# Landgericht Arnsberg, 7 O 691/22

| | |
|---|---|
| **Datum:** | 31.10.2023 |
| **Gericht:** | Landgericht Arnsberg |
| **Spruchkörper:** | 7. Zivilkammer |
| **Entscheidungsart:** | Urteil |
| **Aktenzeichen:** | 7 O 691/22 |
| **ECLI:** | ECLI:DE:LGAR:2023:1031.7O691.22.00 |

**Tenor:**

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits trägt der Kläger.

Das Urteil vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 Prozent des aufgrund des Urteils gegen ihn vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor ihrer Vollstreckung Sicherheit in Höhe von 110 Prozent des jeweils von ihr zu vollstreckenden Betrages leistet.

**T a t b e s t a n d:** 1

Die Parteien streiten um Ansprüche auf Schadensersatz, Auskunft und Unterlassung im Zusammenhang mit der Nutzung der von der Beklagten betriebenen Plattform M. und eines Daten-Scraping-Vorfalls. 2

Die Beklagte betreibt die Social Media Plattform O.. Der Kläger ist Nutzer der M.-Plattform. 3

Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Auf diesen persönlichen Profilen können die Nutzer Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. 4

Wird ein Nutzerkonto eröffnet, werden zur Erstellung eines Nutzerprofils verschiedene Daten abgefragt. Im Registrierungsprozess gibt der Nutzer erforderlicherweise seinen Vor- und Nachnamen, sein Geschlecht und sein Geburtsdatum an. Dabei sind der angegebene Vor- und Nachname, eine von M. erstellte Nutzer-ID und das Geschlecht als „immer öffentliche 5

Nutzerinformationen“ stets öffentlich auf dem eigenen Nutzerprofil zu finden. Andere Daten, die dem Profil hinzugefügt werden können, (wie zum Beispiel E-Mail-Adresse, Geburtsdatum, Land, Stadt oder Beziehungsstatus) sind dann von allen Profilbesuchern einzusehen, sofern dies die jeweiligen persönlichen Profileinstellungen („Zielgruppenauswahl“) vorsehen. Der Nutzer kann diese Einstellungen individuell verändern. Nach der Anmeldung sind zunächst die Vor- bzw. Standarteinstellungen aktiv. Demnach können „alle“/„everyone“ sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse „finden“. Ebenso ist für alle Informationen, die ein Nutzer in sein Profil einträgt, standardmäßig „öffentlich“ als Voreinstellung ausgewählt.

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 möchte (sog. Suchbarkeitseinstellung). Die Grundeinstellung lautete auch insoweit zunächst „alle“. Neben der Option „alle“ konnten Nutzer in den Privatsphäre-Einstellungen im relevanten Zeitraum festlegen, dass nur „Freunde von Freunden“ oder „Freunde“ ihr Profil auf diese Art finden können. Ab Mai 2019 stand Nutzern auch die Option „nur ich“ zur Verfügung, mit der verhindert wird, dass irgendjemand anders das entsprechende Profil so finden kann. 6

Im Zeitraum von Januar 2018 bis September 2019 lasen und persistierten („Scraping“) Dritte M.-Nutzer-ID, Nachname, Vorname, Geschlecht und weitere korrelierende Daten - wobei streitig ist, ob hierzu auch das Land gehörte - über das M.-Tool Contact-Import (CIT). Nutzer konnten während des relevanten Zeitraums ihre Kontakte von ihren Mobilgeräten auf M. hochladen, um diese Kontakte auf der M.-Plattform zu finden und mit ihnen in Verbindung zu treten (Kontakt-Importer-Funktion). 7

Die Parteien gehen davon aus, dass Unbekannte eine Vielzahl von Telefonnummern, die fiktiv waren, aus anderen Leaks stammten oder auf sonstige Weise generiert wurden, in ein virtuelles Adressbuch eingegeben haben. Diese Kontakte wurden mithilfe der Kontakt-Importer--Funktion hochgeladen, um so festzustellen, ob diese Telefonnummern mit einem M.-Konto (in Übereinstimmung mit der jeweiligen Suchbarkeits-Einstellung des Nutzers) verknüpft war. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die einsehbaren Daten gescrapt („abgeschöpft“) und die Telefonnummer den abgerufenen Daten hinzugefügt. 8

Im April 2021 wurde durch die Medien öffentlich über den Scraping-Sachverhalt berichtet, wonach die gescrapten Datensätze von ca. 533 Millionen M.-Nutzern von Dritten in einer ungesicherten Datenbank veröffentlicht wurden. 9

Im relevanten Zeitraum war die Suchbarkeitseinstellung hinsichtlich der Mobilfunknummer für das klägerische Nutzerkonte auf „alle“ eingestellt. Das klägerische Nutzerkonto konnte somit von Scrapern mithilfe der Methode der Telefonnummernaufzählung gefunden werden. 10

Nach dem Scraping-Vorfall deaktivierte die Beklagte die Kontaktimportfunktion. Sie ersetzte diese durch die sogenannte „People-You-May-Know“-Funktion. Bei diesem System wird nicht allein aufgrund der Telefonnummer ein konkret-individueller Nutzer angezeigt, sondern nur noch eine Liste von mehreren Personen, die aufgrund anderer zusätzlicher Zuordnungskriterien der hochgeladenen Kontakte, z.B. des Namens, zuzuordnen sein könnten. 11

Mit anwaltlichem Schreiben vom 23.05.2022 teilte der Kläger mit, dass er ein M.-Konto unter Verwendung der E-Mail-Adresse „E-Mail01“ nutze. Er forderte die Beklagte unter Fristsetzung 12

von vier Wochen zur Zahlung von immateriellen Schadensersatz in Höhe von 2.000,00 €, zur Unterlassung rechtswidriger Verarbeitung personenbezogener Daten, zur Auskunft darüber, welche personenbezogenen Daten verarbeitet und abhandengekommen sind, sowie zur Erstattung vorgerichtlicher Rechtsanwaltskosten in Höhe von 973,66 € auf.

Mit anwaltlichem Schreiben vom 21.06.2022 teilte die Beklagte mit, dass die Nutzer-ID, der Vor- und Nachname, das Land (ggf. anhand der Telefonnummer) und das Geschlecht mit den durch Scraping abgerufenen Daten übereinstimmten, wobei das Land wohl über die Telefonnummer abgegriffen worden sein soll. Die Telefonnummer sei unter Anwendung der Methode der Telefonnummernaufzählung bereitgestellt worden. 13

Sie verwies auf diverse Informations-Tools und Auszüge aus der Datenrichtlinie. 14

Die irische Datenschutzbehörde F. verhängte gegen die Beklagte am 28.11.2022 eine Geldbuße in Höhe von 265 Millionen €. Die F. sieht einen Verstoß der Beklagten insbesondere gegen Art. 25 Abs. 1 und 2 DSGVO. Die Entscheidung ist nicht rechtskräftig. 15

Der Kläger ist der Ansicht, die Beklagte habe eine Persönlichkeitsrechtsverletzung begangen und gegen die Datenschutzgrundverordnung verstoßen. 16

Dazu behauptet er, das Scraping sei dadurch ermöglicht worden, dass die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten „CIT“ zu verhindern. So seien keine Sicherheitscapchas (Abkürzung für „Completely Automated Public Turin Test to tell Computers an Humans Apart“) verwendet worden, um sicherzustellen, dass es sich bei der Anfrage zur Synchronisierung um die Anfrage eines Menschen und nicht um eine automatisch generierte Anfrage handelt. Ebenso wenig sei ein Mechanismus zur Überprüfung der Plausibilität der Anfragen bereitgehalten worden. 17

Durch das Scraping sei ihm ein kausaler Schaden entstanden. Es genüge der bloße Verstoß gegen die DS-GVO und ein möglicher Kontrollverlust für die Annahme eines immateriellen Schadens. Er habe einen erheblichen Kontrollverlust über seine Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch der ihn betreffenden Daten, was sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen manifestiere. Es bestehe ein Gefühl des Kontrollverlusts, des Beobachtetwerdens und der Hilfslosigkeit, mithin zusammenfassend mit einem überschattenden Gefühl der Angst. Die Auswirkungen der bestehenden Ängste, des Stresses, der Komfort- und Zeiteinbußen lägen darin, dass sich die Klägerseite mit dem Datenleak und der Herkunft der Daten auseinandersetzen müsse. Dies sei geeignet, zu einem belastenden Eindruck des Kontrollverlusts zu führen. Dass die benannten Daten in Kombination sogar im sog. Darknet gehandelt würden, vergrößere die Ängste und den Stress der Klägerseite. Im Übrigen ermögliche die Zuordnung von Telefonnummern zu weiteren Daten wie der E-Mail-Adresse oder Anschrift böswilligen Akteuren eine weite Bandbreite an Möglichkeiten wie zum Beispiel Identitätsdiebstahl, die Übernahme von Accounts oder gezielte Phishing-Nachrichten. 18

Einen Zusammenhang zu den Geschehnissen bei M. habe der Kläger dabei nur vermuten und mittelbar über die Medienberichterstattung herleiten können. 19

Darüber hinaus habe es die Beklagte unterlassen, ihn als Betroffenen sowie die zuständige Datenschutzbehörde zu informieren. 20

21

Darüber hinaus sei die Beklagte dem Auskunftsersuchen der Klägerseite nicht in ausreichendem Maße nachgekommen, was einen weiteren Schadenersatzanspruch sowie Auskunftsanspruch begründe.

Das Auskunftsschreiben der Beklagten enthalte lediglich allgemein gehaltene Informationen. Auch treffe die Beklagte keinerlei konkrete Aussagen darüber, welche weitere Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen worden seien. So bleibe etwa offen, wann genau die Daten entwendet worden seien oder wie viele verschiedene Beteiligte diese Funktion ausgenutzt hätten. Es fehlten Angaben zu den konkreten Empfängern der personenbezogenen Daten. 22

Der Kläger beantragt, 23

die Beklagte zu verurteilen, 24

1. an ihn als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Telefonnummer (Tel01) 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, nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen, 25

2. an ihn für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DS-GVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit zu zahlen, 26

3. ihm Auskunft über die die Klägerseite betreffenden weiteren personenbezogenen Daten zu erteilen, die durch Unbefugte erlangt werden konnten, namentlich welche Daten außer der Telefonnummer der Klägerseite durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch „Web Scraping“, die Anwendung des Kontaktimporttools oder auf andere Weise unbefugt erlangt werden konnten, 27

4. 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 sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogene Daten der Klägerseite, insbesondere die Telefonnummer, unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, wie geschehen anlässlich des sogenannten M.-Datenleaks, das nach Aussage der Beklagten im Jahr 2019 stattfand, 28

5. ihn von vorgerichtlichen Rechtsanwaltskosten in Höhe von 487,90 € zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz gegenüber den Prozessbevollmächtigten der Klägerseite freizustellen. 29

Die Beklagte beantragt, 30

die Klage abzuweisen. 31

Die Beklagte ist der Ansicht, die Klage sei bereits teilweise unzulässig. Insbesondere seien der Klageantrag zu Ziff. 1) und der Unterlassungsantrag zu Ziff. 4) nicht hinreichend bestimmt. 32

Im Übrigen sei sie unbegründet. Ihr seien Verstöße gegen die DS-GVO nicht anzulasten. Die Daten seien weder durch Hacking noch infolge eines Fehlers oder Sicherheitsverstoßes in ihrem System, sondern durch das automatisierte, massenhafte Sammeln von ohnehin öffentlich einsehbaren und damit nicht vertraulichen Daten erlangt und an anderer Stelle zugänglich gemacht worden. Die gesammelten Daten umfassten lediglich die immer öffentlichen Nutzerinformationen und diejenigen Daten, die entsprechend der jeweiligen „Zielgruppenauswahl“ öffentlich einsehbar seien. 33

Sie behauptet, es sei Hauptzweck der Plattform, andere Nutzer zu finden und mit ihnen in Kontakt zu treten, woran sich auch die Standard-Voreinstellungen orientierten. Die Scraper hätten dementsprechend lediglich die diesem Zweck dienende Funktionen ausgenutzt. Es sei grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern. Sie habe ihren Nutzern alle Informationen zur Datenverarbeitung zur Verfügung gestellt und umfassend über die Möglichkeiten der Anpassung ihrer Einstellungen informiert. 34

Die Beklagte ist der Ansicht, dass es an einem Verstoß gegen die DS-GVO, insbesondere einem Pflichtverstoß im Sinne des Art. 82 DS-GVO, fehle. Darüber hinaus habe der Kläger einen der Beklagtenzurechenbaren ersatzfähigen immateriellen Schaden weder erlitten noch dargelegt. Es fehle jedenfalls an einem kausalen Zusammenhang zwischen dem Schaden und den angeblichen Pflichtverstößen der Beklagten. 35

Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr. Der Auskunftsanspruch richte sich in erste Linie auf Datenverarbeitungen durch unbekannte Dritte, für die die Beklagte nicht verantwortlich sei. Soweit sich die Klagepartei mit ihrem Verlangen berechtigterweise an die Beklagte richte, sei dieses Verlangen bereits außergerichtlich umfassen beantwortet worden. Anwaltskosten seien mangels Verzuges unbegründet. 36

Zum Sach- und Streitstand im Übrigen wird auf die seitens der Prozessbevollmächtigten der Parteien zur Akte gereichten Schriftsätze nebst Anlagen ergänzend Bezug genommen. 37

**E n t s c h e i d u n g s g r ü n d e:** 38

Die Klage ist teilweise bereits unzulässig, im Übrigen unbegründet. 39

A. 40

Die Klage ist teilweise bereits unzulässig. 41

I. 42

Das Landgericht Arnsberg ist zuständig. 43

Die internationale Zuständigkeit der deutschen Gerichte folgt vorliegend im zeitlichen Anwendungsbereich der DS-GVO (nach Art. 99 Abs. 2 DSGVO ab dem 25.05.2018) aus Art. 79 Abs. 2 S. 1 DS-GVO in Verbindung mit Erwägungsgrund 22 DS-GVO sowie aus Art. 79 Abs. 2 S. 2 Hs. 1 DS-GVO, jeweils als unmittelbar geltendes Recht (Art. 288 Abs. 2 AEUV), und § 44 Abs. 1 S. 2 BDSG, da die Beklagte in Deutschland eine Niederlassung und der Kläger als betroffene Person im Sinne von Art. 4 Nr. 1 DS-GVO ihren gewöhnlichen Aufenthalt in Deutschland hat. 44

Soweit es darauf ankommen sollte, folgt die internationale Zuständigkeit der deutschen Gerichte vorliegend vor dem zeitlichen Anwendungsbereich der DS-GVO aus Art. 7 Nr. 2, 45

Art. 63 Abs. 1 lit. a, lit. c und Abs. 2 EuGVVO, da die Beklagte ihren satzungsgemäßen Sitz, jedenfalls ihre Hauptniederlassung in Irland hat, das schädigende Ereignis aus unerlaubter Handlung auch in Deutschland eingetreten ist und das vorgeworfene Verhalten auch nicht - Vorrang begründend - als Verstoß gegen die vertraglichen Verpflichtungen angesehen werden kann, wie sie sich anhand des Vertragsgegenstands ermitteln lassen.

II. 46

Der Klageantrag zu Ziff. 1) ist zulässig. 47

Insbesondere ist er hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. 48

Da die Bemessung der Höhe des Schmerzensgeldes in das Ermessen des Gerichts gestellt ist, ist die Stellung eines unbezifferten Zahlungsantrags ausnahmsweise zulässig. 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. Zöller/*Greger*, ZPO, 34. Aufl. 2024, § 253 Rn. 14). Diese Voraussetzungen liegen hier vor. Der Kläger hat in der Klagebegründung einen Mindestbetrag von 2.000,00 € angegeben. 49

Soweit der Kläger sein Entschädigungsbegehren auf Verstöße gegen die DS-GVO vor und nach dem Scraping-Vorfall stützt, kann dahinstehen, ob es sich - in Anbetracht der einschlägigen Rechtsprechung zum Streitgegenstandsbegriff *(vgl.* BGH, Urteil vom 31.5.2022, VI ZR 804/20*, zit. nach* NJW-RR 2022, 1071 Rn. 10 *f.;* Beschluss vom 15.12.2020, VIII ZR 304/19*, zit. nach BeckRS 2020, 42398 Rn. 10 f. m. w. N.)* - nicht ohnehin nur um einen einheitlichen Streitgegenstand handelt und zwar deshalb, weil der Kläger objektiv betrachtet erkennbar von einem einheitlichen durch das Scraping und die Veröffentlichung des Leak-Datensatzes verursachten immateriellen Schaden ausgeht, der durch die nach seiner Ansicht bereits vor dem Scraping-Vorfall begangenen Verstöße gegen die DS-GVO eingetreten und durch die Verstöße gegen die DS-GVO im Nachgang zum Scraping-Vorfall vertieft worden sein soll und keinen eigenständigen Schaden darstelle. Teilt man diese Auffassung nicht, so liegt jedenfalls eine im Hinblick auf § 260 ZPO zulässige Kumulation von Klagegründen / Streitgegenständen vor. 50

Es besteht im Hinblick auf die Grenze der Rechtshängigkeit und der Rechtskraft keinerlei Zweifel daran, dass sämtliche auf Grund des Scraping-Vorfalls gerügten Datenschutzverstöße und Persönlichkeitsverletzungen des Klägers und der dadurch bis zum Schluss der letzten mündlichen Verhandlung entstandene immaterielle (Gesamt-)Schaden umfassend und abschließend - also auch nicht etwa als verdeckte Teilklage - rechtshängig geworden sind und abschließend einer rechtskräftigen Entscheidung zugeführt werden sollen (vgl. insgesamt OLG Hamm, Urteil vom 15.08.2023, 7 U 18/23, zit. nach juris Rn. 51 f.). 51

III. 52

Der mit dem Antrag zu Ziff. 4) verfolgte Unterlassungsanspruch ist dagegen bereits unzulässig. 53

Die Klage ist im Hinblick auf § 259 ZPO unzulässig. Vorliegend fordert der Kläger mit dem Antrag zu Ziff. 4) im Schwerpunkt ein aktives Tun. Da der Antrag tatsächlich auf ein 54

zukünftiges aktives Tun gerichtet ist, ist er an § 259 ZPO zu messen, dessen Voraussetzung der Besorgnis nicht rechtzeitiger Leistung, nicht vorliegt.

Der Kläger hat einen gesetzlichen Anspruch gegen die Beklagte aus Art. 25 Abs. 1 und Art. 32 DS-GVO auf Wahrung der Sicherheitsanforderungen. Dieser ist aber nach erfüllt. Er ist allein deshalb erfüllt, weil es die Such- und Kontaktimportfunktion hinsichtlich der Mobilfunktelefonnummer gar nicht mehr gibt, sondern nur noch die "People-You-May-Know"-Funktion. Die Klage ist also auf zukünftige Leistung der Beklagten für den Fall gerichtet, dass es droht, dass die Scraper Wege finden, die neue Funktion zu umgehen. 55

Insoweit besteht bis heute und bestand auch bei Klageerhebung den Umständen nach keine Besorgnis nicht rechtzeitiger Leistung im Sinne des § 259 ZPO. Die Beklagte hat nach (interner) Aufdeckung des Scraping-Vorfalls die streitgegenständliche Funktion eliminiert. Es ist seitdem nicht wieder zu einem Vorfall gekommen. Sie hat innerhalb ihres subjektiven Beurteilungsspielraums zur Umsetzung der Schutzmaßnahmen ein hohes Eigeninteresse daran, die gesetzlichen Vorgaben auch zukünftig zu erfüllen. Sie hat nie - und schon gar nicht ernsthaft - geltend gemacht, sie brauche nicht zu leisten oder sie wolle den gegen sie erhobenen, gesetzlichen Anspruch nicht erfüllen. Es ist nicht ersichtlich, warum dennoch zu besorgen wäre, dass sie die gesetzlichen Vorgaben nicht umsetzen werde. Insbesondere ist angesichts der Feststellungen der Irischen Datenschutzbehörde (F.) in der Entscheidung vom 28.11.2022 und der dort festgesetzten Geldbuße und angesichts der obigen Feststellungen nicht davon auszugehen, dass die Beklagte zukünftig erneut verspätet auf ein festgestelltes Scraping im Rahmen der nur noch bestehenden, neuen - also gerade keine konkrete "Wiederholungsgefahr" begründenden - "People-You-May-Know"-Funktion reagiert (OLG Hamm, Urteil vom 15.08.2023, 7 U 18/23, zit. nach juris Rn. 226). 56

Im Übrigen ist der Antrag zu Ziff. 4) auch unbestimmt (§ 253 Abs. 2 Nr. 2 ZPO), weil er keinerlei Konkretisierung des verlangten Tuns für den vermeintlich drohenden Fall der Erstbegehung im Hinblick auf die derzeit nur bestehende "People-You-May-Know"-Funktion – auch unter Berücksichtigung des subjektiven Beurteilungsspielraums der Beklagten zur Umsetzung der Schutzmaßnahmen – benennt (OLG Hamm, Urteil vom 15.08.2023, 7 U 18/23, zit. nach juris Rn. 231). 57

B. 58

Die Klage ist im Übrigen unbegründet. 59

I. 60

Der Kläger hat keinen Anspruch auf immateriellen Schadensersatz (in geltend gemachter Höhe von mindestens 2.000,00 €) als Ausgleich für angebliche Datenschutzverstöße und die angebliche Ermöglichung der unbefugten Ermittlung der Telefonnummer sowie weiterer personenbezogener Daten des Klägers. 61

Insbesondere ergibt sich ein Anspruch nicht aus Art. 82 Abs. 1 DS-GVO. 62

Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoß gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. 63

Nach der Rechtsprechung des EuGHs gibt es drei Voraussetzungen für die Entstehung eines Schadensersatzanspruchs nach Art. 82 DS-GVO, nämlich ein Verstoß gegen die 64

Bestimmungen der DS-GVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen Verstoß und Schaden (EuGH, Urteil vom 04.05.2023, C-300/21, zit. nach NJW 2023, 1930, 1932).

a) 65

Es fehlt es an einem ersatzfähigen Schaden des Klägers im Sinne des Art. 82 Abs. 1 DS-GVO. 66

Es oblag dem Kläger, einen über die angeblichen Datenschutzverstöße und über den damit mittelbar einhergehenden Kontrollverlust hinausgehenden immateriellen Schaden in Form einer persönlichen / psychologischen Beeinträchtigung aufgrund der Datenschutzverstöße und des Kontrollverlustes darzulegen. 67

Der bloße Verstoß gegen die Vorschriften der DS-GVO reicht nicht aus, um einen Schadensersatzanspruch zu begründen (EuGH, Urteil vom 04.05.2023, C-300/21, zit. nach NJW 2023, 1930, 1933). 68

Es bedarf darüber hinaus der Darlegung und des Nachweises eines konkreten Schadens. 69

Ein bestimmter Grad an Erheblichkeit muss hierbei nicht erreicht werden (EuGH, Urteil vom 04.05.2023, C-300/21, zit. nach NJW 2023, 1930, 1933 f.). 70

In den Erwägungsgründen Nr. 75 und 85 werden einige mögliche Schäden aufgezählt, darunter Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, aber auch der Verlust der Kontrolle über die eigenen Daten sowie die Erstellung unzulässiger Persönlichkeitsprofile. Der Schaden ist zwar weit zu verstehen, er muss jedoch auch wirklich „erlitten“ (Erwägungsgrund Nr. 146 S. 6), also „spürbar“, objektiv nachvollziehbar und von gewissem Gewicht sein, um bloße Unannehmlichkeiten auszuschließen. 71

Der nicht näher konkretisierte Klagevortrag dazu, der Kläger habe Gefühle eines Kontrollverlusts, eines Beobachtetwerdens und einer Hilflosigkeit, insgesamt also das Gefühl der Angst entwickelt, reicht zur Darlegung persönlich belastender Folgen der Datenschutzverletzung nicht aus, weil hiermit nicht genug Beweisanzeichen objektiver Art vorgetragen sind, in denen sich solche Gefühle widerspiegeln, und zwar bezogen auf den konkreten Einzelfall. 72

Es fehlt jeglicher konkret-individuelle Vortrag dazu, wann, wie häufig und auf welchem Weg der Kläger konkret von Missbrauchsversuchen betroffen war und vor allem wie er darauf jeweils reagiert hat oder wie er unabhängig von diesen Versuchen allein durch die Veröffentlichung des Leak-Datensatzes betroffen war. 73

Unerwünschte Anrufe oder Nachrichten erhalten gerichtsbekannt auch Personen, die keinen M.-Account haben oder dort ihre Telefonnummer hinterlegt haben. 74

Ferner trägt der Kläger nicht dazu vor, wie er auf die Entdeckung des Scraping-Vorfalls im April 2021 reagiert hat, also ob er die Plattform nicht mehr nutzt oder seine Profileinstellungen geändert hat. Insbesondere hat sich der Kläger wegen des Kontrollverlustes bis heute nicht gehalten gesehen, seine Mobilfunktelefonnummer zu wechseln. Insoweit ist die Angabe, Furcht vor einem Kontrollverlust über seine Daten zu haben, nicht plausibel. 75

Demnach lässt sich mangels Darlegung der konkreten Missbrauchsfolgen gerade nicht einzelfallbezogen beurteilen, ob nach der Lebenserfahrung eine durchschnittlich im 76

Datenschutz sensibilisierte Person solch negative Gefühle entwickeln würde, die nach klägerischer Behauptung über jene hinausgehen, welche man automatisch entwickelt, wenn ein Gesetz zu seinen Ungunsten verletzt wird.

Obwohl bereits die Gegenseite mehrfach und schon seit der Klageerwiderung die fehlende Individualisierung gerügt und darauf hingewiesen hat, dass der Klagevortrag in allen von den klägerischen Prozessbevollmächtigten geführten Rechtsstreiten nahezu wortgleich sei, hat der Kläger nicht ergänzend vorgetragen. 77

c) 78

Darüber hinaus fehlt es vorliegend auch an einer Kausalität (vgl. insgesamt OLG Hamm, Urteil vom 15.008.2023, 7 U 19/23, zit,. nach juris Rn. 189 ff.; LG Bielefeld, Urteil vom 10.03.2023, 19 O 147/22, zit. nach juris; LG Essen, Urteil vom 10.11.2022, 6 O 111/22; LG Münster, Urteil vom 07.03.2023, 2 O 54/22, zit. nach GRUR-RS 2023, 4183 Rn. 56 ff.; LG Kaiserlautern, Urteil vom 09.03.2023, 2 O 352/22, zit. nach GRUR-RS 2023, 14639 Rn. 37; LG Duisburg, Urteil vom 14.06.2023, 10 O 126/22, zit. nach GRUR-RS 2023, 14602 Rn. 133). 79

Bei der Kausalität zwischen der Datenverarbeitung unter Verstoß gegen die DS-GVO und einem (unterstellten) Schaden in Form persönlicher / psychologischer Beeinträchtigungen durch den Kontrollverlust geht es entscheidend darum, ob die persönlichen / psychischen Folgen, die bei dem Kläger eingetreten sind, auf die (unterstellten) Datenschutzverstöße der Beklagten zurückzuführen sind, und zwar entweder mittelbar durch die negative Folge eines Kontrollverlustes oder erst weiter mittelbar durch verdächtige Kontaktversuche etc.. 80

Der klägerische Vortrag reicht für die Annahme einer Mitursächlichkeit der Datenschutzverstöße für die (hier unterstellten) persönlichen / psychischen Beeinträchtigungen bereits nicht aus. 81

Mit Blick auf den Kontrollverlust als solchen hätte es konkreter Darlegung bedurft, dass bzw. warum der Kläger welche Beeinträchtigungen hierdurch entwickelt hat. Insoweit geht es im Wesentlichen erneut um innere Vorgänge - mit der Folge, dass Beweisanzeichen objektiver Art darzulegen sind. Ein solches Beweisanzeichen könnte z. B. sein, dass der M.-Account gelöscht wurde oder zumindest Such- und Sichtbarkeit auf die "immer öffentlichen" Daten beschränkt wurden, um jeglichem weiteren schädigenden Kontrollverlust vorzubeugen. Hierzu trägt der Kläger nicht vor. 82

Mit Blick darauf, dass der Kontrollverlust zunächst ursächlich für die verdächtigen Kontaktaufnahmen etc. gewesen sein muss, fehlt jeglicher Umstand, der hierfür spräche; denn es ist allgemein bekannt, dass auch auf anderer Weise beschaffte Telefonnummern hierfür verwendet werden. Es ist insoweit weder konkret dargetan noch sonst ersichtlich, dass die Kontaktaufnahmen erst erstmals oder gehäuft nach dem Kontrollverlust auftraten. 83

Es ist auch völlig unbekannt, ob und welche Daten der Kläger an anderer Stelle freigegeben hat und ob ein unberechtigter Datenzugriff an anderer Stelle zu diesem – zu Gunsten des Klägers als wahr unterstellten vermehrten unerwünschten SMS und Anruf-Aufkommens – geführt hat. 84

II. 85

Es besteht auch kein Schadensersatzanspruch des Klägers gegen die Beklagte wegen Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen 86

Datenauskunft.

Denn die Beklagte ist ihrer Auskunftspflicht außergerichtlich ausreichend nachgekommen. 87

Art. 15 Abs. 1 DS-GVO verleiht ein verfahrensmäßiges Recht, Informationen über die Verarbeitung personenbezogener Daten zu verlangen. 88

Nach Art. 15 Abs. 1 DS-GVO kann Auskunft über die erfolgten Abfragen personenbezogener Daten einschließlich Identität der Abrufenden, Zeitpunkt und Zwecke der Abrufe verlangt werde. 89

Dieses Auskunftsbegehren hat die Beklagte mit dem Schreiben vom 21.06.2022 erfüllt. 90

Das zur Akte gereichte anwaltliche Antwortschreiben der Beklagten vom 21.06.2022 enthält insbesondere eine Auflistung, dass bestimmte Datenpunkte (Nutzer-ID, Vorname, Nachname, Geschlecht) und die Telefonnummer abgerufen bzw. verknüpft wurden, eine Erläuterung des Datenabrufs über die immer öffentlichen Daten, das M.-Profil und die Kontaktimportfunktion, die zeitliche Angabe "zu einem Zeitpunkt vor September 2019" und den Hinweis auf das Handeln mehrerer Scraper, nicht eines Scrapers mit Blick auf die Frage nach der konkreten Person. 91

Nähere Informationen zu der (unbefugten) Datenerhebung und -verarbeitung durch unbekannte Dritte, können nicht nach Art. 15 DS-GVO von der Beklagten verlangt werden (LG Lübeck, Urteil vom 25.05.2023, 15 O 74/22, zit. nach GRUR-RS 2023, 11984 Rn. 125; LG Essen, Urteil vom 10.11.2022, 6 O 111/22, zit. nach GRUR-RS 2022, 34818; LG Tübingen, Urteil vom 06.06.2023, 7 O 144/22, zit. nach GRUR-RS 2023, 13839 Rn. 67; LG Bonn, Urteil vom 23.02.2023, 10 O 142/22, zit. nach GRUR-RS 2023, 2619 Rn. 35). 92

III. 93

Aus den oben genannten Gründen steht dem Kläger auch kein (weiterer) Auskunftsanspruch gegen die Beklagte zu. 94

IV. 95

Mangels Anspruchs in der Hauptsache besteht auch kein Anspruch auf Freistellung von außergerichtlichen Rechtsanwaltskosten gemäß § 280 Abs. 1 BGB oder aus Art. 82 Abs. 1 DS-GVO. 96

V. 97

Die Zinsforderungen folgen ebenfalls dem Schicksal der Hauptforderungen. 98

C. 99

Die Nebenentscheidungen beruhen auf §§ 91 Abs. 1 S. 1, 708 Nr. 11, 711 ZPO. 100

D. 101

Der Streitwert wird auf 5.250,00 EUR festgesetzt. 102

Zur Begründung wird auf den Beschluss zur vorläufigen Streitwertfestsetzung (Bl. 179 d.A.) Bezug genommen. 103