Aktenzeichen: 24 O 56/22

Landgericht Stuttgart

Im Namen des Volkes

Urteil

In dem Rechtsstreit

[redacted]
- Kläger -

Prozessbevollmächtigte:
Rechtsanwälte **Wilde Beuger Solmecke**, Kaiser-Wilhelm-Ring 27-29, 50672 Köln, Gz.: [redacted]

gegen

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

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

wegen Verstöße

hat das Landgericht Stuttgart - 24. Zivilkammer - durch den Richter [redacted] als Einzelrichter aufgrund der mündlichen Verhandlung vom 07.02.2023 für Recht erkannt:

1. Die Beklagte wird verurteilt, an den Kläger 1.000,00 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 23.08.2022 zu zahlen.

2. Die Beklagte wird verurteilt, dem Kläger Auskunft über den Kläger betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen.

3. Die Beklagte wird verurteilt, an den Kläger vorgerichtliche Rechtsanwaltskosten in Höhe von 220,27 € nebst Zinsen hieraus in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit dem 23.08.2022 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Von den Kosten des Rechtsstreits haben der Kläger 81 % und die Beklagte 19 % zu tragen.

6. Das Urteil ist vorläufig vollstreckbar. Die Partei, gegen die vollstreckt wird, kann die Vollstreckung der anderen Partei durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die vollstreckende Partei vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

Beschluss

Der Streitwert wird auf 6.500,00 € festgesetzt.

Tatbestand

Die Parteien streiten vor dem Hintergrund von dem Kläger behaupteter Datenschutzverstöße über immateriellen Schadensersatz, Unterlassung und Auskunft.

Die Beklagte betreibt unter der Internetseite www.facebook.com das soziale Netzwerk Facebook.

Die Plattform Facebook verfügt über eine Kontakt-Import-Funktion (Contact-Import-Tool, im Folgenden CIT), mithilfe derer Nutzer des sozialen Netzwerks die Adressbücher ihrer Mobiltelefone bei Facebook mit dort hinterlegten Mobilfunknummern synchronisieren können. Das CIT verknüpft dabei die Mobilfunknummern im Adressbuch mit Nutzerprofilen, bei denen die entsprechenden Nummern hinterlegt sind. Diese Funktion soll es Nutzern erleichtern, ihre Telefonkontakte bei Facebook zu finden und dort Kontakt mit diesen aufzunehmen und sich zu vernetzen. Ein Nutzer kann dabei insbesondere auch dann über das CIT durch Eingabe seiner Mobilfunknummer gefunden werden, wenn er diese nicht - sei es öffentlich für alle Nutzer oder nur für befreundete Nutzerprofile - auf seinem Profil preisgibt. Ausreichend ist vielmehr, dass er seine Mobilfunknummer auf seinem Profil hinterlegt hat und die Auffindbarkeit dieser Nummer über das CIT in den Privatsphä-

reeinstellungen seines Nutzerprofils aktiviert ist. Hierbei handelt sich um eine von der Anzeige der Mobilfunknummer auf dem Nutzerprofil verschiedene, separat einstellbare Option. Diese Option ist bei Angabe der Mobilfunknummer bei Facebook als Voreinstellung aktiviert und muss von einem Nutzer zunächst manuell deaktiviert werden, wenn er diese nicht nutzen möchte.

Zwischen Januar und September 2019 verbreiteten Unbekannte Datensätze mit personenbezogenen Daten von ca. 533 Millionen Facebook-Nutzern aus 106 Ländern öffentlich im Internet. Die Unbekannten gelangten dabei durch die Methode des sog. „Scraping“ an die von ihnen verbreiteten Daten. Das Scraping spielte sich konkret so ab, dass die Unbekannten eine Vielzahl möglicher Mobilfunknummern über das CIT mit den bei Facebook hinterlegten Mobilfunknummern der Nutzer abgleichen ließen. Auf diese Weise war es ihnen möglich, einzelne Mobilfunknummern existierenden Nutzern zuzuordnen und die auf den Nutzerprofilen öffentlich einsehbaren Daten mit den so ermittelten Mobilfunknummern in Verbindung zu bringen.

Der Prozessbevollmächtigte des Klägers forderte die Beklagte mit E-Mail vom 02.06.2021 zur Zahlung immateriellen Schadensersatzes i.H.v. 500,00 € sowie zur Unterlassung und Auskunft wegen der behaupteten Veröffentlichung personenbezogener Daten durch Unbekannte im Rahmen des Scrapings auf Seiten im Internet auf. Außerdem verlangte er die Bezahlung vorgerichtlicher Rechtsanwaltskosten aus einem Gegenstandswert i.H.v. 8.501,00 €. Mit Schreiben vom 30.08.2021 antwortete die Beklagte durch ihre Prozessbevollmächtigten auf die klägerische E-Mail in Bezug auf den Scraping-Vorfall, ohne dass eine Zahlung erfolgte.

Der Kläger behauptet, er habe auf der Plattform Facebook ein Profil unter dem Namen „Kobra Kahn (EngBern V. Almero)“ eingerichtet, dessen Inhaber er auch sei. Auf diesem Profil teile er Inhalte von sich selbst und seiner Familie. Zu dem ihm zuzuordnenden Daten auf diesem Profil gehöre jedenfalls sein Profilname, das Geschlecht und die Nutzer-ID. Im Zuge des „Scrapings“ und der sich anschließenden Veröffentlichung von Datensätzen seien auch den Käger betreffende personenbezogene Daten im Internet auf Seiten veröffentlicht worden, z.B. auf der Seite raidforums.com. In einer unter anderem im Darknet für jedermann abrufbaren Datenbank seien seine nachfolgenden personenbezogenen Daten der enthalten:

„[redacted]“

Dabei handele es sich um die Mobilfunknummer, die Facebook-ID und den Benutzernamen des Klägers.

Der Kläger ist der Ansicht, die Privatsphäreeinstellungen auf der Plattform Facebook seien in-

transparent und unübersichtlich gestaltet. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere.

Er behauptet zudem, die Beklagte nehme keinerlei Sicherheitsvorkehrungen gegen die Ausnutzung des CIT und das Vorgehen mittels „Scraping“ vor. 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 handele. Ebenso wenig würde 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.

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. Aufgrund der Vorgänge habe er jedenfalls ab dem Jahr 2022 verstärkt Fake- bzw. Spam-Nachrichten per SMS mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks erhalten.

Der Kläger beantragt,

1. die Beklagte zu verurteilen, 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 zu verurteilen, 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, FacebookID, Familiennamen, Vornamen, Geschlecht, Bundesland, 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 zu verurteilen, 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 zu verurteilen, 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 bestreitet, dass der Kläger Inhaber des streitgegenständlichen Facebook-Profils ist bzw. behauptet, dass sie dies auf der Grundlage der vom Kläger zur Verfügung gestellten Informationen nicht (zeitnah) prüfen könne.

Die Beklagte bestreitet zudem mit Nichtwissen, dass es sich bei den vom Kläger benannten Datenpunkten um einen authentischen Auszug aus den durch Scraping abgerufenen Daten handele.

Die Beklagte behauptet, es läge kein Kausalzusammenhang vor zwischen dem Vorfall des Scrapings und etwaigen Spam-Nachrichten, welche die Klagepartei erhalte oder erhalten habe.

Es gäbe keine formellen oder vorgeschriebenen Branchen- oder Industriestandards zur Bekämp-

fung von Scraping. Im Einklang mit der Marktpraxis habe die Beklagte während des relevanten Zeitraums sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt. Die Beklagte habe ihre Maßnahmen zudem zur Verringerung von Scraping und als Reaktion auf sich ständig ändernde Bedrohungen fortlaufend weiterentwickelt. Sie beschäftige zudem 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, dass Scraping-Aktivitäten unternommen werden. 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 zudem mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen Scraper vor. Es sei jedoch nicht möglich Scraping von Daten, welche Nutzer öffentlich zugänglich gemacht hätten, zu einhundert Prozent auszuschließen, noch könne dies von der Beklagten verlangt werden.

Die Beklagte rügt zudem die sachliche Zuständigkeit des Landgerichts, weil der Streitwert unter 5.000,00 € liege, und beantragt die Verweisung an das Amtsgericht.

Das Gericht hat den Kläger im Vorfeld der mündlichen Verhandlung persönlich und informell angehört. Wegen des weiteren Sach- und Streitstands wird auf die zwischen den Parteien gewechselten Schriftsätze nebst Anlagen sowie das Protokoll der mündlichen Verhandlung vom 07.02.2023 (Bl. 324 ff. d.A.) Bezug genommen.

Entscheidungsgründe

A.

Die Klage ist im Hinblick auf die Klageanträge Ziffer 1, 4 und 5 zulässig und hinsichtlich der übrigen Klageanträge bereits unzulässig. Begründet ist sie lediglich im Hinblick auf den Klageantrag Ziffer 1 sowie teilweise Ziffer 4 und Ziffer 5.

I.

Die vor dem zuständigen Landgericht Stuttgart erhobene Klage ist im Hinblick auf die Klageanträge Ziffer 1, 4 und 5 zulässig. Im Übrigen ist die Klage unzulässig.

1.

Das Landgericht Stuttgart ist international, örtlich und sachlich zuständig.

a)

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

Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Nach Art. 18 Abs. 1 Alt. 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher, hier also der Kläger, seinen Wohnsitz, hier also in der Bundesrepublik Deutschland, hat. Die internationale Zuständigkeit deutscher Gerichte ergibt sich zudem aus Art. 79 Abs. 2 DSGVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

b)

Das Landgericht Stuttgart ist örtlich zuständig, weil der Kläger seinen Wohnsitz im Landgerichtsbezirk Stuttgart hat. Das folgt zum einen aus Art. 18 Abs. 1 Alt. 2 EuGVVO, zum anderen aus Art. 79 Abs. 2 Satz 2 DS-GVO.

c)

Das Landgericht Stuttgart ist gemäß §§ 23, 71 GVG auch sachlich zuständig, weil der Zuständigkeitsstreitwert 6.500,00 € beträgt und damit 5.000,00 € überschreitet (OLG Stuttgart, Beschl. v. 03.01.2023 - 4 AR 4/22).

Der Streitwert für den Klageantrag Ziffer 1 ergibt sich aus dem vom Kläger vorgestellten (Mindest-)Schadensersatzbetrag in Höhe von 1.000,00 Euro.

Der Streitwert für den Klageantrag Ziffer 2 orientiert sich an den Vorstellungen des Klägers im Hinblick auf den Klageantrag Ziffer 1, ist allerdings nur mit einem angemessenen Bruchteil von 50 % zu bemessen und beträgt daher 500,00 €-

Der Streitwert für die Unterlassungsanträge in Ziffer 3 beträgt entsprechend der ursprünglichen Einschätzung der Beklagten 4.500,00 Euro.

Der auf Erteilung von Auskunft nach Art. 15 DSGVO gerichtete Klageantrag Ziffer 4 geht wertmä-

ßig zum größten Teil in den Klageanträgen Ziffer 1 und 2 auf, weshalb ihm lediglich ein Streitwert von 500,00 Euro zuzumessen ist.

2.

Der Klageantrag Ziffer 1 ist hinreichend bestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO. Entgegen der Ansicht der Beklagten liegt dem Antrag 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 keiner Stelle des klägerischen Vortrags.

Die unbezifferte, lediglich mit einem Mindestbetrag erhobene Leistungsklage 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).

3.

Für die mit dem Klageantrag Ziffer 2 begehrte Feststellung fehlt das erforderliche Feststellungsinteresse. Denn der Kläger hat bereits nicht substantiiert dargelegt, inwiefern ihm aufgrund des Scrapings und der Datenveröffentlichung unbekannte oder zukünftige Schäden drohen, welche der Beklagten zuzurechnen sein könnten. Der bloße Erhalt weiterer, auf den Vorfall zurückzuführender Spam-Nachrichten würde keinen weiteren Schaden des Klägers begründen. Denn die Spam-Nachrichten an sich stellen keinen materiellen oder immateriellen Schaden dar. Ein der Beklagten zuzurechnender immaterieller Schaden wird vielmehr allein dadurch begründet, dass personenbezogene Daten des Klägers, welche der Beklagten anvertraut worden waren, abgeschöpft und veröffentlicht wurden und somit die Möglichkeit eines Missbrauchs durch Dritte eröffnet wird. Die Abschöpfung und Veröffentlichung sind allerdings bereits erfolgt und eine weitere Verbreitung vertieft nicht ohne weiteres den entstandenen Schaden. Ein Missbrauch durch Dritte ist der Beklagten hingegen nicht mehr zuzurechnen, da sie hierauf keinen Einfluss hat und diesen auch nicht mehr verhindern kann. Ein dadurch entstehender materieller Schaden, dass der Kläger auf eine der Spam-Nachrichten eingeht, wodurch in der Folge durch betrügerische Handlungen Dritter Vermögensschäden entstehen, wäre der Beklagten erst recht nicht zuzurechnen. Zudem hat der Kläger im Rahmen seiner informatorischen Anhörung ohnehin überzeugend darge-

legt, dass er Spam-Nachrichten erkennen und folgerichtig ignorieren kann, so dass der Eintritt eines solchen materiellen Schadens auch nicht wahrscheinlich ist.

4.

Im Hinblick auf das mit Klageantrag Ziffer 3 geltend gemachte Unterlassungsverlangen fehlt es an einem Rechtsschutzbedürfnis des Klägers. Das Rechtsschutzbedürfnis ist ein schutzwürdiges Interesse an der gerichtlichen Geltendmachung des eingeklagten Rechts, welches zwingende Prozessvoraussetzung für jede Klage ist (BGH NJW-RR 1989, 263 (264); BGH NJW 1999, 1337 (1338)). Das Rechtsschutzbedürfnis kann hierbei fehlen, wenn das verfolgte Begehren auf einem einfacheren Weg zu erlangen ist (BGH NJW-RR 2010, 19 Rn. 20), wobei der Kläger sich nicht auf einen prozessual unsicheren oder weniger effektiven Weg verweisen lassen muss (BeckOK ZPO/Bacher, 47. Ed. 1.12.2022, ZPO § 253 Rn. 29).

Im vorliegenden Fall kann der Kläger die begehrte Unterlassung der Verarbeitung seiner Mobilfunknummer durch die Beklagte allgemein oder im speziellen mittels des CIT selbst dadurch verhindern, dass er die Mobilfunknummer aus dem bei seinem Facebook-Profill hinterlegten Datenbestand entfernt oder jedenfalls manuell die Funktion der Suchbarkeit mittels des CIT deaktiviert. Dies ist ihm ohne jeglichen Aufwand über die Privatsphäreeinstellungen bei Facebook möglich und verhindert eine Verarbeitung auch effektiv.

In welcher Weise über die streitgegenständliche und dem Scraping-Vorfall zugrunde liegende Verarbeitung durch das CIT hinaus „über eine Software zum Importieren von Kontakten“ personenbezogene Daten des Klägers Dritten durch die Beklagte zugänglich gemacht werden könnten, erschließt sich nicht und wurde vom Kläger auch nicht dargelegt.

Sofern der Kläger bezogen auf die von der Beklagten betriebene Facebook-Messenger-App seinen Unterlassungsantrag bedingt formuliert, ist dies bereits unzulässig, da unbestimmt i.S.d. § 253 Abs. 2 Nr. 2 ZPO.

II.

Die Klage ist teilweise begründet.

1.

Der Kläger hat einen Anspruch aus Art. 82 Abs. 1 DSGVO auf Ersatz immateriellen Schadens i.H.v. 1.000,00 € gegen die Beklagte.

Der Kläger ist als Inhaber des streitgegenständlichen Facebook-Profils von einem Scraping-Vor-

fall betroffen und es liegen seitens der Beklagten mehrere Verstöße gegen die DSGVO vor, welche in diesem Zusammenhang zur Auslösung einer entsprechenden Schadensersatzpflicht geeignet sind.

a)

Der Kläger ist Inhaber des streitgegenständlichen Facebook-Profils „[redacted]“. Zwar mag es zutreffend sein, dass das streitgegenständliche Facebook-Profil nicht mit der vom Kläger ursprünglich genannten E-Mail-Adresse [redacted] verknüpft ist, wie die Beklagte vorträgt. Der Kläger hat zu einem späteren Zeitpunkt aber dargelegt, dass das streitgegenständliche Facebook-Profil mit seiner Handynummer verknüpft ist (Bl. 192 d.A.). Bereits dies hat die Beklagte nicht mehr substantiiert bestritten, sondern lediglich eingewandt, die Inhaberschaft am streitgegenständlichen Facebook-Profil sei aufgrund der widersprüchlichen Angaben des Klägers nicht zweifelsfrei aufklärbar und sie werde im Verfahren keine Auskünfte erteilen, um keinen Datenschutzverstoß zu begehen. Überdies hat der Kläger sich im Rahmen der mündlichen Verhandlung an seinem Handy auch in das streitgegenständliche Facebook-Profil eingeloggt, was seine Inhaberschaft nach Überzeugung des Gerichts selbst im Falle eines substantiierten Bestreitens durch die Beklagte belegen würde. Die Beklagte hat zudem nicht substantiiert bestritten, dass die vom Kläger genannten personenbezogenen Daten vom Scraping-Vorfall betroffen waren und im Darknet von jedermann abgerufen werden können.

c)

Die Beklagte hat zudem mehrere Verstöße gegen die DSGVO begangen, welche zur Auslösung einer entsprechenden Schadensersatzpflicht geeignet sind.

aa)

Es fehlt bereits eine ordnungsgemäße, ausreichende Belehrung des Klägers durch die Beklagte zum Zeitpunkt der Datenerhebung hinsichtlich der Mobilfunknummer des Klägers gemäß Art. 13 DSGVO.

Das Gericht nimmt insoweit in rechtlicher Hinsicht Bezug auf die Ausführungen des Landgerichts Paderborn in dessen Urteil vom 19.12.2022 im dortigen Rechtsstreit mit dem Aktenzeichen 2 O 236/22, welches eine andere Klagepartei gegen die hiesige Beklagte führte und welchem ein in wesentlichen Teilen identischer, im Übrigen jedenfalls vergleichbarer Sachverhalt zugrunde lag. Das Landgericht Paderborn führt aus:

„Die Verletzung der nach Art. 13 DSGVO bestehenden Informations- und Aufklärungspflichten ist vom Anwendungsbereich des Schadensersatzanspruches des Art. 82 DSGVO erfasst.

Ein Schadensersatzanspruch nach Art. 82 DSGVO kann nur dann begründet werden, wenn nach dessen Absatz 2 Satz 1 ein Schaden durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen die Informations- und Aufklärungspflichten des Art. 13 DSGVO bereits mit der Erhebung personenbezogener Daten. Bereits zu diesem Zeitpunkt hat der Verantwortliche – wie noch auszuführen sein wird – gegenüber dem Betroffenen umfangreiche Informationspflichten zu erfüllen. Bildet – wie hier – die Einwilligung des Betroffenen nach Art. 6 Abs. 1 lit. a) DSGVO die Grundlage des Datenerhebungs- und somit auch des Datenverarbeitungsvorganges, kann eine solche Einwilligung unter Berücksichtigung der in der DSGVO vorherrschenden Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten keinen Bestand haben, wenn dem Betroffenen nicht bereits bei Datenerhebung sämtliche nach Art. 13 DSGVO erforderlichen Informationen mitgeteilt werden.

Gemäß Art. 13 DSGVO hat der Verantwortliche eines Datenverarbeitungsprozesses gegenüber dem Betroffenen, dessen personenbezogene Daten verarbeitet und bei diesem erhoben werden, umfangreiche Informations- und Aufklärungspflichten zu erfüllen. Entsprechend der Legaldefinition des Art. 4 Ziffer 2 DSGVO entstehen diese Informations- und Aufklärungspflichten bereits mit der Erhebung personenbezogener Daten. Teilt der Verantwortliche dem Betroffenen bereits bei Datenerhebung die in Art. 13 Abs. 1 und Abs. 2 DSGVO vorgesehenen Informationen nicht vollständig oder inhaltlich unrichtig mit, verletzt er seine Informationspflichten.

Nach Art. 13 Abs. 1 lit. c) DSGVO besteht eine Informationspflicht insbesondere dahingehend, dass der Verantwortliche dem Betroffenen die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung mitteilt. Sinn und Zweck dieser Regelung ist, dass der Betroffene eines Datenverarbeitungsprozesses unter Berücksichtigung der Grundsätze einer fairen und transparenten Verarbeitung von personenbezogenen Daten nicht nur über die Existenz des Verarbeitungsvorganges, sondern darüber hinaus auch über die Zwecke der Verarbeitung unterrichtet wird (Ehmann/Selmayr/Knyrim, 2. Aufl. 2018, DS-GVO Art. 13 Rn. 1).

Die Beklagte hat den Kläger bei Datenerhebung hinreichend darüber aufgeklärt, dass dessen Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“, zu Werbezwecken sowie zum Zweck der Kommunikation mit Facebook verwendet wird.

(...)

Die Beklagte hat den Kläger allerdings bei Erhebung der Daten seiner Mobilfunknummer unzureichend über den Zweck der Verwendung seiner Mobilfunknummer für das seitens der Beklagten verwendete Contact-Import-Tool (kurz: CIT) aufgeklärt. Hierdurch hat sie ihre Informations- und Aufklärungspflichten nach Art. 13 Abs. 1 lit. c) DSGVO verletzt.

Die Kammer vermochte nicht festzustellen, dass die Beklagte den Kläger bei Datenerhebung über den Zweck, seine Mobilfunknummer über die „Zwei-Faktor-Authentifizierung“ hinaus auch für das durch sie verwendete CIT zu verwenden, aufgeklärt hat. Eine solche Aufklärung kann weder bei Hinzufügen der Mobilfunknummer im Rahmen der Registrierung unter Bezugnahme der Datenrichtlinie noch bei späterem Hinzufügen der Mobilfunknummer in der Rubrik „Handy-Einstellungen“ festgestellt werden.

Die Beklagte hatte gegenüber dem Kläger bei Datenerhebung eine Informations- und Aufklärungspflicht nach Art. 13 Abs. 1 lit. c) DSGVO dahingehend, diesen über die beabsichtigte Verwendung seiner Mobilfunknummer für das CIT aufzuklären.

Durch die Verwendung des CIT ermöglicht die Beklagte einem Benutzer den Abgleich, der in seinem Smartphone gespeicherten Personenkontakte mit auf Facebook registrierten Benutzerprofilen, die ihr Benutzerprofil jeweils mit einer Mobilfunknummer verknüpft haben. Durch die Eingabe einer beliebigen Mobilfunknummer wird dem Benutzer ermöglicht, das mit der Mobilfunknummer verknüpfte Benutzerprofil als „Freunde“ hinzuzufügen.

Der Datenrichtlinie lässt sich eine Aufklärung über das von der Beklagte verwendete CIT nicht entnehmen.

Der mit der Anlage B9 überreichten Datenrichtlinie aus dem Jahr 2018 lässt sich auf den Seiten 3 und 4 unter der Überschrift „Wie verwenden wir diese Informationen“ entnehmen, dass die von einem Benutzer bereitgestellten Informationen zur Bereitstellung, Verbesserung und Entwicklung der Dienste, zur Kommunikation mit dem die Informationen bereitstellenden Benutzer, zum Anzeigen und Messen von Werbeanzeigen und Diensten sowie zur Förderung der Sicherheit verwendet werden. Ein Hinweis auf die Verwendung

der Mobilfunknummer für das CIT erfolgt nicht.

Auch den Hinweisen auf den Seiten 5 und 6 der Datenrichtlinie unter der Überschrift „Wie werden diese Informationen geteilt“ lässt sich ein Hinweis auf die Verwendung der Mobilfunknummer für das CIT nicht entnehmen.

Dass die Beklagte den Kläger über das durch sie verwendete CIT aufgeklärt hat, lässt sich auch nicht der Rubrik „Handy-Einstellungen“ sowie der Unterverlinkung durch einen Klick auf „Mehr dazu“ entnehmen.

Dort findet sich – wie bereits ausgeführt – zum einen die Aufklärung seitens der Beklagten über die Verwendung der Mobilfunknummer zum Zweck der „Zwei-Faktor-Authentifizierung“.

Zum anderen erfolgt der Hinweis, dass durch das Hinzufügen der Mobilfunknummer eben diese mit dem Benutzerkonto verknüpft ist und der jeweilige Benutzer festlegen kann, welche Personen dessen Mobilfunknummer sehen können und welche Personen auf Facebook nach der betroffenen Person suchen können. Ein weitergehender Hinweis, dass die betroffene Person durch das CIT der Beklagten im Wege eines Kontaktabgleichs durch Eingabe einer Mobilfunknummer gefunden werden kann, lässt sich den Einstellungen gerade nicht entnehmen.

Ein Hinweis auf die Verwendung des CIT lässt sich ferner nicht den auszugsweise dem Hilfebereich entnommenen Informationen, überreicht als Anlagen B5 und B6, entnehmen.

Ungeachtet dessen, dass es auf die Informationen im Hilfebereich schon nicht ankommen dürfte, da die Datenerhebung – entweder durch Hinzufügen der Mobilfunknummer bei der Registrierung oder bei den „Handy-Einstellungen“ – bereits erfolgt ist und eine Aufklärung wie bereits ausgeführt unterblieben ist, findet sich auch in diesem Bereich kein Hinweis auf die Verwendung des CIT.“

Diese Ausführungen des Landgerichts Paderborn sind insbesondere aufgrund derselben Belehrungen, Hinweise und Datenschutzrichtlinie welche im dortigen als auch im hiesigen Fall durch die Beklagte verwendet wurden, vollumfänglich auf den vorliegenden Fall übertragbar. Das Gericht kann die durch das Landgericht Paderborn getroffenen Feststellungen mithin ebenso für den hiesigen Fall treffen, da auch Parteivortrag, welcher entgegenstünde, nicht ersichtlich ist, sodass von einem übereinstimmenden Sachverhalt auszugehen ist. In rechtlicher Hinsicht macht sich

das Gericht die überzeugenden Ausführungen des Landgerichts Paderborn vollumfänglich zu eigen.

b)

Zudem liegt ein datenschutzrechtlicher Verstoß der Beklagten, der die Schadensersatzpflicht nach Art. 82 Abs. 1 DSGVO auslöst, gemäß Art. 32, 24, 5 Abs. 1 lit. f) DSGVO vor.

Auch in dieser Hinsicht nimmt das Gericht auf die Ausführungen des Landgerichts Paderborn in dessen Urteil vom 19.12.2022 im dortigen Rechtsstreit mit dem Aktenzeichen 2 O 236/22 Bezug:

„Art. 32 DSGVO regelt die Pflicht des Verantwortlichen und des Auftragsverarbeiters, bestimmte technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Hinblick auf die verarbeiteten personenbezogenen Daten zu gewährleisten. Er konkretisiert die als Generalauftrag gestalteten Datensicherheitsmaßnahmen des Art. 24 DSGVO und dient damit u.a. der Gewährleistung der Absicherung der Datenschutzgrundsätze der Vertraulichkeit und Integrität nach Art. 5 Abs. 1 f) DSGVO. Zielrichtung ist ein umfassender Schutz der für die Verarbeitung von personenbezogenen Daten genutzten Systeme, also im Kern die Datensicherheit (Sydow/Marsch DSGVO/BDSG/Mantz, 3. Aufl. 2022, DSGVO Art. 32 Rn. 1).

Das Gebot soll insbesondere personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten oder es unbeabsichtigt zu einem Verlust, einer Zerstörung oder Schädigung der Daten kommt (Paal/Pauly/Martini, 3. Aufl. 2021, DSGVO Art. 32 Rn. 2; vgl auch Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DSGVO Art. 32 Rn. 2).

Bei der Implementierung von geeigneten technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DSGVO sind dabei der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen als Faktoren zu berücksichtigen. Dies bedeutet allerdings nur, dass sie in die Verhältnismäßigkeitsprüfung einzustellen, jedoch nicht notwendigerweise absolut zu befolgen sind (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 14).

Die DSGVO legt zur Bemessung der Geeignetheit der Maßnahmen insbesondere weiter fest, dass diese ein dem Risiko der Verarbeitung angemessenes Schutzniveau bieten

müssen. Dabei kommt es letztlich darauf an, wie groß die Risiken sind, die den Rechten und Freiheiten der betroffenen Person drohen und wie hoch die Wahrscheinlichkeit eines Schadenseintritts ist. Damit ergibt sich, dass die Maßnahmen umso wirksamer sein müssen, je höher die drohenden Schäden sind (Ehmann/Selmayr/Hladjk, 2. Aufl. 2018, DS-GVO Art. 32 Rn. 4; Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 4). Dies wird vor allem anhand der Sensibilität der Daten und der Wahrscheinlichkeit eines Schadeneintritts bestimmt (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 41).

Art. 32 Abs. 1 DSGVO verpflichtet den Verantwortlichen und Auftragsverarbeiter aber nicht zu einem absoluten Schutz(niveau) der Daten. Das Schutzniveau muss vielmehr, je nach Verarbeitungskontext, dem Risiko bezüglich der Rechte und Freiheiten der betroffenen Personen im Einzelfall angemessen sein. Dies bedeutet gleichzeitig, dass das Risiko nicht völlig ausgeschlossen werden kann und dies auch nicht Ziel der umzusetzenden Maßnahmen ist (Gola/Heckmann/Piltz, 3. Aufl. 2022, DS-GVO Art. 32 Rn. 11; vgl. auch Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 3).

Zur Bestimmung des angemessenen Schutzniveaus sind gem. Art. 32 Abs. 2 DSGVO insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. Diese sind zwingend in die Risikobetrachtung einzubeziehen (Spindler/Schuster/Laue, 4. Aufl. 2019, DS-GVO Art. 32 Rn. 5).

Ausweislich des Erwägungsgrunds 76 zur DSGVO sollten die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten des betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

Dieser umfassenden Risikobestimmung anhand der genannten Kriterien ist die Beklagte zumindest nicht ausreichend nachgekommen. Denn die von ihr behaupteten „Anti-Scraping-Maßnahmen“ sind selbst, wenn der Beweis zum Vorliegen der Maßnahmen für den streitgegenständlichen Zeitraum geführt werden würde, für sich allein nicht geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Das CIT ermöglicht einen unbefugten Zugang i.S.d. Art. 32 Abs. 2 DSGVO. Beim Zu-

gang zu Daten geht die entscheidende Aktivität vom Empfänger der Daten aus. Der Verantwortliche muss lediglich durch die Ausgestaltung der technischen Bedingungen die Daten grundsätzlich zum Abruf durch Dritte ermöglichen. Dieses Bereithalten der Daten zum Abruf kann z.B. durch das Einräumen von Zugriffsrechten im Rahmen von Netzwerken oder durch Einstellung in eine Datenbank, auf die auch Dritte zugreifen können, erfolgen (Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 32 Rn. 34).

So liegt der Fall hier, da das CIT zweckwidrig nicht zum Auffinden von persönlichen Kontakten auf Facebook, sondern entgegen der Nutzungsbedingungen der Beklagten zu Missbrauchszwecken genutzt werden konnte und wurde. Es wird Dritten eine Zuordnung von Telefonnummer zum Facebook-Profil, bei dem diese angegeben wurde, ermöglicht. Dementsprechend wird in Erfahrung gebracht, welche Person hinter der Telefonnummer steht. Hierbei können durch den Rückgriff auf das Facebook-Profil gleichzeitig weitere Informationen über die Person eingeholt werden. Dies birgt für die Nutzer das Risiko von gezielten Phishing-Attacken, Identitätsdiebstahl und weiteren Missbrauch der Daten und damit dem Eintritt von materiellen oder immateriellen Schäden.

Dieses zwingend zu berücksichtigende Risiko bedingt bereits, dass der Maßstab für die Bestimmung der Angemessenheit des Schutzniveaus entsprechend hoch anzusetzen ist. Dies begründet sich unter anderem daraus, dass das CIT-Verfahren nicht eine reine Erhebung oder Speicherung von Daten durch die Beklagten darstellt. Auch handelt es sich bei den Daten nicht um ohnehin öffentlich einsehbare Daten. Vielmehr wird Dritten ein Zugang zu diesen, insbesondere der Telefonnummer des Nutzers, gewährt. Es erfolgt eine Verknüpfung der zuvor nicht öffentlich einsehbaren Telefonnummer zu den weiteren Daten des Nutzers auf der Facebook-Plattform der Beklagten.

Die Gefahr einer Veröffentlichung aller zusammengetragenen Daten, darunter insbesondere die Verknüpfung von Telefonnummer und Name, ist, wie der vorliegende Datenscraping-Fall aufzeigt, besonders hoch. „Scraping“ ist weit verbreitet und entsprechende Versuche bei dem weltweit genutzten sozialen Netzwerk der Beklagten auch aus einer ex-ante-Sicht zu erwarten gewesen. Dem ist sich auch die Beklagte bewusst. Für sie ist ausweislich ihres Artikels „Die Fakten zu Medienberichten über Facebook-Daten“ vom 06.04.2021 (Anlage B10) Scraping „eine gängige Taktik.“ Die Beklagte musste sich daher darüber bewusst sein, dass Maßnahmen für ein angemessenes Schutzniveau für die personenbezogenen Daten hinsichtlich des Risikos von Scraping zu treffen waren.

Soweit die Beklagte nun darauf abstellt, dass sie gegen Scraper mittels Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren vorgehe, kommt diese Maßnahme bereits erst dann zu tragen, wenn ein Datenscraping tatsächlich eingetreten ist. Die Daten sind in diesem Stadium bereits entwendet worden. Eine Veröffentlichung oder anderweitiger Missbrauch kann in diesem Stadium praktisch nicht mehr verhindert werden.

Des Weiteren ist die behauptete teilweise Einschränkung des CIT auch nach dem Beklagtenvorbringen erst nach dem streitgegenständlichen Vorfall eingeführt worden. Auch die Beschäftigung eines Teams von Datenwissenschaftlern, -analysten und Softwareingenieuren zur Bekämpfung von Scraping, Übertragungsbeschränkungen sowie CAPTCHA-Abfragen genügen den Anforderungen des Art. 32 DSGVO im vorliegenden Fall allein nicht. Die Beklagte legt diesbezüglich bereits nicht dar, wie es bei den – aus ihrer Sicht im hiesigen Verfahren ausreichenden – Sicherheitsmaßnahmen dennoch zum streitgegenständlichen Datenscraping kommen konnte.

Ungeachtet dessen, ist klarzustellen, dass dies nicht bedeutet, dass die genannten Maßnahmen nicht grundsätzlich den Schutz von personenbezogenen Daten fördern. Aufgrund des hohen Risikopotenzials, das von einem Missbrauch des CIT ausgeht, waren jedoch weitergehende Maßnahmen für ein angemessenes Schutzniveau erforderlich.

CAPTCHA-Abfragen werden z.B. bereits bei geringeren Risiken im Umgang mit personenbezogenen Daten eingesetzt. Die Arbeit des EDM-Teams entfaltet des Weiteren ausweislich des Vorbringens der Beklagten in der Regel erst während eines bereits begonnen Scraping-Prozesses ihre Wirkung, sodass Scraper in diesem Zeitpunkt bereits Datensätze erlangt haben. Außerdem ist es Scrapern möglich, Übertragungsbeschränkungen zu umgehen.

Daher wären weitergehende Maßnahmen notwendig gewesen. Diese hätten beispielsweise so ausgestaltet werden können, dass weitergehende Informationen neben der Telefonnummer für die Nutzung des CIT anzugeben sind. Es kann ein Missbrauch des CIT in Form von Datenscraping dann zumindest erschwert werden, so z.B. durch die weitere Angabe eines Vornamens, der sich neben der Telefonnummer ebenfalls hochladen ließe. So würden weitere Variablen hinzutreten, die auf eine den Nutzungsbedingungen entsprechende Nutzung des CIT hindeuten. Datenscraper hingegen werden vor das Problem gestellt, das neben Variablen in Form von Zahlen auch Variablen in Form von Worten hinzutreten. Dies erschwert ein automatisiertes Verfahren. Zudem wäre ein höherer Datenverkehr erfor-

derlich, der ggf. den bereits behaupteten Maßnahmen der Übertragungsbeschränkungen und der Arbeit des EDM-Teams einen größeren Nutzen verleiht. Dies würde auch nicht dem von der Beklagten verfolgten Zweck zuwiderlaufen. Denn laut der Beklagten sei es Hauptzweck der Facebook-Plattform, andere Nutzer zu finden und mit diesen in Kontakt zu treten. Das CIT ermöglicht dementsprechend Nutzer ihre Kontakte ihrer Mobilgeräte auf Facebook hochzuladen und anhand der Telefonnummern die Facebook-Profile ihrer Kontakte zu finden. Weitergehende Angaben laufen diesen Absichten nicht zuwider, zumal diese ggf. ebenfalls über das CIT automatisch über die Kontaktliste des Mobilgeräts des Nutzers in Erfahrung gebracht werden könnte.

Diese oder andere Schutzmaßnahmen, wie die klägerseits angeführten Begrenzungen der abgleichbaren Rufnummern oder Nutzung nur für Freunde von Freunden, implementierte die Beklagte jedoch vor oder während des streitgegenständlichen Datenscrapings nicht. Erst im Nachgang implementierte die Beklagte eine vergleichbare Sicherheitsmaßnahme, der sog. „Social Connection Check". Die Beklagte nahm damit vielmehr erst den Vorfall zum Anlass ihre Schutzmaßnahmen zu evaluieren und traf ausweislich ihres als Anlage B11 vorgelegten Artikel „Scraping nach Zahlen" vom 19.05.2021 „eine Reihe von Verbesserungen" im September 2019."

Diese Ausführungen des Landgerichts Paderborn macht sich das Gericht ebenfalls zu eigen, da sie vollumfänglich auf den hiesigen Sachverhalt zutreffen. Das Gericht konnte eben die vom Landgericht Paderborn getroffenen Feststellungen auch in Bezug auf den hiesigen Sachverhalt treffen. Die überzeugende rechtliche Würdigung des Landgerichts Paderborn ist daher entsprechend auf den vorliegenden Rechtsstreit übertragbar.

c)

Es kann dahinstehen, ob die Beklagte außerdem Melde-, Benachrichtigungs- und Transparenzpflichten aus Art. 33, 34 und 25 DSGVO verletzte und ob eine etwaige Verletzung dieser Vorschriften geeignet wäre, eine Schadensersatzpflicht gemäß Art. 82 Abs. 1 DSGVO auszulösen, da die Beklagte bereits aus den dargelegten Verstößen gegen Art. 13, 32, 24, 5 Abs. 1 lit. f) DSGVO haftet.

d)

Die Beklagte kann sich im Hinblick auf die oben dargelegten Datenschutzverstöße auch nicht mit Erfolg gemäß Art. 82 Abs. 3 DSGVO exkulpieren.

Eine solche Exkulpation wäre nur möglich, wenn die Beklagte sämtliche Sorgfaltsanforderungen erfüllt hätte und ihr nicht die geringste Fahrlässigkeit vorzuwerfen wäre (BeckOK DatenschutzR/Quaas, 42. Ed., Art. 82 DSGVO Rn. 17 ff.). Dies kann im vorliegenden Fall bereits wegen des Verstoßes der Beklagten gegen Art. 13 DSGVO ausgeschlossen werden, weil die Beklagte insoweit nichts vorbringt, was nicht zumindest leichte Fahrlässigkeit hinsichtlich des fehlenden Hinweises auf die Verarbeitung der Mobilfunknummer des Klägers durch das CIT vermuten lässt.

Auch im Hinblick auf die unzureichenden Sicherheitsmaßnahmen gemäß Art. 32 DSGVO konnte die Beklagte nicht jegliche Verantwortung ihrerseits widerlegen. Vielmehr nutzten unbekannte Dritte bereits erkannte oder erkennbare Angriffswege, um auf Daten zuzugreifen, sodass die Nichtverantwortlichkeit des Verantwortlichen nicht nachgewiesen werden kann (Paal/Pauly/Frenzel, 3. Aufl. 2021, DS-GVO Art. 82 Rn. 15; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 54). Scraping ist ausweislich des Beklagtenvorbringens „eine gängige Taktik“. Es war jedenfalls erkennbar, dass das CIT durch Scraping ausgenutzt werden kann. Dies begründet sich bereits aus dem Umstand, dass die Beklagte selbst Schutzmaßnahmen behauptet und somit von der Notwendigkeit dieser ausgeht. Im Übrigen behauptet die Beklagte das Vorliegen ganz ungewöhnlicher Kausalverläufe, einen Fall höherer Gewalt oder ein weit überwiegendes eigenes Fehlverhalten des Klägers nicht (vgl. hierzu ebenso Landgericht Paderborn, Urteil vom 19.12.2022, Az. 2 O 236/22).

e)

Dem Kläger steht aufgrund der vorstehenden Ausführungen ein Anspruch auf immateriellen Schadensersatz zu, der der Höhe nach mit 1.000,00 Euro zu bemessen war.

Hierbei kann es auch dahinstehen, ob im Rahmen des Art. 82 Abs. 1 DSGVO ein über den datenschutzrechtlichen Verstoß des Verantwortlichen hinausgehender Schaden erforderlich ist oder ob bei bloßen Bagatellfällen der Schadensersatz jedenfalls zu verneinen ist (vgl. Gola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 14). Denn der Kläger hat jedenfalls einen konkreten Schaden, welcher nicht lediglich eine Bagatelle darstellt, dargelegt. Ein solcher Schaden i.S.d. Art. 82 Abs. 1 DSGVO ist bereits dann anzunehmen, wenn die datenschutzwidrige Verarbeitung dazu führt, dass die betroffene Person um ihre Rechte und Freiheiten gebracht oder daran gehindert wird, die sie betreffenden personenbezogen Daten zu kontrollieren (ArbG Dresden ZD 2021, 54).

Dass aufgrund des Scraping-Vorfalls lediglich personenbezogene Daten veröffentlicht wurden,

die der Kläger öffentlich auf seinem Facebook-Profil preisgab und welche dort für jedermann einsehbar waren, steht einem Schaden nicht entgegen. Auch der Umstand, dass die Mobilfunknummer von den Unbekannten ermittelt wurde und nicht aus dem Datenbestand der Beklagten abgeschöpft wurde, schließt einen Schaden nicht aus. Entscheidend ist nämlich die Verbindung zwischen der Mobilfunknummer und den sonstigen personenbezogenen Daten, welche den Unbekannten nur aufgrund der Datenschutzverstöße der Beklagten im Zusammenhang mit dem CIT ermöglicht wurde. Gerade diese Korrelation zwischen der nicht durch den Kläger veröffentlichten Mobilfunknummer und den sonstigen öffentlich auf dem Profil des Klägers einsehbaren personenbezogenen Daten war nur aufgrund der Möglichkeit der rechtswidrigen Nutzung des CIT möglich. Dies muss sich die Beklagte vorwerfen lassen, da sie zum Schutz der Daten der Nutzer ihrer Plattform dazu verpflichtet war, einen entsprechenden Vorfall zu verhindern. Hierauf beruht der datenschutzrechtlich relevante Schaden des Klägers.

Denn dem Kläger kam es entscheidend darauf an, dass seine Mobilfunknummer nicht mit den sonstigen personenbezogenen Daten auf seinem Facebook-Profil in Verbindung gebracht werden konnte. Im Zuge der Abschöpfung und Veröffentlichung der Daten fand eine Korrelation mit der Mobilfunknummer des Klägers statt, was nicht nur dazu führte, dass etwaige Facebook-Kontakte des Klägers die Möglichkeit hatten, die private Mobilfunknummer des Klägers zu erfahren und diese seinem Facebook-Profil zuzuordnen, sondern auch sonstige Dritte, welche damit potentiell auch die Möglichkeit hatten und haben, diese Informationen für kriminelle Zwecke gegenüber dem Kläger zu nutzen. Ein solcher Kontrollverlust stellt einen erheblichen Schaden im Sinne des Art. 82 Abs. 1 DSGVO dar. Von untergeordneter Bedeutung ist dabei die Tatsache, dass der Kläger nicht seinen Klarnamen, sondern das Pseudonym „Kobra Kahn“ bei Facebook verwendete. Denn in einem Klammerzusatz findet sich auch der richtige, bürgerliche Namen des Klägers (vgl. Bl. 192 d.A.).

Was das Gewicht des immateriellen Schadens und den hierauf basierenden Schadensersatzanspruch des Klägers anbelangt, ist zu berücksichtigen, dass der Beklagten eine Löschung der veröffentlichten personenbezogenen Daten nicht möglich ist und realistischerweise auch künftig nicht möglich sein wird. Denn diese personenbezogenen Daten kursieren frei und potentiell auf ewige Zeit im Internet. Der Kläger hat auch plausibel und glaubhaft Beeinträchtigungen durch Spam-Nachrichten, insbesondere durch Spam-SMS, dargelegt, welche im kausalen Zusammenhang mit der Veröffentlichung ihrer personenbezogenen Daten stehen können. Auch in Zukunft kann mit einer erhöhten Anzahl an entsprechenden Nachrichten aufgrund dessen gerechnet werden.

2.

Der Zinsanspruch folgt aus §§ 288, 291 BGB.

3.

Dem Kläger steht gegen die Beklagte auch ein Anspruch auf Auskunft gemäß Art. 15 Abs. 1 DS-GVO im aus dem Tenor ersichtlichen Umfang zu. Da die Beklagte sich insbesondere in ihrem vorgerichtlichen Schreiben vom 30.08.2021 auf den Standpunkt gestellt hat, es sei nicht möglich, die Inhaberschaft des Klägers am streitgegenständlichen Facebook-Profil zu prüfen, ist dieser Auskunftsanspruch auch noch nicht erfüllt worden. Anders als der Kläger meint ist die Beklagte aber nicht zu Auskünften bezüglich der ihr unbekannten Aktivitäten von Dritten verpflichtet, da ihr insbesondere nicht bekannt sein kann, ob und in welcher Art und Weise Dritte die abgeschöpften Daten der Klagepartei verarbeiten.

4.

Im Rahmen des ihm zustehenden Anspruchs auf immateriellen Schadensersatz kann der Kläger auch die Erstattung vorgerichtlicher Rechtsanwaltsgebühren beanspruchen.

Ausgehend von den in Ansatz zu bringenden Gegenstandswerten für die jeweiligen Klageanträge ist der Kläger hier hinsichtlich eines Begehrens erfolgreich, dessen Wert mit bis zu 1.500,00 Euro anzunehmen ist. Insgesamt ergeben sich daher Gebühren nach Ziff. 2300, 7002, 7008 VV RVG i.H.v. 220,27 Euro, die ebenfalls nach §§ 288, 291 BGB zu verzinsen sind.

B.

Die Kostenentscheidung folgt aus § 92 Abs. 1 ZPO, wobei zugrunde gelegt wird, dass der Kläger im Hinblick auf den geltend gemachten Auskunftsanspruch zur Hälfte obsiegt hat.

Die Entscheidung über die vorläufige Vollstreckbarkeit hat ihre Rechtsgrundlage in §§ 708 Nr. 11, 711 ZPO.

In Bezug auf die Festsetzung des Streitwerts gemäß § 3 ZPO wird auf die obingen Ausführungen (A.I.1.c)) verwiesen.

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 zugelas-

sen hat.

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

Landgericht Stuttgart
Urbanstraße 20
70182 Stuttgart

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.

[redacted]
Richter