LG München II, Endurteil v. 08.03.2024 – 11 O 705/23

Titel:

Begrenzter Anwendungsbereich von datenschutzrechtlichen Schadensersatzansprüchen auf Verarbeitungshandlungen

Normenketten:

ZPO § 253 Abs. 2 Nr. 2
DSGVO Art. 4 Nr. 2, Art. 5 Abs. 1 lit. a, Art. 13, Art. 32, Art. 33, Art. 34, Art. 82 Abs. 1
GG Art. 1 Abs. 1, Art. 2 Abs. 1

Leitsätze:

1. Art. 82 DSGVO erfasst nur solche Pflichtverstöße, die im Rahmen einer „Verarbeitung“ i.S.v. Art. 4 Nr. 2 DSGVO erfolgen. Informationspflichten aus Art. 13, 15, 33 und 34 DSGVO stellen mangels eigener Verarbeitungshandlungen keine tatbestandsrelevanten Vorgänge dar, sodass aus ihrer Verletzung keine Ansprüche nach Art. 82 DSGVO entstehen können. Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG erweitert den unionsrechtlichen Anwendungsbereich nicht, da Art. 82 DSGVO nur solche nationalen Bestimmungen erfasst, die der Präzisierung unionsrechtlicher Normen dienen. Dies ist bei Grundrechten des Grundgesetzes nicht der Fall. (Rn. 37 – 40) (redaktioneller Leitsatz)
2. Die Anforderungen an Transparenz und Informationserteilung aus Art. 5 Abs. 1 lit. a und Art. 13 DSGVO sind erfüllt, wenn betroffene Personen zum Zeitpunkt der Datenerhebung sämtliche gesetzlich vorgesehenen Angaben in einer klar strukturierten und leicht zugänglichen Mehrebenen-Datenschutzerklärung erhalten, die eine präzise und verständliche Darstellung der eigenen Verarbeitungstätigkeiten ermöglicht und durch zusätzliche, themenspezifische Hilfebereiche ergänzt wird. Einwände gegen die Vollständigkeit der Informationen greifen nicht durch, wenn sich das Auskunftsbegehren auf hypothetische oder fremde Verarbeitungsvorgänge richtet, zu denen der Verantwortliche keine Angaben machen muss, und wenn zugleich die Nutzer durch eigene Einstellungsmöglichkeiten bestimmen können, wer ihre Daten einsehen und über welche Suchfunktionen ihr Profil auffindbar ist. (Rn. 44 – 50) (redaktioneller Leitsatz)
3. Ein Verstoß gegen Art. 32 DSGVO liegt nicht vor, wenn die angeblich unzureichend geschützten personenbezogenen Daten aufgrund der vom Nutzer gewählten Einstellungen ohnehin öffentlich abrufbar waren und damit weder eine unbefugte noch eine unrechtmäßige Verarbeitung i.S.d. Verordnung gegeben ist, sodass keine Pflicht besteht, der Erhebung solcher frei zugänglichen Informationen durch Dritte entgegenzuwirken. Das erforderliche Schutzniveau ist gewährleistet, wenn der Verantwortliche fortlaufende Maßnahmen zur Sicherung der Datenverarbeitung implementiert und frühere Funktionen mit erhöhtem Missbrauchspotenzial abgeschafft oder eingeschränkt hat. (Rn. 51 – 55) (redaktioneller Leitsatz)
4. Ein Anspruch auf immateriellen Schadensersatz nach Art. 82 DSGVO besteht nur, wenn die betroffene Person einen konkreten, tatsächlich eingetretenen immateriellen Schaden substantiiert darlegt und nachweist. Ein bloßer DSGVO-Verstoß, ein abstrakter Kontrollverlust oder ein lediglich diffuses Unwohlsein genügen hierfür nicht. Erforderlich ist der Nachweis nachteiliger Folgen, die über allgemeine Lebensrisiken hinausgehen und in einem hinreichend wahrscheinlichen Kausalzusammenhang mit dem behaupteten Datenschutzverstoß stehen. (Rn. 72 – 79) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatz, Verletzung, Ermessen, hinterlegung, Schaden, Unterlassung, Auskunft, Software, Daten, Technik, Form, Beweislast, Klage, Nutzung, personenbezogene Daten, Stand der Technik, informationelle Selbstbestimmung

Rechtsmittelinstanz:

OLG München, Endurteil vom 26.09.2025 – 36 U 1368/24 e

Fundstelle:

GRUR-RS 2024, 51126

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.

Beschluss

Der Streitwert wird auf 6.500,00 € festgesetzt.

Tatbestand

1
Der Kläger macht Schadensersatz-, Unterlassungs- und Auskunftsansprüche wegen der Verletzung der Datenschutz-Grundverordnung (im Folgenden: DSGVO) seitens der Beklagten aus und im Zusammenhang mit dem sogenannten, im April 2021 öffentlich bekannt gewordenen „Scraping-Vorfall“ von geltend.

2
Die Beklagte betreibt in der Europäischen Union das soziale Online-Netzwerk und bietet u. a. über www..com Dienste an, die für private Nutzer kostenlos sind. Der Kläger ist nutzer dieser Plattform.

3
Bei der Registrierung gab der Kläger seinen Vornamen, Nachnamen, Handynummer, Geburtsdatum und Geschlecht an. Im Rahmen der Erstellung eines -Profils wird der künftige Nutzer Datenschutz- und Cookie Richtlinien hingewiesen.

4
Der im Rahmen der Registrierung angegebene Name, Geschlecht und Nutzer-ID („immer öffentliche Nutzerinformationen“) sind als Teil des Nutzerprofils immer öffentlich einsehbar und somit auch für Personen außerhalb der Plattform der Beklagten. 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 (der „Relevante Zeitraum“) 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.

5
Die Beklagte hat im relevanten Zeitraum, zugängliche Privatsphäre-Einstellungen zur Verfügung gestellt, damit Nutzer – wie auch der Kläger – bestimmen können, inwieweit sie Informationen, die sie zur Verfügung stellen, öffentlich einsehbar machen möchten. Es wird dabei zwischen zwei Arten von Privatsphäre-Einstellungen unterschieden:

6
Die „Zielgruppenauswahl“ bzw. die Sichtbarkeit betrifft Einstellungen, die festlegen, wer einzelne Informationen im -Profil eines Nutzers sehen kann. Nicht hiervon umfasst sind die immer öffentlichen Nutzerinformationen, da diese, wie oben erläutert, immer öffentlich einsehbar sind. Traf der Nutzer keine Zielgruppenauswahl, richtete sich die Zugänglichkeit seiner über die öffentlichen Informationen hinausgehenden Informationen nach der Standardeinstellung, wonach „Freunde des Nutzers“ die weiteren Informationen einsehen konnten.

7
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.

8
Im Relevanten Zeitraum war der Kläger für alle („everyone“) über seine Telefonnummer zu finden.

9

Im Zeitraum vom Januar 2018 bis September 2019 sammelten Dritte unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Daneben erstellten die Scraper Listen mit möglichen Telefonnummern und luden diese in den Kontakt-Importer der Plattform hoch, um festzustellen, ob die hochgeladenen Telefonnummern mit einem Konto eines Nutzers verbunden sind. Der Kontakt-Importer gab, sofern eine der hochgeladenen Telefonnummern mit dem Konto eines Nutzers, der seine Telefonnummer bereitgestellt und die Standard-Suchbarkeits-Einstellungen nicht geändert hatte, verknüpft war, diese Information, also den Umstand der Verknüpfung von Telefonnummer und Konto, an die Scraper. Die Scraper fügten sodann den öffentlich zugänglichen Informationen aus dem betreffenden Profil des Nutzers die mit dem Konto verknüpfte Telefonnummer hinzu.

10
Anfang April 2021 wurden die entsprechend gescrapten Daten von ca. 533 Millionen -Nutzern aus 106 Ländern im Internet öffentlich verbreitet. Davon betroffen waren auch die Daten des Klägers.

11
Der Kläger ist neben auch noch bei und sowie bei und bei unter hinterlegung seiner Telefonnummer registriert.

12
Mit vorgerichtlichen Schreiben vom 21.12.2022 forderte der Kläger durch seine anwaltliche Vertretung die Beklagte zur Zahlung von 3.000,00 EUR Schadensersatz und zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur Auskunft darüber auf, welche konkreten Daten im April 2019 abgegriffen und veröffentlicht wurden.

13
Mit Schreiben vom 06.02.2023 erteilte die Beklagte dem Kläger Auskunft in Form einer Instruktion unter Nutzung eines Selbstbedienungstools zur Einsichtnahme seiner angegebenen personenbezogenen Daten und deren Verwendung. Eine Zahlung lehnte sie ab.

14
Der Kläger behauptet, beim genannten Scraping-Vorfall seien Daten wie Telefonnummer, sog. -ID, Name, Vorname, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus und weitere korrelierende Daten veröffentlicht worden.

15
Der Kläger meint, er habe einen Schaden dadurch, dass er durch die unbefugte Veröffentlichung seiner personenbezogenen Daten einen erheblichen Kontrollverlust über seine Daten erlitten habe.

16
So erhalte er in den letzten zwei Jahren exzessiv Spam-Anrufe, stärker noch in den letzten 15 bis 16 Monaten. Wobei sich die Anrufer als häufig als Mitarbeiter von oder ausgeben würden. Er bekomme Anrufe vier bis sechsmal pro Monat, zu Hoch-Zeiten sogar bis zu vier Anrufe pro Tag. Er könne die Anrufe nicht ignorieren, da er wegen der unterdrückten Nummern nicht wisse, ob der Anrufer seriös ist.

17
Er sei durch die Anrufe zunächst verwundert gewesen, inzwischen sei er genervt, insbesondere da er auch berufliche Anrufe über diese Nummer erhalte. In erster Linie befürchte er, dass mit Kenntnis seiner Daten, ein sogenannter SIM-Swap durchgeführt würde.

18
Der Kläger ist der Auffassung, die Beklagte habe gegen die DSGVO verstoßen und rügt u.a. Verletzungen von Art. 5, 6, 13, 14, 15, 25, 32, 33 und 34 DSGVO. Gemäß Art. 82 DSGVO stehe ihm ein Anspruch auf immateriellen Schadensersatz zu. Zudem folge aus der Verpflichtung der Beklagten zur Leistung von Schadensersatz auch die Verpflichtung, zukünftige Schäden, die aufgrund der entwendeten Daten entstehen, zu ersetzen. Der geltend gemachte Unterlassungsanspruch folge aus §§ 1004 analog, 823 I und II BGB i.V.m. Art. 6 I DSGVO und Art. 17 DSGVO. Der Auskunftsanspruch beruhe auf Art. 15 DSGVO.

19
Der Kläger beantragt,

1. Die Beklagte wird verurteilt, an die Klägerseite als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Handynummer der Klägerseite sowie weiterer personenbezogener Daten der Klägerseite wie Vorname, Nachname, E-Mail-Adresse, Geschlecht, Geburtsdatum einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 3.000,00 aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem jeweiligen Basiszinssatz der EZB zu zahlen.

2. Die Beklagte wird verurteilt, an die Klägerin für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art.15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von € 2.000,00 aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem jeweiligen Basiszinssatz der EZB zu zahlen.

3. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle materiellen 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.

4. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall, der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes biszu €250.000,00,ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen,

a) personenbezogene Daten der Klägerseite, namentlich Telefonnummer, ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nachdem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b) die Telefonnummer des Klägers 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.

5. Die Beklagte wird verurteilt, der Klägerseite Auskunft über personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch eine „Web-Scraping“-Anwendung des Kontaktimporttools erlangt werden konnten und zudem – soweit sie erklärt, Auskünfte nicht abgeben zu können – mögliche Negativ-Auskünfte an Eides statt zu versichern.

6. Die Beklagte wird verurteilt, die Klägerseite von den außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von €1.134,55 nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz der EZB ab Rechtshängigkeit freizuhalten.

20
Die Beklagte beantragt,

Die Klage abzuweisen.

21
Die Beklagte ist der Ansicht, die Klage sei bereits weitgehend unzulässig. Der Klageantrag zu Ziffer 1) sei nicht hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Auch der Klageantrag zu Ziffer 3) sei zu unbestimmt. Zudem habe die Klagepartei kein Feststellungsinteresse gem. § 256 Abs. 2 ZPO dargelegt. Auch der auf Unterlassung gerichtete Antrag hinsichtlich der behaupteten Zugänglichmachung personenbezogener Daten an unbefugte Dritte sei zu unbestimmt. Sie ist der Meinung, beim Scraping liege keine Verletzung der DSGVO vor. Es sei unklar, welche Daten der Klagepartei genau gescrapt worden sein sollen. Soweit die durch Scraping abgerufenen Daten von der -Plattform stammten und Informationen über die Klagepartei enthielten, seien diese Daten entweder tatsächlich nicht durch Scraping abgerufen wurden

oder im Einklang mit den jeweiligen Privatsphäre-Einstellungen öffentlich auf der -Plattform einsehbar gewesen. Dem Kläger sei kein immaterieller Schaden entstanden, jedenfalls fehle es an einem kausalen Zusammenhang zwischen dem behaupteten Schaden und den behaupteten Pflichtverstößen der Beklagten.

22
Zur Ergänzung des Tatbestandes wird wegen der weiteren Einzelheiten des Sach- und Streitstandes auf die gewechselten Schriftsätze nebst Anlagen sowie auf das Protokoll über die mündliche Verhandlung vom 30.01.2024 Bezug genommen.

Entscheidungsgründe

23
Die Klage ist zulässig, jedoch unbegründet.

I.

24
Die Klage ist zulässig. (So auch LG Essen vom 10.11.2022 (Az. 6 O 111/22, GRUR-RS 2022, 34818).

25
1. Das Landgericht München II ist international, sachlich und örtlich zuständig.

26
a) Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO. Danach kann die Klage eines Verbrauchers gegen den Vertragspartner vor dem Gericht des Mitgliedstaats erhoben werden, an dem der Verbraucher seinen Wohnsitz hat.

27
b) Die sachliche Zuständigkeit des Landgerichts richtet sich nach §§ 23 Nr. 1, 71 Abs. 1 GVG. Der klägerseits überhöht behauptete Streitwert war zwar herabzusetzen, überschreitet aber dennoch die Wertgrenze von 5.000,00 €

28
c) Das Landgericht München II ist gem. Art. 18 Abs. 1 Alt. 2 EuGVVO örtlich zuständig.

29
2. Der Klageantrag zu 1) ist – entgegen der Ansicht der Beklagten – hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. 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).

30
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 damit einhergehenden eventuell mangelhaften Benachrichtigung der betroffenen Nutzer.

31
3. Demnach ist auch der Feststellungsantrag zu 3) 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 (vgl. LG München I Endurteil v. 09.12.2021 – 31 O 16606/20, GRURRS 2021, 41707 Rn. 24). 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 21.05.2019 – 9 U 56/18). 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). Das klägerische Begehren wird

vorliegend auf angebliche Verstöße gegen die DSGVO gestützt. Eine möglicherweise damit einhergehende unkontrollierte Nutzung gescrapter Daten schließt somit bei verständiger Würdigung die Entstehung eines materiellen oder immateriellen Schadens nicht aus. Daher ist eine mögliche Schadensentstehung für den Kläger aufgrund der Veröffentlichung seiner persönlichen Daten nicht völlig fernliegend.

32
4. Ferner ist der Antrag zu 4.a – entgegen der Ansicht des Beklagten – zulässig. Das Unterlassungsbegehren ist hinreichend bestimmt, indem es auf die Zugänglichmachung personenbezogener Daten des Klägers, insbesondere der Telefonnummer, gestützt wird.

33
5. Auch der Klageantrag zu 4.b ist – entgegen der Ansicht des Beklagten – zulässig. Im Rahmen der zu berücksichtigenden Klagebegründung wird 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.

II.

34
Die Klage ist jedoch unbegründet. Ein Schadensersatzanspruch besteht insbesondere deshalb nicht, weil die Beklagte nicht gegen die DSGVO verstoßen hat. Daher ist auch der Feststellungsantrag hinsichtlich der Ersatzpflicht zukünftiger Schäden unbegründet. Es besteht weder ein Anspruch auf Erteilung weiterer Auskünfte noch ein Unterlassungsanspruch. Folglich ist auch der Anspruch auf Erstattung vorgerichtlicher Rechtsanwaltskosten und der Zinsen unbegründet.

35
1. Es bestehen keine Schadensersatzansprüche, wie sie mit den Klageanträge zu 1) und 2) geltend gemacht werden.

36
a) Die behaupteten Verstöße sind schon nicht vom Schutzbereich des Art. 82 DSGVO umfasst.

37
Die mit den Klageanträgen zu 1) und 2) geltend gemachten Schadensersatzansprüche scheitern bereits daran, dass die Vorschriften, auf die der Kläger seine vermeintlichen Ansprüche stützt, – also Art. 13 DSGVO und Art. 33, 34 DSGVO sowie das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG (Klageantrag zu 1)) und Art. 15 DSGVO (Klageantrag zu 3) – nicht vom Anwendungsbereich des Art. 82 DSGVO erfasst sind (So auch LG Essen vom 10.11.2022 (Az. 6 O 111/22, GRUR-RS 2022, 34818).

38
Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG fällt schon deshalb nicht in den Anwendungsbereich der unionsrechtlichen Norm des Art. 82 DSGVO, da ein etwaiger Verstoß gegen nationales Recht gem. Erwägungsgrund 146 S. 5 nur dann eine Haftung gem. Art. 82 DSGVO begründen kann, wenn die entsprechenden Rechtsvorschriften des Mitgliedstaats „zur Präzisierung von Bestimmungen der vorliegenden Verordnung“ erlassen wurde (vgl. auch Bergt, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 82 Rn. 24; Nemitz, in: Ehmann/Selmayr, DSGVO, 2 Aufl. 2018, Art. 82 Rn. 9). Dies ist bei Grundrechten des Grundgesetzes ersichtlich nicht der Fall.

39
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“).

40
Art. 13 DSGVO, Art. 34 DSGVO und Art. 15 DSGVO begründen 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.

41
b) Die Beklagte hat nicht gegen die DSGVO verstoßen.

42
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 (So auch LG Essen vom 10.11.2022 (Az. 6 O 111/22, GRUR-RS 2022, 34818).

43
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.

44
(i) Es sind keine Transparenzpflichten gem. Art. 5 Abs. 1 lit. a, 13 DSGVO verletzt.

45
Der Beklagten fällt kein Verstoß gegen Transparenzpflichten gem. Art. 5 DSGVO zur Last.

46
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. Dadurch soll eine faire und transparente Verarbeitung gewährleistet werden (Art. 13 Abs. 2 DSGVO). Dabei handelt es sich um eine Konkretisierung des allgemeinen datenschutzrechtlichen Transparenzgrundsatzes (Art. 5 Abs. 1 lit. a DSGVO).

47
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). Insbesondere die Verwendung einer sog. Mehrebenen-Datenschutzerklärung, bei der der Nutzer auf der ersten Ebene einen Überblick über die ihm hinsichtlich der Verarbeitung seiner personenbezogenen Daten zur Verfügung stehenden Informationen erhält und die weiterführenden Informationen durch Ansteuern des jeweiligen Abschnitts eingesehen werden können, entspricht den Empfehlungen der europäischen Datenschutzbehörden (Art. 29 Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP260 rev.01, Rn. 8, 35 ff. bestätigt durch den Europäischen Datenschutzausschuss (EDSA)). Dies ermöglicht es den betroffenen Nutzern, zu einem bestimmten Teil der Datenschutzerklärungen / –hinweise, den sie sofort abrufen möchten, zu navigieren, anstatt bei der Suche nach einzelnen Themen umfangreiche Texte durchkämmen zu müssen (WP260 rev. 01, Rn. 8).

48
Die von der Beklagten verwendete Mehrebenen-Datenschutzerklärung wird derzeit und wurde auch 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. Auch dieses Vorgehen entspricht den Empfehlungen der europäischen Datenschutzbehörden (WP260 rev. 01, Rn. 37), nach denen Verantwortliche die Verwendung eben solcher Instrumente zur Ergänzung der Pflichtinformationen in Betracht ziehen sollen, um eine noch bessere

Transparenz im Hinblick auf ihre Verarbeitungsprozesse zu erreichen, ohne den durchschnittlichen Nutzer mit einer mit Details überfrachteten Datenschutzerklärung zu überfordern. Speziell im Hinblick auf die Verarbeitung der Telefonnummer ihrer Nutzer stellt und stellte die Beklagte eine Reihe von Artikeln im Hilfebereich bereit. Diese Informationen sind auch leicht zugänglich und direkt auf der Homepage von (https://de-de..com/) verlinkt. Sämtliche Themen können über eine entsprechende Suche (z.B. nach dem Begriff „Handynummer“) leicht gefunden werden.

49
Soweit der Kläger den Inhalt dieser Informationen für unzureichend hält, weil darin etwa die Information fehle, wer die Telefonnummer einsehen könne und an wen sie weitergeleitet werde (Klageschrift vom 23.02.2023, Seite 29, Bl. 29 der Akte), so geht dieser Einwand schon deshalb fehl, weil die Beklagte nur Informationen zur eigenen Verarbeitungstätigkeit erteilen muss (und kann) und nicht zu (hypothetischen) Verarbeitungstätigkeiten Dritter. Über ihre eigenen Verarbeitungstätigkeiten, insbesondere über die Zwecke der Verarbeitung der Telefonnummer und die Suchbarkeitseinstellungen, stellt die Beklagte ausführliche Informationen zur Verfügung.

50
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. Es 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.

51
(ii) Es liegt – entgegen der Ansicht des Klägers – keine Verletzung der Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen gem. Art. 32 DSGVO vor.

52
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. Zweck des Gebots ist u.a. der Schutz personenbezogener Daten durch geeignete technische und organisatorische Maßnahmen vor der unbefugten oder unrechtmäßigen Verarbeitung durch Dritte (vgl. AG Straßburg, Urteil vom 13.10.2022, 25 C 95/21, juris, Rn. 28).

53
Demnach ist der Beklagten kein Verstoß gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, vorzuwerfen. Die Beklagte war insbesondere nicht dazu verpflichtet, Schutzmaßnahmen zu ergreifen, um der Erhebung der immer 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 ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen wie Logins oder ähnliches abrufbar waren. Die Verarbeitung in Form des Scrapens erfolgte auch durch Dritte und nicht durch die Beklagte.

54
Es folgt kein Anspruch auf bestimmte 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. Danach wurde auch die streitgegenständliche Möglichkeit, über die Suchleistenfunktion mit Telefonnummern zu suchen, bereits 2018 komplett abgeschafft und der Kontaktimport ist ebenfalls eingeschränkt worden. Es findet kein exaktes Matching mehr zwischen Profilen und Telefonnummern statt, sondern es wird nur noch

eine Gruppe genannt als „people you might know“. 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.

55
Auch wenn man der Ansicht ist, die Beklagte müsse darlegen und beweisen, dass sie die Vorschriften der DSGVO beachtet hat, so ist dies in Anbetracht der konkreten Ausführungen zu den Hilfeeinstellungen und Hinweisen sowie Ausführungen zu Sicherungs- und Schutzmaßnahmen der Fall.

56
(iii) Benachrichtigungs- und Meldepflichten aus Art. 34, 33 DSGVO sind nicht verletzt.

57
Die Beklagte war nach Art. 33 DSGVO nicht in der Pflicht, der zuständigen Aufsichtsbehörde den Datenschutzvorfall zu melden, da ihr kein Datenschutzverstoß vorzuwerfen ist. Die DSGVO verpflichtet Verantwortliche nicht, rechtswidrige Datenverarbeitungen Dritter an die zuständigen Aufsichtsbehörden zu melden (vgl. Hessel/Potel, DSRITB 2021, 279, 285 f.).

58
(iv) Es ist keine unrechtmäßige Verarbeitung personenbezogener Daten ohne Rechtsgrundlage (Art. 6 DSGVO) gegeben.

59
Der Beklagten fällt auch 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.

60
Der Kläger stützt seinen Vorwurf der rechtswidrigen Datenverarbeitung darauf, dass die Beklagte unbefugten Dritten personenbezogene Daten der Klägerseite zugänglich gemacht haben soll, indem sie diese über das CIT Daten an Unbefugte übermittelte. Zunächst gab es keine „Übermittlung“ von personenbezogenen Daten durch die Beklagte an Dritte; vielmehr wurden die Informationen von dem Kläger für Nutzer der -Plattform öffentlich einsehbar gemacht. Die diesem Vortrag zugrundeliegende klägerische Behauptung einer „Sicherheitslücke“ beruht auf falschen Annahmen des Klägers und ist unzutreffend. So wurde – entgegen der Auffassung des Klägers – seine Telefonnummer gerade nicht durch die Beklagte und ihre Kontakt-Importer-Funktion Dritten „übermittelt“, sondern sie lag unabhängig von einem Zutun der Beklagten bei Dritten vor. Tatsächlich wurden die Daten des Klägers 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.

61
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 (Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung; hier in Bezug auf die Bereitstellung eines sozialen Netzwerks). Dabei handelt es sich um den hier erheblichen Verarbeitungszweck, welcher bedingt, dass bestimmt Daten den Privatsphäre-Einstellungen des Klägers entsprechend öffentlich zugänglich sind.

62
Entgegen des klägerischen Vorbringen ist eine Einwilligung des Nutzers im Sinne von Art. 6 Abs. 1 lit. a DSGVO im gegenständlichen Kontext nicht die maßgebliche Rechtsgrundlage. Der unzutreffende Vortrag des Klägers, wonach seine Einwilligung nicht informiert gewesen sei, geht deshalb fehl, weil die Beklagte sich im streitgegenständlichen Kontext nicht auf eine Einwilligung des Klägers als Rechtsgrundlage stützt.

63
(v) Das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf informationelle Selbstbestimmung ist nicht verletzt.

64

Deutsche Grundrechte sind, wie bereits oben erläutert, im Rahmen des Art. 82 DSGVO nicht anwendbar. Dies gilt auch für eine etwaige mittelbare Drittwirkung: Da Art. 82 DSGVO eine Norm des Unionsrechts ist, sind nationale Grundrechte bei der Auslegung nicht zu berücksichtigen (vgl. EuGH, Urteil vom 8. September 2010, C-409/06, Winner-Wetten, Rn. 61). Zudem erschließt sich aus dem klägerischen Vortrag nicht, worin eine vermeintlich eigenständige Verletzungshandlung der Beklagten liegen soll. Der Kläger beschränkt sich insoweit auf den Vorwurf einer angeblich unrechtmäßigen Übermittlung oder Offenlegung der Daten der Klägerseite und verweist im Übrigen auf seinen Vortrag zu einem vermeintlichen Verstoß gegen Art. 6 DSGVO. Da der Beklagten – wie bereits dargestellt – kein Verstoß gegen Art. 6 DSGVO zur Last fällt, liegt auch kein Verstoß des klägerischen Rechts auf informationelle Selbstbestimmung vor.

65
(vi) Die Auskunftspflicht gem. Art. 15 DSGVO ist nicht verletzt.

66
Der Kläger hat auch nicht schlüssig dargelegt, inwiefern die Beklagte mit ihrer Auskunft gegen Art. 15 DSGVO verstoßen hat.

67
Das klägerische Auskunftsersuchen, vom 21.12.2022, hat die Beklagte am 06.02.2023 ordnungsgemäß beantwortet (so auch in einem parallel gelagerten Fall LG Limburg a. d. Lahn, Urteil vom 24. Januar 2023, Az. 4 O 278/22, S. 8). An diesem Tag hat die Beklagte 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 Auskunftsersuchen nach Art. 15 DSGVO dar.

68
Entgegen dem Vortrag des Klägers ist eine Verletzung der Auskunftspflicht auch nicht etwa darin zu sehen, dass im Schreiben der Beklagten vom 06.02.2022 detailiertere Angaben zu den abgegriffenen Informationen sowie Angaben zu den Empfängern der Informationen fehlten. Insoweit bezogen sich die von dem Kläger im Schreiben, vom 06.02.2023 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 (vgl. LG Limburg a. d. Lahn, Urteil vom 24. Januar 2023, Az. 4 O 278/22, S. 8 f.).

69
Der Kläger scheint Informationen, die von dem Verantwortlichen nach einer Verletzung des Schutzes personenbezogener Daten gem. Art. 33 und 34 DSGVO zur Verfügung zu stellen sind, mit Informationen zu verwechseln, die als Antwort auf eine Anfrage gem. Art. 15 DSGVO zu erteilen sind. So können beispielsweise Informationen über personenbezogene Daten, die von einem Datenschutzvorfall betroffen sind, sowie über den Zeitpunkt und das Ausmaß des Datenschutzvorfalls 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.

70
Im Übrigen ist das Scraping 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. Schließlich ist es dem Beklagten im Rechtssinne unmöglich darzulegen, wann genau das Datenscraping erfolgt ist.

71
c) Davon abgesehen liegt kein ersatzfähiger immaterieller Schaden vor.

72
Der Kläger ist darlegungs- und beweisbelastet (vgl. etwa Brandenburgisches OLG, Beschluss vom 21. Juni 2021, Az. 1 U 69/20, Rn. 20, juris; LG Hamburg, Urteil vom 4. September 2020, Az. 324 S 9/19, BeckRS 2020, 23277 Rn. 29) und dieser Darlegungs- und Beweislast nicht nachgekommen.

73

Der Kläger hat vorliegend im Rahmen des § 287 ZPO keinen Nachweis darüber erbracht, dass ein Schaden für ihn höchstwahrscheinlich eingetreten ist. Die Norm setzt voraus, dass der Schaden „erlitten“ wird. Hieraus folgt, dass der Schaden tatsächlich entstanden sein muss und nicht nur vermutet wird (vgl. OLG Frankfurt a. M. GRUR-RS 2022, 4491, Rn. 55 ff.). Obwohl der Schadensbegriff nach dem Erwägungsgrund 146 S. 3 weit auszulegen ist, um den Betroffenen einen wirksamen Ersatz zu ermöglichen, genügt ein einfacher Verstoß gegen Normen aus der DSGVO nicht für ein (immaterielles) Schadensersatzbegehren (so auch OLG Frankfurt a. M. aaO.). Jedoch muss der eingetretene Schaden nicht erheblich sein. Daher kann auch Ersatz für Bagatellschäden verlangt werden.

74
Die Rechtsauffassung, wonach der Kontrollverlust nicht per se ein ersatzfähiger Schaden ist (so auch OLG München, Verfügung vom 14.09.2023 – 14 U 3190/23 e), ändert der EuGH auch in seiner aktuellen Rechtsprechung nicht (vgl. EuGH Urt. v. 14.12.2023 – C-340/21, BeckRS 2023, 35786 Rn. 84, 85; OLG Hamm (7. Zivilsenat), Beschluss vom 21.12.2023 – 7 U 137/23). Danach hat die klagende Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachzuweisen, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen.

75
Der Kläger hat den Eintritt eines konkreten, immateriellen Schadens, worunter auch Ängste, Sorgen, Stress sowie Komfort- und Zeiteinbußen fallen, nicht ausreichend dargestellt. Er hat angegeben, einen Kontrollverlust über seine personenbezogenen Daten erlitten zu haben.

76
Im Rahmen seiner informatorischen Anhörung sagte der Kläger er sei lediglich verwundert und genervt gewesen. Bei verdächtigen Anrufen lege er auf, könne diese aber nicht immer von seriösen Anrufen unterscheiden. Seine Mobilfunknummer, die zugleich seine Geschäftsnummer sei, könne er nicht so leicht ändern.

77
Die persönlich im Rahmen der informatorischen Anhörung beschriebene Verhaltensänderung ist nicht hinreichend, um einen behaupteten immateriellen Schaden anzunehmen. Aus dem klägerischen Vortrag wird nicht deutlich, wie kriminelle oder auch lediglich lästige Handlungen Dritter aussehen sollen, in denen öffentlich zugängliche Daten des -Nutzers mit der Handynummer kombiniert werden. Er hat lediglich im Zuge seiner persönlichen Anhörung erklärt, häufig verdächtige Anrufe zu erhalten. Inwieweit diese personalisiert waren, ergab sich für das Gericht nicht.

78
Schlussendlich lässt sich nicht nachweisen, dass Anrufe und Benachrichtigungen im Kausalzusammenhang mit dem Scraping-Vorfall bei der Beklagten erfolgen. Dieser Umstand ist vielmehr dem allgemeinen Lebensrisiko, das jedem mit der Nutzung des Internets und der Preisgabe personenbezogener Daten einhergeht, geschuldet, zumal die streitgegenständliche Mobilnummer in Zusammenhang mit dem Klarnamen des Klägers anderweitig öffentlich einsehbar ist.

79
Ein immaterieller Schaden lässt sich aus einem diffusen Bedrohungsgefühl ohne substantiierte Tatsachengrundlage nicht ableiten.

III.

80
1. Es besteht kein Anspruch auf Feststellung der Ersatzpflicht hinsichtlich künftiger Schäden.

81
Daneben ist der Klageantrag zu 3) unbegründet. Der Kläger hat nicht dargelegt und es ist auch nicht erkennbar, dass ihm irgendwie geartete materielle künftige Schäden zumindest erwachsen können. Dies folgt nicht bereits aus dem Umstand, dass immer öffentlich zugängliche Daten und die Handynummer durch Scraper kombiniert werden.

82
2. Ein (weiterer) Auskunftsanspruch ist nicht gegeben (Klageantrag zu 5).

83
Der Klageantrag zu 5) ist unbegründet, da die Beklagte dem Kläger mit Schreiben vom 06.02.2023 (Anlage B16) in angemessener Weise Auskunft über die von ihr verarbeiteten Daten erteilt hat. Es ist nicht erkennbar, dass neben den immer öffentlich einsehbaren Daten und der Handynummer des Klägers weitere Daten von dem Scraping-Vorfall betroffen sind. Es liegen keine Anhaltspunkte dafür vor, dass Daten vom Scraping erfasst sind, die nicht ohnehin öffentlich einsehbar beziehungsweise von den Suchbarkeitskriterien umfasst waren. Andernfalls läge ein Hacker-Angriff vor, der vorliegend nicht erkennbar ist und auch nicht vom Kläger dargetan wird.

84
3. Es sind keine Unterlassungsansprüche gegeben.

85
a) Der Kläger hat keinen vertraglichen Unterlassungsanspruch gegen die Beklagte. Entgegen der klägerischen Auffassung liegt weder eine Vertragsverletzung seitens der Beklagten noch eine Verletzung einer vertraglichen Nebenpflicht, insbesondere Verschwiegenheitspflicht, vor.

86
Sofern sich aus den Nutzungsbedingungen in Bezug auf die personenbezogenen Daten des Klägers eine hier relevante vertragliche Pflicht der Beklagten ergibt, dann kann dies unzweifelhaft nur die Pflicht sein, die Privatsphäre-Einstellungen des Klägers zu befolgen. Es ist deshalb widersprüchlich, wenn der Kläger ein Unterlassen im Hinblick auf Daten verlangt, die im Einklang mit seinen Privatsphäre-Einstellungen auf der -Plattform öffentlich einsehbar waren.

87
Die einschlägige Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten des Klägers war und ist Art. 6 Abs. 1 lit. b DSGVO (Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung; hier in Bezug auf die Bereitstellung eines sozialen Netzwerks). Es liegt somit ein gesetzlicher Erlaubnistatbestand für die Bearbeitung vor.

88
Auch aus einer etwaigen Verletzung vertraglicher Nebenpflichten ergibt sich vorliegend kein vertraglicher Unterlassungsanspruch. Denn selbst wenn eine Verschwiegenheitspflicht als Nebenpflicht aus dem Nutzungsvertrag bestünde, wäre ihre Reichweite durch die individuellen Privatsphäre-Einstellungen bestimmt. Der Kläger konnte anhand der Telefonnummer, im Einklang mit ihren Suchbarkeits-Einstellungen, gefunden werden. Soweit die Informationen in den durch Scraping abgerufenen Daten von der -Plattform stammen, handelt es sich um immer öffentliche Nutzerdaten (auf die in der Datenrichtlinie ausdrücklich hingewiesen wird) oder um Daten, die im Einklang mit der Zielgruppenauswahl des Klägers öffentlich einsehbar waren. Da die Privatsphäre-Einstellungen des Klägers zum Zeitpunkt des Scraping-Vorfalls vorsahen, dass die betreffenden Daten öffentlich einsehbar sein sollten, kann insoweit auch keine Verschwiegenheitspflicht bestehen.

89
b) Dem Kläger stehen zudem keine gesetzlichen Unterlassungsansprüche gegen die Beklagte gem. §§ 1004 analog, 823 Abs. 2 BGB i. V. m. Art. 6 Abs. 1 sowie Art. 32 DSGVO und Art. 13 DSGVO (Klageantrag zu 4.a)) zu. 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.

90
Des Weiteren stellt die Beklagte ihr Kontaktimporttool zur Überzeugung des Gerichts nicht mehr zur Verfügung. Dadurch war es – wie oben dargelegt – jedem möglich, ein öffentlich einsehbares Nutzerprofil abzurufen, indem lediglich die Telefonnummer eingegeben wurde. Darüber hinaus ist zu beachten, dass es jedem Nutzer obliegt, jederzeit seine Suchbarkeitseinstellungen anzupassen, was der Kläger vorliegend auch getan hat. Deshalb ist eine Wiederholungsgefahr nicht zu befürchten.

91
Aus den eben genannten Gründen scheitert auch ein Unterlassungsanspruch nach dem Klageantrag zu 4.b).

IV.

92
Die Kostenentscheidung beruht auf § 91 Abs. 1 S. 1 ZPO zu tragen. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 S. 1, S. 2 ZPO.

V.

93
Der Streitwert wir auf 6.500 € festgesetzt.

94
Hinsichtlich des Streitwertes war Ziffer 1 der Klage mit 3.000 € zu bewerten, was dem klägerischen Mindestbetrag entspricht. Der Feststellungsantrag in Ziffer 3 war mit 400 € zu bewerten; bei einem Feststellungsantrag ist der Wert des Gegenstandes des Rechtsverhältnisses maßgeblich. Ziffer 2 bewertet das Gericht mit 2.000 €. Ziffer 5 (Auskunftsanspruch) wird mit 100 € angesetzt. Der Unterlassungsantrag ist nur mit 500 € zu bewerten. Ein erhöhter Wert ist nicht ersichtlich, zumal die Einkommens- und Vermögensverhältnisse der Beklagten hier nicht entscheidungsrelevant sind. Auch der weitere auf Unterlassung gerichtete Antrag ist lediglich mit 500 € anzusetzen, die Einkommens- und Vermögensverhältnisse der Beklagten sind auch in diesem Zusammenhang nicht entscheidungsrelevant.

95
Die einzelnen Streitwerte sind zu addieren.