Aktenzeichen:
4 O 108/22

Landgericht Karlsruhe

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:

gegen

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

Prozessbevollmächtigte:

wegen Persönlichkeitsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

hat das Landgericht Karlsruhe - Zivilkammer IV - durch den Richter am Landgericht
als Einzelrichter aufgrund der mündlichen Verhandlung vom 23.02.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an die Klägerseite 300,00 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 19.07.2022 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, entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der schuldhaften Zuwiderhandlung fälligen Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise am organschaftlichen Vertreter zu vollstreckender Ordnungshaft oder Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

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

   b) die Telefonnummer des Klägers dadurch zu verarbeiten, dass die Telefonnummer durch Verwendung des Contact-Import-Tools verwendet werden kann, es sei denn, der Kläger hat ausdrücklich und aktiv die Einwilligung hierzu – oder generell zu einer Veröffentlichung seiner Telefonnummer – erteilt.

4. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 159,94 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 19.07.2022 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits tragen der Kläger 31 % und die Beklagte 69 %.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger jedoch nur gegen Sicherheitsleistung in Höhe von 10.000,00 €. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

Bei der Festsetzung des Streitwerts auf 7.000 € wurde die Klageanträge gem. § 3 ZPO wie folgt bewertet:

1. Antrag Ziff. 1.: 1.000 Euro

   Hier war der begehrte Zahlbetrag in Ansatz zu bringen.

2. Antrag Ziff. 2: 500 Euro

   Hier war ein Abschlag von 50 % zu machen, weil die materiellen Gefahren für den Kläger überschaubar sein dürften

3. Antrag Ziff. 3.: 5.000 Euro

   Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist letztlich anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen. Bei der Beklagten handelt es sich um einen multinationalen Konzern mit hohen Umsätzen, die Bedeutung der Sache ist auf Grund der Vielzahl der vom Scraping betroffenen Personen für die Beklagte erheblich.

4. Antrag Ziff.4: 500 Euro

   Hinsichtlich des Klageantrags Ziffer 4. erscheint ein Streitwert von 500,00 € € angemessen, da es nur noch um restliche begehrte Auskünfte geht.

Tatbestand

Der Kläger nutzt sein soziales Netzwerk „Facebook“ unter Verwendung der E-Mail-Adresse: .

Er hatte entsprechend der Standard-Voreinstellungen seinen Namen, Geschlecht und die Nutzer-ID öffentlich einsehbar gemacht, nicht aber seine Telefonnummer zur öffentlichen An- und Einsicht bereitgestellt. Für diese Informationen, die der Kläger in sein Profil eingetragen hat, ist auch standardmäßig „öffentlich" als Voreinstellung ausgewählt.

Weitere Daten hatte der Kläger nicht öffentlich bereitgestellt. Er hatte allerdings seine Telefonnummer (Mobilfunknummer) in seinem Profil hinterlegt, ohne dass diese öffentlich einsehbar ist.

Nach den bei der Registrierung vorhandenen Voreinstellungen, die der Kläger nicht abgeändert

hat, können „alle“ Personen den neuen Nutzer über seine Telefonnummer finden, wenn er – wie vorliegend – seine Telefonnummer seinem Profil hinzugefügt hat.

Die Standardeinstellung können die Nutzer im Rahmen des Registrierungsprozesses oder auch danach jederzeit abändern. Der Kläger hatte die Standardeinstellungen nicht verändert.

Die Beklagte bietet ihren Nutzern die Funktion einer Kontakt-Importierung („Contact-Importer-Tool“, im Folgenden: CIT) an, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf Facebook zu synchronisieren. Wenn ein Nutzer in seinem Smartphone eine Telefonnummer als Kontakt eingespeichert hat, erlaubt es die Beklagte ihm durch die Funktionalität CIT, seine Kontakte mit den bei Facebook hinterlegten Telefonnummern abzugleichen, um die hinter den Nummern stehenden Personen als Freunde hinzuzufügen. Auch der Kläger hat diese Funktionalität im streitgegenständlichen Zeitraum genutzt.

Anfang April 2021 wurden Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet worden. Bei diesem Vorfall wurden bei dem Beklagten personenbezogene Daten bereits im Jahr 2019 aus dem Datenbestand von Facebook mittels des Facebook-Tools Kontakt-Importer (CIT) „gescrapt“, d.h. aus öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert und durch unbekannte Dritte im Internet verbreitet. Hierbei wurden die Telefonnummern der Betroffenen – auch die Mobilfunknummer des Klägers – unter Verwendung des CIT mit den restlichen Personendaten korreliert, indem Zahlenfolgen in ein virtuelles Adressbuch eingegeben wurden, um festzustellen, ob diese mit einem Facebook-Nutzer übereinstimmten. Hierdurch gelang es den unbekannten Dritten, Telefonnummern zu ermitteln, die konkreten Facebook-Profilen zugeordnet waren, auch ohne dass die Betroffenen die hinterlegten Telefonnummern öffentlich freigegeben hatten. Sodann wurden die so ermittelten Facebook-Profile aufgesucht und von dort die öffentlichen Daten „gescrapt“ (abgeschöpft). Im Einzelnen ist zwischen den Parteien allerdings umstritten, mit welchen Methode genau die Daten gescrapt wurden.

Die so verbreiteten Datensätze beinhalten – nach Vortrag des Klägers – in katalogisierter Form die Telefonnummer, FacebookID, Name, Vorname und Geschlecht. Folgende personenbezogene Daten der Klägerseite seien insoweit in einer für jedermann abrufbaren Datenbank enthalten:

„

Die Beklagte trägt insoweit vor, dass in den durch Scraping abgeschöpften Daten nach ihrem Kenntnisstand die Datenkategorien Nutzer ID, Vorname, Nachname, Land, Geschlecht und Telefonnummer erschienen, die mit den entsprechenden Informationen aus dem Facebook-Profil des Klägers übereinstimmten. Ob es sich bei dem klägerseits vorgetragenen Datenauszug allerdings

um einen authentischen Auszug handle bestreitet sie mit Nichtwissen.

Mit vorgerichtlichem Schreiben vom 04.10.2021 hat der Kläger die Beklagte zur Zahlung von lediglich 500,- Euro Schadensersatz nach Art. 82 Abs. 1 DSGVO, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft u.a. darüber aufgefordert, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden seien (Anlage K1).

Hierauf hat die Beklagte dem Kläger mit Schreiben vom 28.10.2021 ihren Kenntnisstand hinsichtlich der gescrapten Datenkategorien mitgeteilt (Anlage B16), wobei sie darauf hingewiesen hat, dass nach ihrem Verständnis die Datenkategorien Land und Telefonnummer nicht durch Sraping abgeschöpft worden seien, sondern von den „Scrapern“ im Wege der Telefonnummernaufzählung bereitgestellt worden seien und es sein könne, dass die Datenkategorie „Land“ auch anhand der Telefonnummer ermittelt worden sein könne. Sie teilte ferner mit, dass sie - was unstreitig ist - über keine Kopie der Rohdaten verfüge, welche die durch Scraping abgerufenen Daten des Klägers enthielten. Sie lehnte das Zahlungsverlangen ab und erteilte verschiedentliche Auskünfte und Informationen (hinsichtlich der näheren Einzelheiten wird auf Anlage B16 verwiesen).

Nach Bekanntwerden des Scraping-Sachverhalts hat die Beklagte ihren Nutzern spezifische Informationen zur Verfügung gestellt, anhand derer diese Scraping künftig erschweren können. Unter anderem wird auf der Seite zum Thema „Was ist Scraping und wie kann ich meine Infos auf Facebook schützen“ darauf hingewiesen, dass die Facebook-Einstellungen nicht mehr öffentlich preisgeben sollten als gewollt. Insbesondere könne man im Bereich „So kann man dich finden und kontaktieren“ in den Einstellungen prüfen und festlegen, wer einen Nutzer anhand der E-Mail-Adresse und Telefonnummer finden könne.

Im Nachgang – nach Bekanntwerden des streitgegenständlichen Leaks – hat die Beklagte sodann weitere Schutzmaßnahme für den Kontakt-Importer der Facebook-Plattform eingeführt, die im Wesentlichen darauf abzielen, das mit der vom Nutzer hochgeladenen Telefonnummer verknüpfte Facebook-Profil des Betroffenen nur dann anzuzeigen, wenn der Nutzer zugleich einen Namen für die hochgeladene Telefonnummer importiert, der dem Namen des übereinstimmenden Facebook-Profils des Betroffenen zumindest ähnelt oder wenn dieses (nur) anhand der Telefonnummer übereinstimmende Profil den importierenden Nutzer bereits in seinen Facebook-Kontakten hat. Schließlich ist die Kontakt-Importer-Funktion dergestalt überarbeitet worden, dass sie ein gefundenes Facebook-Profil nicht mehr allein dem Telefonkontakt zuordnet, sondern zusätzlich zu dem Telefonnummernabgleich weitere soziale Indikatoren heranzieht. Als Ergebnis dieser überarbeiteten Suchfunktion wird somit nicht mehr ein ausschließlich telefonnummernbasierter individueller Kontakt angezeigt, sondern eine Liste mit Personen, die der importierende Nutzer

kennen könnte („PYMK-Funktion“). Eine direkte Kontaktübereinstimmung unter Zuordnung der „gesuchten“ Telefonnummer wird nicht mehr angezeigt.

Der Kläger trägt vor:

Von seinem bei der Beklagten gespeicherten Datenbestand seien darüber hinaus auch nicht öffentliche Daten wie sein Wohnort und die Mailadresse abgegriffen worden, möglicherweise auch weitere Daten.

Er habe in die Datenverarbeitung nicht wirksam eingewilligt. Die durch die Voreinstellung ermöglichte Datenerhebung sei von nicht einer wirksamen Einwilligung umfasst. Eine Einwilligung durch ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen müsse, sei nicht wirksam.

Die Suchbarkeitseinstellung nach Rufnummern hätte per Default auf „Freunde“ stehen müssen, zumindest wäre ein Hinweis auf die offene Standardeinstellung für die Suchbarkeit per Telefonnummer geboten gewesen. Eine Suchbarkeit mittels Telefonnummern sei unüblich und keinesfalls für den Verarbeitungszweck unabdingbar. Eine Suchbarkeit könne auch durch einzelne und weniger sensible Daten ermöglichet werden

Die Beklagte hätte die maximale Anzahl mit dem CIT abgleichbarer Rufnummern begrenzen müssen. Auch hätte Ein Monitoring und Alarmierungssystem habe vollständig gefehlt, welches bei Upload von sehr großen Adressbuchchargen eine Information zum Einleiten von Maßnahmen gegeben hätte.

Der Kläger habe deswegen einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten verblieben. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Er habe sich überdies mit dem Datenleak auseinandersetzen müssen, den Sachverhalt ermitteln und um Auskunft gegenüber der Beklagten kümmern müssen.

Darüber hinaus erhalte er seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks. Oft würden auch bekannte Plattformen oder Zahlungsdienstleister wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Das habe dazu geführt, dass die Klägerseite nur noch mit äußerster Vorsicht auf jegliche Emails und Nachrichten reagieren könne und jedes Mal einen Betrug fürchte

und Unsicherheit verspüre.

Das „Scraping“ sei möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Contact-Import Tools zu verhindern, und andererseits, weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könnten. Insbesondere den Voreinstellungen komme besondere Bedeutung zu. Nach den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der Datenminimierung und des „privacy by default" (=datenschutzfreundliche Voreinstellungen) seien hier besonders datenschützende Voreinstellungen geboten. Nur so könnten Nutzer mündig und bewusst entscheiden, welche Daten sie für wen freigeben möchten und erlangten Kontrolle über ihre Daten.

Die Beklagten habe keine Sicherheitsvorkehrungen gegen die Ausnutzung des Programms CIT und des Vorgehens vorgesehen:

- Sie habe keine Sicherheitscapchas verwendet, um zu verhindern, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatische gehandelt habe. (As. 22, Beweis: SV)
- Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt worden seine oder Adressbücher mit auffälligen Telefonnummerabfolgen (z.B. 000001, 000002 usw.) automatisch abgelehnt worden seien.

Der Kläger beantragt mit der am 18.07.2022 zugestellten Klage:

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 Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

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

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

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

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

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

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

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 580,72 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

Die Beklagte beantragt

Klageabweisung.

Sie trägt vor:

Sie habe sämtliche Nutzer auf verschiedenen Kanälen umfassend über die ihnen zur Verfügung stehenden Privatsphäre-Einstellungen informiert.

Eine Einwilligung des Klägers zur Datenverarbeitung sei nicht erforderlich gewesen, weil die erfolgte Datenverarbeitung im Rahmen der Bereitstellung der Facebook-Plattform im Sinne von Art. 6 Abs. 1 lit. b DSG-VO für die Vertragserfüllung – Bereitstellung eines sozialen Netzwerks – erforderlich gewesen sei.

Da der Unternehmenszweck der Beklagten darin bestehe, Menschen die Möglichkeit zu geben, Gemeinschaften zu bilden und die Welt näher zusammenzubringen, müssten ihre Nutzer in der Lage sein, ihre Kontakte und andere Nutzer zu finden, um sich mit ihnen auf der Plattform zu verbinden. Aus diesem Grunde sei es unabdingbar gewesen, dass die Suchbarkeit z.B. anhand von Telefonnummern – zunächst – für „Alle“ eröffnet gewesen sei. Denn andernfalls wäre ein neuer Nutzer, der noch über keine Kontakte („Freunde“) verfügt habe, auf der Plattform isoliert gewesen und hätte keine Möglichkeit bestanden, ihn zu „finden“ und mit ihm in Kontakt zu treten. Die Verarbeitung von Kontaktdaten wie E-Mailadresse oder Telefonnummer und damit die von der Beklagten vorgesehene Standardeinstellung der Suchbarkeit anhand der Telefonnummer für „Alle“ sei deshalb erforderlich gewesen, um den Verarbeitungszweck zu erreichen.

Die Telefonnummern seien nicht im Zuge des Scraping-Sachverhaltes von Facebook-Nutzerprofilen abgerufen, sondern diese vielmehr von den Scrapern mittels eines als Telefonnummernaufzählung bezeichneten Prozesses bereitgestellt worden. Soweit eine Telefonnummer mit einem Facebook-Konto – in Übereinstimmung mit der jeweiligen Suchbarkeits-Einstellung des Nutzers – verknüpft gewesen sei, hätten die Scraper die öffentlich einsehbaren Informationen aus dem betreffenden Nutzerprofil kopiert und die Telefonnummer diesen Daten dann hinzugefügt.

Datenkategorien „Land“, „Bundesland“, „Geburtsort“ und „weitere korrelierende Daten“ entsprächen keinen Profilfeldern auf der Plattform der Beklagten und seien daher nicht vom Scraping-Sachverhalt umfasst.

Bei den im Zuge des Scraping-Sachverhalts abgerufenen Daten von der Facebook-Plattform handele es entweder um immer öffentliche Nutzerinformationen oder um Daten, die in dem Facebook-Profil der Klagepartei entsprechend der jeweiligen Zielgruppenauswahl öffentlich einsehbar gewesen seien. Die unbekannten Dritten hätten lediglich öffentlich ohnehin einsehbare Daten gesammelt und anderweitig im Internet verfügbar gemacht.

Sie habe im relevanten Zeitraum sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt und diese eingesetzt, um das allgegenwärtige Scraping-Risiko zu verringern. Sie beschäftige hierzu ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping. Zur Verringerung von Scraping habe sie Übertragungsbeschränkungen installiert, die die Anzahl von Anfragen von bestimmten Daten reduzieren, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden können. Bereits im April 2018 habe sie überdies die Facebook-Suchfunktion anhand der Telefonnummern deaktiviert, nachdem sie sie festgestellt habe, dass von einer Reihe von IP-Adressen aus Osteuropa – mutmaßlich von Bot-Accounts – die Suchfunktion missbräuchlich genutzt worden sei. Die

telefonnummernbasierte Suche mit Hilfe der Kontakt-Importer Funktion (CIT) sei aktiv geblieben, weil zu diesem Zeitpunkt keine Scraping-Aktivitäten über dieses Programm festgestellt worden seien; allerdings seien die Übertragungsbeschränkungen innerhalb dieser Funktion überprüft und abgesenkt worden.

Im Übrigen könne die Beklagte selbst entscheiden, welche einzelnen technischen und organisatorischen Maßnahmen sie umsetze, um im Rahmen einer ganzheitlichen Bewertung aller Maßnahmen ein angemessenes Schutzniveau zu gewährleisten (Art. 31 Abs. 1, 25 Abs. 1 DSGVO). Diese Bewertung erfolge auf Grundlage einer vorausschauenden (ex ante) Einschätzung der mit der Verarbeitung verbundenen potenziellen Risiken. Zur Ergreifung einzelner, konkreter Maßnahmen sei sie nicht verpflichtet. Sie sei fortlaufend bestrebt, Scraping durch entsprechende Schutzmaßnahmen wirksam zu bekämpfen. Allerdings handle es sich beim „Sraping“ um eine komplexe Herausforderung, die auch durch hochentwickelte Gegenmaßnahmen nur begrenzt, aber nicht völlig verhindert werden könnten.

Es fehle im Übrigen am kausalen Zusammenhang zwischen einem fraglichen Verstoß gegen die DS-GVO und dem behaupteten Schaden, Art. 82 Abs. 1 DS-GVO („wegen“). Hinsichtlich der behaupteten Verstöße gegen Art. 34, 33 und 15 DS-GVO liege dies auf der Hand, da der behauptete immaterielle Schaden unabhängig davon eingetreten wäre, ob die Beklagte ihren Benachrichtigungs- bzw. Auskunftspflichten nachgekommen wäre. Aber auch hinsichtlich des behaupteten Verstoßes gegen Art. 13, 14 DS-GVO bestehe kein kausaler Zusammenhang, da die Telefonnummer von der Beklagten nicht preisgegeben worden sei und eine ordnungsgemäße und angemessene Information erfolgt sei. Hinsichtlich des behaupteten Verstoßes gegen die datenschutzfreundliche Voreinstellung fehle die Kausalität, weil ein datenschutzrechtliches Schadensereignis nur durch eine konkrete Verarbeitung ausgelöst werde, nicht hingegen durch die getroffene Wahl der technischen Gestaltung der Voreinstellung.

Entscheidungsgründe

Die Klage ist zulässig.

I.

Das Landgericht Karlsruhe ist international, örtlich und sachlich zuständig.

1. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs.1 EuGV-

VO. Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher - hier der Kläger - seinen Wohnsitz - hier: in der Bundesrepublik Deutschland - hat.

Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DS-GVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

2. Das Landgericht Karlsruhe ist örtlich zuständig. Das folgt zum einen aus Art. 18 Abs. 1 Alt. 2 EuGVVO, zum anderen aus Art. 79 Abs. 2 Satz 2 DS-GVO.

3. Die sachliche Zuständigkeit ergibt sich aus §§ 39 ZPO. Die Beklagte hat sich in der mündlichen Verhandlung am 23.02.2023 rügelos im Sinne des § 39 S. 1 ZPO zur Sache eingelassen.

II. Die Klage ist im Übrigen zulässig.

1. Der Klageantrag zu 1 ist nicht unbestimmt.

Der Kläger stellt die Bemessung des Schmerzensgeldes, hinsichtlich dessen er eine Größenordnung seiner Vorstellungen angegeben hat, zulässigerweise in das Ermessen des Gerichts. Er hat auch mitgeteilt, worauf sich sein Begehren bezieht und dass er sowohl einen Anteil des Schmerzensgeldes für das Verhalten der Beklagten vor dem Daten-Scraping-Vorfall als auch einen Anteil für das nachfolgende Verhalten begehrt, so dass eine unzulässige alternative Klagebegründung nicht vorliegt.

2. Das Feststellungsinteresse gemäß § 256 Abs. 2 ZPO für den Klageantrag Ziff. 2. liegt vor.

Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BeckOK ZPO/Bacher, 46. Ed. 1.9.2022, ZPO § 256 Rn. 24, Rn. 34). Das kann indes bei dem hier in Rede stehenden Daten-Scraping-Vorfall mit der behaupteten unkontrollierten Nutzung gescrapter Daten bei verständiger Würdigung angesichts der erst im Jahr 2021 erfolgten Veröffentlichung (noch) nicht angenommen werden. Aufgrund der Veröffentlichung der personenbezogenen Daten des Klägers im Internet ist nicht auszuschließen, dass dessen

Daten bereits zu illegalen Zwecken verwendet worden sind, dies dem Kläger allerdings derzeit noch unbekannt geblieben ist. Es ist deshalb nicht ausgeschlossen, dass irgendein materieller Schaden - hierauf beschränkt der Kläger sein Begehren ausweislich der Replik vom 25.11.2022 - entstehen könnte.

3. Auch das Unterlassungsbegehren des Klageantrags Ziff. 3. ist hinreichend bestimmt i.S. von § 253 Abs. 2 Nr. 2 ZPO. Danach darf ein Unterlassungsantrag – und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung – nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich die beklagte Partei deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was ihr verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (vgl. BGH, Urteil vom 09.09.2021, I ZR 90/20, dort Rn. 19).

   a) Vorliegend stützt sich der Kläger auf eine unzulässige Datenerhebung, deren Unterlassen er mit dem Antrag Ziff. 3. begehrt. Er macht geltend, dass die Einwilligung zur Verarbeitung seiner Telefonnummer nicht wirksam sei und die Beklagte sie daher im Rahmen des Contact-Import-Tools und im Facebook-Messenger App nicht verwenden dürfe. Der Lebenssachverhalt, durch den der Streitgegenstand bestimmt wird, ergibt sich aus der mit der Klage gerügten konkreten Verletzungsform – konkret: der ohne wirksame Einwilligung zur Weiterverarbeitung erlangten Telefonnummer. Damit richtet sich das Begehren Ziff. 3. gegen ein konkret beschriebenes Verhalten, das Anlass zu Beanstandungen geben kann. Dann aber bilden alle Rechtsverletzungen, die hierdurch verwirklicht werden können, den Streitgegenstand, so dass der Kläger die nach lit. a) und nach lit. b) geltend gemachten Unterlassungen zum Gegenstand eines zulässigen Klageantrags machen kann.

   b) Der Klageantragt Ziff. 3. ist auch nicht deshalb unzulässig, weil die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ auslegungsbedürftig ist und Vollstreckungsprobleme möglich sind. Denn zum einen beschreibt der Stand der Technik einen Zustand, der aufgrund der sich ständig wandelnden Technik aktuell vorherrscht, sich aber gleichermaßen rasch ändern kann. Insoweit ist es der Klägerseite unmöglich, den derzeitigen Stand der Technik explizit zu benennen. Je nach dem Stand der Technik sind dabei verschiedene, aufeinander aufbauende Sicherheitsmaßnahmen möglich, die nicht näher konkretisiert werden können. Zum anderen kann der Kläger der Beklagten in diesem Zusammenhang nicht vorgeben, welche konkreten Maßnahmen diese zu ergreifen hat. Er hat weder Einblick in die Programmierung der Facebook-Plattform noch in die Organisationsstruktur der Beklagten. Daher muss es genügen, dass das Vollstreckungsorgan gegebenenfalls Wertungen vornehmen muss. Es wäre verfehlt im Lichte des effektiven Rechts-

schutzes i.S. des Art. 19 GG, würde vom Kläger verlangt, dass er für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst ermitteln muss (so auch LG Stuttgart, Urteil vom 26.01.2023 – 53 O 95/22, BeckRS 2023, 1098).

c) Dem Klageantrag zu Ziff. 3.a.) fehlt auch nicht das Rechtsschutzbedürfnis. Das Rechtschutzbedürfnis ist gegeben, wenn der Rechtssuchende ein berechtigtes Interesse daran hat, gerichtliche Hilfe in Anspruch zu nehmen, d.h. sein Ziel nicht auf einem einfacheren, billigeren Weg erreichen kann. Zwar kann die Klägerseite durch die Anpassung der Privacy-Einstellungen die Suchbarkeit über die Telefonnummer deaktivieren. Dieses genügt aber nicht um zukünftige unrechtmäßige Datenverarbeitung zu verhindern, da die Klägerseite keinen Einfluss auf die durch die Beklagte ergriffenen Sicherheitsmaßnahmen und damit das vorgehaltene Schutzniveau hat.

d) Das mit dem Klageantrag zu Ziff. 3.b.) begehrte Anspruchsziel ist ebenfalls hinreichend bestimmt. Das Anspruchsziel wird jedenfalls durch die Klagbegründung hinreichend konkretisiert. Die Klägerseite begehrt ein Unterlassen der Verarbeitung der Telefonnummer ohne die aus ihrer Sicht gebotenen klarstellenden Hinweise bzw. Informationen als Grundlage der erteilten Einwilligung zur Datenverarbeitung.

4. Bedenken gegen die Zulässigkeit des Auskunftsverlangen bestehen nicht.

B.

Die Klage ist hinsichtlich des begehrten immateriellen Schadensersatzes teilweise und hinsichtlich des Feststellungs- und Unterlassungsbegehrens in vollem Umfang begründet. Ein Auskunftsanspruch besteht hingegen nicht mehr. Die Erstattung vorgerichtlich angefallener Rechtsanwaltskosten kann der Kläger nicht in vollem Umfang beanspruchen.

I. Dem Kläger steht gegen die Beklagte, die als Verantwortliche i.S. von Art. 4 Nr. 7 DS-GVO anzusehen ist, ein Anspruch auf - immateriellen - Schadensersatz i.H.v. 300 Euro aus Art. 82 Abs. 1 DS-GVO zu.

1. Art. 82 Abs. 1 DS-GVO erfordert nach seinem Wortlaut einen Verstoß gegen die DSGVO. Gegen welche Vorschrift der DS-GVO verstoßen wurde, ist insoweit zunächst nichtrelevant. Gemäß Art. 82 Abs. 1 DS-GVO haftet der Verantwortliche für Schäden wegen „Verstößen gegen diese Verordnung“. Grund und damit unabdingbare Voraussetzung der Haftung ist eine Pflichtverletzung, wenngleich es auf einen Schutznormcharakter der verletzten Vorschrift nicht ankommt, der Begriff der Pflichtverletzung also denkbar weit gefasst ist und letztlich jede Verletzung materieller oder formeller Bestimmungen der Verordnung einschließt (vgl. OLG Stuttgart, Urteil vom 31.03.2021 - 9 U 34/21, BeckRS 2021, 6282 Rn.25; Kreße in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 7; a.A. Gola/Piltzin Gola/Heckmann, DS-GVO - BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 5).

2. Vorliegend hat die Beklagte gegen die sich aus Art 25 Abs. 2 DS-GVO ergebende Verpflichtung verstoßen.

   a) Danach hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen ist zu gewährleisten, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben. Dass der Anbieter den Nutzern „nur“ die Möglichkeit eröffnet, Datenschutzeinstellungen des Dienstes jederzeit zu ändern, genügt dem normativen Auftrag des Art. 25 Abs. 2 DS-GVO nicht (Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 25, Rn. 46). Das hat zur Folge, dass alle für die Nutzung nicht erforderlichen personenbezogenen Daten anderen Nutzern nicht zugänglich gemacht werden dürfen, es sei denn, die betroffene Person nimmt „aktiv“ entsprechende Änderungen in den Voreinstellungen vor (vgl. Nolte/Werkmeister in Gola/Heckmann, DSGVO- BDSG 3. Aufl. DS-GVO Art. 25 Rn.

28). Die von Nutzern veröffentlichten Informationen dürfen nicht ohne Einschränkungen der allgemeinen Öffentlichkeit zugänglich gemacht werden, sondern dies muss aktiv erst in den Einstellungen zur Privatsphäre durch den Nutzereingerichtet werden (so Hartung in Kühling/Buchner, DS-GVO – BDSG, 3. Aufl. DS-GVO, Art. 25 Rn. 26).

Dies ist durch die Beklagte nicht gewährleistet (z.B. a.A. LG Essen, Urteil vom10.11.2022 - 6 O 111/22, GRUR-RS 2022, 34818). Die Suchbarkeit des Facebook-Profils anhand der Telefonnummer des Klägers beruhte vorliegend darauf, dass der Kläger dies in den Voreinstellungen nicht geändert hatte, nachdem die Standard-Einstellung für die Suchbarkeit von Telefonnummern während des relevanten Zeitraums „Alle“ gewesen ist. Diese Voreinstellung („default“) ist gegenüber einer neutralen Voreinstellung, bei der der Nutzer aktiv wählen muss, ob er der Suchbarkeit seines Profils zustimmt oder nicht, weniger datenschutzfreundlich und verstößt damit gegen Art. 25 Abs. 2 DSGVO.

Nicht ausreichend ist insoweit, dass etwaige Einstellungen vom Nutzer geändert werden *können* und auf diesen Umstand mehr oder weniger transparent hingewiesen wird. Dasselbe gilt für den von der Beklagten angeführten „Privatsphäre-Check“.

b) Die durch die Voreinstellungen ermöglichte Datenerhebung ist nicht für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich (Art. 6 Abs. 1 Satz 1 lit. b DS-GVO), ebenso wenig zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 Satz 1 lit. f DS-GVO). Sie mag im Einzelnen je nach Geschmack des Nutzers für die Nutzung der Facebook-Plattform nützlich und behilflich sein. Erforderlich für die Nutzung schlechthin ist sie aber nicht. Diesbezügliche Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Datenmüssen sich auf das absolut Notwendige beschränken. Die Daten sind für eine Nutzung der Facebook-Plattform durch Dritte bzw. für den Betrieb derselben durch die Beklagte nicht unabdingbar. Das zeigt sich auch daran, dass die fragliche Voreinstellung auch im streitgegenständlichen Zeitraum ohne weiteres abgewählt werden konnte, ohne dass dies ersichtlich der weiteren Vertragsdurchführung entgegengestanden hätte (so auch KG, Urteil vom 20.12.2019 - 5 U 9/18, BeckRS 2019, 35233 Rn. 39).

Insoweit kann sich die Beklagte nicht darauf zurückziehen, dass der Zweck der Facebook-Plattform gerade darin bestehe, es Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden und dass die Funktionen gezielt so konzi-

piert worden seien, dass sie den Nutzern helfen, („X-beliebige“) andere zu finden, sich mit ihnen zu verbinden und mit ihnen in Kontakt zu treten. Gerade dies – jedenfalls wenn es, wie vorliegend, durch einen entsprechenden „default“ ermöglicht wird – widerspricht den Anforderungen der DSGVO. Die Beklagte darf nicht durch die Definition ihres Leistungsangebots den Umfang der zulässigen Datenverarbeitung unter Hintanstellung der Nutzerinteressen allein an ihrem Interesse an der Vermarktung eines durch die Internetnutzung innerhalb und außerhalb von Facebook generierten Bestands personenbezogener Daten seiner Nutzer ausrichten und über das für die Benutzung des sozialen Netzwerkes erforderliche Maß ausweiten (so BGH, Beschluss vom 23.06.2020 - KVR 69/19 Rn. 110; LG Stuttgart, a.a.O.).

c) Der Einzelrichter folgt nicht der Auffassung, dass ein Verstoß gegen Art. 25 Abs. 2 DS-GVO einen Ersatzanspruch nicht auszulösen vermag (so aber z.B.: Nolte/Werkmeister in Gola/Heckmann, DS-GVO - BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 3, 34). Vielmehr kann aus der Verletzung der sich aus Art. 25 DS-GVO ergebenden Pflichten eine Erhöhung der Gefahreines Schadens resultieren (vgl. Mantz in Sydow/Marsch, DS-GVO | BDSG, 3. Aufl. DS-GVO Art. 25 Rn. 77; Martini in Paal/Pauly, DS-GVO - BDSG 3. Aufl. DS-GVO Art. 25 Rn. 6). Das wird hier augenscheinlich dadurch, dass bei einer Voreinstellung, die mit Art. 25 Abs. 2 DS-GVO konform gewesen wäre, die Mobiltelefonnummer des Klägers und deren Verknüpfung mit dessen Facebook-Profil nicht ohne weiteres durch die Sraper hätte „ermittelt“ werden können. Denn bei einer entsprechenden Voreinstellung wäre die Suchbarkeit anhand der Mobilfunknummer nicht jedermann eröffnet gewesen, sondern allenfalls einem – aufgrund einer individuellen Auswahl des Klägers begrenztem - Nutzerkreis.

3. Die Beklagte kann sich mit Blick auf den Daten-Scraping-Vorfall nicht nach Art. 82 Abs.3 DS-GVO entlasten.

   Insofern kann dahinstehen, ob überhaupt ein Verschulden erforderlich ist bzw. ob die Haftung nach Art. 82 DS-GVO zur Sicherstellung eines möglichst wirksamen Schadensersatzes als Gefährdungshaftung gestaltet ist (so z.B. Geissler/Ströbel, NJW 2019, 3414). Denn der Beklagten ist bereits nach ihrem eigenen Vorbringen eine Entlastung, hinsichtlich derer ihr die Darlegungs- und Beweislast obliegt (vgl. nur Nemitz in Ehmann/Selmayr, DS-GVO 2. Aufl. Art. 82 Rn. 19), nicht gelungen. Sie bringt vor, dass die Daten-Scraper Verfahren eingesetzt hätten, um in großem Umfang Daten mit automatisierten Tools und Methoden zu sammeln, was nach den Nutzungsbedingungen von Facebook untersagt gewesen sei. Damit räumt sie die technische Möglichkeit des Abgreifens von Daten durch die von ihr ge-

wählte Architektur der Facebook- Plattform ein. Wenn aber der Beklagten bewusst ist, dass Daten-Scraper bestimmte Funktionen missbrauchen können, dann wäre es an der Beklagten gewesen, gerade das zu unterbinden. Auch wenn das dem eigenen Verständnis der Facebook-Plattform zuwiderlaufen mag, dem Interesse der Nutzer an der Wahrung ihrer datenschutzrechtlichen Belange entspräche das indes sehr wohl.

Im Übrigen liegt es auf der Hand, dass der vorliegend unzulässige „default“ hinsichtlich der allgemein zugänglichen Suchbarkeit per Telefonnummereingabe durch entsprechend sorgfältige Überprüfung anhand der Vorgaben des Art. 25 DSGVO von der Beklagten mit überschaubarem Aufwand hätte erkannt und vermieden werden können. Hierdurch hätte – ohne eine durch den Nutzer veranlassten Änderung der dann datenschutzfreundlicheren Voreinstellung – das vorliegende „Sraping“ der Nutzerddaten und die Verknüpfung mit den Telefonnummern anhand der öffentlich zugänglichen Telefonnummernsuche nicht stattfinden können und es wäre nicht zum streitgegenständlichen „Datenleak“ gekommen. Insoweit verfängt auch der Einwand der Beklagten nicht, wonach nicht sie, sondern die „Sraper“ die Telefonnummern bereitgestellt und damit die Rufnummernsuche missbraucht hätten. Denn es wäre Sache der Beklagten gewesen, durch entsprechende datenschutzfreundliche Voreinstellungen ein solches automatisiertes Verfahren, wie es von den Srapern angewendet wurden, von vornherein zu unterbinden.

4. Dem Kläger ist im Zusammenhang mit dem Daten-Scraping-Vorfall auch ein nach Art. 82 DS-GVO ersatzfähiger - immaterieller - Schaden entstanden, für den die Verstöße der Beklagten gegen die DS-GVO kausal waren.

   a) Hierbei kann dahinstehen, ob ein Datenschutzverstoß als solcher für das Entstehen eines Schadensersatzanspruchs ausreicht oder es darüber hinaus der Darlegung und des Nachweises eines konkreten - auch immateriellen - Schadens bedarf. Denn ein solcher Schaden ist vom Kläger ausreichend dargetan worden und das Gericht ist aufgrund der persönlichen Anhörung des Klägers auch davon überzeugt, dass die – eine Bagatellgrenze überschreitenden Beeinträchtigungen – auch auf dem streitgegenständlichen „Datenleak“ beruhen. Der Kläger hat insoweit in lebendiger und zusammenhängender Schilderung berichtet, wie er auf das Datenleak aufmerksam geworden sei und in welchem Umfang er seit ca. 2-3 Jahren eine signifikant höhere Zahl an offensichtlichen betrügerisch motivierten Anrufen und SMS auf seine Mobilfunknummer erhalte. Diese Angaben waren nicht nur etwa allgemeiner Art und floskelhaft, sondern der Kläger schilderte im Einzelnen, welche Art von Anrufen und SMS unbekannter Herkunft er in jüngerer Zeit verstärkt erhalte (z.B. Anrufe vermeintliche Telefondienstleister oder

sonstige Unternehmen mit der Zielrichtung der Preisgabe seiner Bankverbindung; offensichtlich betrügerische Zahlungsaufforderungen, Mahnungen angeblicher Zahlungsrückstände etc.; zum Teil gebrochen Deutsch bzw. mit starkem osteuropäischem Akzent sprechende Anrufer). Seine Angabe waren auch deshalb glaubhaft, weil er sich keineswegs nur als „Opfer“ ruchloser Machenschaften darstellte, sondern – im Gegenteil – ungefragt auch Aspekte berichtete, die gegen eine schwere Verletzung seiner persönlichen Datenintegrität sprechen. So teilte er ungefragt mit, dass er derartige Anrufe und SMS zwar einerseits als lästig und bedenklich empfinde, andererseits aufgrund seines beruflichen Hintergrundes im IT-Bereich mit derartigen Betrugsversuchen umzugehen wisse und sich teilweise sogar darüber amüsiere – wenn er gut aufgelegt sei und Zeit habe, verwickle er die offensichtlich kriminell agierenden Anrufer sogar in Gespräche, in deren Verlauf diese irgendwann „entnervt“ aufgeben und den Anruf abbrechen würden. Andererseits verspüre er angesichts seiner nunmehr im Internet veröffentlichten Personendaten – insbesondere der mit ihm verknüpften Mobilfunknummer – schon ein Unwohlsein angesichts der Tatsache, dass seine Telefonnummer nun jedermann – auch osteuropäischen Kriminellen etc. – zugänglich sei. Auch sei die signifikant gestiegene Zahl an Anrufen und SMS nicht zu jedem Zeitpunkt amüsant, sondern nach den Umständen auch sehr lästig.

In einer Gesamtschau der vom Kläger glaubhaft berichteten spürbaren Folgen bewertet das Gericht die Beeinträchtigungen als über eine Bagatellgrenze hinausgehend. Hiergegen spricht nicht, dass der Kläger bisher weder seine Mobilfunknummer gewechselt, noch seine Datenschutzeinstellungen bei Facebook geändert hat, was er freimütig einräumte. Denn für beides konnte er nachvollziehbare Gründe anführen.

b) Das Gericht ist aufgrund der vom Kläger berichteten Anrufe und SMS, insbesondere deren signifikante Zunahme in einem mit dem streitgegenständlichen Leak korrespondierenden Zeitraum auch davon überzeugt, dass jedenfalls eine Mitursächlichkeit zwischen dem Datenleak im Jahr 2019 und den vielfältigen „Kontaktversuchen“ unbekannter Anrufer etc. besteht. Zum einen liegt ein zeitlicher Zusammenhang vor, zum anderen entsprechen die tatsächlichen Folgen (betrügerisch motivierte Anrufe, SMS) den mit der missbräuchlichen Veröffentlichung der Daten im Internet bzw. „Darknet“ evident intendierten kriminellen Zwecken.

c) Der dem Kläger zuzuerkennende Schadensersatz für den erlittenen immateriellen Schaden ist entsprechend seinem Begehren für den lediglich als gerechtfertigt angesehen Ersatzanspruch wegen der Verstöße im Zusammenhang mit dem Daten-Scra-

ping-Vorfall mit 300 Euro zu bemessen (§ 287 Abs. 1 Satz 1 ZPO).

Damit kann einerseits der Ausgleichs- und Genugtuungsfunktion genügt werden, andererseits der generalpräventiven Funktion des immateriellen Schadensersatzes hinreichend Rechnung getragen werden. Zum einen ist - mit Blick auf den generalpräventiven Auftrag des Art. 82 DS-GVO (vgl. Gola/Piltz in Gola/Heckmann, DS-GVO- BDSG, 3. Aufl. DS-GVO Art. 82 Rn. 5) - insoweit zu berücksichtigen, dass die Art und Weise der Datenerhebung durch die Beklagte systematisch gegen die Vorgaben der DS-GVO verstößt, um damit Sinn und Zweck der von ihr betriebenen Facebook-Plattform zu fördern. Andererseits ist auch der Umfang der Daten des Klägers, die abgegriffen worden sind, zu berücksichtigen. Hierunter ist seine Mobilfunknummer, die über den Vorfall nunmehr für die Allgemeinheit mit seinem Namen verbunden werden kann, ebenso auch das Profil bei Facebook, so dass der Kläger über diesen Weg kontaktiert werden kann. Letztgenannte Profildaten (Vor- und Name, Facebook ID und Geschlecht) hatte der Kläger allerdings ohnehin bereits vor dem streitgegenständlichen Vorfall im Grunde für jedermann zugänglich gemacht, indem diese Daten in seinem öffentlichen Facebook-Profil enthalten waren.

Weitergehende Daten, die eine Kontaktaufnahme ermöglichen könnten, sind - nach derzeitigem Kenntnisstand - nicht „gescrapt“ worden. Daher ist der mögliche Schaden, auch die Gefahr eines Identitätsdiebstahls und des „social engineering“ beim Kläger, ist damit – auch aufgrund dessen Versiertheit im Umgang mit den einschlägigen Gefahren – letztlich noch überschaubar.

II. Feststellungsantrag

Der mit dem Klageantrag Ziff. 2. geltend gemachte Feststellungsantrag ist ebenfalls 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 Datenverlust des Klägers. Dass dem Kläger durch das Datenleak künftig noch (materielle) Schäden – etwa infolge erfolgreicher Phising-Anrufe unter Nutzung der veröffentlichten Mobilfunknummer – entstehen können, ist nach den konkreten Umständen zwar eher unwahrscheinlich, indes nicht ausgeschlossen.

III. Unterlassung

Der mit dem Klageantrag Ziff. 3. beanspruchte Unterlassungsanspruch ist überwiegend – im tenorierten Umfang – begründet.

Soweit es für den vorbeugenden Unterlassungsschutz eine gesonderte Anspruchsgrundlage in der DS-GVO nicht gibt, bleibt im Hinblick auf die Vorgaben des Art. 79 DS-GVO entweder ein Rückgriff auf § 823 Abs. 2, § 1004 BGB analog möglich, um Schutzlücken zu vermeiden (vgl. nur OLG München, Urteil vom 19.01.2021 - 18 U 7243/19, juris Rn. 62), oder ein solcher Anspruch folgt mit Blick auf die unrechtmäßige Datenverarbeitung seitens der Beklagten aus Art. 17 Abs. 1 lit. d DS-GVO, falls man annimmt, aus dem dort normierten Löschungsrecht lasse sich auch ein Unterlassungsanspruch herleiten (vgl. BGH, Urteil vom 13.12.2022 - VI ZR 60/21 Rn. 10; zum Ganzen auch: OLG Frankfurt, Urteil vom 14.04.2022 - 3 U 21/20, GRUR-RS 2022, 10537).

Die Beklagte hat – wie oben festgestellt –gegen Art. 25 Abs. 2 DS-GVO verstoßen. Dieser Verstoß gibt dem Kläger einen darauf bezogenen Anspruch auf Beseitigung und künftige Unterlassung.

a) Daher kann der Kläger verlangen, dass die Beklagte es unterlässt, personenbezogenen Daten – im Einzelnen: Telefonnummer, FacebookID, Name, Vorname und Geschlecht – unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsvorkehrungen vorzusehen.

   Die weiteren Daten „Beziehungsstatus“, „Stadt“, „Land“ und „Bundesland“ sind hiervon ausgenommen, weil nach dem Vortrag des Klägers diese Daten nicht durch den Scraping-Vorfall bei ihm abgeschöpft wurden und somit auch nicht Teil der Datenveröffentlichung im Internet geworden sind. Insofern war die Klage teilweise abzuweisen.

b) In gleicher Weise kann der Kläger beanspruchen, dass die Beklagte es unterlässt, dass seine Mobilfunknummer durch Verwendung des Contact-Import-Tools verwendet werden kann, es sei denn, es wird ausdrücklich und aktiv die Einwilligung hierzu erteilt. Dieses begründete Begehren ist nach sachgerechtem Verständnis – unter Berücksichtigung der Klagebegründung und auch der mündlichen Anhörung im Termin – vom Klageantrag Ziff. 3.b) umfasst.

c) Ein weitergehender Unterlassungsanspruch besteht hingegen nicht, weshalb der Unterlassungsanspruch auch aus diesem Grunde teilweise unbegründet ist.

d) Soweit die Beklagte darauf verweist, dass der Kläger durch eine Änderung der Einstellungen auf der Facebook-Plattform die von ihm gewünschte Rechtsfolge erreichen kann, steht dies Unterlassungsansprüchen des Klägers nicht entgegen. Durch mögliche, vom Kläger selbst vorzunehmende Änderungen von Einstellungen in seinem Facebook-Profil ist eine Wiederholungsgefahr nicht entfallen, und der Kläger kann grundsätzlich Unterlassung jeder einmal getätigten rechtswidrigen Datenverarbeitung verlangen. Denn im Fall eines rechtswidrigen Eingriffs

in ein geschütztes Rechtsgut des Betroffenen besteht nach ständiger Rechtsprechung des Bundesgerichtshofs eine tatsächliche Vermutung für das Vorliegen der Wiederholungsgefahr (so auch LG Stuttgart, Urteil vom 26.01.2023 – 53 O 95/22, BeckRS 2023, 1098). An eine Entkräftung der Vermutung sind strenge Anforderungen zu stellen, im Regelfall bedarf es hierfür der – hier nicht vorliegenden – Abgabe einer strafbewehrten Unterlassungsverpflichtungserklärung gegenüber dem Gläubiger. Die Ordnungsmittelandrohung folgt aus § 890 ZPO.

IV. Auskunft

Der Auskunftsanspruch nach Art. 15 DSGVO besteht nicht. Die Beklagte hat einen solchen Auskunftsanspruch bereits vorgerichtlich und überdies – diese ergänzend und vertiefend – auch durch die Sachangaben im gegenständlichen Verfahren (z.B. Schriftsatz vom 15.02.2023, dort S. 7 ff., 16 ff.) erfüllt.

Der Kläger hatte sich mit Schreiben seines Prozessbevollmächtigten vom 4.10.2021 an die Beklagte gewandt und konkrete Fragen formuliert, hinsichtlich derer er eine Erklärung der Beklagten wünsche. Diese betreffen ausschließlich die abhanden gekommenen - gescrapten- personenbezogenen Daten und nicht die Frage, über welche personenbezogenen Daten die Beklagte überhaupt verfügt. Dieses Auskunftsverlangen, das sich aus Art. 15 DS-GVO ableiten lässt, hat die Beklagte mit ihrem Schreiben vom 28.10.2021 (Anlage B16) erfüllt. Eine Erfüllung ist dann anzunehmen, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen (vgl. nur BGH, Urteil vom 03.09.2020 - III ZR 136/18 Rn. 43). Die Beklagte hat mitgeteilt, dass sie eine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthielten, nicht habe. Auf Grundlage der bislang vorgenommenen Analysen sei es ihr jedoch gelungen, der Nutzer-ID des Klägers die folgenden Datenkategorien zuzuordnen, die nach ihrem Verständnis in den durch Scraping abgerufenen Daten erschienen und mit den auf dem Facebook-Profil des Klägers verfügbaren Informationen übereinstimmten: Nutzer-ID, Vorname, Nachname, Land, Geschlecht. Dagegen sei die Telefonnummer „nach unserem Verständnis in den durch Scraping abgerufenen Daten enthalten“. Zudem hat die Beklagte erläutert, wie das Daten-Scraping erfolgte. Damit hat die Beklagte zum Ausdruck gebracht, dass sie die von ihr geschuldeten Angaben mitgeteilt hat.

V. Die vorgerichtlichen Rechtsanwaltskosten sind als Teil des zu ersetzenden Schadens gem. Art. 82 Abs. 1 DSGVO zu erstatten. Aufgrund der Schwierigkeit der Sach- und Rechtslage war die Hinzuziehung eines Rechtsanwalts zur effektiven Durchsetzung der klägerischen Ansprüche erforderlich und notwendig. Ausgehend von einem Wert des berechtigten Verlangens des

Klägers von bis zu 1.000,00 € zum Zeitpunkt der außergerichtlichen Tätigkeit – diese bezog sich auf die Geltendmachung eines Schadensersatzes in Höhe von 500,00 € und das Auskunftsbegehren, vgl. Anlage K1 – ergibt dies Kosten in Höhe von 159,94 € (1,3-fache Geschäftsgebühr nebst Pauschale nach Nr. 7002 VV RVG zzgl. 19% MwSt.). Der Zinsanspruch folgt aus §§ 288, 291 BGB.

VI. Die Kostenentscheidung beruht auf § 92 ZPO. Verteilungsmaßstab für die Entscheidung nach § 92 Abs. 1 ZPO ist der Gebührenstreitwert, der wiederum vom Streitgegenstand abhängt (vgl. Herget, in: Zöller, Zivilprozessordnung, 34. Aufl. 2022, § 92 Rn. 2). Ausgehend von einem Gesamtstreitwert von 7.000 € obsiegt der Kläger mit einem Anteil von 4.800 €, nämlich hinsichtlich des Klageantrags Ziff. 1 mit 300 €, hinsichtlich des Klageantrags Ziff. 2 mit 500 €, hinsichtlich des Klageantrags Ziff. 3 mit 4.000 € und hinsichtlich des Klageantrags Ziff. 4 mit 0 €. Dies entspricht einem Obsiegen im tenorierten Verhältnis (4.800/7.000).

VII. Die Entscheidung hinsichtlich der Vollstreckbarkeit stützt sich für den Kläger auf §§ 709 Satz 1 ZPO, für die Beklagte auf §§ 708 Nr. 11, 711 ZPO.

Richter am Landgericht