Abschrift

28 O 393/23

Landgericht Köln

IM NAMEN DES VOLKES

Urteil

In dem Rechtsstreit

Klägers,

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

gegen

die Meta Platforms Ireland Limited, gesetzl.vertr.d.d. Mitglieder des Board of Directors, Merrion Road, D04 X2K52 Dublin 4, Irland,

Beklagte,

Prozessbevollmächtigte: Rechtsanwälte Freshfields Bruckhaus Deringer,
Josephsplatz 1, 90403 Nürnberg,

hat die 28. Zivilkammer des Landgerichts Köln
auf die mündliche Verhandlung vom 25.03.2024
durch den Richter als Einzelrichter

für Recht erkannt:

Die Beklagte wird verurteilt, an den Kläger 100 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz ab dem 17.08.2023 zu zahlen.

Im Übrigen wird die Klage abgewiesen.

Die Kosten des Rechtsstreits werden dem Kläger auferlegt.

Das Urteil ist vorläufig vollstreckbar. Dem Kläger wird nachgelassen, die Zwangsvollstreckung durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abzuwenden, wenn nicht die Beklagte zuvor Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrags leistet.

Tatbestand

Die Beklagte betreibt das soziale Netzwerk Facebook. Der Kläger unterhält auf diesem ein Nutzerkonto. Die Plattform ermöglicht es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Bei der Registrierung müssen die Nutzer bestimmte Informationen angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name und Geschlecht. Die Nutzer-ID eines Profils ergibt sich u.a. aus der URL. Im Hilfebereich der Beklagten wird die Nutzer-ID als Teil des öffentlichen Profils geführt (Anlage B1). Im Rahmen der Registrierung wird der Nutzer unter anderem auf die Datenrichtlinie der Beklagten hingewiesen und es wird ein Link zu dieser bereitgestellt. Hinsichtlich des Inhalts der Datenrichtlinie wird auf die Anlage B9 verwiesen.

Neben den immer einsehbaren Pflichtangaben können die Nutzer in ihrem Profil weitere Daten zu ihrer Person angeben und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf diese Daten zugreifen können. Die Beklagte stellt hierfür Privatsphäre-Einstellungen zur Verfügung, mit denen die Nutzer bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten. Die Privatsphäre-Einstellungen sind über den Abschnitt „*Privatsphäre*“ des Haupteinstellungsmenüs im Konto des Nutzers und auf weiteren Wegen zu erreichen und umfassen insbesondere die Instrumente der sog. Zielgruppenauswahl und der Suchbarkeits-Einstellungen.

Im Rahmen der Zielgruppenauswahl kann der Nutzer durch individuelle Anpassung bestimmen, wer bestimmte Datenelemente (zum Beispiel die Telefonnummer, den

Wohnort, den Geburtstag und die E-Mail-Adresse) im Facebook-Profil des Nutzers sehen kann. So können Nutzer beispielsweise anstelle der Zielgruppenauswahl „Öffentlich“ festlegen, dass nur ihre „Freunde“ auf der Facebook-Plattform oder „Freunde von Freunden“ die jeweiligen Informationen sehen können. Soweit keine individuellen Einstellungen gewählt werden, richtet sich die Einsehbarkeit der Informationen nach den Standard-Einstellungen. Die Zielgruppenauswahl für die Telefonnummer war standardmäßig auf „Freunde“ voreingestellt.

Die Suchbarkeits-Einstellung ermöglicht es Nutzern unter anderem, festzulegen, ob ihr Nutzerkonto auf Facebook anhand der von ihnen angegebenen Telefonnummer gefunden werden kann. Im Rahmen der Suchbarkeits-Einstellung war es im streitgegenständlichen Zeitraum zum einen möglich, die Option „Alle“ sowie die Optionen „Freunde von Freunden“ oder „Freunde“ zu wählen. Dabei war die Suchbarkeits-Einstellung standardmäßig auf „Alle“ voreingestellt. Seit Mai 2019 steht Nutzern nunmehr zusätzlich auch die Option „Nur ich“ zur Verfügung.

Jedenfalls dann, wenn die Suchbarkeits-Einstellung eines Nutzers im Hinblick auf die Telefonnummer auf „Alle“ gestellt war, erlaubte es das von der Beklagten implementierte sog. „Contact-Importer-Tool“ (CIT) im streitgegenständlichen Zeitraum jedem Facebook-Nutzer, das Profil eines anderen Nutzers mit Hilfe der von diesem hinterlegten Telefonnummer zu finden. Hierzu konnten Nutzer Kontakte von Mobilgeräten auf Facebook hochladen, um mit Hilfe der Telefonnummer die jeweiligen Nutzer zu finden. Dies war auch dann möglich, wenn die Zielgruppenauswahl des jeweiligen Nutzers im Hinblick auf die Telefonnummer nicht auf „Öffentlich“ gestellt war.

Hinsichtlich des Kontos des Klägers war die Suchbarkeits-Einstellung im Hinblick auf die Telefonnummer auf die Standard-Einstellung „Alle“ gestellt (Anlage B17).

Im „Hilfebereich“ des Nutzerkontos stellte die Beklagte ihren Nutzern im streitgegenständlichen Zeitraum Informationen über die Privatsphäre-Einstellungen zur Verfügung. Unter anderem wurde erläutert, wie Nutzer die allgemeinen Informationen in ihrem Profil bearbeiten und wie sie durch die Anpassung ihrer Zielgruppenauswahl bestimmen können, wer auf die Profil-Informationen zugreifen kann (Anlage B3 und B4). Auch wurde erläutert, wie Nutzer bestimmen können, wer ihr Nutzerkonto finden kann (Anlage B5). Ferner wurden die Nutzer im Hilfebereich

über die Verwendung und weitere Einstellungsmöglichkeiten bezüglich der Telefonnummer informiert. So wird erläutert, dass die Telefonnummer möglicherweise zu Zwecken der „Passwort-Vergessen-Funktion“, zum Schutze des Kontos im zweistufigen Authentifizierungsverfahren und zum Vorschlag anderer Nutzer, die der Nutzer kennen könnte, verwendet wird (Anlage B6). Weiterhin wurden Nutzer darüber informiert, dass sie ihre Telefonnummer jederzeit zu ihrem Facebook-Konto hinzufügen und entfernen können (Anlage B7).

Anfang April 2021 wurden Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet. Bei den Datensätzen handelt es sich um Telefonnummer, FacebookID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten. Darunter befanden sich auch personenbezogene Daten des Klägers. Die veröffentlichten Daten (jedenfalls Facebook Nutzer ID, Name und Geschlecht) waren von unbekannten Dritten im Wege des sog. Scrapings bei der Beklagten erlangt worden. Charakteristisch für ein Datenscraping ist, dass Funktionen verwendet werden, die für die ordnungsgemäße Nutzung entworfen wurden und bei Nutzern beliebt sind, um die auf einer Website oder App verfügbaren Informationen einsehen zu können. Das Datenscraping unterscheidet sich insofern von der ordnungsgemäßen Nutzung einer Website oder App, als dass Scraper Verfahren einsetzen, um in großem Umfang Daten mit automatisierten Tools und Methoden zu sammeln, was nach den Nutzungsbedingungen von Facebook untersagt war und ist. Die Beklagte ist nicht im Besitz einer Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten.

Die genaue Vorgehensweise der Scraper ist im Einzelnen zwischen den Parteien streitig. Es ist davon auszugehen, dass die Scraper mithilfe des Contact-Importer-Tools Kontakte hochluden, welche mögliche Telefonnummern von Nutzern enthielten, um so festzustellen, ob diese Telefonnummern mit einem Facebook-Konto verbunden sind. Soweit die Scraper feststellen konnten, dass eine Telefonnummer mit einem Facebook-Konto (in Übereinstimmung mit der jeweiligen Suchbarkeits-Einstellung des Nutzers) verknüpft war, kopierten sie die auf dem Profil öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil und fügten die Telefonnummer – die den Scrapern insoweit nunmehr auch dann bekannt wurde, wenn sie nicht bereits im Rahmen der Zielgruppenauswahl als „*öffentlich*“ verfügbar eingestellt war und in der Folge auch das „Land“ des Nutzers, welches jedenfalls

anhand der Telefonnummer erkannt werden konnte – den abgerufenen, öffentlich einsehbaren Daten sodann hinzu.

Die Beklagte informierte weder die zuständige Datenschutzbehörde, die Irish Data Protection Commission, noch den Kläger über den Vorfall.

Mit anwaltlichem Schreiben vom 08.04.2023 (Anlage K1) forderte der Kläger die Beklagte auf, Schadensersatz nach Art. 82 Abs. 1 DSGVO in Höhe von 1.000,00 Euro zu zahlen. Ferner forderte er Unterlassung der zukünftigen Zugänglichmachung seiner Daten an unbefugte Dritte und Auskunft darüber, welche konkreten Daten im April 2019 abgegriffen und im Nachgang veröffentlicht wurden. Mit anwaltlichem Schreiben vom 08.05.2023 (Anlage B16) teilte die Beklagte dem Kläger einen Link zu Seite der Beklagten mit, auf der die über einen individuellen Nutzer gespeicherten Daten eingesehen werden können, im Übrigen wies die Beklagte die geltend gemachten Ansprüche zurück.

Der Profilname des Klägers im sozialen Netzwerk der Beklagten war von diesem – abweichend von seinem richtigen Namen – als angegeben. Diesen Namen gab der Kläger so ausschließlich bei Facebook an. Nach Veröffentlichung des Datensatzes erhielt der Kläger vereinzelte Spam-/Betrugsanrufe, bei denen er mit dem Namen angesprochen wurde.

Der Kläger behauptet von dem Datenschutzvorfall betroffen zu sein. In der u.a. im Darknet für jedermann abrufbaren Datenbank seien nachfolgende personenbezogene Daten der Klägerseite enthalten, die im Wege des Scrapings erlangt worden seien: Telefonnummer, die Facebook-ID, Name, Geschlecht.

Er behauptet, dass Scraping auch dann mittels des Kontakt-Importer-Tools möglich gewesen sei, wenn die Suchbarkeitseinstellung in dem jeweiligen Profil nicht auf „Alle“ gestellt war. Zudem sei die Nutzer-ID nicht öffentlich einsehbar im Profil des jeweiligen Nutzers.

Er trägt vor, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern, und dass die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und

kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Es seien keine Sicherheitscaptchas verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte handelt. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt oder Adressbücher mit auffälligen Telefonnummernabfolgen (z.B. 000001, 000002 usw.) automatisch abgelehnt werden.

Er ist der Ansicht, dass ihm ein Anspruch auf Schadensersatz gemäß Art. 82 DSGVO zustehe. Das Verhalten der Beklagten begründe mehrere Verstöße gegen die DSGVO. Zunächst habe die Beklagte nicht im ausreichenden Maße über die Verarbeitung der ihn betreffenden personenbezogenen Daten, welche der Kläger bei der Registrierung auf der Facebook-Plattform angab, informiert bzw. aufgeklärt. Insbesondere die Erläuterung über die Verwendung und Geheimhaltung der Telefonnummer stelle einen Verstoß dar. Hinsichtlich der unzureichenden Informationen verstoße die Beklagte gegen die Vorschriften Art. 5 Abs. 1 lit. a und Art. 13, 14 DSGVO. Weiterhin habe die Beklagte gegen den Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. f DSGVO verstoßen, indem sie die personenbezogenen Daten des Klägers nicht im ausreichenden Maße und nicht den Anforderungen der DSGVO entsprechend geschützt habe, sodass hierdurch erst das Abschöpfen der Daten möglich gewesen sei. Dies stelle einen Verstoß gegen Art. 32, Art. 24 und Art. 25 DSGVO dar. Darüber hinaus habe die Beklagte auch gegen die in Art. 25 DSGVO niedergelegten Grundsätze „Privacy by Design“ und „Privacy by Default“ verstoßen, da sie – entgegen der Regelung in Art. 25 Abs. 2 DSGVO – keine datenschutzfreundlichen Voreinstellungen verwendet habe. Es sei wenig datenschützend, dass standardmäßig „jedermann“ ein Profil mit Hilfe der hinterlegten Telefonnummer finden könne. Ferner habe die Beklagte gegen die in Art. 33 DSGVO normierte Pflicht, im Falle eines Datenschutzverstoßes die zuständige Aufsichtsbehörde zu informieren, verstoßen, da eine entsprechende Meldung unterblieben sei. Auch sei die Beklagte nicht ihrer Pflicht aus Art. 34 Abs. 1 DSGVO, die von einem Datenschutzvorfall betroffenen Personen über diesen zu informieren, nachgekommen, da eine solche Meldung unterblieben sei. Zudem habe die Beklagte

gegen ihre Auskunftspflicht aus Art. 15 Abs. 1 DSGVO verstoßen, da sie dem Auskunftsersuchen nicht in ausreichendem Maße nachgekommen sei. Denn die Beklagte habe lediglich allgemein Auskunft darüber erteilt, welche personenbezogenen Daten des Klägers sie verarbeite, nicht jedoch über die weiteren Umstände des Datenschutzvorfalles. So habe sie nicht darüber informiert, wer auf die Daten zugegriffen habe und welche Daten genau auf diesem Wege abgegriffen worden seien. Es sei keine Information darüber erteilt worden, welche Daten zum Zeitpunkt des Datenschutzvorfalls im Jahr 2019 für Dritte einsehbar gewesen seien.

Der Kläger ist der Auffassung, ihm sei durch die Datenschutzverstöße ein konkreter ersatzfähiger Schaden entstanden. Hierzu behauptet er, er habe einen erheblichen Kontrollverlust über seine Daten erlitten und verbleibe in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner Daten. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Darüber hinaus erhalte er seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks, insbesondere die SMS-Benachrichtigungen enthielten dubiose Aufforderungen zum Anklicken von unbekannten Links. 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 Emails und Nachrichten reagiere und jedes Mal einen Betrug fürchte und Unsicherheit verspüre. Der Kläger gebe seine Telefonnummer stets bewusst und zielgerichtet weiter, und mache diese nicht wahl- und grundlos der Öffentlichkeit zugänglich, wie etwa im Internet. Auch läge ein Schaden darin, dass er sich infolge von Ängsten, Stress und Komfort- und Zeiteinbußen mit dem Datenleak auseinandersetzen müsse. Dies führe zu einem Kontrollverlust. Er habe sich mit dem Datenleak auseinandersetzen müssen, den Sachverhalt ermitteln und sich um Auskunft gegenüber der Beklagten kümmern und weitere Maßnahmen ergreifen müssen. Der Kläger erhalte regelmäßig Anrufe von unbekannten Telefonnummern. Außerdem erhalte die Klägerseite regelmäßig SMS-Benachrichtigungen mit dubiosen Aufforderungen zum Anklicken von Links (Anlage K7).

Er ist der Ansicht, dass die Beklagte zudem zukünftige Schäden, die aufgrund der erlangten Daten entstünden, zu tragen habe. Dies folge aus der Verpflichtung der

Beklagten zur Leistung von Schadensersatz. Es sei noch nicht absehbar, für welche kriminellen Zwecke die Daten zukünftig missbraucht würden.

Des Weiteren stehe ihm ein Unterlassungsanspruch aus §§ 1004 analog, 823 Abs. 1 und Abs. 2 BGB i.V.m. Art. 6 Abs. 1 DSGVO sowie Art. 17 DSGVO zu. Datenschutzrechtliche Ansprüche könnten im Wege des Unterlassungsanspruchs gelten gemacht werden, sie seien nicht aufgrund von Art. 79 DSGVO gesperrt. Die Beklagte habe gegen Art. 6 DSGVO verstoßen, indem sie unrechtmäßig personenbezogene Daten des Klägers verarbeitet habe. Eine Einwilligung in die Verarbeitung sei mangels einer hinlänglichen Informierung durch die Beklagte nicht freiwillig erteilt worden. Weiterhin habe die Beklagte gegen die Informationspflichten aus Art. 13 und 14 DSGVO verstoßen. Diese Verstöße habe der Kläger auch nicht zu dulden. Er sei in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt.

Schließlich habe er einen Anspruch auf Datenauskunft gemäß Art. 15 DSGVO sowie auf vorgerichtliche Rechtsanwaltskosten ausgehend von einem Gegenstandswert in Höhe von 8.501,- €. Wegen der Einzelheiten der Berechnung wird auf die Anlage K 1 Bezug genommen.

Der Kläger beantragt,

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

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

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

(Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. 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,

b. 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;

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

5. die Beklagte zu verurteilen, an ihn vorgerichtliche Rechtsanwaltskosten in Höhe von 737,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, dass die Klage bereits weitgehend unzulässig sei. Der Klageantrag zu Ziffer 1) sei nicht hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Der Kläger mache einen Zahlungsantrag geltend, stütze das Begehren jedoch auf zwei zeitlich auseinanderfallende angebliche Verstöße und damit auf unterschiedliche Lebenssachverhalte. Auch der Klageantrag zu Ziffer 2) sei zu unbestimmt, zudem habe der Kläger kein Feststellungsinteresse gem. § 256 Abs. 2 ZPO dargelegt. Zuletzt sei auch der Klageantrag zu Ziffer 3) zu unbestimmt.

Die Klage sei auch unbegründet.

Sie ist der Ansicht, dass der Kläger keinen immateriellen Schaden erlitten habe. Der Schutzbereich des Art. 82 DSGVO erfasse keine Verstöße gegen Art. 13, 14, 15, 24, 25 und Art. 34 DSGVO. Darüber hinaus fehle es schon an einem Verstoß der Beklagten gegen die DSGVO. Der Kläger trage die Darlegungs- und Beweislast für seine Behauptungen, wonach die Beklagte gegen die DSGVO verstoßen habe. Sie ist der Ansicht, dass sie ihren Nutzern – auch dem Kläger – alle in den Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung stelle, die sie zum Zeitpunkt der Datenerhebung im Anwendungsbereich der Datenrichtlinie durchführe. Mithin erfolgte kein Verstoß gegen die Transparenzpflichten der DSGVO. Darüber hinaus habe sie alle Nutzer umfassend und transparent über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl informiert, die in diesem Zusammenhang regelten, wer bestimmte persönliche Informationen, die der Nutzer in seinem Facebook-Profil hinterlegt habe, einsehen könne. Diese Einstellungen konnten von dem Kläger jederzeit nach ihren Wünschen angepasst werden. Die Informationen im Hilfebereich zu den Privatsphäre-Einstellungen seien derart gestaltet, dass Nutzer die gesuchten Informationen schnell aufrufen und einfach einsehen könnten. Auch der Vorwurf des Verstoßes gegen die Pflicht gem. Art. 24, 32 DSGVO, angemessene technische und organisatorische Maßnahmen zu gewährleisten, gehe ins Leere. Sie behauptet, Maßnahmen getroffen zu haben, um das Risiko von Scraping zu unterbinden und ihre eigenen Maßnahmen zur Bekämpfung von Scraping kontinuierlich und als Reaktion auf die sich ständig ändernden Techniken und Strategien weiter zu entwickeln. Es sei grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern. Es gebe allenfalls Mittel, um Scraping zu begrenzen. Da die Funktionen, welche Scraper ausnutzen, 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 kann, beschränkt. Sie habe während des relevanten Zeitraums sowohl über Übertragungsbegrenzungen, die die Anzahl von Anfragen von bestimmten Daten reduzierten, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden können, als auch eine Bot-Erkennung verfügt. Zudem habe sie Captcha-Abfragen genutzt. Sie ist der Ansicht, dass der Kläger nicht

dargelegt habe, dass die Maßnahmen den Anforderungen der Art. 24 und 32 DSGVO nicht genügten. Die bloße Tatsache, dass Scraping erfolgt sei, könne die Ungeeignetheit der technischen und organisatorischen Maßnahmen nicht belegen, da deren Angemessenheit ex ante und nicht ex post zu beurteilen sei. Im Übrigen seien die durch Scraping abgerufenen Daten – soweit sie von der Facebook-Plattform stammen – im Einklang mit den Privatsphäre-Einstellungen des Klägers in seinem Facebook-Profil öffentlich einsehbar gewesen, d.h. diese durch Scraping abgerufenen Daten seien nicht vertraulich gewesen. Auch eine Melde- oder Benachrichtigungspflicht habe in Folge des Scraping-Sachverhalts nicht bestanden. Es fehle an einer Verletzung der Sicherheit i.S.d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten. Die Beklagte ist der Ansicht, auch nicht gegen die Pflicht zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen gemäß Art. 25 DSGVO verstoßen zu haben, indem sie geeignete technische und organisatorische Maßnahmen implementiert habe.

Im Hinblick auf die geltend gemachte Verletzungen der DSGVO habe der Kläger einen der Beklagten zurechenbaren ersatzfähigen immateriellen Schaden i.S.d. Art. 82 DSGVO weder erlitten noch dargelegt. Selbst wenn der Kläger tatsächlich den behaupteten Schaden erlitten hätte, so fehle es jedenfalls an einem kausalen Zusammenhang zwischen dem Schaden und den angeblichen Pflichtverstößen der Beklagten.

Der Feststellungsantrag sei mangels Verstoßes gegen die DSGVO auch unbegründet, im Übrigen habe der Kläger nicht dargelegt, dass ein zukünftiger Eintritt eines materiellen oder immateriellen Schadens wahrscheinlich sei.

Der Unterlassungsanspruch scheitere daran, dass keine Anspruchsgrundlage für diese Forderung ersichtlich sei. Überdies beruhe der Unterlassungsanspruch auf der unzutreffenden Annahme, dass die Beklagte unbefugten Dritten Zugriff auf Nutzerdaten gewährt hätte. Vor diesem Hintergrund mangele es sowohl an einer Erstbegehungs- als auch an einer Wiederholungsgefahr.

Der Auskunftsanspruch des Klägers richte sich in erster Linie auf Datenverarbeitungen durch unbekannte Dritte, für die die Beklagte nicht verantwortlich sei. Soweit sich der Kläger mit seinem Verlangen aber

berechtigterweise an die Beklagte richte, sei dieses Verlangen bereits außergerichtlich umfassend beantwortet worden.

Vorgerichtliche Anwaltskosten wären dem Kläger nur unter Verzugsgesichtspunkten zuzusprechen. Die Voraussetzungen einer Verzugshaftung seien vorliegend jedoch nicht erfüllt

Wegen der weiteren Einzelheiten wird auf die Schriftsätze der Parteien nebst Anlagen Bezug genommen.

Entscheidungsgründe

Die Klage ist bezüglich des Feststellungsantrags (Antrag zu 2.) und des Unterlassungsantrags (Antrag zu 3.a.) unzulässig und im Übrigen in dem aus dem Tenor ersichtlichen Umfang begründet. Im Einzelnen gilt Folgendes:

I.

1.
Das Landgericht Köln ist infolge der rügelosen Einlassung der Beklagten sachlich zuständig, § 39 S. 1 ZPO.

Anlass für die Einleitung eines Vorabentscheidungsverfahren nach Art. 267 AEUV oder für die Aussetzung des vorliegenden Verfahrens bis zur Entscheidung des Europäischen Gerichtshofs in den Verfahren C-189/22, C-741/21, C-687/21, C-667/21, C-340/21 und C-307/22 oder mit Blick auf die vom Bundesgerichtshof im Verfahren VI ZR 97/22 formulierten Vorlagefragen sieht die Kammer in Übereinstimmung mit dem Oberlandesgericht Köln (Urteil vom 07.12.2023, 15 U 108/23), auf dessen Ausführungen Bezug genommen wird, nicht.

2.
Der auf Zahlung von Schmerzensgeld gerichtete Antrag zu 1) ist zulässig. Dem steht nicht entgegen, dass der geltend gemachte Schmerzensgeldanspruch auf mehrere behauptete Verstöße gestützt würde. Ein Fall der unzulässigen alternativen Klagehäufung liegt nicht vor.

Ein Klageantrag ist hinreichend bestimmt, wenn er den erhobenen Anspruch durch Bezifferung oder gegenständliche Beschreibung so konkret bezeichnet, dass der Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) klar abgegrenzt ist, Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennbar sind, das Risiko des eventuell teilweisen Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abgewälzt und eine etwaige Zwangsvollstreckung nicht mit einer Fortsetzung des Streits im Vollstreckungsverfahren belastet wird. Es genügt nicht, sich auf gesetzliche Vorschriften zu berufen, die den erhobenen Anspruch vorsehen, vielmehr müssen die sich aus den Normen ergebenden Konsequenzen im Einzelfall von der klagenden Partei bei der Formulierung ihres Klageantrags berücksichtigt werden (BGH, Urt. v. 21.11.2017 – II ZR 180/15, juris Rn. 8). Eine alternative Klagehäufung, bei der der Kläger ein einheitliches Klagebegehren aus mehreren prozessualen Ansprüchen (Streitgegenständen) herleitet und dem Gericht die Auswahl überlässt, auf welchen Klagegrund es die Verurteilung stützt, verstößt grundsätzlich gegen das Gebot des § 253 Abs. 2 Nr. 2 ZPO, den Klagegrund bestimmt zu bezeichnen (BGH a.a.O.) Inhalt und Reichweite des Klagebegehrens werden nicht allein durch den Wortlaut des gestellten Klageantrages bestimmt. Vielmehr ist der Klageantrag unter Berücksichtigung der Klagebegründung auszulegen (BGH, Urteil vom 15.6.2021 – VI ZR 576/19, juris Rn. 32; Zöller/Greger, 34. Auflage 2022, § 253 Rn. 13 m.w.N.).

Vorliegend ergibt sich aus der Klageschrift, dass dem Klageantrag zu 1) ein zusammenhängender, sich zwar auf einen längeren Zeitraum erstreckender, aber in sich abgeschlossener Lebenssachverhalt zu Grunde liegt. Denn der Schadensersatzanspruch bezieht sich nach dem Vortrag des Klägers auf die Vorgänge ab der Anmeldung des Klägers auf der Facebook-Plattform über das „Scraping“ seiner Daten bis hin zu einer angeblich unzureichenden Information des Betroffenen. Der Klageschrift lässt sich überdies entnehmen, dass der Schaden aufgrund eines kumulativen Zusammenwirkens der gerügten Datenschutzverstöße geltend gemacht wird, die Bezifferung des Schadens dabei indes in zulässiger Weise in das Ermessen des Gerichts gestellt wird (vgl. Zöller/Greger a.a.O., § 253 Rn. 14 f.). Der Einwand der Beklagten, es handele sich um mehrere Streitgegenstände die in einem unzulässigen Alternativverhältnis stünden, verfängt daher nicht (so auch LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 38; LG Paderborn, Urt. v. 19.12.2022 – 3 O 99/22, Rn. 40).

3.

Die Klage ist unzulässig, soweit der Kläger mit dem Antrag zu 2) die Feststellung der Ersatzpflicht der Beklagten für künftige Schäden begehrt.

Der Antrag ist allerdings hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Dem steht nicht entgegen, dass mit der Formulierung „durch den unbefugten Zugriff Dritter“ ein unbestimmter Begriff verwendet wird. Denn der Begriff dient nur dazu, den Lebenssachverhalt zu beschreiben, auf den die vermeintlichen Ersatzansprüche des Klägers gestützt werden. Diese Umschreibung des Scraping-Geschehens im Jahr 2019 genügt aber den Bestimmtheitsanforderungen, ohne dass dafür im Vollstreckungsverfahren Überlegungen zu der Frage angestellt werden müssten, ob der Zugriff durch die Scraper „unbefugt“ erfolgte oder nicht. Der Inhalt und die Reichweite des Klagebegehrens werden nicht allein durch den Wortlaut des gestellten Antrags bestimmt, vielmehr ist dieser unter Berücksichtigung der Klagebegründung auszulegen (vgl. BGH NJW 19, 507). Aus der Klagebegründung ergibt sich vorliegend eindeutig, dass mit dem unbefugten Zugriff Dritter das Scraping-Geschehen im Jahr 2019 gemeint ist.

Dem Antrag fehlt es aber am erforderlichen Feststellungsinteresse, § 256 Abs. 1 ZPO. Nach dieser Vorschrift kann auf Feststellung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses geklagt werden, wenn der Kläger ein rechtliches Interesse daran hat, dass das Rechtsverhältnis durch richterliche Entscheidung alsbald festgestellt wird. Nachdem die immateriellen Schäden des Klägers bereits Gegenstand eines gegenüber dem Feststellungs- vorrangigen Zahlungsantrages sind, kann insofern lediglich auf bislang nicht eingetretene, aber vom Kläger für die Zukunft befürchtete Vermögensschäden abgestellt werden. Insofern wäre es ausreichend, dass nach der Lebenserfahrung und dem gewöhnlichen Verlauf der Dinge mit hinreichender Wahrscheinlichkeit ein erst künftig aus dem Rechtsverhältnis erwachsender Schaden angenommen werden kann. Dagegen besteht ein Feststellungsinteresse (§ 256 Abs. 1 ZPO) für einen künftigen Anspruch auf Ersatz eines allgemeinen Vermögensschadens regelmäßig dann nicht, wenn der Eintritt irgendeines Schadens noch ungewiss ist (BGH, Urteil vom 15. Oktober 1992 - IX ZR 43/92, WM 1993, 251, 259 f., Urteil vom 21. Juli 2005 - IX ZR 49/02, WM 2005, 2110, Urteil vom 10. Juli 2014 – IX ZR 197/12 –Rn. 11, juris). So liegt der Fall hier. Es ist völlig ungewiss, ob der Scraping-Vorfall jemals zu einer konkreten Vermögensschädigung des Klägers führen wird. Allein die theoretische

Möglichkeit, dass sich das entsprechende Risiko gerade bei dem Kläger als einem der mehr als 500 Millionen Betroffenen realisieren könnte, reicht hierfür nach Auffassung der Kammer nicht aus.

4.

Die Klage ist darüber hinaus unzulässig, soweit der Kläger die Beklagte auf Unterlassung der Zugänglichmachung seiner personenbezogenen Daten in Anspruch nimmt (Antrag zu 3a), weil es dem Antrag an der hinreichenden Bestimmtheit fehlt, § 253 Abs. 2 Nr. 2 ZPO. Die hinreichende Bestimmtheit des Klageantrages setzt voraus, dass Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennbar sind, das Risiko des eventuell teilweisen Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abgewälzt und eine etwaige Zwangsvollstreckung nicht mit einer Fortsetzung des Streits im Vollstreckungsverfahren belastet wird. Die letztere Voraussetzung ist aber nicht gegeben, soweit der Kläger von der Beklagten verlangt, es zu unterlassen, „keine ausreichenden Maßnahmen nach dem Stand der Technik zu ergreifen, um das Ausnutzen des Systems für andere Zwecke als die Kontaktaufnahme zu verhindern“. Soweit die Einhaltung von nach dem Stand der Technik ausreichenden Sicherheitsmaßnahmen verlangt wird, würde sich aus einer zusprechenden Entscheidung gerade nicht bereits ergeben, was die Beklagte im Zeitpunkt einer möglichen Zwangsvollstreckung gerade schuldet; vielmehr würde der Streit über die Frage, was „ausreichende“ Sicherheitsvorkehrungen sind, gerade in das Zwangsvollstreckungsverfahren verlagert.

5.

Die Klage ist hinsichtlich des Antrages zu 3b), mit welchem der Kläger Unterlassung der Verwendung seiner Telefonnummer begehrt, zulässig. Der Antrag ist hinreichend bestimmt gemäß § 253 Abs. 2 Nr. 2 ZPO.

6.

Bezüglich der Anträge zu 4) und 5) bestehen keine Zulässigkeitsbedenken.

II.

1.

Der Antrag zu 1) ist in einem Umfang von 100 € begründet. Dem Kläger steht ein Anspruch auf Ersatz immateriellen Schadens in Höhe von 100 € gegen die Beklagte nach Art. 82 Abs.1 DSGVO zu. Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

a)

Der Anwendungsbereich von Art. 82 Abs. 1 DSGVO ist in zeitlicher und sachlicher Hinsicht eröffnet und die Beklagte Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO (vgl. OLG Köln, Urteil vom 07.12.2023, 15 U 108/23). Der Kläger ist ausweislich des Auszugs aus dem Datensatz auch von dem Scraping-Vorfall betroffen. Soweit die Beklagte die Betroffenheit des Klägers bestritten hat, war dieses Bestreiten prozessual unbeachtlich, nachdem der Kläger seine Betroffenheit durch Vorlage des Auszugs des Leak-Datensatzes substantiiert vorgetragen hat.

Der Beklagten sind darüber hinaus jedenfalls Verstöße gegen Art. 5 Abs. 1 lit. b), 25 Abs. 2, 32 Abs. 1 DSGVO vorzuwerfen, weil sie keine geeigneten technischen und organisatorischen Maßnahmen getroffen hat, die sicherstellen konnten, dass durch die von ihr gewählten Voreinstellungen im Rahmen der Suchbarkeit des Profils mithilfe der Telefonnummer und das Zur-Verfügung-Stellen des CIT nur solche personenbezogenen Daten des Klägers verarbeitet wurden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich waren. Insoweit kann auf die Ausführungen des OLG Hamm, Urteil vom 15.08.2023, 7 U 19/23, Rn. 92 ff., juris verwiesen werden, die sich die Kammer zu eigen macht. Im Einzelnen:

Insbesondere hat die Beklagte einen Verstoß gegen Art. 5 Abs. 1 lit. b, Art. 25 Abs. 2, Art. 32 Abs. 1 DSGVO nicht ausgeräumt. Da der Kläger am 25.05.2018 schon bei der Beklagten registriert war (wie sich aus der Anlage B17 ergibt), hätte die Beklagte sicherstellen müssen, dass nicht geänderte, datenschutzunfreundliche Voreinstellungen (wie die Voreinstellung der Suchbarkeitseinstellung auf „alle“) zum 25.05.2018 unter Abkehr vom „Opt-Out“-System geändert werden (vgl. OLG Hamm, Urteil vom 15.08.2023, 7 U 19/23, Rn. 127 ff., juris).

Weiter hat die Beklagte trotz der sie treffenden Darlegungs- und Beweislast konkret weder substantiiert dargelegt noch bewiesen, dass sie den Vorgaben des Art. 32 DSGVO zur Sicherheit der Verarbeitung genügt hätte. Die Beklagte trägt vor, sie habe ihre Anti-Scraping-Maßnahmen im relevanten Zeitraum regelmäßig überprüft und gegebenenfalls entsprechend den Marktgepflogenheiten zu den Sicherheitsstandards sukzessive aus der maßgeblichen ex-ante-Betrachtung in angemessener Weise angepasst habe, z. B. durch Übertragungsbegrenzungen, Boterkennung, Captchas und den "Social Connection Check" (Anzeige von Personen, nur, wenn diese sich zu kennen schienen).

Diese Maßnahmen genügen den Anforderungen des Art. 32 DSGVO nicht. Es ist weder von der Beklagten dargetan noch sonst ersichtlich, dass trotz ex-ante-Betrachtung
wie geboten ab Geltung der DSGVO im Mai 2018 ausreichende Sicherheitsvorkehrungen gegen Scraping getroffen wurden. Konkret durfte die Beklagte, der ein Scraping bereits spätestens im März 2018 aufgefallen war, sich nicht auf die Deaktivierung der Suchfunktion der Plattform im April 2018 beschränken. Es war für sie ohne Weiteres möglich und im Hinblick auf die Datensicherheit ihrer Nutzer geboten sowie zumutbar
- auch wenn es ihrem wirtschaftlichen Interesse möglicherweise widersprach -, die Kontaktimportfunktion auf Facebook, im Friend Center und im Facebook-Messenger unverzüglich einzuschränken und somit einen massiven weiteren Datenverlust an Unbefugte zu unterbinden. Es ist nicht ersichtlich oder vorgetragen, warum die Deaktivierung der Suchfunktion im April 2018 bereits nach nicht einmal ein bis vier Monaten seit der Kenntniserlangung vom Vorfall erfolgte, die vollständige Deaktivierung der Kontaktimportfunktionen aber noch weitere rund sechszehn Monate dauerte oder warum nicht wenigstens andere weniger einschneidende, aber wirkungsvolle Maßnahmen getroffen wurden (vgl. OLG Hamm, Urteil vom 15.08.2023, 7 U 19/23, Rn. 143 ff., juris)

Ob die Beklagte darüber hinaus gegen Art. 33, 34 DSGVO verstoßen hat kann offenbleiben, nachdem der Kläger einen hierauf basierenden kausalen Schaden nicht dargelegt hat. Ein solcher ist auch ersichtlich.

b)

Der Kläger hat auch dargelegt, dass ihm ein immaterieller Schaden entstanden. Nach der Entscheidung des EuGH (Urteil vom 04.05.2023, Rs. C-300/21, juris) gilt Folgendes:

Art. 82 Abs. 1 DSGVO ist dahin auszulegen, dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung nicht ausreicht, um einen Schadenersatzanspruch zu begründen (EuGH, Urteil vom 04.05.2023, Rs. C-300/21, juris). Vielmehr muss der Kläger einen konkreten immateriellen oder materiellen Schaden darlegen und beweisen, ebenso wie das Vorliegen eines Verstoßes gegen die DSGVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (EuGH, Urteil vom 04.05.2023, Rs. C-300/21, Rn. 32). Die nationalen Gerichte haben bei der Festsetzung der Höhe des Schadenersatzes die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden (EuGH, a.a.O.). Erwägungsgrund 146 S. 3 DSGVO spricht für eine weite Auslegung des Begriffs des Schadens in Art. 82 Abs. 1 DSGVO. Damit ist etwa eine Erheblichkeitsschwelle in dem Sinne, dass immaterielle Bagatellschäden nicht ausgeglichen werden müssen, nicht zu vereinbaren (EuGH, a.a.O.).

Mit Urteil vom 14.12.2023 (EuGH, Urteil vom 14.12.2023, Rs. C-340/21) hat der EuGH die Anforderungen an einen immateriellen Schaden weiter konkretisiert:

Eine Auslegung von Art. 82 Abs. 1 DSGVO dahin, dass der Begriff „immaterieller Schaden“ im Sinne dieser Bestimmung keine Situationen umfasst, in denen sich eine betroffene Person nur auf ihre Befürchtung beruft, dass ihre Daten in Zukunft von Dritten missbräuchlich verwendet werden, wäre nicht mit der Gewährleistung eines hohen Schutzniveaus für natürliche Personen bei der Verarbeitung personenbezogener Daten in der Union vereinbar, die mit diesem Rechtsakt bezweckt wird (EuGH, a.a.O., Rn. 83). Allerdings ist darauf hinzuweisen, dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen muss, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (EuGH, a.a.O., Rn. 84). Insbesondere muss das angerufene nationale Gericht, wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes

missbräuchlich verwendet werden, prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (EuGH, a.a.O., Rn. 85). Nach alledem kann ein „Kontrollverlust“ einen immateriellen Schaden im Sinne von Art. 82 Abs. 1 DSGVO darstellen (EuGH, a.a.O., Rn. 86).

aa)

Einen derartigen kausalen immateriellen Schaden hat der Kläger in Form einer Belästigung mit Spam- /Betrugsanrufen dargelegt. Der in der mündlichen Verhandlung erschienene Kläger hat erklärt, dass er auf Facebook als Profilname angegeben habe. Diesen (falschen) Namen habe der Kläger so ausschließlich bei Facebook angegeben. Nach Veröffentlichung des Datensatzes habe der Kläger vereinzelte Spam- /Betrugsanrufe erhalten, bei denen sich der Anrufende als Mitarbeiter eines Callcenters ausgegeben und den Kläger mit dem Namen angesprochen habe. Die Prozessbevollmächtigte der Beklagten hat sich – auf ausdrückliches Befragen der Kammer hin – nicht weiter zu diesem Vortrag des Klägers erklärt, sodass dieser Vortrag als unstreitig zu behandeln ist. Damit ist unstreitig, dass der Kläger infolge der Datenschutzverstöße bei der Beklagten vereinzelt belästigende Anrufe erhalten hat.

bb)

Einen weitergehenden (immateriellen) Schaden hat der Kläger jedoch nicht dargelegt. Der Kläger trägt weiter vor, er habe einen erheblichen Kontrollverlust über seine Daten erlitten und verbleibe in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner Daten. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Darüber hinaus erhalte er seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks, insbesondere die SMS-Benachrichtigungen enthielten dubiose Aufforderungen zum Anklicken von unbekannten Links. 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 Emails und Nachrichten reagiere und jedes Mal einen Betrug fürchte und Unsicherheit verspüre. Der Kläger gebe seine Telefonnummer stets bewusst und zielgerichtet

weiter, und mache diese nicht wahl- und grundlos der Öffentlichkeit zugänglich, wie etwa im Internet. Auch läge ein Schaden darin, dass er sich infolge von Ängsten, Stress und Komfort- und Zeiteinbußen mit dem Datenleak auseinandersetzen müsse. Dies führe zu einem Kontrollverlust. Er habe sich mit dem Datenleak auseinandersetzen müssen, den Sachverhalt ermitteln und sich um Auskunft gegenüber der Beklagten kümmern und weitere Maßnahmen ergreifen müssen. Der Kläger erhalte regelmäßig Anrufe von unbekannten Telefonnummern. Außerdem erhalte die Klägerseite regelmäßig SMS-Benachrichtigungen mit dubiosen Aufforderungen zum Anklicken von Links (Anlage K7).

i)

Soweit der Kläger seinen immateriellen Schaden auf die Veröffentlichung derjenigen Daten stützt, die auf seinem Profil bei der Beklagten als „immer öffentlich“ eingestellt waren (Name und Geschlecht) sowie im Hinblick auf die Facebook-ID, die bei der Beklagten im Hilfebereich als immer öffentliches Datum (erkennbar an der URL des Profils) geführt wird (Anlage B1), scheidet die Annahme eines immateriellen Schadens schon deswegen aus, weil sich der Kläger durch seine im Zuge der Registrierung auf der Plattform der Beklagten erklärte Zustimmung mit den dort geltenden Nutzungsbedingungen damit einverstanden erklärt hat, dass diese Daten in die Öffentlichkeit gelangen. Im Hinblick darauf bestand schon keine Verpflichtung der Beklagten, diese Daten des Klägers durch datenschutzkonforme Voreinstellungen oder technische Sicherheitsmaßnahmen vor einer Kenntnisnahme durch Dritte weitergehend zu schützen. Jedenfalls – und das ist maßgeblich – können sich die vom Kläger angeblich verspürten Gefühle wie Angst, Unwohlsein oder Misstrauen nicht darauf beziehen, dass gerade solche personenbezogenen Daten von den Scrapern im sog. Darknet veröffentlicht worden sind, die er selbst auf der Plattform der Beklagten der Öffentlichkeit zugänglich gemacht hat (OLG Köln, Urteil vom 7. Dezember 2023 – 15 U 108/23 –, Rn. 35, juris).

ii)

Soweit der Kläger vorträgt, er habe einen erheblichen Kontrollverlust über seine Telefonnummer erlitten, vermag die Kammer einen solchen Kontrollverlust, unabhängig von der Frage, ob dieser im Einzelfall geeignet wäre, bereits einen immateriellen Schaden darzustellen, schon nicht festzustellen. Wie bereits dem Wortlaut dieses Begriffes zu entnehmen ist, setzt ein Kontrollverlust voraus, dass der Betroffene zunächst die Kontrolle über das konkrete personenbezogene Datum hatte

und diese Kontrolle später gegen seinen Willen verloren. Der Kläger hat jedoch nicht dargelegt, dass er vor dem streitgegenständlichen Scraping-Vorfall die Kontrolle über seine Mobilfunknummer hatte und diese erst durch die streitgegenständliche Veröffentlichung der Telefonnummer im sog. Darknet verloren gegangen ist. Vielmehr beschränkt sich der Kläger auf die in mehreren Verfahren wortgleiche Formulierung, er gebe die Telefonnummer stets nur „bewusst und zielgerichtet weiter“, und mache „diese nicht wahl- und grundlos der Öffentlichkeit zugänglich, wie etwa im Internet“. Substantiierte Angaben zur konkreten Verwendung seiner Telefonnummer vor dem streitgegenständlichen Scraping-Vorfall hat der Kläger hingegen nicht gemacht. Eine solche Darlegung einer zunächst ausgeübten Kontrolle über die eigene Telefonnummer ist auch nicht entbehrlich. Denn bei einer Telefonnummer handelt es sich nicht um ein per se sensibles oder der Geheimhaltung unterliegendes personenbezogenes Datum, sondern vielmehr um ein solches, das nach seiner Zweckbestimmung dem Betroffenen ermöglichen soll, in Kontakt mit anderen Personen zu treten und das daher im täglichen Leben auch solchen anderen Personen oft in großem Umfang zugänglich gemacht wird (vgl. OLG Köln, Urteil vom 7. Dezember 2023 – 15 U 108/23 –, Rn. 38, juris).

iii)

Selbst wenn man einen tatsächlichen Kontrollverlust im Hinblick auf die Telefonnummer unterstellen würde, führt dies im konkreten Fall – auch unter Berücksichtigung der Rechtsprechung des EuGH Urteil vom 14.12.2023, Rs. C-340/21 – nicht zu einem immateriellen Schaden. Insoweit hat der EuGH zwar festgestellt, dass bereits der Kontrollverlust über personenbezogene Daten und die damit einhergehende Befürchtung eines Missbrauchs als immaterieller Schaden im Sinne des Art. 82 DSGVO ausreichen kann. Allerdings hat der EuGH auch festgestellt, dass nationale Gericht zu überprüfen haben, wenn sich eine Person, die nach Art. 82 DSDGVO Schadensersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (EuGH Urteil vom 14.12.2023, Rs. C-340/21, Rn. 85). Vorliegend ist dies gerade nicht der Fall. Anders als in dem vom EuGH (a.a.O.) entschiedenen Fall geht es vorliegend auch nicht um den Kontrollverlust sensibler Finanz- und Steuerdaten, bei denen sich die Befürchtung des Missbrauchs aufdrängt, sondern allein um die Zuordnung von Daten, die der Kläger selber der

Öffentlichkeit zur Verfügung gestellt hat, zu seiner Telefonnummer. In Fällen wie dem vorliegenden, in denen sich der geltend gemachte Kontrollverlust aber alleine auf eine Telefonnummer bezieht, die ihrem Wesen nach nicht ohne weiteres auf strikte Geheimhaltung angelegt ist und hinsichtlich derer der Betroffene – wie hier der Kläger – auch keine in der Vergangenheit praktizierte Geheimhaltung vorgetragen hat, fehlt es jedoch an tatsächlichen Anhaltspunkten, die den Rückschluss darauf erlauben, dass der entsprechende Kontrollverlust über dieses personenbezogene Datum schon einen immateriellen Schaden darstellt (vgl. so auch schon OLG Köln, Urteil vom 7. Dezember 2023 – 15 U 108/23 –, Rn. 42, juris).

iv)
Soweit der Kläger weiter geltend macht, er leide aufgrund der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Vor- und Nachnamen unter Angst, Sorge und Unwohlsein, ist auch damit kein immaterieller Schaden hinreichend substantiiert vorgetragen worden.

Bei den vom Kläger geschilderten Beeinträchtigungen handelt es sich um psychische Folgen des Datenschutzverstoßes der Beklagten, die als solche nur von ihm selbst wahrgenommen werden können. Um daraus einen Schaden ableiten zu können, also einen Nachteil des Betroffenen, der im Sinne von Erwägungsgrund 146 konkret „*erlitten*“ wurde (vgl. EuGH, Urt. v. 4.5.2023 – C-300/21, NJW 2023, 1930 Rn. 58) und damit über die reine Behauptung des entsprechenden Gefühls hinausgeht, muss der Kläger konkrete Indizien vortragen und unter Beweis stellen, die eine solche psychische Beeinträchtigung seiner Person stützen können, wonach für die vom Kläger behaupteten immateriellen Schäden in Form von Angst, Sorge und Unwohlsein jedenfalls auch objektive Beweisanzeichen vorhanden sein müssen, da andernfalls die bloße Bekundung des Betroffenen, einen immateriellen Schaden in Form belastender Gefühle erlitten zu haben, für einen Ersatzanspruch ausreichen würde (OLG Köln, Urteil vom 7. Dezember 2023 – 15 U 108/23 –, Rn. 45; OLG Hamm, Urteil vom 15.8.2023 – 7 U 19/23, juris Rn. 163 ff.; OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, GRUR-RS 2023, 32883, Rn. 124). Mag bei einer Veröffentlichung besonders sensibler Daten(wie Bank- oder Gesundheitsdaten bzw. Finanz- und Steuerdaten wie in dem vom EuGH in C-340/21 entschiedenen Fall) bereits deren sensibler Charakter im Einzelfall im Rahmen des § 286 Abs. 1 ZPO indiziell dafür sprechen können, dass der Kontrollverlust darüber dem Betroffenen tatsächlich Angst, Sorge oder Unwohlsein bereitet, so ist dies bei einer

Telefonnummer - einem personenbezogenen Datum, welches üblicherweise im Alltag der Kommunikation mit anderen Personen im privaten und beruflichen Bereich zu dienen bestimmt ist - gerade so nicht der Fall. Insofern wäre es Aufgabe des Klägers gewesen, konkret in seiner Person liegende Umstände vorzutragen, die einen Rückschluss darauf zulassen, dass er durch die Veröffentlichung seiner Telefonnummer im sog. Darknet tatsächlich Angst, Ärger oder Unwohlsein erlitten hat (OLG Köln, Urteil vom 7. Dezember 2023 – 15 U 108/23 –, Rn. 46). Derartige konkretisierende Umstände hat der Kläger jedoch nicht vorgetragen und sind auch nicht aus dem sonstigen Akteninhalt ersichtlich.

v)

Auch soweit der Kläger einen immateriellen Schaden geltend macht, den er in Form einer Belästigung mit Spam-SMS und mit (im Vergleich zu den unstreitigen Spam-Anrufen weiteren) Spam-Anrufen erlitten haben will, verfängt dies nicht. Der Kläger legt hierzu Screenshots von Anrufen unbekannter Nummern und diverse SMS vor, wobei sich hieraus schon nicht ergibt, dass die Anrufe und SMS auf der veröffentlichten Telefonnummer der Klägerin eingingen. Zum anderen ist schon nicht ersichtlich, dass die Spam-Kontaktversuche kausal auf dem Scraping-Geschehen beruhen, insbesondere fehlt jedweder Bezug zu den angeblich veröffentlichten Daten des Klägers. Damit ist ein Zusammenhang zu dem Scraping Geschehen schon nicht nachvollziehbar vorgetragen. Ein solcher scheidet zudem von vornherein aus, soweit der Kläger vorträgt, verdächtige E-Mails erhalten zu haben, nachdem ausweislich des klägerischen Vorbringens seine E-Mail-Adresse gerade nicht zu den von den Scrapern abgegriffenen Daten zählte.

vi)

Auch soweit der Kläger vorträgt, er habe sich mit dem Datenleak auseinandersetzen, den Sachverhalt ermitteln, sich um eine Auskunft der Beklagten kümmern und weitere Maßnahmen ergreifen müssen, da er Ängste, Stress, Komfort- und Zeiteinbußen erlitten habe, verfängt dies mangels Substantiierung nicht. Es ist weder vorgetragen, wie und wann er sich – in welcher Form – überhaupt näher mit dem Scraping-Vorfall auseinandergesetzt hat noch hat der Kläger dargetan, welche konkreten Maßnahmen er ergriffen hat, um sich vor künftigem Missbrauch seiner Daten zu schützen.

c)

Der Höhe nach erachtet die Kammer einen Schadensersatz in Höhe von 100 € als angemessen. Der Kläger hat unstreitig nur vereinzelt belästigende Spam-Anrufe erhalten. Weiter ist zu beachten, dass der Kläger derartige Anrufe, in denen er mit seinem falschen Namen angesprochen wird, ohne weiteres als Spam-/Betrugsanrufe erkennen kann, sodass die Gefahr weitergehender Schäden gerade nicht besteht. Vor diesem Hintergrund hält die Kammer als Ersatz für die verhältnismäßig sehr geringe Belästigung mit Spam-Anrufen 100 € als angemessenen Ausgleich.

2.

Der Antrag zu 3b) ist unbegründet. Dem Kläger steht auch der mit dem Klageantrag zu 3b) geltend gemachte Unterlassungsanspruch aus § 1004 analog, 823 Abs. 1 und Abs. 2 BGB in Verbindung mit Art. 6 DSGVO und Art. 17 DSGVO nicht zu. Es kann hier dahinstehen, ob es sich bei den zuvor genannten Normen um Schutzgesetze im Sinne des § 823 Abs. 2 BGB handelt. Denn jedenfalls ist der Antrag zu weitgehend und daher unbegründet, nachdem es zum jetzigen Zeitpunkt nicht ausgeschlossen werden kann, dass die Beklagte ihr „Kontaktvorschläge-System“ derart ausgestaltet, dass eine rechtmäßige Verarbeitung der Telefonnummer auch ohne ausdrückliche Einwilligung des Klägers möglich wäre (Art. 6 Abs. 1 lit. b)-f) DSGVO).

3.

Der Antrag zu 4) ist unbegründet. Der Kläger kann von der Beklagten keine weitere Auskunftserteilung nach Art. 15 Abs. 1 DSGVO verlangen:

Soweit dem Kläger aufgrund von Art. 15 Abs. 1 DSGVO von der Beklagten Auskunft über die ihn betreffenden, von ihr verarbeiteten personenbezogenen Daten verlangen kann, ist der Anspruch durch Erfüllung erloschen, nachdem dem Kläger mit Schreiben vom 08.05.2023 (Anlage B16) ein Link zu einer Seite der Beklagten mitgeteilt wurde, auf der die über einen individuellen Nutzer gespeicherten Daten eingesehen werden können. Die Auskunftserteilung mittels Fernzugriffs auf ein elektronisches Auskunftssystem des Datenverantwortlichen genügt den an die Auskunftserteilung zu stellenden formellen Anforderungen (vgl. Mester, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 15 DSGVO Rn. 15 m.w.N.).

Soweit der Kläger darüber hinausgehend Auskunft darüber verlangt, welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten, steht einem Anspruch des Klägers § 275 Abs. 1 BGB entgegen. Insofern weist die Beklagte unwidersprochen darauf hin, dass ihr die Identitäten der Scraper nicht bekannt seien, weswegen ihr eine Auskunftserteilung bereits unmöglich ist.

4.

Dem Kläger steht auch kein Anspruch auf Erstattung vorgerichtlich entstandener Rechtsanwaltskosten zu, nachdem er seine Aktivlegitimation nicht schlüssig dargelegt hat. Auf das entsprechende Vorbringen der Beklagten wird verwiesen (GA 234).

5.

Die Zinsentscheidung beruht auf §§ 288, 291 BGB.

III.

Die prozessualen Nebenentscheidungen beruhen auf §§ 92 Abs. 2 Nr. 1 ZPO analog, 708 Nr. 11, 711 ZPO.

IV.

Streitwert: 3.500 Euro

- Antrag zu 1: 1.000 Euro
- Antrag zu 2: 500 Euro
- Antrag zu 3a+b: 1.500 Euro
- Antrag zu 4: 500 Euro