LG Augsburg, Endurteil v. 09.06.2023 – 022 O 2669/22

Titel:

Keine Ansprüche eines Nutzers gegen Facebook-Betreiber wegen Scraping-Vorfall

Normenketten:

DS-GVO Art. 5 Abs. 1 lit. a u. lit. f, Art. 6 Abs. 1, Art. 13, Art. 14, Art. 17, Art. 25 Abs. 2, Art. 82 Abs. 1
BGB § 823 Abs. 2, § 1004 Abs. 1 S. 2
GG Art. 1 Abs. 1, Art. 2 Abs. 1

Leitsätze:

1. Eine Social Media Plattform, deren Ziel es ist, Kontakte zu suchen und zu finden, ist nicht gem. Art. 25 Abs. 2 DS-GVO dazu verpflichtet, die Voreinstellungen so zu treffen, dass die Suchbarkeitsfunktion für die Telefonnummern der Nutzer gesperrt ist. (Rn. 36) (redaktioneller Leitsatz)
2. Ein Scraping-Vorfall stellt keinen nach Art. 33 DS-GVO meldepflichtigen Verstoß dar. (Rn. 37) (redaktioneller Leitsatz)
3. Ein nach Art. 82 Abs. 1 DS-GVO ersatzfähiger immaterieller Schaden muss zumindest einen realen und sicheren emotionalen Schaden bilden und nicht nur ein Ärgernis oder eine sonstige Unannehmlichkeit. (Rn. 40) (redaktioneller Leitsatz)

Schlagworte:

Datenschutzrechtliche Voreinstellung, Datenschutzverstoß

Fundstellen:

LSK 2023, 13763
ZD 2024, 118
GRUR-RS 2023, 13763

Tenor

1. Die Klage wird abgewiesen.

2. Die Klägerin hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Die Klägerin 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.

Tatbestand

1
Die Klägerin fordert von der Beklagten wegen Verstößen gegen die Datenschutzgrundverordnung Schadensersatz, Unterlassung und Auskunft.

2
Die Beklagte ist Anbieterin der F.-Plattform auf dem Gebiet der Europäischen Union. Die Klägerin ist deutsche Nutzerin dieser Plattform; sie meldet sich mit ihrer E-Mail-Adresse … an. Ihr Name, Geschlecht und Nutzer-ID waren auf dem Nutzerkonto öffentlich einsehbar (Anlage B 1 5), denn es handelt sich bei diesen Informationen um immer öffentliche Nutzerinformationen. Die Sichtbarkeit der sonstigen Daten der Klägerin (Telefonnummer, E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus) war von der Zielgruppenauswahl der Klägerin abhängig. Die Daten „Land“, „Bundesland“, „Geburtsort“ und „weitere korrelierende Daten“ entsprechen keinen Profilfeldern auf der F.-Plattform.

3
Bei der erstmaligen Anmeldung trägt der Nutzer die ihn betreffenden personenbezogenen Daten, konkret Vor- und Zuname, Handynummer oder E-Mail-Adresse, Geschlecht und Geburtsdatum, in die

Registrierungsmaske ein. Er wird auf die Nutzungsbedingungen und nach der Registrierung auf eine Fülle an Einstellungen und Untereinstellungen hingewiesen. Insoweit hat die Beklagte Voreinstellungen getroffen.

4
Die Angabe der Telefonnummer kann für eine Sicherheitsabfrage (Passwort-Rücksetzung) verwendet werden. Im Profil der Klägerin war die diesbezüglich verwendete Telefonnummer für ihre Freunde öffentlich freigegeben und daher teilweise öffentlich einsehbar. Zudem konnte die Klägerin über ihre Telefonnummer gefunden werden. Diese Einstellung war vorgegeben, aber dahingehend abänderbar, dass der Nutzer nicht anhand seiner Telefonnummer gefunden werden kann. Die Beklagte verwendet einen Kontaktimporter (Contakt-Import-Tool; Cl T). Dieser dient dazu, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf F. zu synchronisieren; dies geschieht über die hinterlegte Handynummer. Ebenso funktioniert die von der Beklagten betriebene F.-Messenger-App. Jegliches automatisiertes Sammeln von Daten (Scraping) ohne Erlaubnis war durch die Nutzungsbedingungen der Beklagten verboten.

5
Vor September 2019 generierten Unbekannte Telefonnummern und synchronisierten diese über das Kontaktimporter bzw. die F.-Messenger-App mit Profilen von F.nutzern. Die dort öffentlich abgelegten Daten wurden in der Folge abgeschöpft (gescrapt) und mit den Handynummern zusammengeführt (Anlage B 11).

6
Am 03.04.2021 veröffentlichte der Business Insider einen Artikel, wonach Informationen einer Vielzahl von F.-Nutzern von Dritten im Internet zugänglich gemacht worden seien. Die Beklagte wandte sich mit einem am 06.04.2021 in F. zugänglichen Artikel an ihre Nutzer (Anlage B 10).

7
Mit anwaltlicher E-Mail vom 02.07.2021 forderte die Klägerin die Beklagte zur Zahlung von Schadensersatz in Höhe von € 500,- sowie zur Unterlassung und Auskunft auf (Anlage K 1). Die Beklagte antwortete mit anwaltlichem Schreiben vom 30.09.2021 (Anlage B 16).

8
Die irische Datenschutzbehörde DPC verhängte gegen die Beklagten mit Bescheid vom 25.11.2022 wegen Verstoßes gegen Art. 25 I und II DSGVO eine Geldbuße in Höhe von 265 Mio. Euro und gab der Beklagten auf, Abhilfe zu schaffen (Anlage K 3).

9
Die Klägerin wurde bisher nicht Opfer eines Identitätsdiebstahls; ihr Account bei F. wurde auch nicht durch unbekannte Dritte übernommen. Die Klägerin änderte die Einstellungen in ihrem Account zwischenzeitlich dahingehend, dass ihre Telefonnummer nicht mehr über das Contakt-Import-Tool abgegriffen werden kann.

10
Die Klägerin behauptet im Wesentlichen:

11
Ihre E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus, Telefonnummer seien in den durch Scraping abgerufenen Daten enthalten gewesen.

12
Die Klägerin trägt weiter vor, sie sei von einem Datenschutzvorfall betroffen; die Beklagte habe ihre Daten unbefugten Dritten zugänglich gemacht. Eine im Darknet für jedermann abrufbare Datenbank enthalte ihre Telefonnummer, ihren Namen, ihren Wohnort und ihre Mailadresse. Diese Datensätze seien veröffentlicht worden und ermöglichten böswilligen Akteuren eine weite Bandbreite von kriminellen Machenschaften wie etwa Identitätsdiebstahl, die Übernahme von Accounts, gezielte Phishing-Nachrichten oder „Sim-Swap“-Angriffe, um Passwörter zu ändern, die durch telefonnummernbasierende Authentifizierung geschützt sind.

13
Die Klägerin gibt weiter an, sie habe aufgrund der Veröffentlichung der gescrapten Daten einen erheblichen Kontrollverlust erlitten und sei in einem Zustand des großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer Daten verblieben. Sie erhalte seit der Veröffentlichung unregelmäßig unbekannte Kontaktversuche via SMS. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen. Konkret

habe sie seit Anfang bis Mitte 2019 mehrmals wöchentlich SMS erhalten, dass beispielsweise Pakete nicht hätten zugestellt werden können oder mit ihrem P.-Konto etwas nicht stimme.

14
Ferner habe sie anfangs Anrufe aus dem Ausland erhalten, die sie jedoch nicht angenommen habe und die auch schnell wieder aufgehört hätten. Die gehe davon aus, dass diese auf das Datenscraping bei der Beklagten zurückgehen würden. Einen Schaden habe sie bisher nicht erlitten.

15
Die Klägerin behauptet schließlich, die Beklagte habe keinerlei Sicherheitsvorkehrungen gegen die Ausnutzung des Kontaktimporttools getroffen, insbesondere nicht sichergestellt, dass es sich bei der Anfrage der Synchronisierung um die Anfrage eines Menschen und nicht eines Computerprogramms gehandelt habe; ebenso wenig sei die Plausibilität der Anfragen überprüft worden, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse oder mit auffälligen Telefonnummernabfolgen automatisch abgelehnt worden wären.

16
Die Beklagte habe die Klägerin zudem zu keinem Zeitpunkt darüber informiert, dass ihre Daten durch Dritte entwendet und veröffentlicht wurden; sie habe auch die zuständige Datenschutzbehörde in Irland nicht über den Vorfall informiert.

17
Die Klägerin ist im Wesentlichen der Ansicht:

18
Die Klage sei zulässig, insbesondere bestimmt genug und es bestehe ein Feststellungsinteresse. Der Schadensersatzanspruch ergebe sich aus Art. 82 DSGVO. Der Schutzbereich sei eröffnet, die Beklagte habe gegen mehrere Pflichten der DSGVO verstoßen (Verletzung der Transparenzpflichten, Verletzung der Pflicht zur Gewährleistung angemessener technischer und organisatorischer Maßnahmen, Verletzung der Pflicht zu datenschutzfreundlichen Voreinstellungen, Verletzung der Benachrichtigungs- und Meldepflicht sowie der Auskunftspflicht)

19
Die Beklagte habe mangels wirksamer Einwilligung der Klägerin ihre Daten ohne Rechtsgrundlage und ausreichende Information verarbeitet; die Beklagte treffe die Darlegungs- und Beweislast.

20
Der Kläger beantragt zu erkennen:

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 € 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 unbefugte Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Der Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft, oder an einer ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) personenbezogene Daten der Klägerseite namentlich, Telefonnummer, F.-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugängig 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 wird und im Falle der Nutzung der F.-Messenger-App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogenen 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 fünf Prozentpunkten über dem Basiszinssatz.

21
Die Beklagte beantragt,

Klageabweisung.

22
Die Beklagte ist im Wesentlichen der Ansicht:

23
Die Klage sei weitgehend schon unzulässig, da die Klageanträge 1) bis 3) zu unbestimmt seien und der Feststellungsklage das Feststellungsinteresse fehle. Die Voraussetzungen für einen Schadensersatzanspruch nach Art. 82 DSGVO lägen nicht vor. Scraping sei kein Hacking. Weder sei der Schutzbereich eröffnet, noch lägen Verstöße gegen die DSGVO vor. Zudem fehle es an einem kausalen immateriellen Schaden, insbesondere reiche der von der Klageseite behauptete Kontrollverlust nicht aus. Die Klägerin treffe die Darlegungs- und Beweislast. Ferner fehle es an einem Verschulden der Beklagten.

24
Wegen der weiteren Einzelheiten wird auf die gewechselten Schriftsätze sowie das Protokoll der mündlichen Verhandlung vom 05.05.2023 Bezug genommen.

Entscheidungsgründe

25
I. Die zulässige Klage ist unbegründet.

26
Die Klage ist zulässig.

27
1. Das Landgericht Augsburg ist international gemäß Art. 79 II DSGVO und Art. 18 I Alt. 2 iVm Art. 17 I lit. c) VO (EU) 1215/2012 zuständig. Die Klägerin hat ihren gewöhnlichen Aufenthaltsort bzw. ihren Wohnsitz in … und damit im hiesigen Gerichtsbezirk. Die Beklagte betreibt die Plattform gewerblich; die Klägerin nutzt die Plattform für private Zwecke und ist damit Verbraucherin.

28
2. Die Anträge sind hinreichend bestimmt genug iSd § 253 II Nr. 2 ZPO. Dies gilt sowohl für den Antrag Ziffer 1 als auch für den Antrag Ziffer 3a und 3b (dazu: LG Kiel GRUR-RS 2023, 328 Rn. 25 bis 29 sowie LG Aachen GRUR-RS 2023, 2621 Rn. 32 bis 36 und 38 bis 40 zu den jeweils identischen Klageanträgen wie im vorliegenden Fall). Auch das Feststellungsinteresse bezüglich des Antrags Ziffer 2 ist zu bejahen (LG Kiel GRUR-RS 2023, 328 Rn. 30 sowie LG Aachen GRUR-RS 2023, 2621 Rn. 37).

29
II. Die Klage hat in der Sache keinen Erfolg.

30
1. Die Klage ist bereits unschlüssig, da die von der Klägerin geschilderten SMS und Anrufe von Anfang bis Mitte 2019 jedenfalls nicht kausal auf das Datenscraping vor September 2019 bei der Beklagten zurückzuführen sind. Die Daten der Benutzer der Beklagten wurden – wie von der Klägerin selbst in der

Klageschrift vorgetragen – erst ab April 2021 durch unbekannte Dritte im Internet veröffentlicht. Etwaige Anrufe und SMS Anfang bis Mitte 2019 – wie von der Klägerin in ihrer informatorischen Anhörung in der mündlichen Verhandlung vorgetragen – können folglich nicht auf dem Vorfall beruhen.

31
2. Der Klägerin stünde gegen die Beklagte jedoch auch sonst kein Anspruch auf Zahlung eines immateriellen Schadensersatzes zu.

32
a) Ein solcher Anspruch ergäbe sich nicht aus Art. 82 I DSGVO.

33
aa) Auf der Grundlage des klägerischen Vorbringens würde es bereits an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung fehlen.

34
(1) Ein Verstoß gegen die Transparenzpflichten aus Art. 5 I lit. a), 13, 14 DSGVO liegt nicht vor. Die von der Klagepartei vorgelegten Screenshots zu den Abläufen und Unterstrukturen des Internetauftritts der Beklagten sind hinreichend verständlich und transparent gestaltet. Die Klägerin als Nutzerin ist verpflichtet, sich sorgfältig mit den Hinweisen auseinanderzusetzen, um für sich eine Entscheidung zu treffen, in welchem Umfang sie Informationen freigibt und wie weitgehend sie die Kommunikationsplattform der Beklagten nutzen will (ebenso: LG Aachen GRUR-RS 2023, 2621 Rn. 49 bis 55 sowie LG Kiel GRUR-RS 2023, 328 Rn. 37 bis 41).

35
(2) Es liegt auch kein Verstoß gegen die Datenschutzpflichten aus Art. 5 I lit. f), 32 DSGVO vor. Denn es wurde ausdrücklich darauf hingewiesen, dass Name, Profilbild, Titelbild, Geschlecht, Nutzername und Nutzer-ID für alle sichtbar sind; für einen Schutz dieser Daten bestand daher kein Anlass, da diese ohnehin öffentlich waren. Hinsichtlich der Telefonnummer der Klägerin ist die Beklagte ihren Schutzpflichten ausreichend dadurch nachgekommen, dass sie in zureichender Weise darauf hingewiesen hat, dass die Klägerin die Suchbarkeits-Einstellungen abändern kann (ebenso: LG Aachen GRUR-RS 2023, 2621 Rn. 56 bis 63 sowie LG Kiel GRUR-RS 2023, 328 Rn. 42f). Zudem war durch die Nutzungsbedingungen der Beklagten jegliches automatisiertes Sammeln von Daten (Scraping) ohne Erlaubnis der Beklagten verboten.

36
(3) Die Beklagte hat auch nicht gegen die Pflicht zu datenschutzfreundlichen Voreinstellungen gemäß Art. 25 I, II DSGVO verstoßen. Die Beklagte war insoweit insbesondere nicht verpflichtet, die Voreinstellung so zu treffen, dass eine durch die Klägerin eingegebene Telefonnummer nicht dazu verwendet wird, sie über eine Suchbarkeitsfunktion zu finden. Denn bei der von der Beklagten betriebenen Plattform handelt es sich um eine Sozial Media Plattform, deren Ziel es gerade ist, Kontakte zu suchen und zu finden. Eine Sperrung der Suchbarkeitsfunktion würde diesem Ziel diametral widersprechen (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 64f sowie LG Kiel GRUR-RS 2023, 328 Tz. 44 bis 47). An dieser Einschätzung ändert sich auch nichts dadurch, dass die irische Datenschutzbehörde DPC gegen die Beklagten mit Bescheid vom 25.11.2022 wegen Verstoßes gegen Art. 25 I und II DSGVO eine Geldbuße in Höhe von 265 Mio. Euro verhängt hat (Anlage K 3). Dabei kann dahinstehen, ob dieser Bescheid Bindungswirkung entfaltet, da er unstreitig noch nicht bestandskräftig ist (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 66).

37
(4) Schließlich ist der Beklagten kein Verstoß gegen die Meldepflicht nach Art. 33 DSGVO vorzuwerfen, da es schon an einem meldepflichtigen Verstoß gegen die Datenschutzgrundverordnung fehlt (ebenso: LG Aachen GRUR-RS 2023, 2621 Rn. 67 sowie LG Kiel GRUR-RS 2023, 328 Rn. 48).

38
(5) Endlich liegt auch kein Verstoß gegen die Auskunftspflicht der Beklagten nach Art. 15 DSGVO vor. Denn die Beklagte hat gegenüber der Klägerin mit anwaltlichem Schreiben vom 30.09.2021 (Anlage B 16) Auskunft erteilt. Zu einer von Klageseite geforderte, darüber hinausgehende Auskunft war die Beklagte nicht verpflichtet; eine weitergehende Auskunft ist der Beklagten zudem nicht möglich.

39
bb) Weiter würde es an einem immateriellen Schaden der Klägerin fehlen.

40
(I) Zu den Anspruchsvoraussetzungen des Art. 82 I DSGVO zählt neben dem Verstoß gegen die Datenschutzgrundverordnung auch der Eintritt eines immateriellen Schadens (vgl. OLG Frankfurt GRUR 2022, 1252 Rn. 61 bis 64). In Anbetracht der Erwägungsgründe 75, 85, 146 und 148 der DSGVO hatte der Verordnungsgeber insoweit Diskriminierung, Identitätsdiebstahl, Identitätsbetrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden persönlichen Daten oder gesellschaftliche Nachteile ohne den Ausschluss von Bagatellschäden im Blick. Hinsichtlich eines möglichen künftigen Missbrauchs personenbezogener Daten wird ein immaterieller Schaden aber nur dann zu begründen sein, wenn es sich um einen realen und sicheren emotionalen Schaden handelt und nicht nur um ein Ärgernis oder eine Unannehmlichkeit (vgl. EuGH, Schlussanträge vom 27.04.2023 – C-340/21).

41
(2) Gemessen an diesen Maßstäben ist ein immaterieller Schaden der Klägerin zu verneinen. Die Klägerin wurde bisher unstreitig nicht Opfer eines Identitätsdiebstahls; ihr Account bei F. wurde auch nicht durch unbekannte Dritte übernommen. Die SMS und Anrufe im Jahr 2019 können – wie bereits oben ausgeführt – nicht auf das Datenscraping zurückgeführt werden. Selbst wenn etwaige Anrufe und SMS erst im Jahr 2021 erfolgt wären, bliebe streitig und unklar, ob diese auf das Datenscraping zurückzuführen sind, insbesondere auch, ob insoweit ein zeitlicher Zusammenhang bestanden hätte. Dies gilt umso mehr, als die Klägerin ihre Telefonnummer auf der F.seite für ihre Freunde öffentlich einstellte. Da allein durch das Bekanntwerden einer Telefonnummer ein Identitätsdiebstahl unwahrscheinlich ist (dazu: LG Karlsruhe, ZD 2022, 55) und die übrigen Daten der Klägerin mit deren Einwilligung ohnehin öffentlich sind, stellt die Möglichkeit eines künftigen Missbrauchs der klägerischen Daten nur eine Unannehmlichkeit dar, die gerade keinen immateriellen Schaden zu begründen vermag. Schließlich darf nicht aus den Augen verloren werden, dass nicht die Beklagte, sondern unbekannte Dritte die Daten der Klagepartei gescrapt und ins Darknet eingestellt haben sollen.

42
b) Ein Anspruch auf immateriellen Schadensersatz ergäbe sich auch nicht aus nationalem Recht. Das ergibt sich schon daraus, dass nach § 253 Abs. 1 BGB wegen eines Schadens, der nicht Vermögensschaden ist, nur in den durch das Gesetz bestimmten Fällen gefordert werden kann. Die im Gesetz genannten Ausnahmen (§ 253 Abs. 2 BGB) lägen aber ebenso wenig vor, wie eine schwerwiegende Verletzung des Persönlichkeitsrechts der Klägerin (Art. 1 I, 2 I GG).

43
2. Der Antrag der Klägerin auf Feststellung, dass die Beklagte verpflichtet ist, alle künftigen materiellen Schäden zu ersetzen, wäre ebenfalls unbegründet. Denn es liegt kein Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung vor (siehe oben Ziffer II 2 a aa).

44
3. Der Klägerin stünde gegen die Beklagte ferner kein Anspruch auf Unterlassung der Verwendung der Kontakt-Importer-Software aus §§ 1004 1 2 BGB analog iVm Art. 1 I, 2 I GG oder aus § 823 II BGB iVm Art. 6 I, 17 DSGVO zu. Auch insoweit fehlt es an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung (siehe oben Ziffer II 2 a aa).

45
4. Der Klägerin stünde gegen die Beklagte auch kein Anspruch auf Unterlassung der Verarbeitung ihrer Telefonnummer aus SS 1004 Abs. I S. 2 BGB analog iVm Art. 1 I, 2 I GG oder aus § 823 II BGB iVm Art. 6 I, 17 DSGVO zu. Auch insoweit fehlt es an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung (siehe oben Ziffer II 2 a aa). Zudem fehlt es insoweit an einer Wiederholungsgefahr. Die Klägerin gibt selbst an, dass sie die Einstellungen in ihrem Account zwischenzeitlich dahingehend geändert hat, dass ihre Telefonnummer nicht mehr von dem Kontaktimporttool abgegriffen werden kann. Eine Wiederholungsgefahr ist daher nicht erkennbar.

46
5. Schließlich stünde der Klägerin gegen die Beklagte kein Anspruch auf Auskunftserteilung nach Art. 15 I DSGVO zu. Dieser Anspruch ist gemäß § 362 I BGB erloschen, da die Beklagte mit anwaltlichem Schreiben vom 30.09.2021 (Anlage B 16) insoweit Auskunft erteilt hat. Soweit die Klageseite darüber hinaus Auskunft begehrt, inwieweit ihre Daten durch das Scraping von welchen Dritten verarbeitet wurden, ist ein Anspruch

der Klageseite bereits dem Grunde nach zu verneinen. Eine derartige Auskunft wäre der Beklagten zudem nicht möglich.

47
6. Mangels Hauptanspruch ist endlich ein Anspruch der Klägerin auf Ersatz von vorgerichtlichen Rechtsanwaltskosten zu verneinen.

48
7. Andere, durchgreifende Anspruchsgrundlagen sind nicht ersichtlich.

49
I . Die Kostenentscheidung ergibt sich aus § 91 I ZPO.

50
2. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 I Nr. 1, 71 I 1 und 2 ZPO.