Aktenzeichen:
9 O 69/23

Landgericht Heilbronn

Im Namen des Volkes

Urteil

In dem Rechtsstreit

- Kläger -

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

gegen

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

Prozessbevollmächtigte:
Rechtsanwälte **Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater Partnergesellschaft mbB**, Bockenheimer Anlage 44, 60322 Frankfurt

wegen Persönlichkeitsrechtsverletzung

hat das Landgericht Heilbronn - 9. Zivilkammer - am 05.04.2024 durch den Vorsitzenden Richter am Landgericht als Einzelrichter aufgrund der mündlichen Verhandlung vom 12.03.2024 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger immateriellen Schadensersatz in Höhe von 250,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 19.07.2023 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, dem Kläger alle weiteren künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, noch entstehen werden.

3. Im Übrigen wird die Klage abgewiesen.

4. Von den Kosten des Rechtsstreits trägt der Kläger 89 % und die Beklagte 11 %.

5. Das Urteil ist vorläufig vollstreckbar. Die Beklagte kann die Vollstreckung des Klägers durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht der Kläger vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet. 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.

6. Der Streitwert wird auf bis zu 7.000,00 € festgesetzt.

Tatbestand

Die Parteien streiten vor dem Hintergrund vom Kläger behaupteter Datenschutzverstöße über das Bestehen von Ansprüchen des Klägers auf Schadensersatz, Unterlassung und Auskunft.

Der Kläger nutzte die von der Beklagten betriebene Social-Media-Plattform facebook.com, insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. Bei der Registrierung müssen die Nutzer zunächst bestimmte Informationen angeben, die als Teil des Nutzerprofils immer öffentlich einsehbar sind. Dazu gehören Name, Geschlecht und Nutzer-ID („immer öffentliche Nutzerinformationen“). Auch der Name und das Geschlecht des Klägers war in dem Zeitraum, in dem das Datenscraping im Rahmen des Scraping-Sachverhalts stattfand, öffentlich auf seinem Facebook-Profil einsehbar. Die Beklagte stellt den Nutzern dann verschiedene Privatsphäre-Einstellungen zur Verfügung, wodurch die

Nutzer bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten. Bei der Zielgruppenauswahl“ legen die Einstellungen fest, wer einzelne Informationen im Facebook-Profil eines Nutzers sehen kann. Dies umfasst Informationen wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-MailAdresse auf dem Profil eines Nutzers. Nicht von der Zielgruppenauswahl umfasst sind die immer öffentlichen Nutzerinformationen, die immer öffentlich einsehbar sind. Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers anhand einer Telefonnummer finden kann, z.B. um sich mit ihm zu vernetzen, indem eine „Freundschaftsanfrage“ gestellt wird. Der Kläger hatte keine Änderungen an der Grundeinstellung der Suchbarkeitseinstellungen vorgenommen, so dass diese für das klägerische Nutzerkonto auf „Alle“ gestellt waren.

Anfang April 2021 wurden durch unbekannte dritte Personen Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern im Internet öffentlich verbreitet, die im Jahre 2019 unter Nutzung der sogenannten Kontakt-Importer-Funktion unter Verwendung von fiktiven Telefonnummern auf den Internetprofilen der Facebook-Nutzer aufgefunden und sodann gescrapt („abgeschöpft“) worden waren. Zu den vom Scrapingsachverhalt betroffenen Personen gehörte auch der Kläger, dessen Daten zumindest in Form von Telefonnummer, Nutzer ID, Vorname, Land und Geschlecht unstreitig vom Scraping erfasst wurden.

Der Kläger trägt vor:

Bei dem betreffenden Vorfall seien bei der Beklagten personenbezogene Daten aus zum Teil öffentlich zugänglichen Daten bei Facebook ausgelesen und persistiert worden. Die Telefonnummern der Benutzer hätten wegen einer Sicherheitslücke bei der Beklagten mit den restlichen Personendaten korreliert werden können, indem ein Programm unzählige Telefonnummern auf ihre Übereinstimmung mit Facebook- Nutzern getestet und im Falle von Treffern sämtliche Daten des Nutzers abgefragt und exportiert habe. Auch vom Kläger seien Daten wie Nachname, Wohnort und Mailadresse abgegriffen worden.

Möglich sei dies nur geworden, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern. Insbesondere wären besonders datenschützende Standardeinstellungen bei der Suchbarkeit und Zielgruppenauswahl geboten gewesen. Demgegenüber könnten - was für sich genommen nicht streitig ist - nach den Voreinstellungen der Beklagten „alle“ Personen den neuen Nutzer über seine E-Mail-Adresse oder Telefonnummer finden und - was von der Beklagten bestritten wird - die gespeicherten Informationen seien standardmäßig „öffentlich“. Selbst in den Fällen, in denen im maßgeblichen Zeitraum

eine Umstellung der Suchbarkeitseinstellungen durch den einzelnen Nutzer erfolgt sei, habe dies keinerlei Auswirkungen auf das Scraping und dessen Umfang gehabt.

Zudem seien pflichtwidrig auch keine Sicherheitscapchas oder andere Sicherungsmaßnahmen ergriffen worden, um zu verhindern, dass durch automatisierte Anfragen Daten abgeschöpft werden.

Auch sei das weitere Verhalten der Beklagten nach Bekanntwerden des Scrapingsachverhaltes zu beanstanden. Die Beklagte habe den Kläger zu keinem Zeitpunkt darüber informiert, dass seine Daten durch Dritte entwendet und veröffentlicht worden seien. Insoweit sei weder eine persönliche Benachrichtigung des Klägers noch eine allgemeine öffentliche Bekanntmachung des Vorfalls erfolgt. Weiterhin habe es die Beklagte unterlassen, die zuständige Datenschutzbehörde Irish Data Protection Commission zu informieren.

Die Beklagte habe gegen zahlreiche Vorschriften der Datenschutzgrundverordnung verstoßen. So habe die Beklagte als Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO im Jahr 2019 die Klägerseite betreffende personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO ohne Rechtsgrundlage im Sinne der Art. 6, 7 DSGVO und ausreichender Informationen im Sinne von Art. 13, 14 DSGVO verarbeitet und damit gegen Art. 4 Nr. 2 DSGVO verstoßen.
Weiterhin habe die Beklagte diese Daten unbefugten Dritten zugänglich gemacht und hierbei die Pflichten aus Art. 5 Abs. lit. a, lit. b, lit. c, lit. f (Grundsätze für die Verarbeitung personenbezogener Daten), 25 Abs. 1, Abs. 2 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), 32 (Sicherheit der Verarbeitung), 34 Abs. 1, Abs. 2 DSGVO (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) verstoßen und die Betroffenenrechte der Klägerseite gemäß Art. 15, 17, 18 DSGVO verletzt.

Durch das Abschöpfen und Veröffentlichen seiner Daten habe der Kläger einen erheblichen Kontrollverlust über seine Daten erlitten und er sei deswegen in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner Daten verblieben. Dies habe sich insbesondere in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen manifestiert. Darüber hinaus habe der Kläger seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail erhalten. Hierdurch sei dem Kläger ein der Beklagten zurechenbarer ersatzfähiger immaterieller Schaden im Sinne des Art. 82 DSGVO entstanden, der die Zahlung eines angemessenen Schadensbetrages rechtfertige.

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 € nebst Zinsen seit Rechtshängigkeit in Höhe von fünf 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 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. personenbezogene 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.

Sie trägt vor:

Die Behauptungen des Klägers beruhten auf einem grundlegenden Missverständnis über den Scraping-Sachverhalt. Das Abschöpfen der Daten sei nicht auf eine Sicherheitsverletzung der Beklagten zurückzuführen. Insbesondere seien die Daten nicht infolge einer Schwachstelle in den Systemen der Beklagten erlangt worden. Vielmehr habe es sich lediglich um ein massenhaftes automatisiertes Sammeln von Daten gehandelt, die sämtlich ohnehin öffentlich einsehbar gewesen seien. Vor diesem Hintergrund sei zu bestreiten, dass die Datenpunkte Nachname, E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt und Beziehungsstatus des Klägers in den durch Scraping abgerufenen Daten enthalten sind. Soweit die in den durch Scraping abgerufenen Daten enthaltenen Informationen vom Facebook-Profil des Klägers stammten, handele es sich entweder um immer öffentliche Nutzerinformationen oder um Daten, die der Kläger in seinem Facebook-Profil öffentlich einsehbar gemacht habe. Es habe dem Kläger freigestanden, wie er die Einstellungen für sein Facebook-Profil gestaltet. Die Standard-Einstellung für die Zielgruppenauswahl sei im relevanten Zeitraum auf „Freunde“ voreingestellt gewesen, d.h. nur Freunde des Nutzers hätten die Telefonnummer auf dem Facebook-Profil des Nutzers sehen können. Da jedoch beim streitgegenständlichen Scrapingfall die Telefonnummern - unstreitig - von den Scrapern bereitgestellt worden seien, sei es ohnehin nicht von Bedeutung gewesen, ob ein Nutzer seine Telefonnummer zu seinem Profil hinzugefügt habe. Bei der Suchbarkeitseinstellung hätten neben der vom Kläger genutzten Option „Alle“ - unstreitig - auch eingeschränktere Einstellungsmöglichkeiten bestanden, worüber die Nutzer in übersichtlicher und verständlicher Weise informiert worden seien.

Die Beklagte habe umfangreiche Anti-Scraping Maßnahmen getroffen und entwickele diese laufend weiter. Dazu gehörten u.a. auch Captchas, so dass der anderslautende Vortrag des Klägers zu bestreiten sei. Dennoch könne hierdurch Scraping nicht völlig verhindert werden.

Auch habe die Beklagte den Nutzern, so auch dem Kläger, spezifische Informationen zum Thema Scraping zur Verfügung gestellt.
Zu einer Benachrichtigung der Aufsichtsbehörde oder des Klägers nach Bekanntwerden des Scrapingsachverhaltes sei die Beklagte nicht von sich aus verpflichtet gewesen, da es zu keiner Verletzung des Schutzes personenbezogener Daten gekommen sei, zumal die gescrapten Daten bereits öffentlich einsehbar gewesen seien. Das klägerische Auskunftsersuchen habe die Beklagte ordnungsgemäß beantwortet.

Zur Zahlung immateriellen Schadensersatzes sei die Beklagte nicht verpflichtet, da dem Kläger ein entsprechender Schaden nicht entstanden sei. Schlichte Unannehmlichkeiten ohne Beeinträchtigung persönlichkeitsrelevanter Belange begründeten keinen immateriellen Schaden. Auch der behauptete Kontrollverlust stelle keinen solchen Schaden dar und wäre dann auch nicht der Beklagten zuzurechnen, da es für jeden Online-Dienstleister technisch unmöglich sei, das Risiko gänzlich auszuschließen, dass Dritte öffentlich zugängliche Daten sammeln und diese an einem anderen Ort verfügbar machen.

Hinsichtlich des weiteren umfangreichen Vorbringens der Parteien wird auf deren Schriftsätze nebst Anlagen sowie das Protokoll zur mündlichen Verhandlung in den Akten Bezug genommen.

In der mündlichen Verhandlung wurde der Kläger ausführlich informatorisch zum Sachverhalt befragt.

Entscheidungsgründe

I.

Die Klage ist zulässig.

1. Die internationale Zuständigkeit deutscher Gerichte ergibt sich insbesondere aus Art. 79 Abs. 2 (VO) 2016/679 (Datenschutz-Grundverordnung, DSGVO).

Danach sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter ei-

ne Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnlichen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Die Beklagte ist Verantwortliche im Sinne der DSGVO; der Kläger hat seinen gewöhnlichen Aufenthaltsort in Deutschland.

2. Art. 79 Abs. 2 DSGVO regelt zugleich die örtliche Zuständigkeit. Hiernach ist das Landgericht Heilbronn örtlich zuständig, nachdem der Kläger seinen Wohnsitz im Gerichtsbezirk des Landgerichts Heilbronn hat.

3. Klageantrag Ziff. 1 ist hinreichend bestimmt gefasst und damit zulässig. Insbesondere wird der Klageantrag nicht auf zwei unterschiedliche Lebenssachverhalte gestützt. Vielmehr macht der Kläger immateriellen Schadensersatz im Hinblick auf einen behaupteten einheitlichen Schaden geltend, der durch verschiedene Handlungen der Beklagten verursacht worden sein soll.

4. Auch Klageantrag Ziff. 2 ist zulässig.

a) Der Antrag kann aufgrund der Klagebegründung dahin verstanden werden, dass sich die Feststellung auf die weiteren, d.h. über die mit Klageantrag Ziff. 1 abgedeckten immateriellen Schäden hinaus künftig entstehenden materiellen und immateriellen Schäden beschränken soll, so dass neben den künftigen materiellen Schäden hiervon nach ständiger höchstrichterlicher Rechtsprechung lediglich die derzeit nicht vorhersehbaren künftigen immateriellen Schäden erfasst werden sollen.

b) Der Kläger macht die Verletzung eines absoluten Rechtsgutes geltend. Hier genügt nach ständiger höchstricherlicher Rechtsprechung für die Annahme eines Feststellungsinteresses die bloße Möglichkeit eines Schadenseintrittes (vgl. BGH, Urteil vom 16.01.2001, VI ZR 381/99 u.a.), wovon im vorliegenden Fall auszugehen ist. Denn es ist nicht ausgeschlossen, dass dem Kläger aufgrund der Veröffentlichung seiner privaten Daten künftig ein weiterer materieller oder derzeit noch nicht vorhersehbarer immaterieller Schaden entsteht.

c) Auch wenn verschiedene Verstöße gerügt werden, geht es bei der Feststellung um Folgen aus ein und demselben Scrapingvorgang, weshalb auch der Feststellungsantrag hinreichend bestimmt formuliert ist.

5. Auch Klageanträge Ziff. 3 a und 3 b sind hinreichend konkret und sachdienlich formuliert. Da durch die Anträge eine unbestimmte Zahl verschiedener künftiger Fälle erfasst werden sollen und müssen, ist die Verwendung auslegungsbedürftiger Rechtsbegriffe unabdingbar. Es liegt hier in der Natur der Sache, dass es in Zwangsvollstreckungsverfahren gegebenenfalls richterlicher Würdigung vorbehalten bleiben muss, ob ein Verstoß gegen eine titulierte Unterlassungsverpflichtung gegeben ist.

II.

Die Klage ist jedoch nur teilweise begründet.

Auf das Vertragsverhältnis der Parteien ist deutsches Recht anzuwenden. Der Vertrag unterliegt nach Art. 3 Abs. 1, Art. 6 Abs. 2 der VO (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I-VO; ABl. 2008 L 177, Seite 6) dem von den Parteien ausweislich der Ziffer 4 der Nutzungsbedingungen gewählten deutschen Recht (OLG Stuttgart, Urteil vom 22.11.2023, 4 U 20/23; BGH, Urteil vom 12.07.2018, III ZR 183/17, NJW 2018, 3178, 3179 Rn. 20).

1. Klageantrag Ziff. 1:

Die Beklagte ist gemäß Art. 82 Abs. 1 DSGVO verpflichtet, dem Kläger immateriellen Schadensersatz in Höhe von 250 € zuzüglich Prozesszinsen (§§ 291, 288 Abs. 1 S. 2 BGB) zu zahlen.

a) Art. 82 Abs. 1 DSGVO ist im Hinblick auf seinen Anwendungsbereich weit zu verstehen. Aus dem Wortlaut der Vorschrift ergibt sich gerade nicht, dass Art. 82 Abs. 1 DSGVO durch Art. 82 Abs. 2 DSGVO konkretisiert und eingeschränkt werden soll, so dass nur Pflichtverletzungen im Zusammenhang mit einer *Verarbeitung von Daten* den Schadensersatzanspruch auslösen könnten (hierzu näher OLG Köln, Urteil vom 14.07.2022, I-15 U 137/21; LG Aachen, Urteil vom 10.02.2023, 8 O 177/22 - juris). Vielmehr erfasst die Norm jedweden Verstoß gegen die DSGVO, der zu einem Schaden geführt hat (OLG Stuttgart, Urteil vom 22.11.2023, 4 U 20/23).

b) Die Beklagte hat insbesondere ausweislich der Anlagen B 1 ff. gegenüber ihren Nutzern nicht darauf hingewiesen, dass bei einer Nutzung des Kontakt-Import-Tools auch bei einer Beschränkung der Telefoneinstellungen die Möglichkeit eines Zugriffs auf das Nutzerkonto gegeben

ist, weshalb objektiv keine ausreichende Information über diese Verarbeitungsmöglichkeit erfolgte und die erteilte Einwilligung unwirksam ist (OLG Stuttgart aaO; OLG Hamm GRUR-RS 2023, 22505 Rn. 105 ff.). Da zur Verarbeitung auch jede andere Form der Bereitstellung von Daten gehört (Art. 4 Nr. 2 DSGVO), liegt insoweit eine rechtswidrige Verarbeitung vor (OLG Stuttgart aaO). Der Europäische Gerichtshof hat zudem entschieden, dass bei Voreinstellungen mit einer sogenannten Abwahlmöglichkeit (Opt-out-Voreinstellung) nicht von einer wirksamen Einwilligung in die Datenverarbeitung ausgegangen werden kann, weil die Einwilligung ein aktives Verhalten erfordert (Art 4 Nr. 11 DSGVO). Deshalb ergibt sich auch aus der Tatsache, dass die Suchbarkeit auf „alle“ eingestellt war und nur eine opt-out-Lösung vorgesehen war, dass keine wirksame Einwilligung vorlag (OLG Stuttgart aaO; OLG Hamm GRUR-RS 2023, 22505 Rn. 104).

c) Durch die Möglichkeit eines Zugriffs auf die persönlichen Daten des Klägers im Kontakt-Import-Tool hat die Beklagte gegen Art. 5 Abs. 1 lit. f) DSGVO verstoßen, denn zur Verarbeitung von Daten zählt auch jede Form der gegebenenfalls auch nicht beabsichtigten Bereitstellung von Daten (Art. 4 Nr. 2 DSGVO). Durch die eingeräumte Möglichkeit des Hochladens von Telefonnummern für eine Verknüpfung der Kontakte wurden die persönlichen Daten des Klägers (Name, Facebook-ID etc.) für eine Verknüpfung bereitgestellt beziehungsweise zur Verfügung gestellt. Soweit die Beklagte auf dem Standpunkt steht, es fehle an einem Verstoß, da die Telefonnummern von den Scrapern bereitgestellt worden seien und nur Informationen eingesammelt wurden, die ohnehin öffentlich einsehbar waren, ist dem nicht zu folgen. Die Beklagte hat selbst ausdrücklich eingeräumt, dass nach ihren Nutzungsbedingungen der Abgriff untersagt war, weshalb sie selbst von einer Rechtswidrigkeit des Verhaltens ausgeht. Angesichts des Schutzzwecks der DSGVO, den Schutz personenbezogener Daten zu gewährleisten, kommt es nicht darauf an, dass die (fingierten) Telefonnummern von den Scrapern stammten (so OLG Stuttgart aaO).

d) Zudem hat die Voreinstellung einer Zugriffsmöglichkeit auf die Telefonnummer für jedermann gegen die Vorgaben aus Art. 25 Abs. 2 DSGVO verstoßen. Die Norm enthält nach Wortlaut und Systematik ein sogenanntes Opt-out-Verbot für nicht erforderliche Daten. Danach ist durch die standardmäßige Konfiguration von (Privatsphäre-) Einstellungen zu gewährleisten, dass Nutzer eines sozialen Netzwerks die nicht erforderlichen Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, den sie vorab selbst festgelegt haben (OLG Stuttgart aaO).

e) Nachdem ein Abgriff von Daten möglich war, weil keine ausreichend datenschutzfreundlichen Voreinstellungen vorgenommen worden waren und die Daten auch nicht ausreichend geschützt waren, hat die Beklagte gegen die sie aus Art. 33, 34 DSGVO treffenden Melde- und Be-

nachrichtigungspflichten verstoßen. Allerdings hat dieser Verstoß keinen (weiteren) Schaden ausgelöst (OLG Stuttgart aaO).

f) Dem Kläger ist aufgrund der vorgenannten Verstöße zu b) bis e) ein immaterieller Schaden entstanden.

aa) Der Kläger ist von dem Datenvorfall in Form des Scrapings im Jahre 2019 aufgrund der vorgenannten Pflichtverletzungen der Beklagten persönlich betroffen. Es ist unstreitig, dass der Kläger zu den vom Scrapingsachverhalt betroffenen Personen gehörte und dessen Daten zumindest in Form von Telefonnummer, Nutzer ID, Vorname, Land und Geschlecht unstreitig vom Scraping erfasst wurden.

bb) Allerdings ist es in der Instanzrechtsprechung streitig, welche konkreten Anforderungen an einen immateriellen Schaden im Sinne des Art. 82 Abs. 1 DSGVO zu stellen sind. Der EuGH hat nunmehr mit Urteil vom 14.12.2023, C-340/21 klargestellt, dass allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen diese Verordnung befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, einen „immateriellen Schaden“ im Sinne dieser Bestimmung darstellen kann. Dabei indiziert die Verwendung des Begriffes „fear“ (= Furcht), dass die betroffene Person aufgrund des Datenverstoßes einer gewissen psychischen Belastung in Form einer Sorge oder - stärker - spürbaren Angstgefühlen ausgesetzt wird oder wurde. Nachdem gemäß EuGH, Urteil vom 04.05.2023, C-300/21, die Vorschriften der DSGVO dahin auszulegen sind, dass ein „immaterieller Schaden“ Anspruch auf Schadenersatz eröffnen kann, ohne dass eine wie auch immer geartete Erheblichkeitsschwelle überschritten sein muss, genügt für die Begründung eines entsprechenden Schadens auch eine lediglich vorübergehende Sorge der betroffenen Person vor Missbrauch ihrer abgegriffenen Daten, ohne dass hiermit tiefgreifendere seelische Belastungen einhergehen müssen.

cc) Das Gericht ist aufgrund der persönlichen Anhörung des Klägers davon überzeugt, dass dieser zumindest wiederkehrend für gewisse Zeitspannen eine solche Sorge empfunden hat.

(1) Der Kläger hat zunächst glaubhaft dargelegt, dass er seit relativ kurzer Zeit „vor Beginn von Corona“, also wohl seit ca. Ende des Jahres 2019 oder Anfang 2020, nahezu tägliche Anrufe von zum Teil ausländischen Nummern, zum Teil unterdrückten Nummern erhalten habe, wobei teilweise Computerstimmen zu hören gewesen seien, teilweise auch reelle Personen. Ihm seien dann u.a. Geldanlageangebote unterbreitet worden, wobei er teilweise sofort mit Namen angesprochen worden sei, obwohl er sich nicht mit Namen gemeldet habe.

Das Gericht erachtet die dahingehenden Angaben des Klägers deshalb für glaubhaft, weil dieser ersichtlich um eine sachliche Darstellung des Sachverhaltes bemüht war ohne jede Übertrei-

bung und übermäßige Belastung der Beklagten im Sinne der Klagebegründung. So hat der Kläger ohne weiteres eingeräumt, dass es sich ausschließlich um Anrufe gehandelt habe, seiner Erinnerung nach nicht auch um Emails in diesem Zusammenhang. Zudem hat der Kläger auch seine eigene, durch die Anrufe ausgelöste emotionale und psychische Belastung in keiner Weise hochgespielt oder in anderer Weise herausgestellt (vgl. sogleich unten zu (2)).

Es ist daher auch glaubhaft, wenn der Kläger versichert hat, dass es vor dem von ihm genannten Zeitraum jedenfalls keine solche Anhäufung von entsprechenden Anrufen gegeben hatte. Insofern ist auch der zeitliche und damit auch sachliche Zusammenhang der beim Kläger eingehenden unerwünschten Anrufe mit dem streitgegenständlichen Datenvorfall, der sich im Jahre 2019 zugetragen haben soll, nicht von der Hand zu weisen.

(2) Der Kläger hat weiterhin dargelegt, dass die nahezu täglichen Anrufe für ihn in erster Linie lästig waren und sind, zumal er hierdurch in seiner Arbeitszeit unterbrochen worden sei und weiterhin werde. Dies stellt allerdings keinen immateriellen Schaden des Klägers im Sinne der DS-GVO dar. Zudem machte sich der Kläger aber eigenem Bekunden nach nach Eingang der ersten Anrufe, in denen sein Name genannt wurde, und nachdem er durch Internetrecherchen herausbekommen habe, dass es einen Datenklau bzw. ein Scraping gegeben habe und dass auch seine Daten davon betroffen seien, schon Gedanken darüber, was man damit jetzt alles anstellen könnte. Mittlerweile sei es aber so, dass er das Ganze ausblende bzw. sich keine größeren Gedanken darüber mache, aber halt damit beschäftigt sei, wenn es immer wieder diese Anrufe gebe. Der Kläger wollte auf diesbezügliche gerichtliche Nachfrage nicht von einer seelischen Belastung sprechen - was für die Wahrhaftigkeit seiner eigenen Angaben und Einschätzungen spricht -, jedoch kann seinen Angaben eine gewisse, wenn auch vorübergehende Sorge vor Datenmissbrauch entnommen werden, die als - wenn auch relativ geringfügige - psychische Belastung zu werten ist.

(3) Bei Abwägung der immer wiederkehrenden, relativ geringfügigen psychischen Beeinträchtigungen des Klägers im Zusammenhang mit dem streitgegenständlichen Datenvorfall, der ihn nicht einmal veranlasst hatte, tiefgreifender zu recherchieren, welche konkreten Abwehrmaßnahmen gegen die Wiederholung eines Scrapings seiner Daten durch Einstellungsänderungsmöglichkeiten auf seinem Facebook-Profil bestehen, und der konkreten Verstöße der Beklagten gegen Bestimmungen der DSGVO erscheint die Zuerkennung eines Schadensersatzanspruches in Höhe von 250 € angemessen, aber auch ausreichend zu sein.

Klageantrag Ziff. 2:

Der Antrag des Klägers auf Feststellung der Verpflichtung der Beklagten zum Ersatz aller weiteren künftigen Schäden, die dem Kläger durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten im Jahre 2019 entstehen werden, ist begründet.

Hinsichtlich der Frage einer Ersatzpflicht für künftige Schäden können die Grundsätze der höchstrichterlichen Rechtsprechung für Feststellungsanträge nach einem Gesundheitsschaden übertragen werden. Der Anspruch auf Feststellung beim Schmerzensgeld als immaterieller Schaden ist bereits begründet bei einer nicht eben entfernt liegenden Möglichkeit künftiger Verwirklichung der Schadensersatzpflicht durch das Auftreten weiterer, bisher noch nicht voraussehbarer und erkennbarer Leiden oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung des Krankheitsverlaufs. Die Feststellungsklage ist bei noch nicht voraussehbaren und erkennbaren weiteren Beeinträchtigungen oder bei einer noch nicht abschließend überschaubaren weiteren Entwicklung begründet (vgl. OLG Stuttgart, Urteil vom 22.11.2023, 4 U 20/23). Das ist auch vorliegend der Fall, denn es besteht die evidente Möglichkeit, dass mit einer weiteren Verbreitung der Telefonnummer des Klägers weitere materielle oder immaterielle Beeinträchtigungen bei ihm eintreten können.

Klageantrag Ziff. 3:

Dieser Antrag ist unbegründet. Dem Kläger steht gegen die Beklagte kein Anspruch auf das begehrte Verhalten zu.

1. Ein Anspruch des Klägers auf Unterlassung gemäß §§ 1004, 823 BGB im Zusammenhang mit den Verstößen der Beklagten gegen Vorschriften der DSGVO scheidet bereits deshalb aus, weil Unterlassungsansprüche nicht auf nationales Rechts, sondern lediglich auf Art. 17 DSGVO gestützt werden können (vgl. OLG Stuttgart, aaO; BGH GRUR 2022, 258).

2. Aber auch auf Art. 17 DSGVO können die vom Kläger konkret geltend gemachten Unterlassungsansprüche nicht gestützt werden. Diese Norm sieht lediglich ein Löschungsrecht bezüglich personenbezogener Daten vor, jedoch gerade keine weitergehenden Rechte bezüglich der Datenverarbeitungsvorgänge an sich, weshalb keine Unterlassungsansprüche geltend gemacht werden können, die im Ergebnis die Verarbeitungsvorgänge des Verantwortlichen reglementieren können (vgl. OLG Stuttgart aaO).

Klageantrag Ziff. 4:

Auch der Antrag des Klägers auf Auskunft über die ihn betreffenden personenbezogenen Daten, welche die Beklagte verarbeitet, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten, ist nicht begründet. Denn die Beklagte hat nachvollziehbar dargelegt, dass ihr die Scraper des streitgegenständlichen Datenvorfalls namentlich nicht bekannt sind, weshalb die Beklagte über die mit Schreiben vom 01.03.2023 (Anlage B 16) erteilten Auskünfte hinaus keine weiteren Auskünfte und Informationen mehr erteilen könnte.

Klageantrag Ziff. 5:

Auch ein Anspruch des Klägers gegen die Beklagte auf Erstattung vorgerichtlicher Rechtsanwaltskosten besteht nicht.

1. Es ist bereits nicht ersichtlich, dass dem Kläger tatsächlich entsprechende gesonderte Kosten entstanden sind. Aus der Anlage K 1 mit der beigefügten Vollmacht des Klägers für seine Prozessbevollmächtigten ergibt sich, dass sich diese bereits auf die gerichtliche Geltendmachung von Ansprüchen erstreckt hat, was eine entsprechende Mandatierung indiziert. Dann aber hätte es sich beim entsprechenden Tätigwerden der Klägervertreter um eine der Vorbereitung der Klage dienende Tätigkeit nach § 19 Abs. 1 Satz 2 Nr. 1 RVG gehandelt, die zum Rechtszug gehört und daher mit der Verfahrensgebühr nach Nr. 3100 RVG VV abgegolten wäre (vgl. OLG Stuttgart aaO).

2. Zudem hat die Beklagte unwidersprochen vermutet, dass dem Kläger Kostendeckung für die Tätigkeit seiner anwaltlichen Vertreter durch einen Rechtsschutzversicherer gewährt worden ist, so dass im Falle einer entsprechenden Leistung etwaige Kostenersatzansprüche gemäß § 86 Abs. 1 VVG auf den Versicherer übergegangen wären.

III.

1. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO.

2. Die Entscheidung zur vorläufigen Vollstreckbarkeit ergeht gemäß §§ 708 Nr. 11, 711 ZPO.

3. Der Streitwert gliedert sich wie folgt auf:

Klageantrag Ziff. 1: 1.000 €

Klageantrag Ziff. 2: 500 € (die Hälfte von Klageantrag Ziff. 1; vgl. OLG Stuttgart, Beschluss vom 30.08.2023, 4 W 87/23)

Klageantrag Ziff. 3: 5.000 € (vgl. OLG Stuttgart aaO)

Klageantrag Ziff. 4: 250 € (vgl. OLG Stuttgart aaO)

Klageantrag Ziff. 5: kein eigener Streitwert

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 Heilbronn
Wilhelmstraße 8
74072 Heilbronn

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.

Vorsitzender Richter am Landgericht