Aktenzeichen:
6 O 40/23

Landgericht Heidelberg

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.LEGAL**, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Ltd., vertreten durch d. Mitglieder des Board of Directors, Merrion Road, Dublin 4, D04 X2K5, Irland
- Beklagte -

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB**, Josephsplatz 1, 90403 Nürnberg, Gz.:

wegen Persönlichkeitsverletzung u.a.

hat das Landgericht Heidelberg - 6. Zivilkammer - durch die Vorsitzende Richterin am Landgericht als Einzelrichterin aufgrund der mündlichen Verhandlung vom 15.03.2024 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 300,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 01.11.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle weiteren materiellen und immateriellen Schäden zu ersetzen, die dieser durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahr 2019 entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, 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, 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, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 367,23 € zuzüglich Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 01.11.2023 zu zahlen.

5. Im Übrigen wird die Klage abgewiesen.

6. Von den Kosten des Rechtsstreits tragen der Kläger 54 % und die Beklagte 46 %.

7. Das Urteil ist vorläufig vollstreckbar, für den Kläger hinsichtlich Ziffer 3 aber nur gegen Sicherheitsleistung in Höhe von 2000 €. Im Übrigen wird der Beklagten nachgelassen, die Vollstreckung durch den Kläger gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet. Dem Kläger wird nachgelassen, die Vollstreckung durch die Beklagte gegen Sicherheitsleistung in Höhe von 110 % des auf Grund des Urteils vollstreckbaren Betrages abzuwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des jeweils zu vollstreckenden Betrages leistet.

Beschluss

Der Streitwert wird auf 6.000,00 € festgesetzt.

Tatbestand

Der Kläger macht gegen die Beklagte einen Schadensersatzanspruch sowie Unterlassungs- und Auskunftsansprüche wegen unzureichenden Schutzes von persönlichen Daten geltend.

Die Beklagte bietet für Nutzer in der Europäischen Union die Social Media Plattform Facebook an, auf die sowohl über die Internetseite www.facebook.com als auch über eine gleichnamige App mittels Smartphone oder Tablet zugegriffen werden kann. Der Kläger ist Nutzer dieser Plattform. Bei der Anmeldung muss ein Nutzer bestimmte persönliche Daten angeben, u. a. Name, Vorname und Geschlecht.

Ein Nutzer kann bezüglich seiner persönlichen Daten zwei Arten von Privatsphäre-Einstellungen vornehmen: In der Zielgruppenauswahl kann der Nutzer festlegen, wer ein bestimmtes Datenelement in seinem Facebook-Profil sehen kann. Dabei sind sein Name und sein Geschlecht nach den Vorgaben der Beklagten immer und vom Nutzer nicht veränderbar „öffentlich“. Zwischen den Parteien streitig ist, ob auch die Facebook-ID immer öffentlich ist. Im Hilfebereich von Facebook ist erläutert, was öffentlich heißt, nämlich, dass alle Facebook-Nutzer und alle Nicht-Facebook-Nutzer diese Daten sehen können. Die Angabe der Telefonnummer ist fakultativ. Entschied sich ein Nutzer vor Mai 2019 zur Angabe seiner Telefonnummer, war insoweit die Zielgruppenauswahl von der Beklagten nach deren Vortrag auf „Freunde“ voreingestellt nach dem Vortrag des Klägers so, dass nur er seine Nummer sehen konnte. Daneben kann ein Nutzer, der seine Telefonnummer angegeben hat, Suchbarkeitseinstellungen vornehmen und festlegen, wer sein Facebook-Profil anhand seiner Telefonnummer finden können soll, um z. B. eine Freundschaftsanfrage zu stellen. Dabei war von der Beklagten die Voreinstellung „alle“ vorgenommen worden. Zudem stellte und stellt die Beklagte ein Kontakt Import Tool (CIT) zur Verfügung, mit dessen Hilfe die Nutzer ihre Kontakte von ihren Mobilgeräten auf Facebook hochladen konnten, um diese Kontakte

auf der Facebook-Plattform zu finden.

Im April 2021 wurde bekannt, dass Daten von 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet waren. Zugrunde lag ein sogenannter „Scraping“-Vorfall. Scraping ist das Sammeln von im Internet öffentlich zugänglichen Daten im großen Stil mittels Softwareprogrammen oder automatisierten Tools. Diese Art der Datensammlung ist nach den Nutzungsbedingungen der Beklagten verboten. Zwischen Januar 2018 und September 2019 wurden auf diese Weise persönliche Daten von Facebook-Nutzern gesammelt.

Auf einer allgemein zugänglichen Seite im Darknet waren nach dem Vortrag des Klägers folgende Daten des Klägers veröffentlicht:

Dabei soll es sich um die Telefonnummer, die Facebook-ID, den Vornamen, den Namen, und das Geschlecht des Klägers handeln

Der Kläger hat sich mit Schreiben vom 21.03.2023 an die Beklagte gewandt und Schadensersatz- und Unterlassungsansprüche geltend gemacht. Die Beklagte antwortete mit Schreiben vom 19.04.2023 (Anlage B 16) u. a., dass sie keine Kopie der gescrapten Daten des Klägers vorhalte und dass betroffene Daten des Klägers aber nach ihren Feststellungen Nutzer-ID, Vorname, Nachname, Land und Geschlecht sein könnten.

Der Kläger ist der Ansicht, die Privatsphäreeinstellungen auf der Plattform Facebook seien intransparent und unübersichtlich gestaltet und verstießen daher gegen Art. 13 DSGVO. Zudem seien die Voreinstellungen entgegen Art. 25 Abs. 2 DSGVO nicht nutzerfreundlich gewählt. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere.

Er behauptet, die Beklagte nehme keine ausreichenden Sicherheitsvorkehrungen gegen die Ausnutzung des Kontakt Import Tools und das Vorgehen mittels „Scraping“ vor, was einen Verstoß gegen Artt. 24, 32 DSGVO darstelle. Es würden keine Sicherheits-Captchas verwendet, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handele. Eben-

so wenig werde ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse auf einmal geblockt würden oder Adressbücher mit auffälligen Telefonnummerabfolgen automatisch abgelehnt würden. Dadurch sei es denkbar einfach, das System für kriminelle Zwecke zu missbrauchen.

Ferner lägen Verstöße gegen Art. 15 DSGVO (Auskunftspflicht) und Artt. 33, 34 DSGVO (Meldepflicht bei der Aufsichtsbehörde sowie Informationspflicht der Betroffenen) vor.

Der Kläger behauptet schließlich, er habe durch das Scraping und die Veröffentlichung seiner personenbezogenen Daten einen erheblichen Kontrollverlust über diese erlitten und verbleibe in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Seit April 2021 erhalte er vermehrt dubiose Nachrichten und Emails.

Der Kläger beantragt:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit 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 Meiclung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, Facebook ID,

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

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

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

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

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, ein Verstoß gegen die DSGVO liege nicht vor. Zunächst biete sie in ausreichendem Umfang Informationen über die bei ihr gespeicherten Daten an. Sowohl im Privatsphärecheck als auch im Hilfebereich würden die Nutzer eingehend über die Verwendung ihrer Daten aufgeklärt.

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 Beklagte trägt vor, sie habe die persönlichen Daten des Klägers ausreichend vor Scraping geschützt. Einen internationalen Schutzstandard gebe es dafür nicht. Im Einklang mit der üblichen Praxis habe die Beklagte während des relevanten Zeitraums sowohl über Übertragungsbegrenzungen als auch über eine Bot-Erkennung verfügt. Sie habe ihre Maßnahmen zudem zur Verringerung von Scraping und als Reaktion auf sich ständig ändernde Bedrohungen fortlaufend weiterentwickelt. Sie beschäftige sogar ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping (konkret das External Data Misuse-Team, EDM-Team). Das EDM-Team solle Scraping-Aktivitäten erkennen, unterbrechen und, soweit möglich, verhindern. Die Experten der Beklagten täten dies beispielsweise, indem sie Aktivitätsmuster und Verhaltensweisen, die typischerweise mit automatisierten Computeraktivitäten in Zusammenhang stünden, identifizierten. Die Beklagte gehe grundsätzlich auch mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor. Es sei jedoch nicht möglich, das Scraping von Daten, welche Nutzer öffentlich zugänglich gemacht hätten, zu einhundert Prozent auszuschließen, noch könne dies von der Beklagten verlangt werden.

Die Beklagte bestreitet den Eintritt eines relevanten Schadens. Eine über eine unterstellte Pflichtverletzung der Beklagten hinausgehende Beeinträchtigung des Klägers sei nicht feststellbar. Art. 82 DSGVO sei im Übrigen schon gar nicht anwendbar, weil er nur Fehler bei der Datenverarbeitung umfasse, die hier nicht betroffen sei.

Die Beklagte bestreitet weiter einen kausalen Zusammenhang zwischen einem fraglichen

Verstoß gegen die DSGVO und dem behaupteten Schaden, Art. 82 Abs. 1 DSGVO. Hinsichtlich der behaupteten Verstöße gegen Art. 34, 33 und 15 DSGVO 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 DSGVO 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.

Wegen der Einzelheiten des Parteivorbringens wird auf den Inhalt der gewechselten Schriftsätze nebst Anlagen sowie das Protokoll der mündlichen Verhandlung vom 15.03.2024 Bezug genommen.

Entscheidungsgründe

A. Die Klage ist zulässig.

I. Die internationale Zuständigkeit der deutschen Gerichte ergibt sich aus Art. 79 Abs. 2 Satz 2 DSGVO.

II. Die Klageanträge sind hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

a) Klageantrag Ziffer 1 enthält keine unzulässige alternative Klagenhäufung. Dem Antrag liegt ein einheitlicher Lebenssachverhalt zugrunde. Der Kläger behauptet hierzu mehrere Handlungen bzw. Unterlassungen der Beklagten, welche Datenschutzverstöße begründen könnten. Es kann dahinstehen, ob diese jede für sich oder nur im Zusammenspiel geeignet sein sollen, den vom Kläger geltend gemachten Anspruch zu tragen. Dass diese Vorgänge in einem Alternativverhältnis stehen sollen oder lediglich alternativ für einen etwaigen Schaden des Klägers verantwortlich sein sollen, ergibt sich jedenfalls aus dem klägerischen Vortrag nicht.

Dass die Leistungsklage nicht beziffert, sondern nur mit einem Mindestbetrag versehen ist, ist vor dem Hintergrund der Regelung des Art. 82 Abs. 1 DSGVO, nach der ausdrücklich immaterieller Schadensersatz verlangt werden kann, ebenfalls zulässig (vgl. BeckOK DatenschutzR/Quaas, 42. Ed., Art. 82 DSGVO Rn. 31; BGH NJW 2002, 3769).

b) Der Feststellungsantrag ist auch hinreichend bestimmt. Wie bei einer Leistungsklage muss zur Individualisierung des Anspruchs der Anspruchsgrund bereits im Antrag so konkret benannt werden, dass der Umfang der Rechtshängigkeit und der Rechtskraft feststehen (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 253 Rn. 72). Bei Ansprüchen auf Schadensersatz ist eine bestimmte Bezeichnung des zum Ersatz verpflichtenden Ereignisses erforderlich (BGH, Urteil vom 10.01.1983 - VIII ZR 231/81- NJW 1983, 2247, 2250). Zur Ermittlung des Klagebegehrens ist jedoch nicht allein auf den Antrag selbst abzustellen, Der Scraping-Vorfall mit der Veröffentlichung persönlicher Daten des Klägers im Internet ist im Klägervortrag klar umrissen. Soweit der Kläger auf Schäden abstellt, die bereits entstanden sind und die damit im Rahmen des Leistungsantrags zu berücksichtigen sind, ergibt sich daraus, dass der Feststellungsantrag weiterhin künftig entstehende Schäden enthält, dass der Kläger jedenfalls Schäden meint, die noch nicht von dem Leistungsantrag umfasst sind. Das können bezüglich bereits entstandener Schäden sowohl materielle Schäden sein, als auch immaterielle Schäden, die noch nicht bekannt sind.

Weiterhin liegt ein Feststellungsinteresse gemäß § 256 Abs. 1 ZPO vor. Ein Feststellungsinteresse besteht bereits dann, wenn die Schadensentwicklung noch nicht gänzlich abgeschlossen und der Kläger aus diesem Grund nicht im Stande ist, seinen Anspruch deshalb ganz oder teilweise zu beziffern. Das Feststellungsinteresse ist nur dann zu verneinen, wenn aus der Sicht des Geschädigten keinerlei Besorgnis besteht, zumindest mit dem Eintritt eines Schadens zu rechnen (BGH, Beschluss vom 09.01.2007 –VI ZR 133/06). Ein derartiger Zustand besteht hier nicht. Der Kläger, der erst seit 2021 weiß, dass seine Daten im Darknet veröffentlicht worden sind, hat keinerlei Überblick darüber, ob und wer diese Daten schon zu welchen, gegebenenfalls auch illegalen Zwecken, genutzt hat oder dies in Zukunft noch tun wird. Angesichts dieses offenen Zustands kann dem Kläger ein Feststellungsinteresse nicht abgesprochen werden.

c) Auch der Unterlassungsantrag Ziffer 3 a ist hinreichend bestimmt. Ein Verbotsantrag darf nicht derart undeutlich gefasst sein, dass Gegenstand und Umfang der Entscheidungsbe-

fugnis des Gerichts (§ 308 Abs. 1 ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und letztlich die Entscheidung darüber, was dem Beklagten verboten ist, dem Vollstreckungsgericht überlassen bliebe (BGH, Urteil vom 06.10.2011 – I ZR 54/10 – juris Tz. 9). Die Verwendung auslegungsbedürftiger Rechtsbegriffe ist daher nur zulässig, wenn entweder über den Sinngehalt der verwendeten Begriffe kein Zweifel besteht oder wenn zum Verständnis des Begriffs auf die konkrete Verletzungshandlung und die gegebene Klagebegründung zurückgegriffen werden kann (BGH, aaO, juris Tz. 11). Weiterhin kann eine auslegungsbedürftige Antragsformulierung hinzunehmen sein, wenn eine weitere Konkretisierung nicht möglich ist und die Antragsformulierung zur Gewährung effektiven Rechtsschutzes im Hinblick auf eine bestimmte Geschäftspraxis erforderlich erscheint (BGH, aaO, juris Tz. 15). Der Verbotsantrag Ziffer 3 a gründet zwar auf dem unbestimmten Rechts- /Tatsachenbegriff der „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“. Nachdem der Kläger jedoch selbst kein IT-Spezialist ist, ist es ihm nicht möglich, die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen konkret zu umschreiben. Zudem sind diese einer Entwicklung ausgesetzt, der der Klageantrag nur durch eine offene Formulierung begegnen kann, sonst müsste bei jeder technischen Neuerung eine neue Klage erhoben werden. Schließlich kann der Kläger auch – wie bei Unterlassungsanträgen üblich - keine konkrete Verletzungshandlung nennen, weil die Beklagte den von ihr tatsächlich gebotenen Sicherheitsstandard nicht preisgibt. Welche Schutzmechanismen sie konkret installiert hat, hat sie nicht offengelegt, so dass zur Gewährung effektiven Rechtsschutzes nur ein Klageantrag mit ausfüllungsbedürftigen Begriffen in Betracht kommt.

d) Klageantrag Ziffer 3 b ist ebenfalls hinreichend bestimmt.

aa) Zwar sind die Begriffe „unübersichtliche und unvollständige Informationen“ auslegungsbedürftig. Diese auslegungsbedürftigen Begriffe werden jedoch hinreichend konkret umschrieben und mit Beispielen unterlegt bzw. das Begehren an der konkreten Verletzungshandlung ausgerichtet (BGH GRUR 2021, 1425 Rn. 12 – Vertragsdokumentengenerator, mwN; BGH, GRUR 2022, 1308 Rn. 26) durch den Zusatz „namentlich ohne eindeutige Informationen darüber, dass die Telefonnummern auch bei der Einstellung „privat“ noch durch die Verwendung des Kontaktimporttools verwendet werden kann…“.

bb) Dem Antrag ist auch nicht mit der Begründung das Rechtsschutzinteresse zu versagen,

dass die Klagepartei die Nummer in ihrem Facebookprofil löschen könnte. Denn solange die Beklagte die Möglichkeit zur Angabe der Telefonnummer eröffnet und diese dann verarbeitet, darf der Kunde dies auch wahrnehmen und hat dann einen Anspruch darauf, dass die Beklagte die Anforderungen der DSGVO – die vorliegend gerade streitgegenständlich sind – bei der Verarbeitung dieser Daten einhält (LG Freiburg, Urteil vom 15.09.2023 - 8 O 21/23 - juris Tz. 76).

B. Die Klage ist in der Sache teilweise begründet.

I. Der Kläger hat gegen die Beklagte einen Anspruch auf Schadensersatz aus Art. 82 Abs. 1 DSGVO. Danach 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. Dabei ist ein weiter Rahmen der Vorschriften, deren Verstoß einen Schadensersatzanspruch nach sich ziehen kann, zugrunde zu lagen. Es kommen materielle wie formelle Verstöße in Betracht. Auch ist nicht allein auf die Datenverarbeitung abzustellen, sondern sämtliche Maßnahmen, so auch Vorbereitungsmaßnahmen, können einen entsprechenden Anspruch begründen (OLG Köln, Urteil vom 14. Juli 2022 – I-15 U 137/21 –, Rn. 24; Frenzel in Paal/Pauly, DSGVO/BDSG, 3. Aufl. 2021, Art. 82 DSGVO Rn. 8).

1. Die Beklagte ist Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO für die Erhebung, Speicherung und Nutzung der persönlichen Daten des Klägers.

2. Die Beklagte hat gegen Art. 25 Abs. 2 DSGVO verstoßen. Nach dieser Vorschrift 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. Nach Satz 3 soll insbesondere sichergestellt werden, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Anzahlt von natürlichen Personen zugänglich gemacht werden. Daraus ergibt sich, dass persönliche Daten eines Nutzers anderen Nutzern nur zugänglich gemacht werden dürfen, wenn dies von dem jeweiligen Nutzer in den Privatsphäreeinstellungen selbsttätig so eingestellt worden ist. Nur

für den Fall, dass der Verarbeitungszweck ohne eine bestimmte Voreinstellung nicht erreicht werden kann, darf durch den Verantwortlichen eine Datenverarbeitung durch Voreinstellungen erfolgen. Für alle anderen Daten darf eine Datenverarbeitung durch Voreinstellung nicht erfolgen (vgl. Hartung in Kühling/Buchner, DSGVO – BDSG, 3. Auflage, Art. 25 DSGVO Rn. 26; Nolte/Werkmeister in Gola/Heckmann, DSGVO – BDSG, 3. Aufl., Art. 25 DSGVO Rn. 28).

Diesen Grundsätzen genügt die Handhabung der Voreinstellungen durch die Beklagte nicht.

a) Dies gilt zunächst für die zwingend öffentlich einsehbaren Daten Name, Vorname und Geschlecht. Es ist nicht ersichtlich, dass jedenfalls das Geschlecht der Nutzer im Hinblick auf die Zwecke der Verarbeitung öffentlich einsehbar sein müsste. Art. 5 Abs. 1 lit. b DSGVO lässt grundsätzlich auch eine gewillkürte Zweckbestimmung des Verantwortlichen zu. Die Beklagte beruft sich insoweit darauf, dass Sinn und Zweck der Facebook-Plattform die kommunikative Verbindung der Welt sei und es deshalb im Interesse der Nutzer sei, dass sie mit ihren persönlichen Daten öffentlich auffindbar sind. Dabei mag es notwendig sein, den jeweiligen Nutzernamen zu kennen, um mit ihm in Kontakt treten zu können. Für eine Kontaktaufnahme nicht erforderlich ist jedoch die Kenntnis des Geschlechts des Nutzers. Dies ist eine Information über sich selbst, die jeder Nutzer – soweit er sie nicht bereit im Vorfeld selbst öffentlich zugänglich gemacht hat - im Rahmen einer aufgenommenen Kommunikation nach seiner eigenen Entscheidung preisgeben oder geheim halten können muss.

b) Auch die Voreinstellung in den Suchbarkeitseinstellungen, dass über die Telefonnummer eines Nutzers jeder beliebige andere Nutzer oder Nichtnutzer feststellen konnte, ob eine Person mit dieser Telefonnummer einen Facebook-Account hat, ist nicht mit Art. 25 Abs. 2 DSGVO vereinbar (Voreinstellung auf „alle“). Vielmehr ergibt sich gerade daraus, dass die Telefonnummer in den Zielgruppeneinstellungen auf eine andere Einstellung als „öffentlich“ gestellt werden konnte, dass ein von der Beklagten anerkanntes Interesse der Nutzer daran bestand, dass ihre Telefonnummer nicht für jedermann einsehbar war. Dieses Interesse wurde durch die Suchbarkeit eines Nutzers über seine Telefonnummer aufgehoben, weil darüber von jedermann eine Verknüpfung einer Telefonnummer mit einem Facebook-Nutzer ermöglicht wurde.

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

a) Nachdem die Beklagte ein Kontakt-Import-Tool (CIT) angeboten hat, gleichzeitig bestimmte Daten ihrer Nutzer für jede beliebige Person einsehbar waren und die Technik des Scrapings ein bekanntes Phänomen war, war die Beklagte zum Schutz der Daten ihrer Nutzer verpflichtet. Zwar kann, wie die Beklagte zu Recht ausführt, nicht aus dem erfolgten Scraping-Vorfall automatisch darauf geschlossen werden, dass die Beklagte Schutzpflichten verletzt hätte. Angesichts der beschriebenen Konstellation mit CIT, immer öffentlichen Daten und Bekanntheit des Scrapings lag die Möglichkeit, dass über das CIT Daten von Nutzern zusammengeführt werden konnten, die die Nutzer nicht zusammengeführt haben wollten, auf der Hand. Dass diese Gefahr der Beklagten bewusst war, ergibt sich bereits daraus, dass Scraping nach ihren Nutzungsbedingungen verboten war.

b) Die Beklagte hat nicht schlüssig vorgetragen, dass sie die Daten des Klägers in einem den Kriterien des Art. 32 Abs. 1 DSGVO entsprechenden Umfang – die ihr einen gewissen Beurteilungsspielraum einräumen - geschützt hätte. Unabhängig davon, ob Art. 5 Abs. 2 DSGVO zu einer Beweislastumkehr führt (so Pötters in Gola/Heckmann, DSGVO – BDSG, 3. Auflage 2022, Art. 5 DSGVO Rn. 35; EuGH, Urteil vom 24. Februar 2022— C-175/20 - juris Tz. 81), fordert diese Vorschrift jedenfalls von dem Verantwortlichen Rechenschaft über die von ihm getroffenen Maßnahmen u. a. zum Schutz personenbezogener Daten vor unbefugter oder unrechtmäßiger Verarbeitung (Art. 5 Abs. 1 lit. f DSGVO). Der Verantwortliche muss also zumindest darlegen, welche konkreten Maßnahmen er zum Schutz der von ihm verarbeiteten Daten getroffen hat. Die Beklagte hat jedenfalls persönliche Daten ihrer Nutzer erhoben und gespeichert und damit verarbeitet. Zu den getroffenen Schutzmaßnahmen vor einem nach ihren Nutzungsbedingungen unbefugten Scraping hat sie sich jedoch nur so vage geäußert, dass eine Beweisaufnahme darüber nicht möglich ist. Die Beklagte trägt vor, sie habe Übertragungsbeschränkungen vorgenommen, 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. Diese Aussage ist absolut allgemein gehalten und definiert den Begriff der Übertragungsbeschränkung, ohne konkret anzugeben, in welchem Umfang die Beklagte Übertragungsbeschränkungen vorgenommen hat. Bezüglich der weiteren Schutzmaßnahme der Bot-Erkennungen hat die Beklagte ebenfalls nur allgemein ausgeführt, dass sie eine Bot-Erkennung hatte und Captchas eingesetzt hat. Der Umfang der Maßnahme bleibt ebenfalls offen. Anhand dieser Ausführungen kann nicht geprüft werden, ob unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete Maßnahmen zum Schutz von deren persönlichen Daten getroffen wurden. Dies geht zu Lasten der dafür darlegungspflichtigen Beklagten, so dass von einem nicht ausreichenden Schutzniveau ausgegangen werden muss.

4. Schließlich hat die Beklagte auch gegen ihre Informationspflichten aus Art. 13 DSGVO verstoßen, und zwar gegen die gemäß Art. 13 Abs. 1 lit. c DSGVO bestehende Informationspflicht bei Erhebung von personenbezogenen Daten, indem sie den Kläger bei der Anmeldung auf der Facebook-Plattform nicht ausreichend über die Zwecke, für die seine Telefonnummer verwendet werden sollte, informiert hat. Nach dieser Vorschrift muss der Verantwortliche dem Betroffenen zum Zeitpunkt der Erhebung der Daten die Zwecke mitteilen, für die personenbezogene Daten verarbeitet werden sollen. Die Informationspflicht aus Art. 13 DSGVO soll die betroffenen Personen von Beginn an in die Lage versetzen, bestimmen und einschätzen zu können, wer was wann über sie weiß (Sydow/Marsch DSGVO/BDSG/Ingold, 3. Aufl. 2022, DSGVO Art. 13 Rn. 8). Genau das ist auch nach dem Vortrag der Beklagten bezüglich der Telefonnummern der Facebook-Nutzer nicht geschehen. Die Nutzer konnten fakultativ ihre Telefonnummer angeben und in der Zielgruppeneinstellung darüber entscheiden, welcher Personenkreis die Telefonnummer sehen können sollte. Weiterhin konnten sie darüber entscheiden, wer sie über ihre Telefonnummer bei Facebook finden können sollte. Beide Einstellungen konnten im Privatsphärebereich vorgenommen werden. Bei Vornahme dieser Einstellungen wurden die Nutzer aber nicht darüber informiert, wie ihre Telefonnummer im Rahmen des CIT verwendet wird, insbesondere nicht darüber, dass bei der unveränderten Voreinstellung „alle“ eine in der Zielgruppeneinstellung

angestrebte Privatheit der Telefonnummer nicht garantiert war. Dazu hätte den Nutzern erläutert werden müssen, dass damit jedermann, der vom Nutzer gewollt oder ungewollt im Besitz seiner Telefonnummer ist, allein über diese Telefonnummer auf sein öffentliches Facebook-Profil zugreifen und sich als Freund hinzufügen kann. Soweit die Beklagte auf ihre verlinkte und damit erreichbare Datenrichtlinie verweist, ist eine entsprechende Information dort nicht auffindbar. Zwar könnte ein sehr weit denkender Nutzer eventuell selbst derartige Überlegungen zu Datenverknüpfungen anstellen. Sinn und Zweck des Art. 13 Abs. 1 DSGVO ist es aber, dem Durchschnittsnutzer die nötigen Informationen klar und deutlich zur Verfügung zu stellen. Daran fehlt es hier.

5. Ob zudem Verstöße gegen Artt. 33 und 34 DSGVO sowie Art. 15 DSGVO vorliegen, ist unerheblich, weil weder eine ordnungsgemäße Meldung der Verstöße an die Aufsichtsbehörde noch eine frühzeitige Auskunft einen bereits eingetretenen Schaden des Klägers gemindert hätten. Vortrag dazu liegt nicht vor. Derartige Verstöße wären daher nicht kausal für einen Schaden geworden.

6. Der Kläger hat zudem bewiesen, dass er einen Schaden erlitten hat, der auf die Verstöße der Beklagten gegen die DSGVO zurückgeführt werden kann. Das Gericht geht davon aus, dass die Nutzer-ID, der Vorname, der Nachname und das Geschlecht des Klägers zusammen mit seiner Telefonnummer im Internet veröffentlicht worden sind. Der vorgelegte Leak-Datensatz wirkt authentisch. Dass weitergehende Daten veröffentlicht worden sind, hat der Kläger nicht schlüssig dargetan. Insbesondere hat er nichts dazu ausgeführt, ob er weitere Daten, z. B. die E-Mail-Adresse, bei Facebook angegeben und in den Privatsphäreeinstellungen auf „öffentlich“ gestellt hatte.

a) Art. 82 Abs. 1 DSGVO setzt die Entstehung eines Schadens voraus. Bereits nach dem klaren Wortlaut fordert die Vorschrift neben einem Verstoß gegen die DSGVO den Eintritt eines Schadens und die Kausalität zwischen dem Verstoß und dem Schaden, wobei es für den Schaden keine Bagatellgrenze gibt (vgl. EuGH, Urteil vom 04.05.2023 - C 300/21 - NZA 2023, 621, 625).

b) Der Kläger hat einen immateriellen Schaden erlitten. Die Schwelle für die Annahme eines immateriellen Schadens ist dabei relativ gering. Denn Art. 82 Abs. 1 DSGVO unterscheidet nicht danach, ob der infolge eines erwiesenen Verstoßes gegen die Bestimmun-

gen der DSGVO von der betroffenen Person behauptete „immaterielle Schaden“ mit einer zum Zeitpunkt ihres Schadenersatzantrags bereits erfolgten missbräuchlichen Verwendung ihrer personenbezogenen Daten durch Dritte verbunden ist oder ob er mit ihrer Angst verknüpft ist, dass eine solche Verwendung in Zukunft erfolgen könnte. Diese wörtliche Auslegung wird zweitens durch den 146. Erwägungsgrund der DSGVO bestätigt, der speziell den in Art. 82 Abs. 1 DSGVO vorgesehenen Schadenersatzanspruch betrifft und in dessen drittem Satz es heißt, dass „[d]er Begriff des Schadens … im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht.“ Eine Auslegung des Begriffs „immaterieller Schaden“ im Sinne von Art. 82 Abs. 1 DSGVO, die nicht die Fälle umfasst, in denen die von einem Verstoß gegen die DSGVO betroffene Person sich auf die Befürchtung beruft, dass ihre eigenen personenbezogenen Daten in Zukunft missbräuchlich verwendet werden, entspräche jedoch nicht einer weiten Auslegung dieses Begriffs, wie sie vom Unionsgesetzgeber beabsichtigt ist. Zudem heißt es im ersten Satz des 85. Erwägungsgrundes der DSGVO, dass „[e]ine Verletzung des Schutzes personenbezogener Daten …– wenn nicht rechtzeitig und angemessen reagiert wird - einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen [kann], wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder finanzielle Verluste … oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person“. Aus dieser beispielhaften Aufzählung der „Schäden“, die den betroffenen Personen entstehen können, geht hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen „Verlust der Kontrolle“ über ihre eigenen Daten infolge eines Verstoßes gegen die DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte. Drittens und letztens wird diese Auslegung durch die Ziele der DSGVO gestützt, denen die Definition des Begriffs „Schaden“ in vollem Umfang entsprechen muss, wie es im dritten Satz des 146. Erwägungsgrundes der DSGVO heißt. 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 jedoch 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, Urteil vom 14.12.2023, C-340/21, juris Tz. 75 ff.).

c) Es ist allerdings so, 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. 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, aaO, Tz. 84 f.).

d) Diesen Nachweis hat der Kläger geführt. Er hat schriftsätzlich vorgetragen, er sei in einem Zustand großen Unwohlseins und großer Sorge über eine missbräuchliche Verwendung seiner Daten verblieben. Dies habe sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen manifestiert, aber auch in der ständigen Sorge, dass die veröffentlichten Daten von Kriminellen für unlautere Zwecke verwendet werden könnten. Dieser Vortrag hat sich bei der persönlichen Anhörung des Klägers in der mündlichen Verhandlung im Kern bestätigt. Der Kläger hat in seiner persönlichen Anhörung, die gemäß § 286 ZPO auch Grundlage der Überzeugungsbildung des Gerichts ist, ausgeführt, dass er seit April 2021 verstärkt Spam-SMS mit Links erhalten habe. Daraufhin habe er überprüft, ob er von einem Datenleck betroffen sei und habe festgestellt, dass er von dem Datenscraping bei Facebook betroffen sei. Er habe abendende Telefonnummern bei der Bundesnetzagentur gemeldet, damit sie dort gesperrt werden könnten. Seit er von seiner Betroffenheit erfahren habe, sei er in Sorge um die Kontrolle über seine Daten und habe die Befürchtung, dass etwas mit ihnen gemacht werden könne, was nicht in seinem Sinne sei. Er befürchte beispielsweise, dass seine Daten für Vertragsabschlüsse verwendet werden könnten. Diese Sorge hält das Gericht für bewiesen. Der Kläger hat dies nachvollziehbar geschildert und auch nach außen hin gezeigt, dass er in Sorge ist, indem er Nummern von Spam-SMS und -anrufen bei der Bundesnetzagentur gemeldet hat. Unabhängig, davon, ob diese Spam-SMS und -anrufe auf den Scraping-Vorfall zurückzurühren sind, hat er damit die Sorge um den Missbrauch seiner Daten nach dem Scrapingvorfall auch nach außen hin zum Ausdruck gebracht.

e) Der Schaden des Klägers ist auch kausal auf die Verletzung der DSVGO durch die Beklagten zurückzuführen. Wäre der Kläger ohne Verstoß gegen die Informationspflichten nach Art. 13 Abs. 1 lit. c DSGVO ordnungsgemäß darüber aufgeklärt worden, dass seine Telefonnummer im Rahmen des Einsatzes des CIT angesichts der Standardvoreinstellung für die Suchbarkeit über die Telefonnummer auf „alle“ dazu verwendet wird, um ihn auf Facebook zu finden, hätte er seine Telefonnummer nicht eingetragen oder die Standardeinstellungen insoweit verändert. Denn aus seiner persönlichen Anhörung ergibt sich deutlich, dass er an einem Schutz seiner persönlichen Daten sehr interessiert ist. Das Gericht geht auch davon aus, dass der Kläger diese Voreinstellung der Beklagten beibehalten hat. Er hat zwar ausgeführt, er habe über seine Freunde gefunden werden wollen, war sich aber nicht sicher, ob er eine entsprechende Einstellung vorgenommen hatte. Entsprechend hat auch die gegen Art. 25 Abs. 2 DSGVO verstoßende datenschutzunfreundliche Standardvoreinstellung der Suchbarkeit über die Telefonnummer auf „alle“ zur Schadensentstehung beigetragen. Schließlich ist der Schaden auch kausal auf den Verstoß der Beklagten gegen Art. 32 Abs. 1 DS-GVO zurückzuführen, denn durch die unzureichenden Schutzmaßnahmen ermöglichte die Beklagte das missbräuchliche Abgreifen der Daten des Klägers (vgl. LG Heidelberg, Urteil vom 31.03.2023 – 7 O 10/22). d

f) Die Beklagte hat sich nicht nach Art. 82 Abs. 3 DSGVO entlastet.

g) Der von dem Kläger erlittene immaterielle Schaden rechtfertigt eine Geldentschädigung in Höhe von 300,00 €.

aa) Die Höhe des Schadensersatzes im Rahmen des Art. 82 Abs. 1 DSGVO richtet sich nach den innerstaatlichen Vorschriften der einzelnen Mitgliedsstaaten, sofern dabei die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden (EuGH, Urteil vom 04.05.2023 - C 300/21 - NZA 2023, 621, 625).

bb) Art. 82 Abs. 1 DSGVO hat - anders als andere, ebenfalls in Kapitel VIII dieser Verordnung enthaltene Bestimmungen, nämlich die Art. 83 und 84, die im Wesentlichen einen Strafzweck haben, da sie die Verhängung von Geldbußen bzw. anderen Sanktionen erlauben – keine Straf-, sondern eine Ausgleichsfunktion. Da der in Art. 82 Abs. 1 DSGVO vorgesehene Anspruch auf Schadenersatz keine abschreckende oder sogar Straffunktion erfüllt, kann sich die Schwere des Verstoßes gegen diese Verordnung, durch den der betref-

fende Schaden entstanden ist, nicht auf die Höhe des auf der Grundlage dieser Bestimmung gewährten Schadenersatzes auswirken, auch wenn es sich nicht um einen materiellen, sondern um einen immateriellen Schaden handelt (EuGH, Urteil vom 21.12.2023 - C 667/21 - GRUR-RS 2023, 36822, Tz. 84, 86). Abweichend vom deutschen Zivilrecht, in dem das Schmerzensgeld eine Doppelfunktion - einerseits Ausgleichsfunktion und andererseits Genugtuungsfunktion - hat, ist daher bei der Bestimmung der Höhe des Schadens lediglich die Ausgleichsfunktion zu beachten. Dabei ist insbesondere zu berücksichtigen, dass keine sensiblen Daten des Klägers wie Gesundheits- oder Finanzdaten, sondern lediglich Daten, die eine Verknüpfung seiner Person (Vorname, Name, Geschlecht) mit seiner Telefonnummer ermöglichen, abgegriffen und veröffentlicht wurden. Unerwünschte Spam-Nachrichten mit Betrugshintergrund können auch versandt werden, wenn automatisch Telefonnummern generiert werden, die Kenntnis der Identität des Nummerninhabers ist dazu nicht erforderlich. Auszugleichen ist daher die Möglichkeit eines Identitätsdiebstahls durch die Kenntnis des Inhabers einer bestimmten Mobilfunknummer und dessen Facebook-ID. Die Furcht vor einem derartigen Identitätsdiebstahl hat der Kläger real geschildert. Die Möglichkeiten, allein mit der Telefonnummer, der Facebook-ID und dem Namen eine Identität zu fälschen, dürften allerdings eher gering sein. Angesichts des vielfältigen Einsatzes von Mobiltelefonen ist es zudem eine allgegenwärtige Gefahr, dass über Dritte, die diese Nummer befugt kennen, auch Personen von der eigenen Mobilfunknummer Kenntnis erlangen, von denen man es nicht möchte. Vor diesem Hintergrund ist dem Kläger nur ein geringer Schaden entstanden, zu dessen Ausgleich in Betrag von 300,00 € angemessen erscheint.

II. Der Feststellungsantrag ist begründet, soweit er sich auf Zukunftsschäden richtet. Nachdem durch die Verstöße der Beklagten gegen die DSGVO ein absolutes Recht des Klägers, nämlich sein allgemeines Persönlichkeitsrecht, das sowohl über § 823 Abs. 1 BGB als auch auf europäischer Ebene in Art. 8 GrCH geschützt ist, verletzt wurde, genügt für die Begründetheit des Feststellungsantrags die nicht nur abstrakte Möglichkeit des Eintritts weiterer Schäden. Nachdem völlig unklar ist, wer die Daten des Klägers wozu verwendet hat oder verwenden wird, ist sowohl der Eintritt materieller Schäden, z. B. in Form von Schadensfeststellungskosten bei illegaler Datennutzung, als auch der Eintritt künftiger immaterieller Schäden des Klägers aufgrund der unberechtigten Nutzung seiner Daten möglich. Nicht ernsthaft zu rechnen ist dagegen mit bereits eingetretenen noch unbekannten Schäden des Klägers, denn der Kläger hat nach eigener Aussage bereits eine Überprüfung

seiner Passwörter und seines Online-Kontos vorgenommen.

III. Der Unterlassungsantrag Ziffer 3 a ist unbegründet, weil der Kläger Unterlassung in einem Umfang begehrt, auf den er nach der DSGVO keinen Anspruch hat. Art. 32 Abs. 1 DS-GVO verlangt von dem Verantwortlichen, dass er unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen trifft, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Vorschrift verlangt gerade nicht, dass, wie der Kläger es beantragt, der Verantwortliche die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorsieht, sondern gibt weitere Kriterien vor, die bei der Entscheidung über das gewählte Schutzniveau zu berücksichtigen sind und sich nicht einseitig an dem Interesse des Inhabers der Daten an dem technisch maximal möglichen Schutz orientiert.

IV. Der Unterlassungsanspruch 3b ist hingegen begründet, weil die Klagepartei zum einen bereits aus dem mit der Beklagten bestehenden Vertragsbeziehung die Einhaltung der Anforderungen der DSGVO als vertragliche Nebenpflicht verlangen kann. Zudem folgt hier aus dem vergangenen Verstoß gegen Art. 13 Abs. 1c DS-GVO, insbesondere der unbefugten Offenlegung unter Verwendung unzureichender Standardeinstellungen als Verstöße gegen Art. 5 Abs. 1 lit. a DSGVO und Art. 25 Abs. 2 DSGVO ein legitimes Interesse der Klagepartei, der Beklagten für die Zukunft einen kerngleichen Verstoß gegen diese Vorschrift zu verbieten. Es besteht auch Wiederholungsgefahr, weil die Beklagte die Verstöße bestritten hat und weiterhin bestreitet.

Unterlassungsansprüche sind auch unter der Geltung der DSGVO nicht durch deren Vorrang ausgeschlossen. Soweit die DSGVO als solche keinen gesonderten Anspruch auf eine Unterlassung vorsieht, wird der Unterlassungsanspruch teilweise direkt auf Art. 17 Abs. 1 d) DSGVO (BGH, Urteil vom 13. Dezember 2022 – VI ZR 60/21 –, Rn. 10, juris; Urteil vom 27. Juli 2020 – VI ZR 405/18 –, BGHZ 226, 285-310, Rn. 20), teilweise auf § 823 Abs. 2

BGB, § 1004 BGB analog (OLG München, Urteil vom 19. Januar 2021 – 18 U 7243/19 –, Rn. 62, juris) gestützt und sind jedenfalls nach übereinstimmender Ansicht möglich (vgl. (LG Freiburg, Urteil vom 15.09.2023 - 8 O 21/23 - juris Tz. 150).

V. Der Auskunftsanspruch besteht nicht mehr, weil er erfüllt ist. Gemäß Art. 15 Abs. 1 DGVO hat die betroffene Person zwar einen Anspruch auf Auskunft darüber, ob und gegebenenfalls wie ihre personenbezogenen Daten verarbeitet werden. Die Beklagte hat einen solchen Auskunftsanspruch jedoch vorgerichtlich und durch ihren Vortrag im hiesigen Verfahren erfüllt. Soweit der Kläger allgemein Auskunft über seine bei der Beklagten verarbeiteten Daten verlangt, ist der Antrag bereits zu weit gefasst. Welche Daten die Beklagte beim Kläger erhoben hat oder welche Daten der Kläger freiwillig zur Verfügung gestellt hat, weiß er selbst. Soweit es konkret um den Scraping-Sachverhalt geht, den der Kläger zur Konkretisierung des Auskunftsanspruchs genannt hat, ist der Anspruch durch Erfüllung erloschen. 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 mit Schreiben vom 03.03.2023 (B 16) dem Kläger Auskunft darüber erteilt, welche Datenkategorien mittels Scraping bei ihm erlangt worden sein könnten (Nutzer ID, Vorname, Nachname, Geschlecht, Land) und wie der Scraping-Vorfall sich nach dem Verständnis der Beklagten ereignete, nämlich durch die Methode der Telefonnummernaufzählung über das Kontakt-Import-Tool. Nach der Rechtsprechung des EuGH gehört zwar zum Inhalt des Auskunftsanspruchs auch, dass der Verantwortliche eine Kopie der verarbeiteten Daten übermittelt und die Identität der Empfänger der Daten mitteilt (EuGH, Urteil vom 12.01.2023, C-154/21, NJW 2023, 973). Dies gilt allerdings nicht, wenn dem Verantwortlichen die Empfänger nicht bekannt sind (EuGH, aaO). Die Beklagte hat in der mündlichen Verhandlung erklärt, dass ihr die Person der Scraper nicht bekannt seien. Weiterhin hat sie mitgeteilt, keine Kopie der Rohdaten des Klägers vorzuhalten. Damit ist die geforderte Auskunft erteilt.

VI. Der Zinsanspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB.

VII. Der Anspruch auf Erstattung vorgerichtlicher Rechtsanwaltskosten ist Teil des Schadens nach Art. 82 Abs. 1 DSGVO, § 249 BGB. Angesichts der Komplexität des Falles durfte der Kläger die Einschaltung eines Rechtsanwalts für erforderlich halten. Der Zinsanspruch folgt aus §§ 288, 291, 187 Abs. 1 BGB.

C. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO, die Entscheidung über die vorläufige Vollstreckbakreit auf §§ 708 Nr. 11, 709, 711 ZPO. Die Streitwertfestsetzung folgt aus § 3 ZPO (Klageantrag Ziffer 1: 1.000,00 €; Klageantrag Ziffer 2: 500,00 €; Klageantrag Ziffer 3 a und b jeweils 2.000,00 €; Klageantrag Ziffer 4: 500,00 €).

Rechtsbehelfsbelehrung:

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

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

Landgericht Heidelberg
Kurfürsten-Anlage 15
69115 Heidelberg

einzulegen.

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

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

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

Schriftlich einzureichende Anträge und Erklärungen, die durch einen Rechtsanwalt, durch eine Behörde oder durch eine juristische Person des öffentlichen Rechts einschließlich der von ihr zu Erfüllung ihrer öffentlichen

Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind als elektronisches Dokument zu übermitteln. Ist dies aus technischen Gründen vorübergehend nicht möglich, bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig. Die vorübergehende Unmöglichkeit ist bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen; auf Anforderung ist ein elektronisches Dokument nachzureichen.

Vorsitzende Richterin am Landgericht