

Titel:

Öffentliche Profildaten müssen nicht vor der Erhebung durch Dritte geschützt werden

Normenkette:

DSGVO Art. 4 Nr. 2, Art. 13, Art. 14, Art. 15, Art. 25, Art. 34, Art. 82 Abs. 1

Leitsätze:

1. Ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO setzt voraus, dass der Verstoß auf eine nicht DSGVO-konforme Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO zurückzuführen ist. Reine Informationspflichten nach Art. 13, Art. 14, Art. 15 oder Art. 34 DSGVO begründen demgegenüber keine Verarbeitung und können daher keinen Schadensersatzanspruch auslösen. Gleiches gilt für die organisatorischen Verpflichtungen des Verantwortlichen aus Art. 25 Abs. 1, Abs. 2 DSGVO. (Rn. 36 – 39) (redaktioneller Leitsatz)

2. Die Transparenzpflichten nach Art. 5 Abs. 1, Art. 13 und Art. 14 DSGVO sind erfüllt, wenn der Verantwortliche die erforderlichen Informationen in einer mehrstufig aufgebauten Datenschutzerklärung bereitstellt, die durch leicht zugängliche Zusatzinformationen ergänzt wird, und die Nutzer damit in klarer und verständlicher Weise über Zwecke und Funktionsweisen der eigenen Verarbeitung aufgeklärt werden. Eine Pflicht zur Information über hypothetische Verarbeitungsvorgänge Dritter besteht nicht. (Rn. 42 – 46) (redaktioneller Leitsatz)

3. Der Verantwortliche ist nach Art. 32 DSGVO nicht verpflichtet, personenbezogene Daten, die aufgrund der selbst gewählten Einstellungen des Nutzers öffentlich zugänglich sind, vor der Erhebung durch Dritte zu schützen. Maßgeblich ist, dass ein insgesamt angemessenes Schutzniveau durch technische und organisatorische Maßnahmen gewährleistet wird, während ein Anspruch auf konkrete Sicherungsmaßnahmen nicht aus der DSGVO abgeleitet werden kann. (Rn. 48 und 51 – 52) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatzanspruch, Feststellungsinteresse, Unterlassungsanspruch, Auskunftspflicht, Beweislast, Datenschutzverletzung, Kausalzusammenhang

Rechtsmittelinstanz:

OLG München, Endurteil vom 06.06.2025 – 36 U 4233/23 e

Fundstelle:

GRUR-RS 2023, 56727

Tenor

1. Die Klage wird abgewiesen.
2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.
3. Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrags vorläufig vollstreckbar.
4. Der Streitwert wird auf Euro 2.500 festgesetzt.

Tatbestand

1

Die Parteien streiten über Ansprüche auf Schadensersatz, Unterlassung, Auskunft und Rechtsverfolgungserstattung wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung im Zusammenhang mit sog. Daten-Scraping im Zeitraum von Januar 2018 bis September 2019.

2

Der Kläger ist Nutzer der Plattform Die Beklagte ist Anbieterin der ...-Plattform auf dem Gebiet der Europäischen Union.

3

Im Zeitraum vom Januar 2018 bis September 2019 wurden bei der Beklagten personenbezogene Daten aus dem Datenbestand von ... mittels des ...-Tools Kontaktimporter „gescrap“ , also Daten bei ... ausgelesen und persistiert. Die Telefonnummern der Benutzer konnten mit restlichen Personendaten korreliert werden und waren somit Bestandteil des jeweiligen unbefugt verbreiteten Datensatzes. Hierzu wurden mit Hilfe des Contact-Import-Tools Telefonnummern geprüft und der zugehörige ...-Nutzer wurde angezeigt. Diese Datensätze wurden ab April 2021 durch unbekannte Dritte im Internet verbreitet und für Interessenten bereitgestellt. Anfang April 2021 wurden die entsprechend gescrapten Daten von ca. 533 Millionen ...-Nutzern aus 106 Ländern im Internet öffentlich verbreitet.

4

Bei der Erstellung eines ...-Accounts trägt der angehende Nutzer die ihn betreffenden personenbezogenen Daten, Vor- und Nachname, Handynummer oder E-Mailadresse, Geschlecht und Geburtsdatum in die Registrierungsmaske ein. Während des relevanten Zeitraums waren Name, Geschlecht und Nutzer-ID der Klagepartei als immer öffentliche Nutzerinformationen öffentlich auf dem klägerischen Nutzerkonto einsehbar und sind es auch weiterhin (Screenshot Bl. 102 d.A.). Die Sichtbarkeit der sonstigen Daten – Telefonnummer, E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus – sind von der Zielgruppenauswahl der Klagepartei abhängig.

5

Damit Nutzer mit anderen Nutzern leichter in Kontakt treten können, sind die im Rahmen der Registrierung angegebene Name, Geschlecht und Nutzer-ID als Teil des Nutzerprofils immer öffentlich einsehbar. Dementsprechend waren der Name und das Geschlecht des Klägers im Zeitraum von Januar 2018 bis September 2019, d.h. in dem Zeitraum, in dem das Datenscraping im Rahmen des Scraping-Sachverhalts stattgefunden hat, öffentlich auf seinem ...-Profil einsehbar. Dies wird und wurde im Hilfebereich der Beklagten erläutert, wo zudem auch erklärt wird, was es bedeutet, wenn Informationen „öffentlich“ sind.

6

Die Beklagte stellte im maßgeblichen Zeitraum, zugängliche Privatsphäre-Einstellungen zur Verfügung, damit Nutzer – wie auch der Kläger – bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten. Es wurde dabei zwischen zwei Arten von Privatsphäre-Einstellungen unterschieden:

7

Die „Zielgruppenauswahl“ betrifft Einstellungen, die festlegen, wer einzelne Informationen im ...-Profil eines Nutzers sehen kann. Dies umfasst Informationen wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus und E-Mail. Nicht hiervon umfasst sind die immer öffentlichen Nutzerinformationen, da diese, wie oben erläutert, immer öffentlich einsehbar sind. Der Nutzer konnte beispielsweise anstelle der Zielgruppenauswahl „öffentlich“ festlegen, dass nur „Freunde“ oder „Freunde von Freunden“ die jeweilige Information sehen können. Soweit keine individuellen Einstellungen gewählt wurden, richtete sich die Sichtbarkeit der über die immer öffentlichen Informationen hinausgehenden Informationen nach den Standard-Einstellungen.

8

Die „Suchbarkeits-Einstellungen“ legen fest, wer das Profil eines Nutzers unter anderem anhand einer Telefonnummer finden kann. Soweit keine individuellen Einstellungen gewählt wurden, richtete sich im streitgegenständlichen Zeitraum die Suchbarkeit nach den Standard-Einstellungen, wonach es allen Personen, die über die Telefonnummer des Nutzers verfügen, möglich war, das Profil des Nutzers, sofern dieser seine Telefonnummer bereitgestellt hatte, zu finden.

9

Der Kläger forderte mit vorgerichtlichem anwaltlichen Schreiben (Email vom 14.09.2021, K1) die Beklagte unter Darlegung der Sach- und Rechtslage vergeblich zur Zahlung von 500 EUR Schadensersatz nach Art. 82 Abs. 1 DSGVO und zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunft, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht wurden. Die Beklagte wies in ihrem Schreiben vom 23.08.2021.2021 (K 2) den Schadensersatz und den Unterlassungsanspruch zurück und erteilte dem Kläger einige Auskünfte, die dem Kläger jedoch nicht ausreichen.

10

Der Kläger behauptet, die Telefonnummern der Benutzer hätten wegen einer Sicherheitslücke mit den restlichen Personendaten korreliert werden können. Einerseits habe die Beklagte keinerlei Sicherheitsmaßnahmen wie Sicherheitscapchas oder ein Mechanismus zur Überprüfung der Plausibilität etwa ungewöhnlich vieler Anfragen vorgehalten, um ein Ausnutzen des bereitgestellten Tools zu verhindern und andererseits seien die Einstellungen zur Sicherheit der Telefonnummer auf ... so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Mit keinem Wort sei erwähnt, dass die angegebene Nummer dazu verwendet werden könne, in irgendeiner Art das Profil des Nutzers zu identifizieren. Nutzer gäben im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf ...preis. Neben den gewöhnlichen Funktionen der ...-Seite existiere auch noch eine separate Messenger-App, in der separate Sicherheitseinstellungen vorgenommen werden könnten.

11

Die Klägerseite habe einen erheblichen Kontrollverlust über ihre Daten erlitten und verbleibe in einem Zustand großen Unwohlsein und großer Sorge über möglichen Missbrauch ihrer Daten. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen. Darüber hinaus erhalte die Klägerseite seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail mit Nachrichten offensichtlicher Betrugsversuchen und Virenlinks. Bestehende Ängste, Stress, Komfort- und Zeiteinbußen würden sich darin auswirken, dass sich die Klägerseite mit dem Datenleak, der Herkunft der Daten auseinandersetzen habe müssen und Identitätsdiebstahl oder Betrugsversuche befürchte.

12

Der Kläger ist der Auffassung, ihm stehe ein Schadensersatzanspruch aus Art. 82 I DSGVO zu. Die Beklagte habe gegen die DSGVO verstoßen, indem sie personenbezogene Daten der Klägerseite ohne Rechtsgrundlage Art. 6, 7 DSGVO und ausreichender Information nach Art. 13, 14 DSGVO verarbeitet sowie diese Daten unbefugten Dritten zugänglich gemacht und hierbei Pflichten aus Art. 5, 25, 32 und 34 DSGVO sowie Betroffenenrechte der Klägerseite nach Art. 15, 17, 18 DSGVO verletzt habe. Ferner stehe dem Kläger auch ein Unterlassungsanspruch aus §§ 1004 analog, 823 Abs. 1 und 823 Abs. 2 BGB i.V.m. Art. 6 I, 17 DSGVO wie auch ein Auskunftsanspruch nach Art. 15 DSGVO zu.

13

Der Kläger beantragt,

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

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

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

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

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

14

Die Beklagte beantragt,

Klageabweisung.

15

Die Beklagte behauptet, die Privatsphäre-Einstellungen seien leicht zu bedienen. Separate Privatsphären-Einstellungen in der Messenger-App gäbe es nicht, die Einstellungen der Klagepartei zur Zielgruppenauswahl und Suchbarkeit im ... habe den Einstellungen im ...-Konto der Klagepartei entsprochen. Die Suchbarkeit des Klägers sei seit dem 01. November 2013 bis zum Ende des relevanten Zeitraums auf „Everyone“, d.h. „Alle“ eingestellt gewesen (Screenshot Bl. 102 d.A.). Die Beklagte habe ihre Nutzer – inklusive der Klagepartei – umfassend und transparent über die Möglichkeiten der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl informiert. Zweck der ...-Plattform bestehe jedoch gerade darin, es Menschen zu ermöglichen, sich mit Freunden, Familie und Gemeinschaften zu verbinden und andere zu finden.

16

Beim Datenscraping würden Funktionen einer Website verwendet werden, die für ordnungsgemäße Nutzer entworfen worden und bei diesen beliebt seien. Die Beklagte habe Maßnahmen getroffen, um das Risiko von Scraping zu unterbinden und entwickle ihre eigenen Maßnahmen zur Bekämpfung von Scraping kontinuierlich und als Reaktion auf die sich ständig ändernden Techniken und kriminellen Strategien weiter.

17

Schließlich sei die Beklagte außerstande mitzuteilen, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen worden seien. Die Beklagte halte keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten würden.

18

Die Beklagte ist der Auffassung, die Klage sei wegen Unbestimmtheit und mangels Feststellungsinteresse weitgehend unzulässig.

19

Sie sei auch unbegründet, weil der Scraping-Sachverhalt nicht auf einen Datenschutzverstoß beruhe. Verstöße gegen Art. 13-15, 24, 25 und 34 DSGVO seien von Art. 82 DSGVO nicht umfasst. Weiter hätten Dritte allein solche Daten gesammelt, die ohnehin öffentlich einsehbar gewesen seien, und dann anderweitig im Internet zugänglich gemacht. Soweit die im Zuge des Scraping-Sachverhalts abgerufenen Daten der Klagepartei von der ...-Plattform stammen würden, handle es sich dabei um öffentlich einsehbare Daten im ...-Profil des Klägers, die entweder immer öffentliche Nutzerinformationen oder im Einklang mit den Privatsphäre-Einstellungen der Klagepartei nicht vertraulich und öffentlich einsehbar gewesen seien. Schließlich habe der Kläger keinen immateriellen Schaden erlitten. Auch bei Annahme eines vorübergehenden Kontrollverlusts über personenbezogene Daten des Klägers falle dies nicht in den Verantwortungsbereich der Beklagten, da die öffentliche Sichtbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe.

20

Der Feststellungsantrag sei mangels Verstoßes gegen die DSGVO ebenso unbegründet. Der Unterlassungsanspruch scheide mangels einer Erstbegehungs- und Wiederholungsgefahr aus. Das Auskunftsverlangen sei außergerichtlich beantwortet worden.

21

Das Gericht hat am 13.09.2023 mündlich verhandelt, der Kläger wurde informatorisch angehört. Diesbezüglich wird auf das Sitzungsprotokoll verwiesen.

22

Zur Ergänzung des Tatbestandes und wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze samt Anlagen Bezug genommen.

Entscheidungsgründe

23

Die zulässige Klage ist unbegründet und war daher abzuweisen.

A.

24

Die Klage ist zulässig.

25

I. Das Landgericht München II ist international und örtlich nach Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO sowie sachlich jedenfalls aufgrund des rügelosen Einlassens der Beklagten.

26

II. Der Leistungsantrag (Klageantrag zu 1) ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO.

27

Ein Antrag ist hinreichend bestimmt, wenn der Gegenstand und Umfang der Entscheidungsbefugnis des Gerichts klar umrissen sind, sich der Beklagte erschöpfend verteidigen kann und nicht dem Vollstreckungsgericht die Entscheidung überlassen bleibt, was dem Beklagten aufgegeben oder verboten ist. Der Inhalt eines Antrags ist der Auslegung zugänglich. Zur Auslegung sind auch die Ausführungen in der Begründung mit heranzuziehen (BeckOK ZPO/Bacher, 48. Ed. 1.3.2023, ZPO § 253 Rn. 57, 58).

28

Der Klagebegründung lässt sich entnehmen, dass das Zahlungsbegehren aus einem zusammenhängenden, obgleich sich über einen längeren Zeitraum erstreckenden, jedoch in sich abgeschlossenen Lebenssachverhalt folgt. Maßgeblich wird dabei Bezug genommen auf die Anmeldung des Klägers auf der Plattform der Beklagten bis hin zu dem Scraping-Vorfall und der Benachrichtigung der betroffenen Nutzer. Die Geltendmachung verschiedener behaupteter Verstöße durch die Beklagte ist hierbei unschädlich.

29

III. Demnach ist auch der Feststellungsantrag (Klageantrag zu 2) hinreichend bestimmt. Zudem hat der Kläger sein Feststellungsinteresse hinreichend dargetan, indem er die Möglichkeit vorbringt, dass weitere Schäden durch die Verwendung der illegal erlangten Daten entstehen können.

30

Die Zulässigkeit eines Feststellungsantrags ist bereits gegeben, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger daher seinen Anspruch ganz oder teilweise nicht festsetzen kann (OLG Hamm, Urteil vom 21. Mai 2019 – 9 U 56/18 –, Rn. 22, juris). Das Feststellungsinteresse wäre nur dann nicht gegeben, wenn aus der Sicht des Klägers bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. Bacher BeckOK ZPO, Vorwerk/Wolf 43. Edition Stand: 01.12.2021 § 256 Rn. 24).

31

Das klägerische Begehren wird vorliegend auf behauptete Verstöße gegen die DSGVO gestützt. Eine möglicherweise damit einhergehende unkontrollierte Nutzung gescrapter Daten schließt somit bei verständiger Würdigung die Entstehung eines materiellen oder weiteren immateriellen Schadens nicht aus.

Ein weiterer Schadenseintritt ist bei einer Veröffentlichung persönlicher Daten des Klägers nicht völlig fernliegend.

32

IV. Auch das Unterlassungsbegehren (Klageantrag zu 3) ist hinreichend bestimmt, indem es auf die Zugänglichmachung personenbezogener Daten des Klägers, insbesondere der Telefonnummer, gestützt wird. Im Rahmen der zu berücksichtigenden Klagebegründung wird auch deutlich, woraus sich die konkrete Datenverarbeitung, auf die der Kläger Bezug nimmt, ergibt. Der Kläger ist der Auffassung, dass er keine wirksame Einwilligung für die Veröffentlichung seiner – nicht bereits auf seinem ...-Profil für jeden einsehbaren – personenbezogenen Daten, insbesondere der Telefonnummer, erteilt hat.

B.

33

Die Klage ist jedoch unbegründet, da dem Kläger weder ein Schadensersatz in Höhe von 1.000 € aus Art. 82 Abs. 1 DSGVO, noch ein Anspruch auf entsprechende Feststellung oder auf Unterlassung aus §§ 1004 analog, 823 Abs. 1 und 823 Abs. 2 BGB i.V.m. Art. 6 I, 17 DSGVO oder auf Auskunft nach Art. 15 DSGVO zusteht.

34

Demnach hat er auch keinen Anspruch auf vorgerichtliche Rechtsanwaltskosten aus Art. 82 Abs. 1 DSGVO oder Zinsen aus §§ 291, 288 BGB.

35

I. Dem Kläger steht kein Schadensersatzanspruch aus Art. 82 I DSGVO (Klageantrag zu 1) und damit auch kein Anspruch auf Feststellung der Ersatzpflicht zukünftiger Schäden (Klageantrag zu 2) zu, weil die behaupteten Verstöße nicht vom Schutzbereich des Art. 82 DSGVO umfasst sind, die Beklagte nicht gegen die DSGVO verstoßen hat und der Kläger keinen kausal eingetretenen Schaden nachweisen konnte.

36

1. Die behaupteten Verstöße gegen Art. 13, 14 DSGVO und Art. 34 sowie Art. 15 DSGVO und Art. 25 DSGVO sind schon nicht vom Anwendungsbereich des Art. 82 DSGVO erfasst.

37

Art. 82 DSGVO erfasst von vornherein nur solche Pflichtverstöße, die im Rahmen einer „Verarbeitung“ geschehen (etwa OLG Stuttgart, Urteil vom 31. März 2021, Az. 9 U 34/21, Rn. 61, Juris; LG Düsseldorf, Urteil vom 28. Oktober 2021, Az. 16 O 128/20, GRUR-RS 2021, 33076 Rn. 27; Nemitz, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 8). Dies folgt bereits aus dem Wortlaut des Art. 82 Abs. 2 S. 1 DSGVO „durch eine nicht dieser Verordnung entsprechende Verarbeitung“.

38

Art. 13, 14 DSGVO, Art. 34 DSGVO und Art. 15 DSGVO begründen hingegen Informationspflichten gegenüber betroffenen Personen. Die Erteilung von Informationen über die Verarbeitung personenbezogener Daten, die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten gegenüber Nutzern und die Erteilung einer beantragten Auskunft stellen jedoch selbst keine Verarbeitungen personenbezogener Daten i. S. v. Art. 4 Nr. 2 DSGVO dar. Dementsprechend kann ein Schadensersatzanspruch nach Art. 82 DSGVO nicht aus einer Verletzung dieser Vorschriften resultieren.

39

Ebenso wenig kann ein Verstoß gegen Art. 25 Abs. 1, Abs. 2 DSGVO einen Schadensersatz nach Art. 82 Abs. 1 DSGVO auslösen, weil die Normen nicht in direktem Zusammenhang mit einer konkreten Verarbeitung stehen und in erster Linie eine organisatorische Verpflichtung für den Verantwortlichen darstellen (Gola/Heckmann, DSGVO, 3. Auflage 2022, Art. 25 Rn. 34).

40

2. Der geltend gemachte Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO besteht auch deshalb nicht, weil der darlegungs- und beweisbelastete Kläger einen Verstoß gegen die DSGVO nicht dargelegt oder bewiesen hat.

41

Art. 82 Abs. 1 DSGVO sieht ausdrücklich vor, dass ein Anspruch auf Schadensersatz nur besteht, wenn „wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“. Der Kläger trägt die Beweislast für das Vorliegen der notwendigen Anspruchsvoraussetzungen des geltend gemachten Schadensersatzanspruchs. Dies umfasst insbesondere die Darlegung und den Beweis für die Tatsachen, aus denen sich der angebliche Pflichtverstoß ergibt (Spindler/Horvath, in: Spindler/Schuster, DSGVO, 4. Aufl. 2019, Art. 82 Rn. 11; Quaas, in: BeckOK, DSGVO, 36. Aufl., 1. August 2022, Art. 82 Rn. 51). Der Kläger hat einen Verstoß der Beklagten gegen ihre Pflicht aus der DSGVO weder substantiiert dargelegt noch bewiesen.

42

2.1. Es sind keine Transparenzpflichten gem. Art. 5 Abs. 1, 13, 14 DSGVO verletzt.

43

Nach Art. 13 DSGVO hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Datenerhebung die in Art. 13 Abs. 1 und Abs. 2 DSGVO aufgeführten Informationen zur Verfügung zu stellen. Vergleichbare Vorgaben sieht Art. 14 DSGVO für den Fall vor, dass der Verantwortliche die Daten nicht bei der betroffenen Person erhebt. Dadurch soll eine faire und transparente Verarbeitung gewährleistet werden (Art. 13 Abs. 2, Art. 14 Abs. 2 DSGVO), wobei es sich um eine Konkretisierung des allgemeinen datenschutzrechtlichen Transparenzgrundsatzes (Art. 5 Abs. 1 DSGVO) handelt.

44

Die Beklagte stellt ihren Nutzern, den Kläger eingeschlossen, sämtliche in Art. 13 DSGVO aufgeführten Informationen in Bezug auf die von ihr durchgeführten Datenverarbeitungen zum Zeitpunkt der Datenerhebung im Rahmen ihrer Datenrichtlinie zur Verfügung. Die Darstellung der Informationen erfolgt im Einklang mit den Vorgaben der DSGVO, die eine Darstellung in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache voraussetzt (vgl. Art. 12 Abs. 1 DSGVO).

45

Die von der Beklagten verwendete Mehrebenen-Datenschutzerklärung wurde unbestritten im relevanten Zeitraum durch weitergehende Informationen im Hilfebereich ergänzt. Hierdurch werden den Nutzern nicht nur die nach Art. 5 Abs. 1 lit. a, 13 und 14 DSGVO gesetzlich vorgeschriebenen Pflichtinformationen zur Verfügung gestellt, sondern auch übersichtliche Zusammenfassungen besonders relevanter Themen.

46

Soweit der Kläger den Inhalt dieser Informationen für unzureichend hält, weil darin etwa die Information fehle, dass „das öffentliche Teilen der Telefonnummer die Möglichkeit eröffnet, dass durch automatische Software eine Kategorisierung und Abgreifung durch böswillige Dritte erfolgen kann“, so geht dieser Einwand schon deshalb fehl, weil die Beklagte nur Informationen zur eigenen Verarbeitungstätigkeit erteilen muss und nicht zu (hypothetischen) Verarbeitungstätigkeiten Dritter. Über ihre eigenen Verarbeitungstätigkeiten, insbesondere über die Zwecke der Verarbeitung der Telefonnummer und die Funktionsweise der Kontakt-Importer-Funktion, stellt die Beklagte ausführliche Informationen zur Verfügung.

47

Soweit der Kläger den Inhalt der Datenschutzinformationen für unzureichend hält, weil er durch die Beklagte nicht ausreichend über die Verwendung der Telefonnummer belehrt worden sei, ist dies unzutreffend. Der Kläger selbst legt Screenshots von Seiten der Beklagten vor, die eben diese Hinweise enthalten. Darauf sind die Zwecke, zu denen die Telefonnummer verarbeitet wird, klar aufgeführt und erläutert (etwa Screenshots Klageschrift Bl. 11 ff d.A.).

48

Im Rahmen der Entscheidung ist auch der Umstand zu berücksichtigen, dass die Nutzung der Plattform als solche freiwillig erfolgt. Die Angabe der Mobilfunknummer ist für die bloße Nutzung der Plattform nicht zwingend erforderlich. Es reicht aus, wenn Name, Geschlecht und ID hinterlegt sind. Zudem obliegt es dem Nutzer festzulegen, „wer deine Telefonnummer sehen kann und wer auf ... nach dir suchen kann“. Daher sind die von der Beklagten gewählten Voreinstellungen nicht zu bemängeln, weil der jeweilige Nutzer umfassend und verständlich über Änderungsmöglichkeiten informiert wird. Die Einstellungsmöglichkeiten finden sich in einer Sammlung von Links und Unterlinks. Die Beklagte hat über die Nutzungs- und Findungsmöglichkeiten aufgeklärt. Dabei ist zu beachten, dass das Profil eines Nutzers über die

Mobilfunknummer als solches im relevanten Zeitraum auffindbar war, wenn wie im Falle des Klägers die Suchbarkeitsfunktion über die Mobilfunknummer überhaupt und überdies für jedermann eröffnet war.

49

2.2. Es liegt auch keine Verletzung der Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DSGVO vor. Selbst bei unterstelltem Fehlen von Sicherheitsvorkehrungen durch die Beklagte ist der Beklagten kein Verstoß gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, vorzuwerfen.

50

Verarbeitungsprozesse sind im Sinne des Art. 32 DSGVO so zu gestalten, dass ein ausreichendes Schutzniveau für die Sicherheit personenbezogener Daten für einen angemessenen Systemdatenschutz gegeben ist.

51

Vorliegend war die Beklagte jedoch nicht dazu verpflichtet, Schutzmaßnahmen zu ergreifen, um der Erhebung der öffentlich zugänglichen Informationen des klägerischen Profils aufgrund seiner selbst gewählten Einstellung entgegenzuwirken. Im relevanten Zeitraum war der Kläger für alle („everyone“) über seine Telefonnummer zu finden. Es bestand keine Verpflichtung der Beklagten, diese Daten vor der Verarbeitung gem. Art. 4 Nr. 2 DSGVO durch die Scraper zu schützen, weil die Daten nicht unbefugt oder unrechtmäßig verarbeitet worden sind. Die gescrapten personenbezogenen Daten des Klägers sind Daten, die im relevanten Zeitraum für jedermann abrufbar waren. Dies gilt vor allem vor dem Hintergrund, dass Zweck der Plattform jedenfalls auch darin besteht, Menschen mittels bestimmter Funktionen aufzufinden und zu kontaktieren (vgl. Screenshots Klageschrift Bl. 11 d.A.).

52

Überdies folgt kein Anspruch auf konkrete Sicherungsmaßnahmen aus der DSGVO. Es genügt, wenn die Beklagte ein hinreichendes Schutzniveau sicherstellt. Dies ist vorliegend der Fall. Es wird ein EDM-Team (External-Data-Misuse-Team) bei der Beklagten beschäftigt. Die Beklagte hat auch überzeugend erläutert, dass immer wieder konkrete Maßnahmen ergriffen werden, um Scraping zu verhindern. Ob auch nach diesen Maßnahmen weiter Scraping möglich ist, kann die Beklagte nicht wissen, da die Scraper professionell und auch kriminell handeln und ihre Vorgehensweisen auch den neuen Sicherheitsgegebenheiten anpassen.

53

2.3. Weiter trifft die Beklagte kein Verstoß gegen Art. 25 DSGVO. Insbesondere entspricht die Standard-Einstellung für die Suchbarkeit von Telefonnummern während des streitgegenständlichen Zeitraums „Alle“ dem Zweck der ...-Plattform. Denn die Verarbeitung von Kontaktdaten wie E-Mail-Adresse oder Telefonnummer ist erforderlich, um den Verarbeitungszweck des gegenseitigen Auffindens und Vernetzens (s.o.) zu erreichen.

54

2.4. Benachrichtigungs- und Meldepflichten aus Art. 34, 33 DSGVO sind ebenso nicht verletzt, weil die Beklagte, wie ausgeführt, den Schutz personenbezogener Daten nicht verletzt hat. Die gescrapten Daten waren öffentlich einsehbar.

55

2.5. Es erfolgte auch keine unrechtmäßige Verarbeitung personenbezogener Daten ohne Rechtsgrundlage nach Art. 6 DSGVO.

56

Der Beklagten fällt kein Verstoß gegen Art. 6 DSGVO zur Last, weil die Verarbeitung der personenbezogenen Daten des Klägers durch die Beklagte im Rahmen der Bereitstellung der ...-Plattform rechtmäßig war. Die von Dritten abgerufenen Informationen waren im Einklang mit der Zielgruppenauswahl des Klägers öffentlich zugänglich und wurden nicht von der Beklagten an Dritte übermittelt. Die Daten des Klägers wurden zu jeder Zeit rechtmäßig durch die Beklagte verarbeitet; auch die übrigen streitgegenständlichen Datenkategorien waren für die Scraper einsehbar – wie für jeden anderen ...-Nutzer – weil der Kläger dies insbesondere durch seine Zielgruppenauswahl festlegte.

57

Die Beklagte verfügt über eine wirksame Rechtsgrundlage für die Verarbeitung der Daten der Klagepartei. Die einschlägige Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten des Klägers im Rahmen der Bereitstellung der ...-Plattform ist Art. 6 Abs. 1 lit. b DSGVO. Dabei handelt es sich um den hier erheblichen Verarbeitungszweck, welcher bedingt, dass bestimmte Daten den Privatsphäre-Einstellungen des Klägers entsprechend öffentlich zugänglich sind. Einer ausdrücklichen Einwilligung des Klägers nach Art. 6 Abs. 1 lit. a DSGVO, welche die Klagepartei wegen Unübersichtlichkeit und Unvollständigkeit von Informationen nicht als erteilt ansieht, bedurfte es damit nicht.

58

2.6. Die Auskunftspflicht gem. Art. 15 DSGVO ist ebenso nicht verletzt, da die Beklagte mit ihrer Auskunft vom 04.11.2021 ihrer Pflicht aus Art. 15 DSGVO nachgekommen ist.

59

Das klägerische Auskunftersuchen (Email K 1) hat die Beklagte am 23.08.2021 (K 2) ordnungsgemäß beantwortet. An diesem Tag hat die Beklagte eine Antwort an den Klägervertreter per beA verschickt, in der sie den Kläger auf die maßgeblichen Abschnitte der Datenrichtlinie und die verfügbaren Selbstbedienungs-Tools („Zugriff auf deine Informationen“ und „Deine Informationen herunterladen“) hinwies, die es ...-Nutzern ermöglichen, ihre ...-Daten aufzurufen und einzusehen. Dies stellt eine hinreichende Antwort auf das klägerische Auskunftersuchen nach Art. 15 DSGVO dar.

60

Eine Verletzung der Auskunftspflicht ist nicht etwa darin zu sehen, dass im Schreiben der Beklagten „keinerlei konkrete Aussagen dazu, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen wurden“ enthalten waren. Insoweit beziehen sich die von dem Kläger begehrten Informationen nämlich auf Verarbeitungstätigkeiten Dritter. Art. 15 Abs. 1 DSGVO verpflichtet den Verantwortlichen indes lediglich zur Auskunft in Bezug auf die eigene Verarbeitungstätigkeit. Die Beklagte ist zur Beantwortung von Fragen betreffend die Verarbeitungstätigkeiten Dritter weder imstande noch nach Art. 15 DSGVO rechtlich verpflichtet ist. Informationen über personenbezogene Daten, die von einem Datenschutzvorfall betroffen sind, sowie über den Zeitpunkt und das Ausmaß des Datenschutzvorfalls können nur gefordert werden, wenn Art. 34 DSGVO greift. Dies ist hier aber nicht der Fall. Demgegenüber ist die Beklagte gem. Art. 15 DSGVO nicht verpflichtet, solche Informationen bereitzustellen. Das Scraping ist von außen erfolgt und es ist nicht ersichtlich, wer diese Daten gescrapt hat. Es ist unmöglich, eine Auskunft über Daten zu erteilen, die während des Scrapens auf „öffentlich“ gestellt waren.

61

3. Letztlich liegt darüber hinaus mangels haftungsausfüllender Kausalität auch kein ersatzfähiger immaterieller Schaden vor. Der darlegungs- und beweisbelastete Kläger konnte das Gericht nicht von der haftungsausfüllenden Kausalität zwischen etwaiger Rechtsgutsverletzung und eingetretenem Schaden überzeugen.

62

Im Rahmen seiner informatorischen Anhörung gab der Kläger an, er habe sich 2010 auf ... registriert. Er sei auch auf weiteren Social-Media-Plattformen wie ... und ... unterwegs, diese nutze er aber kaum aktiv.. Des Weiteren nutze er Online-Shops wie ... und Bei den Online-Shops gebe er natürlich die nötigen Daten an. Insbesondere wenn die Lieferung durch eine Spedition erfolge, habe er auch dort seine Telefonnummer angegeben. In den letzten Jahren habe er des Öfteren Anrufe und SMS auf das Handy bekommen. Wenn er Anrufe erhalte, sei keiner am anderen Ende der Leitung Wenn er SMS erhalte, seien die oft mit Links, das käme ihm komisch vor. Er denke dass diese unberechtigten Anrufe und SMS-Zusendungen auf den Scraping-Vorfall bei ... zurückzuführen seien, denn es würde zeitlich sehr gut passen.

63

Zur Überzeugung des Gerichts lässt sich nicht nachweisen, dass die unberechtigten Anrufe und SMS im Kausalzusammenhang mit dem Scraping-Vorfall bei der Beklagten erfolgt sind. Zum einen gibt der Kläger im Internet auf verschiedenen Plattformen und Shops seine personenbezogenen Daten, insbesondere Email und Telefonnummer an, sodass gerade nicht seine Daten bei ... abgegriffen worden sein müssen. Es ist ebenso denkbar, dass über ... oder ... jemand die Daten abgegriffen hat.

64

4. Ein Anspruch auf Feststellung der Ersatzpflicht hinsichtlich künftiger Schäden (Klageantrag zu 2) besteht mangels Schadensersatzanspruch nach Art. 82 DSGVO nicht. Auf vorstehende Ausführungen wird verwiesen.

65

II. Dem Kläger steht auch kein Unterlassungsanspruch nach §§ 1004 analog, 823 Abs. 1 oder 823 Abs. 2 BGB i.V.m. Art. 6 I, 17 DSGVO (Klageantrag zu 3) zu.

66

Es ist bereits zweifelhaft, ob die DSGVO einen derartigen Unterlassungsanspruch vorsieht. Jedenfalls fehlt es aber an einem Verstoß gegen die DSGVO, da die Verarbeitung der personenbezogenen Daten der Klagepartei, einschließlich ihrer Telefonnummer, rechtmäßig erfolgt ist und insbesondere keine unbefugte Zugänglichmachung ihrer Daten gegenüber Dritten vorliegt.

67

Auch eine Wiederholungsgefahr ist nicht zu befürchten, da es jedem Nutzer obliegt, jederzeit seine Suchbarkeitseinstellungen anzupassen.

68

III. Einen weitergehenden Auskunftsanspruch aus Art. 15 DSGVO (Klageantrag zu 4) hat der Kläger nicht. Die Beklagte hat dem Kläger mit Schreiben vom 04.11.2021 in angemessener Weise Auskunft über die von ihr verarbeiteten Daten erteilt. Es wurden auch keine Anhaltspunkte vorgetragen, dass Daten vom Scraping erfasst sind, die nicht ohnehin öffentlich einsehbar beziehungsweise von den Suchbarkeitskriterien umfasst waren. Andernfalls läge ein Hacker-Angriff vor, der jedoch vom Kläger nicht dargetan wird. Ergänzend wird auf vorstehende Ausführungen Bezug genommen.

69

IV. Mangels Begründetheit der Hauptforderungen sind auch die Nebenforderungen in Form der zu ersetzenden Rechtsanwaltskosten nach Art. 82 DSGVO und Zinsen nach §§ 291, 288 BGB unbegründet.

C.

70

Die Nebenentscheidungen folgen aus §§ 91, 709 Satz 1, 2 ZPO.

71

Hinsichtlich des Streitwertes war Ziffer 1 der Klage mit 1000 Euro zu bewerten, was dem klägerischen Mindestbetrag entspricht. Antrag Ziffer 2 war mit Euro 400 zu bewerten; bei einem Feststellungsantrag ist der Wert des Gegenstandes des Rechtsverhältnisses maßgeblich. Die zukünftigen Schäden sind aufgrund des Umstandes, dass der Kläger selbst die Daten auf der Plattform angab und aufgrund des inzwischen verstrichenen Zeitraumes mit 400 Euro zu bewerten. Ziffer 3 bewertet das Gericht mit 1.000 Euro; Unterlassungsansprüche sind nach dem Interesse des Anspruchstellers zu bemessen. Da der Kläger selbst die Daten auf der Plattform der Beklagten eingab und die Beeinträchtigung des Klägers vom Gericht als gering erachtet wird, sind 1.000 Euro ausreichend. Ziffer 4 (Auskunftsanspruch) wird mit 100 Euro angesetzt, dabei wurde auch berücksichtigt, dass der Kläger selbst diesen mit Null bewertete. Zudem dürften ihm die Daten, die er auf der Plattform der Beklagten eingab, selbst bekannt sein.

72

Die einzelnen Streitwerte waren zu addieren.

73

Auch das Landgericht Bonn und das Landgericht Kiel haben diese Streitwerte angesetzt (10 O 142/22 und 6 O 154/22).