprofile Telefonnummern zugeordnet werden konnten. So erhielten die „Scraper“ die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und konnten sie mit der Telefonnummer verbinden. Im Fall des Klägers erzeugten die „Scraper“ einen Datensatz, der jedenfalls seinen Vor- und Nachnamen, sein Geschlecht, das Land und seine Nutzer-ID beinhalte. Unklar ist, ob das Land möglicherweise nicht anhand des Nutzer-Profils, sondern auf andere Weise festgestellt wurde durch z.B. die Handynummer.

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“, in dem sie erläuterte, dass die Daten nicht durch einen Hackerangriff erlangt worden seien, sondern es sich um öffentlich einsehbare Informationen handele.

Die zuständige Datenschutzbehörde und auch der Kläger wurden von der Beklagten nicht über den Vorfall informiert.

Mit E-Mail vom 11.07.2022 forderte der Prozessbevollmächtigten des Klägers die Beklagte zur Schadensersatzzahlung i.H.v. 1.000,00 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).

Der Kläger trägt vor und ist der Auffassung,

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 personenbezogenen Daten des Klägers seien auf Internetseiten, die illegale Aktivitäten begünstigen sollen, wie das „Hacker-Forum “raidforums.com“ veröffentlicht worden. Folge sei ein Kontrollverlust der Daten des Klägers gewesen. Der Kläger empfange seit 2021 übermäßig viele „Fake-Anrufe“, Spam-SMS und Spam-E-Mails bei denen, unbekannte Dritte versuchen würden, durch Täuschungen ihm einen finanziellen Nachteil zuzufügen. Während er die Spam-Nachrichten per E-Mail oder SMS besser ignorieren könne, falle ihm dies bei der Telefonnummer besonders schwer. Bei Anrufen habe er immer die Sorge, dass es sich um etwas Wichtiges handeln könnte. Da er aufgrund der Häufigkeit der „Fake-Anrufe“ bei Anrufe ihm fremder Telefonnummern nicht mehr abhebe, habe er Angst, dass er wichtige Anrufe verpasse. So z.B., wenn seinen Eltern, welche bereits deutlich über 70 Jahre alt seien, etwas passiere. Die Sorge über den möglichen Missbrauch der ihn betreffenden Daten führe zu einem Zustand des Unwohlseins und Angst.

Die Beklagte habe die Einstellungen zu Sicherheit der Telefonnummer bewusst kompliziert und unübersichtlich gestaltet, sodass Nutzer nur unter großem Aufwand sichere Einstellungen überhaupt erreichen konnten. Durch den Aufbau der Einstellungen, insbesondere der getrennten Behandlung der Telefonnummer unter den Suchbarkeitseinstellungen, sei der Eindruck bei den Nutzern entstanden, dass die Telefonnummer nicht veröffentlicht werde. Genau dies habe die Beklagte jedoch durch die Implementierung der CIT-Software in ihrer App zugelassen.

Zudem habe die Beklagte keine hinreichenden Maßnahmen ergriffen, um Datenscraping zu verhindern. Der Beklagten sei es ohne Weiteres möglich gewesen, durch Abfragebegrenzungen oder sogenannten Captchaabfragen Datenscraping zu verhindern oder jedenfalls deutlich zu erschweren.

Außerdem wäre die Beklagte verpflichtet gewesen, den Kläger und die zuständige Aufsichtsbehörde über ihr Datenleck zu benachrichtigen.

Die Datenauskunft sei nicht vollständig erfolgt, da nicht mitgeteilt worden sei, wem die Daten des Klägers zur Verfügung gestellt worden seien.

Hätte der Kläger gewusst, dass seine Telefonnummer über das CIT auch von Dritten in Erfahrung gebracht werden könne, hätte er die Zustimmung zur Nutzung der Telefonnummer nicht er-

teilt.

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 1.000,00 EUR nebst Zinsen seit 11.01.2023 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 Informationen durch die Beklagte unvollständigen 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 EUR zu zahlen zuzüglich Zinsen seit 11.01.2023 in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte trägt vor und ist der Auffassung,

alle Daten, die durch Scraping bei der Beklagten erlangt wurden, seien Daten, die auf dem Facebook-Konto als öffentliche Nutzerinformationen abrufbar gewesen seien, oder es handele sich um Daten, die aufgrund der jeweiligen Zielgruppenauswahl öffentlich einsehbar gewesen seien. Der Missbrauch der klägerischen Daten werde mit Nichtwissen bestritten.

Kern der Facebook-Plattform sei es, den verschiedenen Nutzern zu ermöglichen, miteinander in Kontakt zutreten bzw. eine Kontaktierung untereinander zu erleichtern. Das vollständige Verhindern von Scraping sei unmöglich, da sonst der Zweck der Facebook-Plattform nicht mehr erreicht werden könne. Die Beklagte versuche jedoch einen möglichen Missbrauch mit entsprechenden Sicherheitsmaßnahmen zu verhindern. Hierfür stehe ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Verfügung. 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.

Die Einstellungen und Hinweise zur Privatsphäre auf der Facebook-Plattform seien übersichtlich und klar. Jedem Nutzer werde es ermöglicht, seine Daten hinreichend zu schützen.

Die Beklagte besitze keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten

enthalte.

Verstöße der Beklagten gegen datenschutzrechtliche Vorschriften lägen nicht vor, weshalb keine Informationspflicht gegenüber dem Kläger oder der Aufsichtsbehörde bestanden habe.

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 17.05.2023 (Bl. 269 ff. d.A.) Bezug genommen

Entscheidungsgründe

Die zulässige Klage (**A.**) hat in dem aus dem Tenor ersichtlichen Umfang Erfolg; im Übrigen ist sie unbegründet (**B.**).

A.

Das Landgericht Ulm ist für die Klage örtlich und international gemäß Art. 18 Abs. 1 2. Alt EuGVVO sowie sachlich gemäß § 71 GVG i.V.m. § 23 Nr. 1 GVG zuständig. Der Klageantrag Ziffer 1 ist hinreichend bestimmt und daher zulässig (I.). Der Klageantrag Ziffer 2 ist nur zulässig, soweit er sich auf künftige materielle Schäden bezieht (II.). Die Klageanträge Ziffer 3a und 3b sind zulässig, da sie nach entsprechender Auslegung jedenfalls hinreichend bestimmbar sind (III.).

I.

Klageantrag Ziffer 1 ist gemäß § 253 Abs. 2 Nr. 2 ZPO hinreichend bestimmt.

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 der Klageschrift ergibt sich eindeutig, dass die Klägerseite ihren Anspruch auf den Scraping-Vorfall aus dem Jahr 2019 stützt, bei dem es zu einem Kontrollverlust der persönlichen Daten des Klägers gekommen sein soll. Insbesondere die Verbindung der Telefonnummer des Klägers mit seinem Facebook-Konto bzw. den dort abrufbaren Informationen ist Gegenstand der Klage. Die Klägerseite stützt ihren Schadensersatzanspruch zwar auf mehrere datenschutzrechtliche Verstöße, wie z.B. die fehlende Mitteilung an den Kläger oder der Aufsichtsbehörde, der Kernsachverhalt ist jedoch eindeutig bestimmbar und abgeschlossen. Aus der 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). 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.).

II.

Der Klageantrag Ziffer 2 ist zulässig, soweit er die Feststellung einer Einstandspflicht der Beklagtenseite für künftige materielle Schäden betrifft. Der Klageantrag war entsprechend auszulegen.

Die Auslegung darf auch im Prozessrecht nicht am buchstäblichen Sinn des Ausdrucks haften, sondern hat den wirklichen Willen der Partei zu erforschen. Bei der Auslegung von Prozesserklärungen ist der Grundsatz zu beachten, dass im Zweifel dasjenige gewollt ist, was nach den Maßstäben der Rechtsordnung vernünftig ist und der wohlverstandenen Interessenlage entspricht (BGH, Urteil vom 16. Mai 2017 – XI ZR 586/15 –, Rn. 11, juris)

Die Formulierung des Klageantrags Ziffer 2 ... *„alle künftigen Schäden“*... *„entstanden sind und/oder noch entstehen werden.“* ist widersprüchlich, da unklar ist, ob der Feststellungsantrag sich nur auf künftige Schäden beziehen soll, oder auch eine allgemeine Feststellung für entstandene Schäden beinhaltet. Die Beklagte hat in der Klageerwiderung vom 18.04.2023 (Bl. 113 d. eA.) hierauf hingewiesen. In der Replik vom 09.05.2023 (Bl. 237 d. eA.) stellte die Klägerseite klar,

dass sie nur eine Feststellung für künftige Schäden begehre. Der Klageantrag Ziffer 2 ist im Zuge der sachgerechten Auslegung dahingehend zu verstehen, dass nur die Feststellung einer Erstattungspflicht für künftige Schäden begehrt wird.

Mit dem auf eine unbeschränkte Klage insgesamt zuerkennenden Schmerzensgeld sind nicht nur alle bereits eingetretenen, sondern auch alle erkennbaren und objektiv vorhersehbaren künftigen unfallbedingten Verletzungsfolgen abgegolten (BGH, Urteil vom 20. Januar 2004 – VI ZR 70/03 –, Rn. 9, juris).

Im Klageantrag Ziffer 1 wird ein unbegrenzter Schmerzensgeldanspruch gelten gemacht, sodass sich die künftigen Schäden im Klageantrag Ziffer 2, nach sachgerechter Auslegung, nur auf materielle Schäden beziehen können. Auch die Formulierung „unbefugt“ erscheint für sich genommen wenig präzise, konnte jedoch im Zuge der Auslegung genauer bestimmt werden und war mit den entsprechenden Ergänzungen zulässig.

III.

Auch die Klageanträge Ziffer 3a und 3b sind zulässig, insbesondere hinreichend bestimmbar gemäß § 253 Abs. 2 Nr. 2 ZPO.

Der Klageantrag Ziffer 3a, der die Formulierung *„nach dem Stand der Technik möglichen Sicherheitsmaßnahmen*“ ist ausreichend bestimmbar und führt nicht zur Unzulässigkeit der Klage.

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).

Unter Berücksichtigung der dargelegten Grundsätze ist der Antrag hinreichend bestimmt und im Lichte des Art. 32 DSGVO auszulegen und zu vollstrecken.

Aufgrund der ständigen Weiterentwicklungen im Bereich der Informatik erscheint es der Klägerseite nicht möglich, genaue Maßnahmen zu benennen. Vor dieser Problematik stand auch Art. 32

DSGVO, weshalb ebenfalls die Formulierung „Stand der Technik“ dort Verwendung fand. Denn letztendlich ist allgemein bekannt, dass Dritte Lücken in verschiedenen Programmen versuchen auszunutzen, bis sie geschlossen werden. Danach erfolgte dann die Suche einer neuen Schwachstelle in der Software. Dies zeigt auch der vorliegende Fall. Der relative Ansatz, der im Hinblick auf Art. 32 DSGVO entwickelt wurde, und zu einer hinreichenden Balance zwischen dem Schutzniveau der Nutzer und dem zu gewährleistenden Aufwand für die Verantwortlichen führen soll (vgl. (BeckOK DatenschutzR/Paulus, 43. Ed. 1.11.2021, DS-GVO Art. 32 Rn. 7), kann hier ebenfalls angewandt werden. Das Gericht verkennt nicht, dass hier schwierige Entscheidungen auf das Vollstreckungsgericht zukommen können, dies ist jedoch im Wege des effektiven Rechtsschutzes hinzunehmen, zumal aufgrund der gesetzlichen Regelungen in Art. 32 DSGVO hinreichend Kriterien für eine Bestimmbarkeit zur Verfügung stehen.

Bezüglich des Klageantrags Ziffer 3b rügt, nach Auffassung des Gerichts, die Beklagtenseite zutreffend, dass die Formulierung „unübersichtlichen und unvollständigen Informationen“ zu unbestimmt sein dürfte.

Bei der Auslegung von Prozesserklärungen ist nicht am buchstäblichen Sinne des Ausdrucks zu haften, sondern schon wegen des verfassungsrechtlichen Anspruchs auf effektiven Rechtsschutz und rechtliches Gehör grundsätzlich dasjenige als gewollt anzusehen, was nach den Maßstäben der Rechtsordnung vernünftig ist und der Interessenlage des Erklärenden entspricht (BGH, Urteile vom 16.05.2017 - Xl ZR 586/15, juris Rn. 11). Inhalt und Reichweite des Klagebegehrens werden deshalb nicht allein durch den Wortlaut des jeweiligen Klageantrags bestimmt. Klageanträge sind vielmehr immer auch unter Berücksichtigung der Klagebegründung auszulegen, denn der prozessuale Anspruch im Sinne des § 253 Abs. 2 Nr. 2 ZPO wird ergänzend durch die vom Kläger in Anspruch genommene Rechtsfolge konkretisiert und den gesamten Lebenssachverhalt, aus dem er die begehrte Rechtsfolge herleitet (vgl. BGH, Urteile vom 17.03.2016 - lX ZR 142/14, juris Rn. 17, Brandenburgisches Oberlandesgericht, Urteil vom 5. April 2019 – 4 U 68/18 –, Rn. 14, juris).

Aus der Klageschrift geht jedoch nach Auffassung des Gerichts eindeutig hervor, dass die Klägerseite begehrt, die Verwendung der Telefonnummer zum Zwecke der Kontaktsuche zu unterlassen. Nach verständiger Auslegung war der Klageantrag Ziffer 3b dahingehend auszulegen und ist daher auch nicht zu unbestimmt.

B.

Die Klage ist teilweise begründet.

Dem Kläger steht ein Schadensersatzanspruch gegen die Beklagte i. H. v. 500,00 EUR gemäß Art. 82 Abs. 1 DSGVO zu (I.). Auch der Feststellungsantrag ist gemäß Art. 82 DSGVO begründet (II.). Ein Unterlassungsanspruch steht dem Kläger gegen die Beklagte in der im Tenor formulierten Weise zu (III.). Der Auskunftsanspruch war abzuweisen (IV.). Der Kläger kann die begehrten vorgerichtlichen Rechtsanwaltskosten nicht in voller Höhe verlangen (V.).

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

I.

Der Kläger hat einen Schadensersatzanspruch gegen die Beklagte in Höhe von 500,00 EUR gemäß Art. 82 Abs. 1 DSGVO, da die Beklagte gegen Art. 13 DSGVO (1.), Art. 32, 24, 5 Abs. 1 f) DSGVO (2.), Art. 33 DSGVO (3.) und Art. 34 DSGVO (4.) verstoßen hat. Die Beklagte kann sich nicht exkulpieren (5.). Es ist dem Kläger ein kausaler immaterieller Schaden entstanden, der mit einem angemessenen Schmerzensgeld i. H. v. 500,00 EUR abzugelten ist (6.).

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).

Unter Anwendung der dargelegten Grundsätze, hätte die Beklagte den Kläger bei der Angabe seiner Mobilfunknummer darüber aufklären müssen, dass die Mobilfunknummer durch die CIT-Software von allen Nutzern abgefragt bzw. abgeglichen wird. Diese fehlende Aufklärung stellt ein Verstoß gegen Art. 13 Abs. 1 lit. c) DSGVO dar. Durch die Eingabe einer beliebigen Telefonnummer können Profile und Telefonnummer zusammengefügt werden. Hierdurch wird dem Missbrauch von Daten Vorschub geleistet. Außerdem sind Fälle denkbar, bei denen ein Nutzer der Facebook-Plattform eine Verbindung zu seiner Mobilfunknummer gerade nicht möchte. Insofern ist eine ausreichende Aufklärung über das CIT und seine Funktionsweise zwingend, erfolgte jedoch weder in Hinweisen auf die Datenschutzrichtlinie der Beklagten, noch ergibt es sich aus den Anlagen B5, B6 oder B8.

Auch der Hinweis nach der Anmeldung im Hilfebereich der Beklagten zur Verwendung der Mobilfunknummer ist nicht ausreichend bzw. nicht rechtzeitig. Dort wird u.a. ausgeführt:

„Um dir Personen, die du kennen könntest, vorzuschlagen, damit du dich mit ihnen auf Facebook verbinden kannst.“

Aus dem Hinweis ergibt sich nicht, dass Dritte durch diese Funktion an die Mobilfunknummer der Nutzer gelangen können. Denn die Funktionsweise des CIT wird nicht erklärt. Ein Nutzer kann also nicht den Schluss ziehen, dass Dritte durch die Funktionsweise des CIT seine Mobilfunknummer in Erfahrung bringen können.

Zudem erfolgte der Hinweis jedenfalls nicht rechtzeitig. 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 transpa-

renten Verarbeitung von personenbezogenen Daten keinen Bestand haben, wenn dem Betroffenen nicht bereits bei Datenerhebung sämtliche nach Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden (LG Ulm, Urteil vom 16.02.2023, Az. 4 O 86/22).

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 gehört die Implementierung von geeigneten technischen und organisatorischen Maßnahmen zu den Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters. Dabei sind diejenigen Maßnahmen zu treffen, die unter Berücksichtigung von acht Kriterien ein dem Risiko angemessenes Schutzniveau gewährleisten. Diese acht Kriterien sind: 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. Teilweise wird dieser Ansatz auch mit IT-Compliance als Teil des Risikomanagements umschrieben. Der Begriff der Geeignetheit ist daher nicht im Sinne einer Einschränkung auf bestimmte Maßnahmen zu verstehen. Vielmehr ist beabsichtigt, alle in Betracht kommenden Maßnahmen einzubeziehen. Grundsätzlich ist es möglich, die Sicherheit der Verarbeitung personenbezogener Daten immer weiter zu erhöhen, allerdings oft nur mit gleichzeitig wachsendem Aufwand. Daher legt die DSGVO zur Bemessung der geeigneten Maßnahmen 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).

Die Auswahl der geeigneten technischen und organisatorischen Maßnahmen hat die Balance zwischen dem Schutzniveau, das dem Stand der Technik entspricht und dem Risiko zu finden. Dies entspricht einem sog. relativen Ansatz, letztlich ist es stetig ein ins Verhältnis setzen von Schutzaufwand und Risiko (BeckOK DatenschutzR/Paulus, 43. Ed. 1.11.2021, DS-GVO Art. 32 Rn. 7).

Diesen Anforderungen genügten die beklagtenseits behaupteten Schutzmaßnahmen nicht. Dabei wird nicht verkannt, das 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.). Dieses 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 aus-

führt, 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).

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.

Die Beklagte hat die Aufsichtsbehörde unstreitig nicht über den „Scraping“-Vorfall informiert. Eine Anzeigepflicht nach Art. 33 DSGVO besteht, wenn der Schutz personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO verletzt wird. Dies ist der u.a. der Fall, wenn Daten unbefugt offenge-

legt werden, oder unbefugt Zugang zu personenbezogenen Daten entsteht.

Ein unbefugter Zugang liegt vor, wenn nicht hierzu autorisierte Personen Kenntnis von den personenbezogenen Daten oder auch nur Zugang zu den Geräten, mit denen personenbezogene Daten verarbeitet werden, erlangt haben (Sydow, Europäische Datenschutzgrundverordnung, DSGVO Art. 4 Rn. 179, beck-online; ZD 2020, 175, beck-online).

Unstreitig ist das Scraping von Daten schon nach den eigenen Nutzungsbedingungen der Beklagten untersagt. Unstreitig haben hier Dritte, die keine regulären Nutzer der Plattform sind, die Telefonnummer jedenfalls mit dem Namen, dem Geschlecht und der Facebook-Nutzer-ID zusammengeführt und entsprechend Kenntnis davon erhalten. Es liegt daher ein unbefugter Zugang nach Art. 4 Nr. 12 DSGVO vor.

Die Meldepflicht entfällt auch nicht nach Art. 33 Abs. 1 S. 1 2. Halbsatz DSGVO, da bei den hier vom Scraping betroffenen Daten, die Gefahr von kriminellen Handeln durch die Verwendung der Daten, z.B. durch Phishing, Identitätsdiebstahl und Ähnliches sehr hoch ist. Vor diesem Hintergrund dürfte die Beklagte (unter anderem) auch die entsprechenden Sicherheitsvorkehrungen gegen Scraping getroffen haben.

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

5.

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

Gemäß Art. 82 Abs. 3 DSGVO wird der Verantwortliche von der Haftung nach Art. 82 Absatz 2 DSGVO 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 sich die Beklagte nicht entlasten.

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.

6.

Des Weiteren liegt auch ein ersatzfähiger Schaden im Sinne von Art. 82 Abs. 1 DSGVO vor.

a.

Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schäden. Ein materieller Vermögensschaden i.S.v. § 249 BGB wurde von der Klägerseite nicht vorgetragen. Sie beruft sich jedoch erfolgreich auf das Vorliegen eines immateriellen Schadens. Ein immaterieller Schaden liegt dabei zwar nicht schon in der bloßen Verletzung einer Norm der DSGVO (EuGH, Urteil vom 4. Mai 2023 – C-300/21 –, juris). Jedoch liegt ein immaterieller Schaden vor, wenn infolge der Verletzung der Norm der DSGVO ein absolut geschütztes Rechtsgut der geschädigten Person verletzt wurde. In Betracht kommt insoweit etwa eine Verletzung des Rechts auf körperliche Unversehrtheit ebenso wie eine Verletzung des Rechts auf informationelle Selbstbestimmung als besondere und ebenfalls absolut geschützte Ausprägung des allgemeinen Persönlichkeitsrechts (vgl. zur Bejahung eines Schadens im Sinne des Art. 82 DSGVO bei Verletzung des allgemeinen Persönlichkeitsrechts etwa EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19ff.). Entsprechend ist insbesondere auch in der deutschen Rechtsprechung anerkannt, dass eine Verletzung des allgemeinen Persönlichkeitsrechts einen Schaden im Sinne des Art. 82 DSGVO darstellen kann. Streitig war bis zuletzt nur, ob diese Verletzung eine gewisse Erheblichkeitsschwelle überschreiten muss (für eine Erheblichkeitsschwelle etwa OLG Dresden, Hinweisbeschluss vom 11. Juni 2019 – 4 U 760/19 (LG Görlitz) –, ZD 2019, 567; gegen eine Erheblichkeitsprüfung etwa EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19ff.; BeckOK DatenschutzR/Quaas DS-GVO Art. 82 Rn. 31-36; LAG Baden-Württemberg, Urteil vom 25. Februar 2021 – 17 Sa 37/20 –, BeckRS 2021, 5529) oder ob zumindest „ganz unerhebliche“ Verletzungen im Sinne einer Bagatelle ausscheiden sollten (EuArbRK/Franzen, 4. Aufl. 2022, EU (VO) 2016/679 Art. 82 Rn. 19-22; Paal, MMR 2020, 14, 16, mit weiterer Rspr. auch Wybitul, NJW 2021, 1190; OLG Dresden, Hinweisbeschluss vom 11. Juni 2019 – 4 U 760/19 (LG Görlitz) –, ZD 2019, 567) – wobei diese Frage nunmehr durch den Europäischen Gerichtshof dahingehend beantwortet wurde, dass keine Erheblichkeitsprüfung durchzuführen ist (EuGH a.a.O.).

Eine für die Bejahung eines Schadens damit ausreichende Verletzung des allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf informationelle Selbstbestimmung liegt hier vor. Das durch Art. 82 DSGVO geschützte Recht auf informationelle Selbstbestimmung enthält die

„Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“ (vgl. BeckOGK/Specht-Riemenschneider, 1.2.2023, BGB § 823 Rn. 1365-1383). Dieses Recht der Klägerseite wurde und wird bis heute fortlaufend verletzt. Infolge der obigen Verstöße gegen die einschlägigen Bestimmungen der DSGVO gelangten die streitgegenständlichen Daten inzwischen unstreitig auf jedenfalls eine online betriebene Seite, auf der sie rechtswidrig und massenhaft zum weiteren Vertrieb angeboten werden und damit fortgesetzt das geschützte Recht der Klägerseite verletzen, selbst zu entscheiden, wo und ob sie diese Daten offenbaren möchte. Dieser Verletzung misst das Gericht dabei auch ein erhebliches Gewicht zu, da die Daten der Klägerseite im „Paket“ mit den Daten Millionen anderer Nutzer und Nutzerinnen angeboten werden, was den derart generierten „Datenpaketen“ einen entsprechend höheren Nutzwert für kriminell handelnde Dritte zukommen lässt und was entsprechend die Intensität der Persönlichkeitsrechtsverletzung und die Gefahr weiterer Weiterungen steigert.

b.

Die festgestellten Verstöße gegen Art. 13, 32, 33, 34 DSGVO sind als kausal für die Schadensverursachung zu betrachten.

Nicht ausdrücklich gesetzlich geregelt ist, wen die Beweislast hinsichtlich der Kausalität des Verstoßes für den Schaden trifft, es ist jedoch von einer Beweislastumkehr zu Lasten des Schädigers auszugehen (vgl. Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 47).

Die Beklagte kann nicht nachweisen, dass die vom Kläger beschriebenen Spam-Nachrichten und Fake-Anrufe nicht erfolgt wären, hätte sie nicht gegen die DSGVO verstoßen.

c.

Die Höhe des Schadensersatzes beziffert das Gericht mit 500,00 EUR, wobei es diesen Betrag für angemessen, aber auch für ausreichend hält, um den immateriellen Schaden auszugleichen und gleichzeitig der erforderlichen Abschreckungswirkung Rechnung zu tragen sowie dabei die besonderen Umstände des Falles zu würdigen. Dem Gericht steht insoweit gemäß § 287 ZPO ein Ermessen zu.

Für den immateriellen Schadensersatz gelten die iRv § 253 BGB entwickelten Grundsätze, die Ermittlung obliegt dem Gericht nach § 287 ZPO (ausdr. so BAG NJW 2022, 2779), da die DS-

GVO insoweit keine Verfahrensmodalitäten regelt. Es können – müssen aber nicht – für die Bemessung die Kriterien des Art. 83 Abs. 2 herangezogen werden (so auch LAG Hamm BeckRS 2021, 21866), bspw. die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung, der Grad des Verschuldens, Maßnahmen zur Minderung des entstandenen Schadens, frühere Verstöße sowie die Kategorien der betroffenen personenbezogenen Daten, die betroffenen Kategorien personenbezogener Daten zur Ermittlung (BeckOK DatenschutzR/Quaas, 43. Ed. 1.2.2023, DSGVO Art. 82 Rn. 31).

Eine Straf- oder Abschreckungswirkung war bei Ermittlung der Schadenshöhe nicht zu berücksichtigten. Nach den Grundsätzen der Schadensbemessung ist der Schadensersatz in Ansehung der tatsächlich erlittenen Beeinträchtigung(en) festzusetzen. Systematik, Wortlaut und Zielsetzung von Art. 82 DSGVO stehen an der Prävention orientierten Zuschlägen oder Strafzielsetzungen entgegen. Der Zuspruch von immateriellem Schadensersatz außerhalb der Kompensationsfunktion würde zu einer Überkompensation und damit einer Bereicherung des Anspruchstellers führen; darüber hinaus drohte die Entstehung von Fehlanreizen zu einem kommerziellen Missbrauch des Schadensersatzes (vgl. NJW 2022, 3673 Rn. 21, beck-online; Höhe des Ersatzes immaterieller Schäden nach Art. 82 DS-GVO von Prof. Dr. Boris Paal). Zudem kann auch bezweifelt werden, ob eine Schadensersatzforderung im dreistelligen Bereich in der Lage ist, eine Straf- bzw. Abschreckungswirkung bei einem der größten Konzerne weltweit (der Jahresumsatz des Meta-Konzerns belief sich im Jahr 2022 auf 116,6 Milliarden US-Dollar) zu entfalten.

Möglicherweise anderweitig drohende Schadensersatzansprüche gegen die Beklagte wirken jedoch nicht schadensmindernd. Auch wenn die Beklagtenseite auf den Multiplikationsfaktor von 533 Mio. betroffenen Nutzern hinweist, beachtet sie nicht, dass völlig unklar ist, ob die weltweiten Nutzer in ihren jeweiligen Rechtssystemen überhaupt einen Schadensersatzanspruch haben und ob sie ihn geltend machen. Zudem wäre es dem deutschen Schadensrecht völlig systemfremd, anderweitige Schadensersatzansprüche schadensmindernd zu berücksichtigen. Denn das deutsche Schadensrecht ist auf eine reine Kompensation des erlittenen Schadens ausgerichtet. Der eigene Schaden kann sich nicht durch Schadensersatzansprüche anderer verringern.

In der mündlichen Verhandlung vom 17.05.2023 legte der Kläger ohne Belastungsdrang, präzise und glaubhaft dar, dass er seit 2021 erheblich mehr Spam-Nachrichten und Fake-Anrufe erhalte und ihn dies belaste. Nachvollziehbar und schlüssig erläuterte er, dass ihn die Fake-Anrufe stark beeinträchtigen würden, da er hierdurch möglicherweise wichtige Anrufe verpasse, da er mittlerweile bei Anrufe ihm unbekannter Telefonnummern nicht mehr abhebe. Spam-Nachrichten könne er vor diesem Hintergrund besser handhaben. Auch die Angst des Klägers, was mit seinen Daten

noch geschehe, konnte er glaubhaft darlegen. Auf Nachfragen konnte der Kläger sofort reagieren und Ungereimtheiten umgehend aufklären. Anknüpfungspunkte, die Zweifel an den Schilderungen des Klägers aufkommen lassen könnten, waren nicht ersichtlich und sind auch von der Beklagtenseite nicht vorgetragen. Für das Gericht stehen dies Schilderung des Klägers daher gemäß § 287 ZPO fest und waren dem Schmerzensgeldanspruch zugrunde zulegen.

Dabei hält die erkennende Einzelrichterin im vorliegenden Einzelfall ein Schmerzensgeld in Höhe von 500,00 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 informatorischen Anhörung - keine besondere persönliche Betroffenheit des Klägers festgestellt werden konnte, sind 500,00 EUR auch ausreichend.

II.

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.

III.

Der Kläger kann gemäß Art. 17 DSGVO verlangen, seine Mobilfunknummer nicht weiter ohne Zustimmung in der CIT-Software zu verwenden und bei Zustimmung ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern. Im Übrigen ist der begehrte Unterlassungsanspruch unbegründet.

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 Perso-

nen, 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).

Eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DSGVO liegt auch vor, wenn personenbezogene Daten verknüpft werden. Durch den vom CIT durchgeführten Abgleich der Mobilfunknummer mit den jeweiligen Facebook-Profilen wurden Daten i. S. d. Art. 4 Nr. 2 DSGVO miteinander verknüpft. Unerheblich ist, dass der Kläger die Zustimmung für die Offenlegung seines Namens erteilt hat. Denn die beanstandete Verknüpfung liegt in der Verbindung von Telefonnummer und Namen, die für Dritte einsehbar sind. Einer solchen Verknüpfung hat der Kläger nicht zugestimmt. Solange der Kläger daher der Verwendung seiner Telefonnummer durch das CIT nicht zustimmt, darf die Telefonnummer nicht hierfür verwendet werden. Durch die Beeinträchtigung besteht eine tatsächliche Vermutung für die Wiederholungsgefahr, die die Beklagte nicht widerlegt hat.

Der Anspruch des Klägers bei einer Zustimmung zur Verwendung seiner Mobilfunknummer durch das CIT von der Beklagten ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern, ergibt sich aus Art. 17, 6, 32 DSGVO.

Gemäß Art. 32 DSGVO müssen die entsprechenden hinreichend Sicherheitsvorkehrungen getroffen werden (s.o.).

Im Übrigen ist der Antrag unbegründet, insbesondere besteht kein Anspruch des Klägers gegen die Beklagte eine Datenverarbeitung ohne Erfüllung der Informationspflichten hinsichtlich der Funktionsweise des CIT und der Verwendung von Telefonnummern zu unterlassen. Denn die Pflichtverletzung der Beklagten bezüglich ihrer Informationspflichten kann keine Folgen mehr haben, da der Kläger spätestens durch diesen Rechtsstreit umfassend über das CIT und die fragliche Art und Weise der Datenverarbeitung informiert wurde.

IV.

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 Klä-

ger 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-Vorfalls zu halten.

V.

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 den in Ansatz zu bringenden Gegenstandswerten für die jeweiligen Klageanträge (dazu unten C) ist der Kläger hier hinsichtlich eines Begehrens erfolgreich, dessen Wert mit bis zu 6.000 EUR anzunehmen ist. Hinzuzurechnen ist noch das zunächst nicht erfüllte Auskunftsverlangen (500 EUR). Insgesamt ergeben sich daher Gebühren nach Ziff. 2300, 7002, 7008 VV RVG i.H.v. 713,76 EUR, die ebenfalls nach §§ 288, 291 BGB zu verzinsen sind.

C.

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

Der Streitwert für den Klageantrag Ziffer 1 erfolgte in Höhe des Zahlbetrags von 1.000,00 EUR. Der Klageantrag Ziffer 2 war mit 500,00 EUR zu bemessen. Hierbei hat das Gericht berücksichtigt, dass der Klageantrag nur künftige materielle Schäden abdecken sollte. Der Kläger hat, trotz erheblichen Zeitablaufs, bisher keine materiellen Schäden erlitten, weshalb auch künftig keine hohen Schäden mehr zu erwarten sind. Zudem handelt es sich um einen Feststellungsantrag, bei dem ein entsprechender Abschlag üblich ist. Der Klageantrag Ziffer 3 ist nach Auffassung des Gerichts der umfangreichste Antrag und dürfte von seiner Zielsetzung mit einem Wert von 5.000,00 EUR ausreichend bemessen sein. Der Klageantrag Ziffer 4 ist mit 500,00 EUR zu bewerten, da die Anzahl der gescrapten Daten gering ist und in ein angemessenes Verhältnis zu den anderen Anträgen gewahrt bleiben muss. Im Übrigen gilt § 43 GKG.

Rechtsbehelfsbelehrung:

Gegen die Entscheidung kann das Rechtsmittel der Berufung eingelegt werden. Die Berufung ist nur zulässig, wenn der Wert des Beschwerdegegenstands 600 Euro übersteigt oder das Gericht des ersten Rechtszuges die Berufung im Urteil zugelassen hat.

Die Berufung ist binnen einer Notfrist von **einem Monat** bei dem

Oberlandesgericht Stuttgart
Olgastraße 2
70182 Stuttgart

einzulegen.

Die Frist beginnt mit der Zustellung der vollständigen Entscheidung, spätestens mit Ablauf von fünf Monaten nach der Verkündung der Entscheidung.

Die Berufung muss mit Schriftsatz durch eine Rechtsanwältin oder einen Rechtsanwalt eingelegt werden. Die Berufungsschrift muss die Bezeichnung der angefochtenen Entscheidung und die Erklärung enthalten, dass Berufung eingelegt werde.

Die Berufung muss binnen zwei Monaten mit Anwaltsschriftsatz begründet werden. Auch diese Frist beginnt mit der Zustellung der vollständigen Entscheidung.

Gegen die Entscheidung, mit der der Streitwert festgesetzt worden ist, kann Beschwerde eingelegt werden, wenn der Wert des Beschwerdegegenstands 200 Euro übersteigt oder das Gericht die Beschwerde zugelassen hat.

Die Beschwerde ist binnen **sechs Monaten** bei dem

Landgericht Ulm
Olgastraße 106
89073 Ulm

einzulegen.

Die Frist beginnt mit Eintreten der Rechtskraft der Entscheidung in der Hauptsache oder der anderweitigen Erledigung des Verfahrens. Ist der Streitwert später als einen Monat vor Ablauf der sechsmonatigen Frist festgesetzt worden, kann die Beschwerde noch innerhalb eines Monats nach Zustellung oder formloser Mitteilung des Festsetzungsbeschlusses eingelegt werden. Im Fall der formlosen Mitteilung gilt der Beschluss mit dem dritten Tage nach Aufgabe zur Post als bekannt gemacht.

Die Beschwerde ist schriftlich einzulegen oder durch Erklärung zu Protokoll der Geschäftsstelle des genannten Gerichts. Sie kann auch vor der Geschäftsstelle jedes Amtsgerichts zu Protokoll erklärt werden; die Frist ist jedoch nur gewahrt, wenn das Protokoll rechtzeitig bei dem oben genannten Gericht eingeht. Eine anwaltliche Mitwirkung ist nicht vorgeschrieben.

Rechtsbehelfe können auch als elektronisches Dokument eingelegt werden. Eine Einlegung per E-Mail ist nicht zulässig. Wie Sie bei Gericht elektronisch einreichen können, wird auf www.ejustice-bw.de beschrieben.

Schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zu Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

[redacted]
Richterin