LG Memmingen, Endurteil v. 29.07.2024 – 26 O 1031/23

Titel:

Datenschutzrechtliche Bewertung von Scraping-Vorfällen bei nutzerveröffentlichten Daten

Normenketten:

DSGVO Art. 5 Abs. lit. a, Art. 13, Art. 14, Art. 24 Abs. 1, 32 Abs. 1, Art. 82 Abs. 1

ZPO § 253 Abs. 2 Nr. 2, § 256 Abs. 1

Leitsätze:

1. Informationspflichten nach Art. 13, 14 DSGVO sind auch bei gestuften und mehrschichtigen Informationen dann erfüllt, wenn die Informationen für den durchschnittlichen Nutzer hinreichend verständlich, klar und zugänglich sind. Eine gewisse Komplexität der Informationen ist angesichts der Vielzahl datenschutzrechtlicher Pflichten hinzunehmen. (Rn. 48 – 54) (redaktioneller Leitsatz)

2. Wird eine freiwillig angegebene Mobilfunknummer öffentlich sichtbar eingestellt, ohne dass die entsprechende Einstellung geändert wird, begründet ein darauf basierender Datenscraping-Vorfall keine Verletzung der Datensicherheitspflichten nach Art. 24, 32 DSGVO, sofern der Nutzer zuvor ausreichend über Risiken und Steuerungsmöglichkeiten informiert wurde. (Rn. 55 – 60) (redaktioneller Leitsatz)

3. Die datenschutzfreundliche Voreinstellung nach Art. 25 Abs. 2 DSGVO ist nicht verletzt, wenn eine Plattform es dem Nutzer nach klarer Information ermöglicht, standardmäßig öffentliche Daten wie Mobilfunknummern nachträglich in ihrer Sichtbarkeit zu beschränken und dieser Gestaltungsspielraum dem sozialen Zweck des Netzwerks dient. (Rn. 62 – 66) (redaktioneller Leitsatz)

4. Zur Erfüllung des Auskunftsanspruchs nach Art. 15 Abs. 1 DSGVO genügt eine hinreichende Information über die verarbeiteten personenbezogenen Daten, ihre Verarbeitungszwecke und Empfänger – eine weitergehende Auskunft über unbekannte Dritte, die durch Scraping öffentlich zugängliche Daten extrahieren, ist dem Verantwortlichen nicht möglich und daher nicht geschuldet. (Rn. 73 – 74 und 102 – 107) (redaktioneller Leitsatz)

Schlagworte:

Internationale Zuständigkeit, Verbrauchervertrag, Social Media Plattform, Schmerzensgeld, Feststellungsklage, Unterlassungsklage, Auskunftsanspruch

Rechtsmittelinstanzen:

OLG München, Hinweisbeschluss vom 13.02.2025 – 24 U 3020/24 e

OLG München, Beschluss vom 17.03.2025 – 24 U 3020/24 e

Fundstelle:

GRUR-RS 2024, 42664

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 8.000,00 € festgesetzt.

Tatbestand

1

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen behaupteter Verletzung von Persönlichkeitsrechten, Grundrechten und Grundfreiheiten, insbesondere um Verletzung der Rechte auf Schutz personenbezogener Daten.

2
Die Beklagte betreibt die Social Media Plattform …, welche es den Nutzern der Plattform ermöglicht, ein persönliches Profil zu erstellen, wobei der Nutzer hier Angaben zu seiner Person machen kann, Bilder hochladen kann, seine Interessen eingeben kann, etc. In dem von der Beklagten vorgegebenen Rahmen kann der Nutzer entscheiden, inwiefern andere Nutzer auf seine angegebenen Daten Zugriff nehmen können.

3
Der Kläger ist Nutzer der von der Beklagten betriebenen Plattform.

4
Jedenfalls ab 2019 sammelten Dritte unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Beim Scraping werden typischerweise öffentlich verfügbare, also öffentlich zugängliche Daten gesammelt, wobei Funktionen einer Website verwendet werden, die für ordnungsgemäße Nutzer entworfen wurden und bei diesen beliebt sind. Scraping unterscheidet sich insofern von der zulässigen Nutzung einer Website oder App, dass die Scraper Verfahren einsetzen, um in großem Umfang Daten zu sammeln.

5
Das Sammeln von Daten über diese automatisierten Methoden ist durch die Nutzungsbedingungen der Beklagten verboten.

6
Das Scraping lief dergestalt ab, dass die Scraper Listen mit möglichen Telefonnummern in den Kontakt-Importer der Plattform hochluden, 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 standardmäßig voreingestellte Suchbarkeits-Einstellung „Alle“ 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.

7
Jedenfalls seit Anfang April 2021 ist öffentlich bekannt, dass es zu dem Scraping Vorfall gekommen war und dass die abgegriffenen Daten von ca. 533 Millionen …-Nutzern aus 106 Ländern im Internet öffentlich verbreitet werden. Hierzu gehörten auch die vom Kläger auf seinem Profil öffentlich zugänglich gemachten Informationen und die mit seinem Konto verknüpfte Telefonnummer. Die Daten der Klägerseite wurden im Internet bereitgestellt.

8
Bei dem Anlegen eines …-Profils wird der künftige Nutzer auf die Datenschutz- und Cookie Richtlinien hingewiesen. Diese sind durch eine Verlinkung getrennt abrufbar. Zudem zeigt er durch das Registrieren, dass er den Nutzungsbedingungen zustimmt. Nach der Anmeldung sind zunächst die Vor- bzw. Standardeinstellungen aktiv. Stets „öffentlich“ sind dabei Name und Geschlecht. Bezüglich der weiteren einzugebenden bzw. eingegebenen Daten ist zwischen den Einstellungen der „Zielgruppenauswahl“, d.h. den Einstellungen, die bestimmen welche Daten eingesehen werden können und den „Suchbarkeits-Einstellungen“, d.h. den Einstellungen, die festlegen wie man den Nutzer finden kann, unterschieden.

9
Demnach können „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse „finden“.

10
Der Nutzer kann diese Einstellungen individuell verändern und sich im Hilfebereich einlesen, wie Facebook die Daten, insbesondere die Mobilfunknummer verwendet. Die Angabe der Mobilfunknummer ist nicht zwingend. Entscheidet sich ein Nutzer aber diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Die Grundeinstellung für die Suchbarkeit lautet auch insoweit zunächst „alle“.

11

Neben den gewöhnlichen Funktionen auf der …-Website wird von der Beklagten noch eine Messenger-App betrieben, die als Schnittstelle für die …-Applikation auf Mobilgeräten arbeitet und eine Messenger-Funktion für Nutzer darstellt. Nutzer melden sich dafür mit ihren bestehenden Facebook-Profilen an. Die Messenger-App und die gewöhnlichen Funktionen von Facebook sind über denselben Zugang zum Account verknüpft.

12
Der Kläger nutzte die Zweifaktor-Authentifizierung und gab im Rahmen dazu seine Mobilfunknummer bei seinem …-Account an.

13
Mit Schreiben vom 22.06.2023 (Anlage K 1) forderte die Klageseite die Beklagte zur Zahlung von 3.000 Euro Schmerzensgeld nach Art. 82 Abs. 1 DSGVO auf sowie zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte auf. Zudem forderte die Klagepartei die Beklagte auf, Auskunft darüber zu geben, welche Daten des Klägers neben seiner Handynummer durch welche Unbefugte und zu welchem Zeitpunkt entweder durch „Scraping“ oder auf andere Art und Weise erlangt werden konnten.

14
Die Beklagte wies die von Klageseite außergerichtlich gelten gemachten Ansprüche mit Schreiben vom 21.07.2023 (Anlage B 2) zurück, erteilte hierbei jedoch weitere Informationen. Für die Einzelheiten wird auf die Anlage B 2 Bezug genommen.

15
Die Klageseite behauptet, das „scrapen“ sei nur möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern und weil die Einstellungen zur Sicherheit der Telefonnummer auf Facebook so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Auch die Suchbarkeitseinstellungen seien schwer zu finden, sodass eine Umstellung sich schwierig darstelle. Der Wortlaut bei der Registrierung führe letztlich dazu, dass Nutzer im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf … preisgäben. Insgesamt gebe es verschiedene Einstellungsmöglichkeiten zur Verwendung der Telefonnummer, über die ein Nutzer keine transparenten Informationen für eine Gewährleistung einer effektiven digitalen Sicherheit erhalte. Diese Sicherheitslücke werde seit 2019 ausgenutzt, ohne dass die Beklagte etwas dagegen unternehme.

16
Der Kläger behauptet weiter, er habe so ungewollt die Kontrolle über seine Daten verloren und erhalte seit dem Vorfall unregelmäßig Emails und Anrufe mit offensichtlichen Betrugsversuchen. Dies bereite dem Kläger ein Unwohlsein und er empfinde Stress, Angst und Verunsicherung. Er fühle sich im Alltag eingeschränkt.

17
Nur aufgrund der fehlenden Sicherheitsvorkehrungen der Beklagten hätten auch seine Daten entsprechend unbefugten Dritten angeboten werden können. Dass eine automatisierte Massenabfrage möglich war, stelle eine Sicherheitslücke dar, für die die Beklagte einzustehen habe.

18
Die Klageseite ist der Ansicht, die Beklagte verstoße gegen die DSGVO, indem sie ohne ausreichende Grundlage im Sinne der Art. 6 und 7 DSGVO Informationen im Sinne von Art. 13, 14 DSGVO verarbeite, Daten unbefugten Dritten zugänglich mache sowie die Rechte des Klägers aus Art. 15, 17 und 18 DSGVO verletze.

19
Die Klagepartei 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 2.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5 %-Punkten über den jeweiligen Basiszinssatz der EZB seit Rechtshängigkeit 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 von pauschal 2.000,00 € nebst Zinsen in Höhe von 5 %-Punkten über den jeweiligen Basiszinssatz der EZB seit Rechtshängigkeit 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 bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu 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 nach dem 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, dem Kläger Auskunft über die personenbezogenen 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.

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 freizustellen.

20
Die Beklagte beantragt:

Klageabweisung.

21
Die Beklagte meint, bei dem Scraping-Vorgang sei zu berücksichtigen, dass die Telefonnummern nicht von den …-Profilen stammen, sondern die Telefonnummern von den Scrapern generiert wurden, um diese dann im Rahmen der Telefonnummernaufzählung zu nutzen. Der klägerische Vortrag beruhe insgesamt auf einem Missverständnis zum Scraping als solchen. Es sei zudem unschlüssig und unsubstantiiert, welche Daten des Klägers genau gescrapt worden sein sollen. Es seien weder E-Mail-Adresse, Wohnort, Geburtsdatum und Beziehungsstatus in den durch Scraping abgerufenen Daten enthalten; das Land sei nur aus der Telefonnummer abgeleitet worden.

22
Ein Datenschutzverstoß liege auf Beklagtenseite, ebenso wie ein Unterlassen des Schließens einer technischen Schwachstelle, nicht vor. Es seien lediglich öffentlich einsehbare Daten durch Dritte in Form des Scraping abgerufen worden, was nach den Nutzungsbedingungen von … untersagt gewesen sei und auch weiterhin untersagt sei. Die Suchbarkeit der Klagepartei sei innerhalb des relevanten Zeitraums auf „Alle“ eingestellt gewesen.

23
Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der …-Plattform gestanden. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem …-Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe der Kläger jederzeit anpassen können.

24
Im Übrigen sei keinerlei Zusammenhang zwischen etwaigen Phishing-Nachrichten und dem Scraping-Sachverhalt erkennbar. Die vorgetragenen Umstände zu den Folgen seien pauschal und daher nicht nachprüfbar. Die Empfänger der gescrapten Daten könnte die Beklagte zudem nicht mitteilen.

25
Die Beklagte ist daher der Auffassung, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Die Beklagte meint, das Scraping stelle bereits keinen Datenschutzverstoß dar. Es fehle an einer Verletzung der Sicherheit, da „lediglich“ öffentlich zugängliche Profilinformationen des Klägers abgerufen und auch keine spezifischen Sicherheitsmaßnahmen oder Zugriffsberechtigungen umgangen oder überwunden wurden. Eine unbefugte Offenlegung von oder Zugang zu den klägerischen Daten sei nicht gegeben. Der Beklagten könne zudem keine Sicherheitslücke zur Last gelegt werden, da die hergestellte Verknüpfung zwischen der Telefonnummer des Klägers und seinem Nutzerkonto lediglich auf die seinerzeitige Suchbarkeitseinstellung des Klägers zurückzuführen sei.

26
Darüber hinaus fehle es an einem immateriellen Schaden, der nicht ausreichend dargelegt sei. Mangels Verstoßes gegen die DSGVO sei der (ohnehin unzulässige) Feststellungsantrag unbegründet. Die Unterlassungsanträge seien ebenfalls unzulässig gefasst und nicht hinreichend bestimmt.

27
Die am 27.07.2023 bei dem Landgericht Memmingen eingegangene Klageschrift vom 25.07.2023 ist der Beklagten am 16.08.2023 zugestellt worden.

28
Das Gericht konnte im Termin zur mündlichen Verhandlung vom 08.07.2024 den Kläger nicht informatorisch anhören, da dieser trotz ordnungsgemäßer Ladung und Anordnung des persönlichen Erscheinens unentschuldigt nicht erschienen ist.

29
Hinsichtlich des weiteren umfassenden Sach- und Rechtsvortrages der Parteien wird Bezug genommen auf die gewechselten Schriftsätze nebst Anlagen wie auf das Protokoll über die mündliche Verhandlung vom 08.07.2024.

Entscheidungsgründe

A.

30
Die teilweise bereits unzulässige Klage ist vollumfänglich unbegründet.

31
I. Die Klage ist nur teilweise zulässig.

32
1. Das Landgericht Memmingen ist international, sachlich und örtlich zuständig.

33
1.1. Die internationale Zuständigkeit ergibt sich aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann ein Verbraucher gegen seinen Vertragspartner vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat, klagen. Gemäß Art. 17 Abs. 1 EuGVVO ist der Kläger als Verbraucher anzusehen. Zwischen den Parteien ist unstrittig, dass der Kläger mit der Beklagten einen Nutzungsvertrag über die Nutzung der Social Media Plattform … zu privaten Zwecken geschlossen hat. Eine entgegenstehende ausschließliche Zuständigkeit nach Art. 24 EuGVVO ist nicht gegeben.

34
1.2. Das Landgericht Memmingen ist nach §§ 23, 71 Abs. 1 GVG sachlich und nach Art. 18 Abs. 1 2. Alt EuGVVO örtlich zuständig.

35
2. Der unbestimmte Klageantrag in Ziffer 1) und 2) der Klage führt nicht zu einer Unzulässigkeit. Vorliegend ist das Stellen eines unbezifferten Klageantrags ausnahmsweise zulässig, da die Bemessung der Höhe des

Schmerzensgeldes in das Ermessen des Gerichts gestellt ist. Ein Verstoß gegen den in § 253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach § 287 ZPO oder vom billigen Ermessen des Gerichts abhängig ist. Die nötige Bestimmtheit soll hier dadurch erreicht werden, dass der Kläger in der Klagebegründung die Berechnungs- bzw. Schätzgrundlagen umfassend darzulegen und die Größenordnung seiner Vorstellungen anzugeben hat (vgl. Greger in Zöller, 34. Auflage 2022, ZPO, § 253 Rn. 14). Diese Voraussetzungen liegen hier vor. Der Kläger hat sowohl in der Klagebegründung als auch bereits in dem Klageantrag zu 1) und zu 2) jeweils einen Mindestbetrag angegeben.

36
3. Hinsichtlich des Klageantrags Ziffer 3) hat die Klageseite das Feststellungsinteresse hinreichend dargelegt. Das rechtliche Interesse des Klägers an einer alsbaldigen Feststellung der Ersatzpflicht der Beklagten im Sinne des § 256 Abs. 1 ZPO ergibt sich daraus, dass sich der anspruchsbegründende Sachverhalt zur Zeit der Klageerhebung noch in der Entwicklung befand. Bei Klageerhebung war erst ein Teil des Schadens entstanden. Die Entstehung weiteren Schadens war nach dem Vorbringen des Klägers noch zu erwarten. In einer derartigen Fallgestaltung ist die Feststellungsklage nach der ständigen Rechtsprechung des Bundesgerichtshofs insgesamt zulässig (vgl. BGH, Beschluss vom 06.03.2012 – VI ZR 167/11 m.w.N.). Ein Feststellungsinteresse ist nur dann zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. BGH, Beschluss vom 09.01.2007 – VI ZR 133/06). Bei den von Klageseite behaupteten Verstößen mit der behaupteten unkontrollierten Nutzung der Daten ist bei verständiger Würdigung der Umstände nach Ansicht des Gerichts jedenfalls nicht gänzlich ausgeschlossen, dass irgendein materieller oder immaterieller Schaden infolge der Veröffentlichung seiner Daten entstehen könnte. Insgesamt war das erforderliche Feststellungsinteresse daher vorhanden.

37
4. Der auf Unterlassung gerichtete Klageantrag in Ziff. 4) wird den Bestimmtheitsanforderungen jedoch nicht gerecht und erweist sich daher bereits als unzulässig. Bei Unterlassungsklagen muss die Verletzungshandlung, deren Unterlassen die Klagepartei begehrt, derartig genau beschrieben werden, dass der Gegenstand des Verfahrens und damit der Umfang der Entscheidungsbefugnis des Gerichts sowie die Rechtskraft der Entscheidung genau fixiert wird. Die Beklagte muss sich gegen den Vorwurf erschöpfend verteidigen können. Die Verurteilung muss deutlich erkennen lassen, was ihr verboten ist. Die Entscheidung darüber darf nicht dem Vollstreckungsverfahren überlassen bleiben (vgl. BGH, Urteil vom 11.10.1990 – I ZR 35/89). Soweit mit der Klage beantragt wird, dass die Beklagte es zu unterlassen hat „personenbezogene Daten der Klagepartei, namentlich Telefonnummer, … ID, Familiennamen, Vornamen, […] unbefugten Dritten […] zugänglich zu machen“, wird sie den oben genannten Anforderungen nicht gerecht. Durch die nicht abschließende Auflistung der personenbezogenen Daten wird für die Beklagte nicht ersichtlich, in welchem Umfang das Verbot gilt. Es ist ihr somit nicht möglich, ihr Verhalten rechtskonform auszuüben. Es ist nämlich nicht so, dass grundsätzlich alle personenbezogenen Daten nicht zugänglich gemacht werden dürfen. Soweit der klägerische Antrag neben der ausdrücklich genannten Telefonnummer auch die personenbezogenen Daten Familienname, Vorname und Geschlecht erfassen soll, handelt sich bei diesen Datenpunkten um immer öffentliche Nutzerinformationen, so dass es schon keine unbefugten Dritten geben kann, welchen der Zugriff verweigert werden kann. Eines Hinweises bedurfte es insoweit nicht, da einerseits bereits die Beklagtenpartei auf die fehlende Bestimmtheit hingewiesen hat, anderseits der Antrag darüber hinaus auch unbegründet gewesen wäre, wie nachstehend noch ausgeführt wird.

38
Der Klageantrag zu 4) ist darüber hinaus deswegen unzulässig, weil der Kläger damit im Kern nicht ein Unterlassen von Kontaktvorschlägen verlangt, sondern, dass er diese unter Wahrung bestimmter Sicherheitsanforderungen nutzen kann. Damit handelt es sich um eine verdeckte und mithin unzulässige Leistungsklage. Die Kammer nimmt insofern zur Vermeidung von Wiederholungen auf das Urteil des OLG Hamm vom 15.08.2023 – 7 U 19/23 sowie den Beschluss des OLG München vom 25.03.2024 – 24 U 1663/23 e Bezug.

39
II. Die Klage ist insgesamt unbegründet. Der Klagepartei stehen die von ihr geltend gemachten Ansprüche nicht zu.

40
1. Ein Anspruch auf Ersatz eines immateriellen Schadens besteht nicht.

41
1.1. Ein Anspruch auf Ersatz des immateriellen Schadens ergibt sich nicht aus Art. 82 DSGVO.

42
1.1.1. Der Anspruch ergibt sich bereits nicht aus Art. 82 DSGVO, da der Schutzbereich nicht eröffnet ist.

43
Art. 82 DSGVO erfasst Verstöße, welche durch eine nicht der Verordnung der DSGVO entsprechende Verarbeitung (von Daten) entstanden sind, vgl. Art. 82 Abs. 2 DSGVO. Erforderlich ist daher von vornherein eine Verarbeitung von Daten im Sinne von Art. 4 Nr. 2 DSGVO. Gemäß Art. 4 Nr. 2 DSGVO handelt es sich bei Datenverarbeitung um jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

44
Soweit die Klageseite der Beklagten Verstöße gegen Informationspflichten vorwirft, kann sich hieraus somit bereits kein Anspruch aus Art. 82 DSGVO ergeben, da es sich um keinen Verstoß im Hinblick auf die Verarbeitung von Daten handelt.

45
Die von der Klagepartei vorgebrachten Verstöße gegen Art. 13, 14 DSGVO, Art. 34 DSGVO und Art. 15 DSGVO betreffen einzig und allein Informationspflichten gegenüber den betroffenen Personen. Die Information über die Verarbeitung von personenbezogenen Daten stellt aber keine Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO dar, sodass der Klagepartei ein entsprechender Schadensersatzanspruch aus etwaigen (nicht vorliegenden, siehe unten) Verstößen nicht zustehen kann (vgl. hierzu u.a. Gola/Piltz in Gola/Heckmann 3. Aufl. 2022, DS-GVO Art. 82 Rn. 20; LG Essen, Urteil vom 10.11.2022 – 6 O 111/22).

46
1.1.2. Unabhängig von der Frage, ob der Schutzbereich eröffnet ist, scheitert der geltend gemachte Anspruch jedoch vorliegend an den entsprechenden Pflichtverletzungen der Beklagten.

47
1.1.2.1. Ein Verstoß gegen die Transparenzpflichten aus Art. 5 Abs. 1 lit. a), Art. 13, 14 DSGVO fällt der Beklagten nicht zur Last.

48
Gemäß Art. 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Diese Grundsätze sind sodann auf die Informations- und Aufklärungspflicht nach Art. 13 DSGVO zu übertragen. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. Ähnliche Anforderungen sieht dabei auch Art. 14 DSGVO für den Fall vor, dass der Verantwortliche die Daten nicht direkt bei der betroffenen Person erhebt. Art. 12 DSGVO sieht ebenso eine Information in präziser, transparenter und leicht zugänglicher Form vor.

49
Diese Vorgaben hält die Beklagte vorliegend ein. Die Beklagte weist den jeweiligen Nutzer bereits bei der Registrierung auf die Datenrichtlinie hin, welche herausarbeitet, welche Daten auf der Plattform einsehbar sind und welche Auswirkungen es hat, je nachdem welche Zielgruppe der Nutzer wählt. Auch im Hilfebereich erläutert die Beklagte den Nutzern die Bedeutung der Einstellung „öffentlich“. Zudem wird explizit im Hilfebereich aufgeklärt, dass der Nutzer auch festlegen kann, wer sehen kann, was der Nutzer teilt. Zur Umstellung dieser Einstellungen wird auch eine Anleitung bereitgestellt. Weiter erfolgt im Hilfebereich auch die Aufklärung, dass der Nutzer ggf. über seine Handynummer oder seine E-Mail-Adresse

gefunden werden kann sowie wie der Nutzer seine Mobilfunknummer hinzufügen, aber auch entfernen kann.

50
Hierbei handelt es sich um Informationen auf mehreren Ebenen. Jedoch schließt gerade dies die Übersichtlichkeit und Transparenz nicht aus. Die Beklagte versuchte über mehrere Ebenen, die vielschichtigen Themen abzuschichten und einzelne Themenbereiche zu bilden. Dies dient letztlich der Vermeidung der Überforderung des Nutzers mit einer Flut an Informationen im Hinblick auf die verarbeiteten Daten. Dabei wird nicht verkannt, dass das Lesen sämtlicher Informationen und Unterbereiche letztlich mit einem gewissen Zeitaufwand verbunden ist, jedoch ist ein solcher Zeitaufwand auch beim Lesen bei Allgemeinen Geschäftsbedingungen der Fall. Hierauf kann es jedoch nicht ankommen. Einzig und allein ist letztlich zu beachten, ob der Nutzer hinreichend klar und verständlich informiert wird. Dies ist vorliegend der Fall. Dabei fand die Aufklärung über die Verwendung der Daten auch in verständlicher Sprache statt, wie es nach Inaugenscheinnahme der streitgegenständlichen Bestimmungen der Datenrichtlinie und des Hilfebereiches zur Überzeugung des Gerichts feststeht.

51
Es ist gerade zu berücksichtigen, dass in Anbetracht der Vorgaben der DSGVO und der damit verbundenen vielseitigen Informationspflichten vielfältige Einstellungsmöglichkeiten nahezu zwingend sind, sodass jeder Nutzer die Einstellungen individuell entsprechend seiner spezifischen Bedürfnisse vornehmen kann.

52
Für eine sachgerechte Betrachtung der Frage ist auch zu berücksichtigen, dass es sich um eine freiwillig von der Klagepartei genutzte Plattform handelt. Soweit die Klagepartei vorliegend neben den für die Anmeldung erforderlichen Daten wie Name, Geschlecht, Geburtsdatum und E-Mail-Adresse zusätzlich ihre Mobilfunknummer angab, ist zu bedenken, dass es sich bei der Mobilfunknummer um eine nicht erforderliche Angabe handelte. Denn soweit man sich zur Nutzung der Plattform entschließt, ist jedenfalls die Angabe der Mobilfunknummer neben der E-Mail-Adresse dafür nicht zwingend erforderlich. Hierbei handelt es sich um ein zusätzliches Angebot der Beklagten, mit welcher der jeweilige Nutzer – wie hier die Klagepartei – weitere Funktionen und Informationen – wie etwa das Zweifaktor-Authentifizierungsverfahren – nutzen kann. Im Rahmen der Datenrichtlinie wird der Nutzer darüber aufgeklärt, dass die Verwendung möglicherweise erfolgt, um dem Nutzer Personen vorzuschlagen, welche der Nutzer kennen könnte. Ebenso wird darauf hingewiesen, dass der Nutzer kontrollieren kann, wer die Nummer sehen kann. Zudem wird dem Nutzer erklärt, dass er über die Privatsphäre-Einstellung regeln kann, wer ihn mit seiner Handynummer suchen kann. Selbst wenn das Auffinden dieser Hinweise unter Umständen mit zeitlichem Aufwand verbunden ist, sind die Hinweise selbst klar und verständlich formuliert. Insbesondere ist auch deutlich, dass zwischen dem Sehen der Telefonnummer und dem auf … nach dir suchen zu unterscheiden ist. Insbesondere ist auch die Einstellung „Wer kann dich anhand der angegebenen Telefonnummer finden?“ mit der Antwort „Alle“ eindeutig.

53
Insgesamt ist damit festzuhalten, dass es der Eingabe der Mobilfunknummer zur Nutzung der Plattform eigentlich nicht bedarf, dass jedoch, wenn der Nutzer sich für die Verwendung der Plattform mit seiner Mobilfunknummer entscheidet, er hinreichend verständlich und übersichtlich aufgeklärt wird, wie die Mobilfunknummer verwendet wird und wie eine solche Verwendung eingeschränkt werden kann. Letztlich ist dabei auch zu bedenken, dass die Plattform … gerade dem Finden und dem Austausch von Informationen in der Form eines sozialen Netzwerks dient. In diesem Fall ist es dem Nutzer auch zuzumuten, sich mit den ihm gegebenen Informationen zum Schutz seiner Daten zu befassen.

54
Unter Berücksichtigung all dieser Umstände ist ein Verstoß auf Beklagtenseite gegen Art. 5 Abs. 1 lit. A) DSGVO nicht zu erkennen.

55
1.1.2.2. Es liegt auch kein Verstoß der Beklagten gegen Art. 24 Abs. 1, 32 Abs. 1 DSGVO vor.

56
Nach diesen Vorschriften hat der Verantwortliche bei der Verarbeitung personenbezogener Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der

Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Anknüpfend an den Gedanken der Schaffung eines Schutzniveaus kann sich eine derartige Verpflichtung in Anbetracht des Wortlautes des Art. 32 Abs. 1 lit. b) DSGVO allerdings nur auf solche Datensätze beziehen, die nicht gerade einem Schutz der Vertraulichkeit entzogen werden sollen.

57
Bei Zugrundelegung dieses Maßstabs hat die Beklagte gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, nicht verstoßen. Die Beklagte war nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils des Klägers aufgrund seiner selbst gewählten Einstellung zu verhindern (vgl. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22).

58
Soweit auf die Daten der Klagepartei wie Name, Geschlecht und Benutzername im Rahmen des Scraping Vorfalls zugegriffen wurde, handelt es sich gerade um Daten die für jedermann öffentlich zugänglich waren. Diesbezüglich können diese Daten für sich bereits kein erhöhtes Schutzniveau in Anspruch nehmen. Denn die Beklagte durfte aufgrund der von ihr zur Verfügung gestellten Nutzungshinweisen sowie der vor Registrierung vom Nutzer zwingend zu bestätigenden Datenverwendungsrichtlinien davon ausgehen, dass der Klagepartei klar ist, dass sein Name, Geschlecht und Benutzername jederzeit für jedermann abrufbar ist (vgl. Landgericht Essen, a.a.O., so auch LG Halle, Urteil vom 28.12.2022 – 6 O 195/22).

59
Soweit man unterstellt im Rahmen des Scraping-Vorfalls sei auch die Mobilfunknummer der Klagepartei abgegriffen worden, ist auch hier kein Verstoß der Beklagten festzustellen.

60
Die Klagepartei hatte die Suchbarkeitseinstellung für ihre Mobilfunknummer nicht verändert, so dass diese auf „Alle“ eingestellt war. Diese Einstellung beinhaltet, dass Dritte die Klagepartei über ihre Mobilfunknummer finden konnten. Hierunter fällt letztlich auch die Möglichkeit, dass Dritte über eine zufällig mittels elektronischer Möglichkeiten erzeugte Mobilfunknummer letztlich eine Verknüpfung zur Klagepartei über deren zum Finden freigegebene Mobilfunknummer herstellen. Zwar ist die Beklagte durchaus verpflichtet, zu gewährleisten, dass nicht jedermann ohne weiteres an die sensibleren Daten, wie beispielsweise die Mobilfunknummer gelangt. Dieser Anforderung kam die Beklagte jedoch nach, indem es sich hier zum einen um eine freiwillige, nicht zwingend erforderliche Preisgabe von Daten des Nutzers gegenüber der Beklagten handelt und zum anderen, indem der Nutzer unter Verweis auf die möglichen Nutzungen der Mobilfunknummer die Möglichkeit hat, jederzeit die Einstellungen zur Suchbarkeit zu ändern. Diese Einstellungen waren – wie bereits dargestellt – hinreichend klar und verständlich. Insofern ist die Beklagte ihrer Verpflichtung nachgekommen, sodass ein Verstoß ebenfalls nicht festzustellen war. Soweit die Klagepartei die hierzu erforderliche Zeit zur Information über die Einstellungen nicht aufbringen wollte, kann dies nicht zu Lasten der Beklagten gehen.

61
Dass nicht öffentlich zugängliche Informationen von Dritten erlangt worden sind, kann nicht festgestellt werden.

62
1.1.2.3. Es liegt auch kein Verstoß der Beklagten gegen Art. 25 Abs. 2 DSGVO vor.

63
Nach Art. 25 Abs. 2 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden. Der Anwendungsbereich von Abs. 2 bezieht sich vor allem auf internetbasierte Dienste wie die der streitgegenständlichen Plattform, bei denen durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen sicherzustellen ist, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben (Nolte/Werkmeister in Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 28). Insofern hat der Betreiber in seinen Voreinstellung vorzusehen, dass alle

nicht für den Zweck der Nutzung erforderlichen personenbezogenen Daten anderen nicht zugänglich gemacht werden, es sei denn der Nutzer nimmt entsprechende Einstellungen vor.

64
Auch hier kann sich der Sinn und Zweck letztlich nicht auf die für die Registrierung erforderlichen Daten Name und Geschlecht beziehen, da der Nutzer auf die öffentlichen Zugänglichmachung bei der Registrierung bereits hingewiesen wird und hier konkludent zustimmt. Soweit jedoch erneut die Mobilfunknummer des Nutzer betrachtet wird, kann das Gericht auch hier keinen Verstoß erkennen. Der Nutzer, der sich entschließt auch seine Mobilfunknummer preis zu geben – obwohl dies für die Nutzung der Plattform in keiner Weise erforderlich ist – macht dies regelmäßig unter anderem aufgrund der damit einhergehenden Komfortfunktion, einfacher gefunden zu werden. Die initiale Einstellung der Such-, beziehungsweise Auffindbarkeit für alle Nutzer dient gerade dem Sozialaspekt und damit dem Verarbeitungszweck der Plattform. Auch wenn die Beklagte mit ihrer Plattform Marketingzwecke verfolgen mag, so ist für den Nutzer aber in der Regel nicht etwa der kommerzielle Aspekt, sondern gerade die soziale Komponente des Netzwerks von Bedeutung. Diese soziale Komponente besteht gerade darin, mit anderen Nutzern in Kontakt zu treten oder in Kontakt zu bleiben, Inhalte aller Art mit der Öffentlichkeit zu teilen, seine Teilnahme an Veranstaltungen zu signalisieren oder sich an öffentlichen Diskussionen zu beteiligen. Soweit der Nutzer nicht an den ausgeführten Möglichkeiten teil haben möchte, bleibt es ihm unbenommen, mit Vornahme der entsprechenden Einstellungen, seine öffentliche Darstellung auf der Plattform einzuschränken. Soweit er dieser Möglichkeit nicht nach kommt, ist dies der Beklagten nicht vorzuwerfen. Überdies war es ihm ohne Weiteres möglich, bei entsprechendem Interesse den Hilfebereich aufzusuchen, wo er über den Reiter „Privatsphäre-Check“ sodann unmittelbar zu den einschlägigen Einstellungen gelangen konnte (vgl. hierzu auch: OLG München, Verfügung vom 14.09.2023 – 14 U 3190/23).

65
Soweit teilweise behauptet wird, dass der kommunikative Zweck ebenso erreicht werden könne, wenn die entsprechenden Voreinstellungen für die Telefonnummern der Nutzer von Anfang an auf „nicht-öffentlich“ beziehungsweise „nicht sichtbar“ gestellt seien, weil die Nutzer der Plattform sich lediglich über ihre Namen und nicht über ihre Telefonnummer suchen, trifft dies nicht zu. Auch wenn es in der Tat unwahrscheinlich erscheint, dass sich Freunde oder Familienmitglieder über ihre Nummern suchen, so ist dies in Bezug auf Externe nicht unbedingt der Fall. Gerade in Anbetracht der Vielzahl an aktiven Nutzern der Plattform können sich die Namen wiederholen, sodass ein einfaches Auffinden des angesteuerten Kontakts nicht immer möglich ist. Vor diesem Hintergrund kann aber gerade die Auffindbarkeit durch die Telefonnummer oder E-Mail-Adresse Abhilfe schaffen, um so eine schnellere und bequemere Kontaktaufnahme zu ermöglichen (so auch LG Kiel, Urteil vom 12.01.2023 – 6 O 154/22).

66
Das Gericht verkennt dabei nicht, dass die Voreinstellungen der Zielgruppenauswahl sowie der Suchbarkeit bei der erstmaligen Nutzung der Plattform nach Eingabe der Mobilfunknummer eine Zugänglichkeit in Form der Einsichtnahme in das Profil des Betroffenen durch einen unbestimmt weit gefassten Personenkreis vorsieht. Dennoch ist es – wie oben bereits ausführlich dargestellt – dem Nutzer gleich nach der Anmeldung möglich, diese Konfiguration zu ändern, um so sein Interesse an der Vertraulichkeit bezogen auf seine Daten zu wahren. Durch diese Möglichkeit, auf die der Nutzer nach seiner Anmeldung durch die Beklagte hingewiesen wird, wird so letztlich dem Zweck der unkontrollierten Weitergabe der Daten des Betroffenen entsprochen.

67
1.1.2.4. Es liegt auch kein Verstoß der Beklagten gegen Art. 33 DSGVO vor.

68
Gemäß Art. 33 DSGVO ist der Verantwortliche verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

69

Einer solchen Verpflichtung unterlag die Beklagte jedoch nicht, da eine Verletzung des Schutzes personenbezogener Daten aufgrund der oben dargelegten Umstände gerade nicht vorlag.

70
1.1.2.5. Es liegt auch kein Verstoß der Beklagten gegen Art. 35 DSGVO vor.

71
Selbst wenn ein Verstoß gegen Art. 35 DSGVO vorlag, indem die Beklagte nach dem Vorfall keine Folgenabschätzung durchführte, ist nicht ersichtlich, inwiefern dies für den von der Klagepartei geltend gemachten Schaden ursächlich bzw. mitursächlich gewesen sein soll. Hiergegen spricht bereits, dass es sich bei den gescrapten Daten um öffentlich zugängliche Informationen auf dem Profil der Klagepartei auf … handelte.

72
1.1.2.6. Es liegt auch kein Verstoß der Beklagten gegen die Auskunftspflicht gemäß Art. 15 DSGVO vor.

73
Die betroffene Person hat gemäß Art. 15 Abs. 1 lit. a und c DSGVO das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob er betreffend den Nutzer personenbezogene Daten verarbeitet hat. Ist dies der Fall, so hat der Nutzer ein Recht auf Auskunft über diese personenbezogenen Daten und über die Verarbeitungszwecke (a) und die Empfänger oder Kategorien von Empfängern (c), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen. Das Schreiben der Beklagtenseite (Anlage B16) informiert die Klagepartei insoweit umfassend. Damit ist der Anspruch insoweit erfüllt und erloschen (§ 362 Abs. 1 BGB).

74
Nicht beantwortet wird durch die Beklagte in dem außergerichtlichen Schreiben einzig, welchen Empfängern die Daten der Klagepartei durch Ausnutzung des Kontakt-Import Tools im Sinne des Art. 15 Abs. 1 c) DSGVO zugänglich gemacht wurden. Das Scraping ist allerdings – wie vorstehend ausgeführt – von außen erfolgt und es nicht erkennbar, wer diese Daten gescrapt hat. Die begehrte Auskunftserteilung ist aufgrund des Vorganges des Scrapings unter Ausnutzung von Daten, die auf „öffentlich“ gestellt sind, unmöglich. Ebenso ist im Rechtssinne unmöglich (und es wird auch nicht näher dargelegt, wie die Beklagte dies mitteilen können soll) zu informieren, wann die Daten gescrapt wurden. Die Beklagte hat der Klagepartei im Ergebnis also alle Informationen mitgeteilt, die ihr selbst bezüglich des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Die Beklagte ist folglich hierzu auch nicht verpflichtet (so auch LG Essen, a.a.O.; LG Ellwangen, Urteil vom 25.01.2023 – 2 O 198/22).

75
1.1.3. Der geltend gemachte Schadensersatzanspruch scheitert darüber hinaus auch daran, dass ein ersatzfähiger Schaden im Sinne von Art. 81 Abs. 1 DSGVO nicht vorliegt.

76
Der Eintritt des Schadens muss dabei im Sinne des § 287 ZPO als überwiegend wahrscheinlich dargetan werden (Foerste in Musielak/Voit, ZPO, 19. Aufl. 2022, § 287, Rn. 7). Das Gericht verkennt dabei nicht, dass der Schadensbegriff im Lichte des Erwägungsgrundes Nr. 146 der DSGVO weit zu verstehen ist, sodass ein genereller Ausschluss von Bagatellschäden im Lichte dieser Erwägungsgründe nicht vertretbar ist (vgl. LG Köln, Urteil vom 18.05.2022 – 28 O 328/21). Dennoch muss jedenfalls ein Schaden tatsächlich „erlitten“ worden sein (Erwägungsgrund Nr. 146 S. 6), das heißt jedenfalls ersichtlich, spürbar, objektiv nachvollziehbar und von einem gewissen Gewicht sein (vgl. LG Essen, a.a.O., m.w.N.).

77
Der Klagepartei ist es letztlich nicht gelungen, eine solche spürbare Beeinträchtigung unter Berücksichtigung der vorgenannten Umstände konkret darzulegen. Die Klagepartei führt schriftsätzlich als immaterielle Schadenspositionen insbesondere Ängste, unter denen sie leide, die daraus resultierten, dass sie einen erheblichen Kontrollverlust über ihre Daten erlitten habe und deshalb großem Unwohlsein und Sorgen in Bezug auf einen potentiellen Missbrauch ihrer Daten durch Dritte ausgesetzt sei. Zudem sei es seit dem Scraping-Vorfall zu einem Anstieg an offenkundigen Betrugsversuchen in Form von Anrufen und Emails gekommen.

78
Insgesamt erweckt der Kläger den Eindruck, dass ihn die erhaltenen Anrufe und Nachrichten verärgern, von einer konkreten Angst, konnte sich das Gericht jedoch nicht überzeugen. Zum Termin zur mündlichen Verhandlung am 08.07.2024 erschien der Kläger trotz ordnungsgemäßer Ladung und Anordnung des persönlichen Erscheinens nicht selbst, sondern nur sein Prozessbevollmächtigter als Vertreter nach § 141 Abs. 3 ZPO. Einen persönlichen Eindruck vom Kläger konnte sich das Gericht folglich nicht verschaffen.

79
Die Daten des Klägers (voller Name, Adresse, Festnetznummer) – insoweit erfolgte keine Streitigstellung seitens der Klägerpartei – sind öffentlich im Telefonbuch, bei „Das Örtliche“, sowie unter seinem Kleinanzeigenkonto (mit Name und Postleitzahl) einzusehen.

80
Dies deutet auf einen eher sorglosen Umgang mit der eigenen Telefonnummer hin und lässt sich mit den geschilderten Sorgen des Klägers nicht in Einklang bringen. Selbst wenn es unwahrscheinlich ist, dass einzelne Telefonnummern von Webseiten abgegriffen werden, würde man erwarten, dass jemand, der sich tatsächlich durch Anrufe von Unbekannten in hohem Maße belästigt fühlt, seine Rufnummer nicht ohne Not öffentlich einsehbar bereit hält. Der Kläger kann deswegen schwer geltend machen, das er sich dadurch beeinträchtigt fühlt, dass seine Daten nun im Netz gelandet sind.

81
Soweit die Klageseite vorbringt, dass bereits ein Verstoß gegen die DSGVO und ein möglicher Kontrollverlust für die Bejahung eines immateriellen Schadens ausreiche und daher schon aufgrund einer bloßen Gefährdung einen Schaden annehmen will, kann sich das Gericht diesen Erwägungen nicht anschließen. Insgesamt erscheint ein Identitätsmissbrauch allein aufgrund einer Telefonnummer eher unwahrscheinlich (so auch LG Karlsruhe, Urteil vom 09.02.2021 – 4 O 67/20). Insbesondere würde der Schadenbegriff so aufgeweicht und ausgedehnt und es würde bereits der Nachweis einer möglichen Betroffenheit genügen, um eine Haftung zu begründen. Dies käme einer reinen Gefährdungshaftung gleich und widerspricht letztlich auch dem Erwägungsgrund Nr. 75 (vgl. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, so auch LG Ellwangen, Urteil vom 25.01.2023 – 2 O 198/22).

82
Ein immaterieller Schaden ist daher – anders als der Kläger meint – nicht bereits in dem Kontrollverlust zu sehen, der durch das Scraping entstanden ist, sondern kann allenfalls Folge dieses Kontrollverlustes sein (OLG München, Beschluss vom 25.03.2024, 24 U 1663/23 e). Es wird seitens der Klagepartei pauschal auf einen erlittenen Kontrollverlust, aufgewendete Zeit, Angst, Stress, Sorge etc. abgestellt, ohne dass hierzu quantitativ oder qualitativ spezifizierter Vortrag bzgl. der Person der Klagepartei erfolgt. Der Vortrag bleibt unsubstantiiert und pauschal. Die umfangreichen Ausführungen zum vermeintlichen Schaden und der Schadenshöhe erschöpfen sich über weite Strecken in theoretischen Ausführungen ohne echten individuellen Bezug zur Klagepartei.

83
Dem Gericht ist aus einer Vielzahl gleichgelagerter Fälle bekannt, dass der Vortrag wortgleich in hunderten von Klagen, die von den Prozessbevollmächtigten des Klägers vertreten werden, enthalten ist.

84
Doch selbst wenn man diesen Vortrag für ausreichend halten sollte, ist dieser nicht nachgewiesen. Denn die Klägerseite ist ohne Entschuldigung zu ihrer persönlichen Anhörung in der mündlichen Verhandlung vom 08.07.2024 nicht erschienen. Sie ist mithin beweisfällig geblieben; ohne ihre Anhörung konnte sich das Gericht die gem. § 286 ZPO erforderliche Überzeugung nicht bilden.

85
1.1.4. Zudem fehlt es an der Kausalität zwischen dem Vorwurf und dem in den Raum gestellten Schaden.

86
Substantiierter Vortrag dahingehend, dass der „Scraping-Vorfall“ ursächlich zu einem konkreten Schaden bei der Klagepartei geführt habe, ist nicht ersichtlich.

87

Hinsichtlich der schriftsätzlich genannten Spam-Anrufe und Emails bleibt ebenfalls unklar, aus welchen konkreten Gründen diese auf das streitgegenständliche Datenleck zurückzuführen sein sollen. Hinzu tritt, dass gerichtsbekanntermaßen auch Inhaber von Telefonnummern, die niemals bei … angemeldet waren, Spam-Anrufe erhalten. Dies trifft häufig ältere Mitbürger, die gerade nicht bei Social Media aktiv sind, sondern deren Telefonnummern auf andere Art und Weise ausgelesen bzw. generiert werden. Insbesondere sind Spam-E-Mails mit Werbung oder Nachrichten mit Hinweis auf eine ausstehende Paketlieferung weit verbreitet. Auch Nachrichten, in welchen sich die unbekannten Täter als Angehörige, Postdienstleister, Bank oder Ähnliches ausgeben, sind üblich und gehen beinahe überall ein. Selbst wenn bei der Klagepartei tatsächlich Spam-Anrufe und SMS-Nachrichten seit 2019 zugenommen haben mögen, so kann dies vielerlei Ursachen haben. Es ist völlig unklar und unbekannt, ob und welche Daten die Klagepartei an anderer Stelle freigegeben hat (beispielsweise im Rahmen weiter verbreiteter Phishing E-Mails) und ob ein unberechtigter Datenzugriff an anderer Stelle zu dem von der Klagepartei behaupteten vermehrten unerwünschten Nachrichtenaufkommen geführt hat. Hätte das Abgreifen von Daten der Klagepartei bereits früher stattgefunden, wäre jedenfalls der hiesige Vorfall für die vorgetragenen Umstände nicht kausal. Dies gilt insbesondere vor dem Hintergrund, dass der Kläger seine Daten öffentlich im Telefonbuch, bei „Das Örtliche“, sowie unter seinem Kleinanzeigenkonto hinterlegt hat.

88
Ein Kausalzusammenhang ist damit weder dargelegt noch bewiesen.

89
1.1.5. Ausführungen zur Höhe des geltend gemachten Schmerzensgeld können daher aufgrund der vorgenannten Umstände unterbleiben.

90
1.2. Ein etwaiger Anspruch auf Schmerzensgeld steht der Klagepartei auch nicht aus sonstigen, nationalen Vorschriften zu.

91
Das Verhältnis der Vorschriften der DSGVO zu denen des materiellen Rechts kann dabei letztlich dahinstehen, da sich auch aus dem nationalen Recht kein Anspruch ergibt.

92
1.2.1. Auf die Vorschriften §§ 280 Abs. 1, Abs. 3, 281, 327, 327e, 327i BGB kann die Klagepartei ein Anspruch bereits deshalb nicht stützen, da die Normen der §§ 327 ff. BGB erst zum 01. Januar 2022 in Kraft getreten sind und damit auf den Zeitpunkt des Abschlusses des Nutzungsvertrags, wie auch auf den Zeitpunkt des Verstoßes nicht anzuwenden sind.

93
1.2.2. Den Anspruch auf Schadensersatz kann die Klagepartei auch nicht auf § 280 Abs. 1 BGB i.V.m. Nutzungsvertrag als Vertrag sui generis stützen (vgl. hierzu, OLG München, Urteil vom 18.12.2020 – 18 U 5493/19).

94
Unabhängig von der Frage, ob die Beklagte eine Pflicht aus dem Nutzungsvertrag verletzt haben soll, fehlt es jedenfalls an einem Schaden gemäß §§ 249 ff. BGB. Das nationale Schadensrecht verlangt für einen Schadensersatzanspruch jedenfalls eine spürbare Beeinträchtigung (Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 9. Aufl. 2020, § 249 BGB, Stand: 8. September 2021, Rn. 26 ff.). An einer solchen fehlt es gerade.

95
1.2.3. An der Darlegung des konkreten materiellen Schadens scheitert letztlich auch der Anspruch aufgrund einer möglichen Verletzung des allgemeinen Persönlichkeitsrechts gemäß §§ 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ebenso wie ein möglicher Anspruch aus § 823 Abs. 2 BGB i.V.m. dem Recht auf informationelle Selbstbestimmung.

96
1.2.4. Aufgrund der obigen Ausführungen kommt auch ein Anspruch aus §§ 1004 BGB analog, 823 Abs. 2 BGB i.V.m. Art. 13, 14 DSGVO nicht in Betracht. Es kann dahin stehen, ob die DSGVO als Schutzgesetz im Sinne von § 823 Abs. 2 BGB anzusehen ist.

97
Die Klagepartei hat der Veröffentlichung ihrer Daten bei der Registrierung unter Zustimmung zu den Nutzungsbedingungen zugestimmt. Insofern hat die Beklagte die Klagepartei hinreichend über die Verarbeitung der Daten aufgeklärt (vgl. hierzu die Ausführungen oben). Soweit der Scraping-Vorfall sich auf die Mobilfunknummer der Klagepartei bezieht, ist auch hier zu berücksichtigen, dass die Klagepartei jederzeit die Einstellungen zur Suchbarkeitsfunktion hätte ändern können. Auch dies war für einen verständigen und interessierten Nutzer ohne weiteres bei Anlegung der entsprechenden Sorgfalt und Inanspruchnahme von Zeit möglich. Dass die Beklagte entgegen der von einem Nutzer getroffenen Einstellungen Telefonnummern eigenständig oder aktiv freigibt oder anderweitig nutzt, hat die Klagepartei schon nicht behauptet.

98
2. Aufgrund der dargelegten Umstände ist auch der Antrag auf Feststellung einer Ersatzpflicht künftiger materieller und immaterieller Schäden unbegründet.

99
3. Darüber hinaus steht der Klagepartei kein Anspruch auf Unterlassung gemäß §§ 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 6 Abs. 1, 17 DSGVO gegen die Beklagte zu. Eine Zuwiderhandlung der Beklagten ist nicht ersichtlich, im Übrigen aber auch für die Zukunft nicht zu befürchten.

100
Soweit vorliegend überhaupt gesichert Daten durch den Scraping-Vorgang durch die unbekannten Täter erlangt wurden, handelte es sich dabei um öffentliche Daten bzw. Daten, auf welche der Kläger den Zugriff erlaubte.

101
Die Klagepartei hat der Veröffentlichung ihrer Daten bei der Registrierung unter Zustimmung zu den Nutzungsbedingungen zugestimmt. Insofern hat die Beklagte die Klagepartei hinreichend über die Verarbeitung der Daten aufgeklärt (vgl. hierzu die obigen Ausführungen). Soweit der Scraping-Vorfall sich auf die Mobilfunknummer der Klagepartei bezieht, ist auch hier zu berücksichtigen, dass die Klagepartei jederzeit die Einstellungen zur Suchbarkeitsfunktion hätte ändern können. Auch dies war für einen verständigen und interessierten Nutzer ohne weiteres bei Anlegung der entsprechenden Sorgfalt und Inanspruchnahme von Zeit möglich. Dass die Beklagte entgegen der von einem Nutzer getroffenen Einstellungen Telefonnummern eigenständig oder aktiv freigibt oder anderweitig nutzt, hat die Klagepartei schon nicht behauptet.

102
4. Der Klageseite steht auch kein Anspruch auf weitergehende Auskunft nach Art. 15 DSGVO zu.

103
Zwar hat nach Art. 15 Abs. 1 DSGVO die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung (BGH Urt. v. 15.6.2021 – VI ZR 576/19, r+s 2021, 525 Rn. 17). Art. 15 Abs. 1 DSGVO verleiht ein verfahrensmäßiges Recht, Informationen über die Verarbeitung personenbezogener Daten zu verlangen (EuGH Urt. v. 22.6.2023 – C-579/21, BeckRS 2023, 14515 Rn. 35).

104
Das Auskunftsbegehren der Klagepartei hat die Beklagte jedoch erfüllt, § 362 Abs. 1 BGB.

105
Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft

erkennbar den Gegenstand des Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (vgl. BGH Urt. v. 15.6.2021 – VI ZR 576/19, r+s 2021, 525 Rn. 19 f. m.w.N.; dem folgend OLG Düsseldorf Urt. v. 9.3.2023 – 16 U 154/21, BeckRS 2023, 4182 = juris Rn. 29).

106
Gemessen daran, ist Erfüllung eingetreten.

107
Mit Schreiben vom 21.07.2023 (Anlage B 2) hat die Beklagte der Klageseite Auskunft über die von ihr verarbeiteten Daten in angemessener Weise zur Verfügung gestellt, sodass der Anspruch bereits teilweise gemäß § 362 Abs. 1 BGB erloschen ist. Die Beklagte ist lediglich angehalten, die von ihr selbst verarbeiteten Daten mitzuteilen. Soweit Dritte durch das Scrapen vorliegend (öffentlich einsehbare) Daten der Klageseite verarbeitet haben, ist die Beklagte hierzu nicht zur Auskunft verpflichtet. Die Beklagte legt darüber hinaus nachvollziehbar dar, dass sie hierzu keine weiteren Angaben machen kann. Die Beklagte hat mithin ungeachtet des von ihr prozessual behaupteten Fehlens einer Auskunftspflicht Auskunft erteilt und hinreichend deutlich gemacht, dass sie keine weiteren Auskünfte zur Identität der Scraper und zum genauen, den Kläger betreffenden Scraping-Zeitpunkt machen kann (OLG Hamm Urt. v. 15.8.2023 – 7 U 19/23, GRUR-RS 2023, 22505 Rn. 228-236, beck-online).

108
5. Die geltend gemachten Nebenforderungen teilen das Schicksal der nicht bestehenden Hauptforderungen und bestehen daher nicht.

B.

109
Die Kostenentscheidung ergibt sich aus § 91 ZPO.

C.

110
Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus § 709 ZPO.

D.

111
Der Streitwert wurde gem. §§ 39 ff. GKG auf 8.000 € festgesetzt. Der Antrag auf Zahlung des immateriellen Schadensersatzes wurde entsprechend seiner Ausgestaltung mit 4.000 € (Ziffer 1: 2.000 €, Ziffer 2: 2.000 €) bemessen.

112
Der Antrag auf Feststellung der Einstandspflicht (Ziffer 3) wurde mit 500 € bemessen. Für den Feststellungsantrag ist für den Streitwert von dem an einem entsprechenden Leistungsantrag orientierten wirtschaftlichen Interesse des Klägers an der Feststellung auszugehen, das sich auf mutmaßliche weitere Schäden ab Klageeinreichung bezieht. Dies bemisst das Gericht nach freiem Ermessen unter Berücksichtigung des beim immateriellen Schadensersatz angesetzten Betrags gemäß § 48 Abs. 1 S. 1 GKG i.V.m. § 3 ZPO.

113
Den Streitwert für den Unterlassungsanspruch (Ziffer 4) bemisst das Gericht insgesamt mit 3.000 € (vgl. OLG München, Beschluss vom 16.05.2024, 24 W 676/24 e)

114
Der Streitwert für den Auskunftsanspruch (Ziffer 5) wird auf 500 € bestimmt. Hierbei schließt sich das Gericht den Erwägungen des OLG Karlsruhe (Beschluss vom 05.07.2023 – 10 W 5/23) an.