Beglaubigte Abschrift

Landgericht Aschaffenburg

Az.: 63 O 74/23

IM NAMEN DES VOLKES

In dem Rechtsstreit

- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **WBS.LEGAL Wilde Beuger Solmecke**, Rechtsanwälte Partnerschaft mbB, Eupener Straße 67, 50933 Köln, Gz.:

gegen

Meta Platforms Ireland Ltd. (vormals: Facebook 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, Bockenheimer Anlage 44, 60322 Frankfurt

wegen Persönlichkeitsrechtsverletzung, Verstöße gegen die Datenschutz-Grundverordnung

erlässt das Landgericht Aschaffenburg - 6. Zivilkammer - durch die Richterin am Landgericht Hergenröder als Einzelrichterin aufgrund der mündlichen Verhandlung vom 07.02.2024 folgendes

Endurteil

1. Die Beklagte wird verurteilt, an den Kläger 250,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit 18.07.2023 zu zahlen.

2. Im Übrigen wird die Klage abgewiesen.

3. Die Beklagte hat die Kosten des Rechtsstreits zu tragen.

4. Das Urteil ist für die jeweilige Partei gegen Sicherheitsleistung in Höhe von 110 % des je-

weils zu vollstreckenden Betrags vorläufig vollstreckbar.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

Tatbestand

Der Kläger macht Schadensersatz-, Unterlassungs- und Auskunftsansprüche wegen der Verletzung der Datenschutz-Grundverordnung (im Folgenden: DSGVO) seitens der Beklagten aus und im Zusammenhang mit dem sogenannten, im April 2021 öffentlich bekannt gewordenen „Scraping-Vorfall“ von Facebook geltend.

Die Beklagte betreibt in der Europäischen Union das soziale Online-Netzwerk Facebook und bietet u. a. über www.facebook.com Dienste an, die für private Nutzer kostenlos sind.

Für die Verarbeitung der Nutzerdaten stützt sich die Beklagte auf den Nutzungsvertrag, den die Nutzer des sozialen Netzwerks Facebook durch Betätigung der Schaltfläche „Registrieren“ abschließen und mit dem sie – mittlerweile – den von diesem Unternehmen festgelegten Allgemeinen Nutzungsbedingungen zustimmen. Die Zustimmung zu diesen Bedingungen ist notwendig, um das soziale Netzwerk Facebook nutzen zu können. Hinsichtlich der Verarbeitung personenbezogener Daten verweisen die Allgemeinen Nutzungsbedingungen auf die von diesem Unternehmen festgelegten Richtlinien für die Verwendung von Daten und Cookies. Danach erfasst die Beklagte nutzer- und gerätebezogene Daten über Nutzeraktivitäten innerhalb und außerhalb des sozialen Netzwerks und ordnet sie den Facebook-Konten der betroffenen Nutzer zu.

Den Nutzern dient das Online-Netzwerk dazu, sich untereinander zu vernetzen, Kontakt zu Freunden zu halten und herzustellen sowie neue Menschen, Gruppen, Unternehmen, Organisationen usw. kennenzulernen. Die Nutzer erhalten zudem eine Plattform, über die sie sich austauschen und ihre Erlebnisse sowie Meinungen kundtun können.

Anfang April 2021 wurde durch die Medien öffentlich über den Scraping Vorfall berichtet, wonach Daten von ca. 533 Millionen Nutzern aus 106 Ländern im Internet durch unbekannte Dritte veröffentlicht worden seien. Hierbei seien von Januar 2018 bis September 2019 die vom jeweiligen Nutzer öffentlich gestellten Daten bzw. stets öffentliche Daten wie Name, Geschlecht und Nut-

zer-Id mittels des Facebook-Tools Kontakt-Importer (CIT, Contact-Import-Tool) „gescraped“ worden. Die Beklagte geht davon aus, dass das CIT zur Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurden, in dem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, d.h., eine fiktive Telefonnummer hochgeladen wurde, die bei einem Abgleich eine Zuordnung zu konkreten Facebook Profilen ermöglichte, um dort die öffentlichen Daten abzuschöpfen.

Automatisierte Scraping-Aktivitäten ohne Erlaubnis der Beklagten waren während des hier gegenständlichen Zeitraums durch die Nutzungsbedingungen der Facebook Plattform verboten und sind auch weiterhin untersagt.

Unabhängig von individuellen Einstellungen sind auf der Plattform der Beklagten die Nutzerdaten Name, Facbook ID und Geschlecht immer öffentlich einsehbar. Einstellungen bzgl. der Telefonnummer konnten Facebook-Nutzer an zwei Orten vornehmen. Im Rahmen der „Privatsphäre-Einstellungen“ konnten unter den von der Beklagtenseite so bezeichneten Bereichen „Zielgruppenauswahl“ und „Suchbarkeits-Einstellungen“ Einstellungen vorgenommen werden. In Bezug auf die Telefonnummer konnte zum einen eingestellt werden, wer die Telefonnummer auf dem Facebook-Profil des Nutzers sehen konnte („Zielgruppenauswahl“), wobei die Optionen „öffentlich“, „Freunde“ und „Freunde von Freunden“ möglich waren. Zum andere konnte eingestellt werden, wer den Nutzer über die Telefonnummer finden konnte (Suchbarkeits-Einstellungen). Insofern war als Voreinstellung eingestellt, dass „alle/jeder“ den Nutzer über die Telefonnummer finden konnte.

In den Suchbarkeits-Einstellungen im Profil der Klagepartei war die Einstellung hinsichtlich der Telefonnummer auf „everyone“ eingestellt (vgl. Screenshot Anlage K6) und bis September 2019 unverändert.

Mit vorgerichtlicher E-Mail vom 22.08.2022 (Anlage K1) forderte die Klagepartei die Beklagte betreffend die Email-Adresse zur Zahlung von 1.000,00 EUR Schadensersatz nach Art. 82 Abs. 1 DSGVO, zur Unterlassung zukünftiger Zugänglichmachung der Daten der Klagepartei an unbefugte Dritte sowie zur Auskunft darüber auf, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden seien. Die Beklagte wies Ansprüche auf Schadensersatz und Unterlassung zurück und erteilte der Klagepartei Auskünfte mit Schreiben vom 22.09.2022 (Anlage B16).

Die Klagepartei trägt im Wesentlichen vor, neben den Einstellmöglichkeiten an zwei verschiedenen Orten auf der Facebook-Plattform seien in der Messenger-App separate Sicherheitseinstellungen möglich. Die App diene als Schnittstelle für Facebook-Applikationen auf Mobilgeräten. Sicherheitseinstellungen seien dort unabhängig vom sonstigen Facebook-Dienst möglich. Die Einstellung, dass Telefonkontakte mit dem Facebook-Dienst synchronisiert werden, sei möglich. Eine Anfrage zur Synchronisierung erfolge bei der Erstanmeldung. Hierbei erfolge keine Information über Risiken über die Verwendung der Telefonnummer bei Verwendung des Kontakt-Import-Tools.

Zudem werde durch die Beklagte angeboten, die Telefonnummer zu hinterlegen, um die Sicherheit des Accounts zu erhöhen (Zwei Faktor-Authentifizierung). Hierbei werde nicht erwähnt, dass die Nummer auch zur Identifizierung des Nutzerprofils verwendet werden. Ein Nutzer der die Telefonnummer nur zu Sicherheitszwecken preisgebe, lege einen gesteigerten Wert auf die Vertraulichkeit der Telefonnummer. Es werde nicht erwähnt, dass die Nummer dazu verwendet werde, in irgendeiner Art das Profil des Nutzers zu identifizieren.

Die Beklagte habe keine zureichenden Sicherheitsmaßnahmen ergriffen, um ein Ausnutzen des Kontakt-Import-Tools zu verhindern. Insbesondere habe die Beklagte keine Sicherheitscaptchas bei der Verwendung des Kontakt-Import-Tools eingesetzt sowie keinen Mechanismus zur Prüfung der Plausibilität von Anfragen. Dies, obwohl Scraping als Methode der Informationsgewinnung bekannt und weit verbreitet sei. Zudem lagen datenschutzunfreundliche Voreinstellungen vor, da durch die technische Gestaltung wesentliche Informationen des Nutzers als „öffentlich“ voreingestellt seien. Das Resultat seien die Veröffentlichung von Datensätzen auf Internetseiten, die illegale Aktivitaten begünstigten, bspw. der Seite „raidforums.com“, Namen und Rufnummern von Nutzern würden für gezielte Phishing-Attacken genutzt.

Im Darknet seien folgende Daten des Klägers auffindbar:

Dabei handele sich um die Telefonnummer, die Facebook ID, den Namen und das Geschlecht der Klägerseite.

Die Klagepartei habe deswegen einen erheblichen Kontrollverlust über ihre Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffenden Daten verblieben. Dies manifestiere sich in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Die Klägerseite erhalte seit dem

Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks.

Der Kläger habe regelmäßig Anrufe von unbekannten Telefonnummern erhalten. Zudem erhalte er SMS-Benachrichtigungen. Der Kläger leide unter dem Kontrollverlust der Daten sowie des Gefühls des Beobachtenwerdens und der Hilfslosigkeit. Dass die Daten in Kombination im sog. Darknet gehandelt werden, vergrößere seine Angst.

Der Klagepartei stehe ein Schadensersatzanspruch nach Art. 82 DSGVO in Verbindung mit Art. 25 DSGVO und ein Unterlassungsanspruch nach Art. 17 DSGVO zu. Durch die Rechtsverletzung werde die Wiederholungsgefahr indiziert. Das Auskunftsbegehren der Klagepartei sei nicht im erforderlichen Umfang erfüllt, so dass der geltend gemachte weitere Auskunftsanspruch bestehe. Es fehlten Angaben zu den konkreten Empfängern der personenbezogenen Daten.

Die Klagepartei 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 Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

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

Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und 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.

Die beklagte Partei beantragt:

Klageabweisung.

Die Klagepartei zähle Datenpunkte auf, bei denen unklar sei, ob sie Gegenstand des Scraping-Sachverhalts sein sollen. Teilweise werden auch Datenpunkte genannt, die keinen Profilfeldern bei Facebook entsprachen (Bundesland, Geburtsort).

Sie bestreite, dass Dritte einen bestimmten Nutzer über das Kontakt-Import-Tool hatten finden können unter Bezugnahme auf eine Telefonnummer, die ausschließlich für die Zwei-Faktor-Authentifizierung hinterlegt worden sei.

Einstellungen in der Messenger-App entsprächen den Einstellungen im Facebook-Konto. Änderungen bei Privatsphäre-Einstellungen auf der Facebook-Plattform würden automatisch auch im Messenger angewandt werden. Eigene Einstellungsmöglichkeiten unabhängig von der Facebook-Plattform bestünden nicht.

Die Beklagte habe bereits zum Zeitpunkt des hier gegenständlichen Scraping-Vorfalles Sicherheitsmaßnahmen, insbesondere ab September 2019 (vgl. Anlage B 11) implementiert gehabt, mit denen die Ausnutzung des CIT habe verhindert werden sollen (Übertragungsbegrenzungen, Bot-Erkennung). Sie habe keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten. Sie gehe gegen Scraper mit Unterlassungsverfügung und Kontosperrungen sowie Gerichtsverfahren vor.

Die Klagepartei sei ausreichend über die Einstellungen unterrichtet worden. Die Möglichkeit, Einstellungen vorzunehmen sei im Privatsphärebereich des Haupteinstellungsmenüs leicht zu finden. Insbesondere im Hilfebereich werde umfassend und verständlich erklärt, zu welchen Zwecken die Telefonnummer verwendet werde.

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

Die Beklagte meint weiter, es bestünden keine Ansprüche der Klagepartei, weil nur ohnehin öffentlich einsehbare Daten der Klagepartei „gescraped“ worden seien. Verstöße gegen die Art. 13, 14, 24, 25 und 34 DSGVO konnten ohnehin keinen Schadensersatzanspruch nach Art. 82 DSGVO auslösen. Eine Benachrichtigungspflicht in Scraping-Fallen bestehe nach der Kommentarliteratur nicht. Im Hinblick auf Art. 82 DSGVO fehle es zudem an einem der Beklagten zurechenbaren ersatzfähigen immateriellen Schaden im Sinne des Art. 82 DSGVO. Die Kausalität des Scaping Vorgangs bzw. der Ausnutzung des Kontakt-Import-Tools für etwaige SMS, die die Klagepartei erhalten zu haben behaupte, werde bestritten. Auch treffe die Beklagte kein Verschulden.

Für einen Unterlassungsanspruch gebe es keine Anspruchsgrundlage. Der geltend gemachte Anspruch stelle tatsächlich keinen Unterlassungsanspruch dar. Die Klagepartei verlange von der Beklagten ein aktives Tun, nämlich die Implementierung von (nicht naher definierten) Sicherheitsmaßnahmen und die Erteilung von (nicht naher definierten) Informationen bzgl. der Erteilung ihrer Telefonnummer. Ein Anspruch auf Implementierung von „nach dem Stand der Technik möglichen“ Sicherheitsmaßnahmen bestehe schon deshalb nicht, weil dieser Anspruch nicht hinreichend bestimmt sei. Zudem finde sich in der DSGVO keine Anspruchsgrundlage für einen Unterlassungsanspruch, andere Anspruchsgrundlagen wie § 1004 BGB seien nicht anwendbar. Überdies beruhe der Unterlassungsanspruch auf der unzutreffenden Annahme, dass die Beklagte unbefugten Dritten Zugriff auf Nutzerdaten gewahrt habe. Vor diesem Hintergrund mangle es sowohl an einer Erstbegehungs- als auch an einer Wiederholungsgefahr.

Der Auskunftsanspruch sei erfüllt, ein Anspruch über die erteilte Auskunft hinaus bestehe nicht. Die Beklagte habe das klägerische Auskunftsersuchen ordnungsgemäß beantwortet und den Auskunftsanspruch vollumfänglich erfüllt. Die von der Klagepartei begehrte Auskunft, welche Da-

ten durch welche Empfänger durch Scraping erlangt werden konnten, sei nicht von Art. 15 DS-GVO erfasst. Es handle sich um Verarbeitungstätigkeiten Dritter und nicht um eigene Verarbeitungstätigkeiten der Beklagten. Die Beklagte sei zur Beantwortung der Fragen bzgl. Verarbeitungstätigkeiten Dritter weder imstande noch rechtlich verpflichtet.

Zur Ergänzung des Sachverhalts wird Bezug genommen auf die gewechselten Schriftsätze der Parteien nebst Anlagen sowie das Protokoll der mündlichen Verhandlung vom 07.02.2024.

Entscheidungsgründe

I.

Die Klageanträge zu 1. und zu 4. sind zulässig und im ausgeurteilten Umfang begründet. Der Kläger hat einen Anspruch auf Schadenersatz in Höhe von 250 € gemäß Art 82, 25 Abs. 1, 32 DS-GVO. Vorgerichtliche Rechtsanwaltskosten wurden nicht beantragt. Die Klageanträge zu Ziffer 2., 3.a. und b. sind bereits unzulässig, der Klageantrag zu Ziffer 4. zulässig aber unbegründet.

1. Antrag Ziffer 1: Schadenersatz

a)

Die Leistungsklage ist zulässig.

Insbesondere ist der Antrag hinreichend bestimmt. Mit dem Antrag verfolgt der Kläger eine Entschädigungszahlung von mindestens 1.000,00 €. Diese Entschädigungszahlung bezieht sich auf einen einheitlichen Streitgegenstand, weil der Kläger objektiv betrachtet erkennbar von einem einheitlichen durch das Scraping und die Veröffentlichung des Leak-Datensatzes verursachten immateriellen Schaden ausgeht, der durch die nach seiner Ansicht bereits vor dem Scraping-Vorfall begangenen Verstöße gegen die DSGVO eingetreten und durch die Verstöße gegen die DSGVO im Nachgang zum Scraping Vorfall vertieft worden ist und letzterer somit keinen eigenständigen Schaden darstellt (vgl OLG Hamm, Urteil vom 15.08.2023, Az. 7 U 19/23, GRUR-RS 2023, 22505, Rn 41.

b)

Die Leistungsklage ist nur in Höhe von 250 € nach Art. 82 Abs. 2, Abs. 1 DSGVO begründet. Ein weitergehender Anspruch steht nicht zur Überzeugung des Gerichts gemäß § 286 ZPO fest.

Das Gericht geht davon aus dass der streitgegenständliche Scraping Vorfall nach dem 24.05.2018 erfolgte. Eine konkrete zeitliche Einordnung durch die insoweit darlegungsbelastete Beklagte ist nicht erfolgt. Für die Annahme spricht jedoch der Umstand, dass die Aktivierung der Sucharbeit über die Mobilfunktelefonnumer über die Kontakt-Importfunktion im Facebook-Messenger erst im September 2019 erfolgt ist, sodass also bis September 2019 ein Scraping möglich war (vgl. hierzu auch OLG Hamm aaO, Rz 55 ff.)

Sofern eine Datenerhebung vor den 24.05.2018 (zeitlichen Anwendungsbereich der DSGVO) fällt, ergibt sich aus Art. 24 Abs. 1 Satz 2 DSGVO die Pflicht, die Datenverarbeitung, die zum Zeitpunkt Anwendung der Lieferung bereits begonnen hatte, bis zu 25.5.2018 in Einklang mit der Verordnung zu bringen.

Diese steht nicht zur Überzeugung des Gerichts fest.

Das Gericht schließt sich insoweit den ausführliche begründeten Urteilsgründen des OLG Hamm (aaO) zur Annahme einer Schadenersatzpflicht dem Grunde nach Art. 82 DSGVO an (so auch EuGH vom 04.05.2023, C-300/21).

(i)

Die Beklagte hat durch die automatisierte Ausführung eines Datenabrufs von personenbezogenen Daten über eine Such- oder Kontaktimportfunktion durch einen Dritten in einem sozialen Netzwerk eine Datenverarbeitung eine Datenverarbeitung als Verantwortliche im Sinne des Art. 4 Nr. 2 DSGVO vorgenommen.

Durch die Suchbarkeits- und Kontaktimportfunktion hat die Beklagte die Daten verarbeitet im Sinne von Art. 4 Nr 2 DSGVO.

(ii)

Die Verarbeitung auch der Mobilfunktelefonnummer eines Nutzers im Rahmen einer Such- und Kontaktimportfunktion durch das soziale Netzwerk Facebook kann nicht auf den Rechtfertigungsgrund der Vertragszweckerfüllung im Sinne von Art. 6 Abs. 1 Unterabs. 1 b DSGVO gestützt werden (in Anwendung von EuGH Urt. v. 4.7.2023 – C-252/21, GRUR-RS 2023, 15772 Rn. 98 ff.).

Die Verarbeitung der personenbezogenen Daten des Klägers (Telefonnumer, Facebook-ID, Fa-

milienstand, Vorname Geschlecht, Geburtsdatum) über die Suchbarkeitseinstellung oder Kontaktimportfunktion waren nicht für die Erfüllung des Vertrages erforderlich im Sinne des Art. 6 Abs. 1 UA 1 b DSGVO, mithin unerlässlich. Die Such- und Kontaktimportfunktion sind Mittel zum Zweck, aber nicht unerlässlich mit Blick auf die Vernetzung der Nutzer.

(iii)

Für die Verarbeitung der Mobilfunktelefonnummer eines Nutzers durch das soziale Netzwerk Facebook im Rahmen einer Such- und Kontaktimportfunktion ist eine Einwilligung im Sinne von Art. 6 Abs. 1 Unterabs. 1 l a, Art. 7 DSGVO erforderlich, die – wie hier – bei unzulässiger Voreinstellung („opt-out“) und unzureichender sowie intransparenter Information über die konkrete Funktionsweise der Such- und Kontaktimportfunktion nicht vorliegen kann (in Anwendung von EuGH Urt. v. 4.7.2023 – C-252/21, GRUR-RS 2023, 15772 Rn. 91 f. und EuGH Urt. v. 11.11.2020 – C-61/19, NJW 2021, 841 Rn. 35 f.).

Eine wirksame Einwilligung des Klägers in die Suchbarkeit des Nutzerprofils über die Mobilfunknummer lag überdies auch nicht vor, Art, 6 Abs. 1 UA 1 a, Art 7 DSGVO. Die vorgesehene „opt-out“ Einwilligung stellt keine wirksame Einwilligung dar. Diese ist nicht hinreichend transparent und ausreichend, um den Nutzer über die Bedeutung der Suchbarkeitseinstellung zu informieren. Die Nutzungsbedingungen lassen insoweit keine Angaben zur Suchbarkeitseinstellung erkennen.

(iv)

Auch eine Rechtfertigung nach Art. 6 Abs. 1 UA 1 f.DSGVO scheidet mangels Erforderlichkeit aus.

Der für die Datenverarbeitung Verantwortliche verletzt seine Pflichten aus Art. 32 und Art. 25 Abs. 1 DSGVO, wenn er – wie hier – bereits konkrete Kenntnis von einem Datenabgriff durch unbefugte Dritte hat und trotzdem – im Einzelfall – bei ex-ante-Betrachtung naheliegende Maßnahmen zur Verhinderung des weiteren unbefugten Datenabgriffs nicht ergreift (im Ergebnis wie Irish Data Protection Commission Entsch. v. 25.11.2022 – IN-21-4-2; siehe auch GA Pitruzzella Schlussanträge v. 27.4.2023 – C-340/21, BeckRS 2023, 8707 Rn. 20, 29 ff., 38 ff.).

Ohne diese Funktion der automatisierten Datenverarbeitung wären die Daten nicht von den Scrapern nutzbar gemacht worden. Dies erfolgte auch unbefugt. Ausreichende Schutzmechanismen wurden seitens der Beklagten nicht ergriffen. So wurde die Übertragungsbeschränkung erst ab September 2019 eingeführt, obwohl die Beklagte bereits zuvor hinreichende Kenntnis von den

Scraping Vorfällen hatte. (vgl. Hierzu auch OLG Hamm aao Rn 125 ff).

c)

Infolge, jedenfalls dieser Verstöße, ist dem Kläger auch ein Schaden entstanden.

Art. 82 DSGVO sieht keine Erheblichkeitsschwelle vor (so auch EuGH vom 04.05.2023, C-300/21), jedoch muss der Schaden tatsächlich und sicher bestehen.

Neben dem Kontrollverlust über personenbezogenen Daten, hat der Kläger infolge des Scrapings einen Schaden erlitten, welcher in der persönlichen Beeinträchtigung im Umgang mit Spam Anrufen und Nachrichten liegt. Der Kläger hat mit der Anlage K 5 die Belästigung mit Spam Nachrichten belegt.

Zwar hat die Beklagte bestritten, dass die vom Kläger behaupteten Anrufe und Spams vom streitgegenständlichen Scraping Vorfall stammen.

Dies steht jedoch zur Überzeugung des Gerichts aufgrund folgender Indizien fest:

Die Spamaktivitäten fingen nach glaubhaften Angaben des Klägers zeitlich zusammenhängend mit dem von Januar 2018 bis September 2019 erfolgten Scraping an. Die Daten des Klägers sind auch unstreitig von Dritten „gescraped“ worden. Konkrete Anhaltspunkte dafür, dass die Daten anderweitig öffentlich gemacht wurden, sind nicht ersichtlich. Vielmehr hat der Kläger in der mündlichen Verhandlung über seinen Prozessvertreter erklären lassen, dass er seine Telefonnummer nicht auf einer eigenen Website etc. veröffentlicht habe.

Infolge des Scrapings ist dem Kläger ein Schaden in Höhe von 250 € entstanden.

Maßgeblich ist insoweit, dass dem Kläger mangels entsprechender Angaben bislang offensichtlich kein materieller Schaden entstanden ist. Der immaterielle Schaden, die Angst Opfer von Phishing Aktivitäten zu werden, sieht das Gericht bei dem Kläger, als gering an. Allerdings hatte der Kläger ausweislich der Anlage K 5 in kurzer Zeit mit einer Vielzahl von Spam Nachrichten zu tun, deren Behandlung seine besondere Aufmerksamkeit erforderte und somit Zeit, Aufwand und Ärger bedeutete. Auf der anderen Seite hat der Kläger seine Telefonnummer nicht geändert, so dass die Belästigung von ihm als noch beherrschbar eingestuft wurde.

Auf der anderen Seite hat die Beklagte die Veröffentlichung durch Datenverstöße lediglich mitverursacht.

Gemessen daran ist dem Kläger ein immaterieller Schaden entstanden, den das Gericht auf 250 € bemisst.

d)

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

2. Antrag Ziffer 2: Feststellung

Der mit dem Antrag zu Ziffer 2 verfolgte Feststellungsantrag ist unzulässig. Es fehlt am Feststellungsinteresse. Dem Kläger ist mangels entsprechender Angaben bislang offensichtlich kein materieller Schaden entstanden. Es ist daher auch nicht damit zu rechnen, dass dem Kläger zukünftig ein Schaden entstehen wird. Eine etwaige Befürchtung wäre lediglich theoretischer Art.

3. Antrag Ziffer 3: Unterlassung

Die mit Ziffer 3 verfolgte Unterlassungsklage ist unzulässig.

Mit Ziffer 3.a. wird kein Unterlassen, sondern ein aktives Tun verlangt, mithin eine vertretbare Handlung im Sinne von § 887 ZPO. Aber auch die Voraussetzungen des § 259 ZPO liegen nicht vor, weil es die Such - und Kontaktimportfunktion seit September 2019 nicht mehr gibt, vgl OLG Hamm aao Rn.204 ff. Im Übrigen ist er zu unbestimmt, vgl OLG Hamm aaO Rn. 212 ff.

Der Antrag zu Ziffer 3.b. ist unzulässig mangels Rechtsschutzbedürfnisses. Die Beklagte hat den Kläger mit personalisiertem Auskunftsschreiben vom 25.10.2021 an seine Prozessbevollmächtigte über die Sichtbarkeit und Suchbarkeitsfunktion informiert und hätte daher die Einstellungen unverzüglich umstellen können.

4. Antrag Ziffer 4: Auskunft

Die mit dem Antrag zu Ziffer 4 verfolgte Auskunftsklage ist unbegründet.

Die Beklagte hat das Auskunftsbegehren des Klägers mit Schreiben vom 22.09.2022 (Anlage B16) erfüllt, gem. § 362 BGB.

In dem Schreiben wird Stellung genommen zu dem Datenvorfall, die Datenpunkte und Telefonnummer, eine Erläuterung des Datenabrufs über die öffentlichen Daten, das Facebook Profil, die zeitliche Angabe „im Zeitraum bis September 2019“, den Hinweis, dass die Beklagte keine Kopie der Rohdaten habe, welche durch Scraping abgerufen wurden, und den Hinweis auf das Handeln mehrerer Scraper.

5.

Vorgerichtliche Rechtsanwaltskosten wurden nicht beantragt.

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

II.

Die Kostenentscheidung folgt aus 92 Abs. 2 Nr. 2 ZPO, die Entscheidung über die Vollstreckbarkeit aus § 709 S. 1 ZPO.

III.

Der Streitwert wurde gem. §§ 3,5 ZPO, 48, 39 GKG festgesetzt.

Für den Klageantrag zu 1) erachtet das Gericht in Anbetracht der geltend gemachten immateriellen Beeinträchtigungen des Klägers einen Streitwert von 1.000,00 € als angemessen.

Für den Feststellungsantrag (Klageantrag zu 2.) und den Auskunftsantrag (Klageantrag zu 4.) waren jeweils 500,00 € festzusetzen. Die Festsetzung auf jeweils 500,00 € erscheint angemessen.

Bezüglich des Unterlassungsantrags (Klageantrag zu 3.) ist ein Streitwert von 5.000,00 € festzusetzen. In nichtvermögensrechtlichen Streitigkeiten ist der Streitwert unter Berücksichtigung aller Umstände des Einzelfalls, insbesondere des Umfangs und der Bedeutung der Sache nach Ermessen zu bestimmen, § 48 Abs. 2 GKG. Im Hinblick auf die Bedeutung der Sache sowie die Marktstellung der Beklagten sowie auf die klägerseits behauptete Pflichtverletzung der Beklagten und angesichts des Umstandes, dass der Kläger unstreitig selbst seine Telefonnummer freiwillig angegeben hat, hält das Gericht im Hinblick auf den Klageantrag zu 3. einen Streitwert von insge-

samt 5.000,00€ für angemessen. Die beiden Unterlassungsanträge sind bei wirtschaftlicher Betrachtung so eng verknüpft, dass die Festsetzung eines Streitwertes von jeweils 5.000,00€ nicht angezeigt ist.

Es ergibt sich somit folgender Streitwert:

Klageantrag zu 1.: (immaterieller Schadensersatz): 1.000,00 €

Klageantrag zu 2. (Feststellungsantrag) 500,00 €

Klageantrag zu 3. (Unterlassungsantrag) 5.000,00 €

Klageantrag zu 4. (Auskunft) 500.00 €

Summe 7.000,00 €

Die hier vorgenommene Festsetzung entspricht der ständigen Rechtsprechung des Oberlandesgerichts Bamberg in vergleichbaren Fällen (vgl. z.B. OLG Bamberg, Beschluss vom 30.08.2023, 5 W 21/23 e; Beschluss vom 29.08.2023, 6 W 7/23 e; Beschluss vom 13.07.2023; 1 W 26/23 e).

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 Aschaffenburg
Erthalstr. 3
63739 Aschaffenburg

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** eingereicht werden. Eine einfache E-Mail genügt den gesetzlichen Anforderungen nicht.

Rechtsbehelfe, die durch eine Rechtsanwältin, einen Rechtsanwalt, durch eine Behörde oder durch eine juris-

tische Person des öffentlichen Rechts einschließlich der von ihr zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse eingereicht werden, sind **als elektronisches Dokument** einzureichen, es sei denn, dass dies aus technischen Gründen vorübergehend nicht möglich ist. In diesem Fall bleibt die Übermittlung nach den allgemeinen Vorschriften zulässig, wobei die vorübergehende Unmöglichkeit bei der Ersatzeinreichung oder unverzüglich danach glaubhaft zu machen ist. Auf Anforderung ist das elektronische Dokument nachzureichen.

Elektronische Dokumente müssen
- mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder
- von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg eingereicht werden.

Ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen ist, darf wie folgt übermittelt werden:
- auf einem sicheren Übermittlungsweg oder
- an das für den Empfang elektronischer Dokumente eingerichtete Elektronische Gerichts- und Verwaltungspostfach (EGVP) des Gerichts.

Wegen der sicheren Übermittlungswege wird auf § 130a Absatz 4 der Zivilprozessordnung verwiesen. Hinsichtlich der weiteren Voraussetzungen zur elektronischen Kommunikation mit den Gerichten wird auf die Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung - ERVV) in der jeweils geltenden Fassung sowie auf die Internetseite www.justiz.de verwiesen.

gez.

Richterin am Landgericht

Verkündet am 20.03.2024

gez.
, JAng
Urkundsbeamtin der Geschäftsstelle

BAYERN LANDGERICHT

Für die Richtigkeit der Abschrift
Aschaffenburg, 21.03.2024

, JAng
Urkundsbeamtin der Geschäftsstelle