Landgericht Detmold, 02 O 184/22

Datum:	02.06.2023
Gericht:	Landgericht Detmold
Spruchkörper:	2. Zivilkammer des Landgerichts Detmold - Einzelrichter/in
Entscheidungsart:	Urteil
Aktenzeichen:	02 O 184/22
ECLI:	ECLI:DE:LGDT:2023:0602.02O184.22.00

Nachinstanz:	Oberlandesgericht Hamm, 7. Zivilsenat - I-7 U 93/23 und I-7 W 40/23

Tenor:

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits hat der Kläger zu tragen.

Das Urteil ist vorläufig vollstreckbar.

Der Kläger kann die Vollstreckung durch Sicherheitsleistung in Höhe von 120 % des zu vollstreckbaren Betrages abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in gleicher Höhe leistet.

Tatbestand: 1

Gegenstand der Rechtsstreits sind Ansprüche des Klägers gegen die Beklagte gerichtet auf Zahlung, Feststellung, Unterlassung und Auskunft vor dem Hintergrund von behaupteten Datenschutzverstößen durch die Beklagte und einem damit in Zusammenhang stehenden Datenverlust im Jahr 2019 bzw. deren Veröffentlichung im Jahr 2021, wobei das Vorliegen von Datenschutzverstößen zwischen den Parteien streitig ist. Der Kläger stützt seine Ansprüche dabei im Wesentlichen auf die Vorschriften der Datenschutz-Grundverordnung (im Folgenden: DSGVO) und macht Persönlichkeitsrechtsverletzungen geltend. 2

Der Kläger war und ist Nutzer der von der Beklagten angebotenen Plattform bzw. des sozialen Netzwerkes „A“. Auf der Plattform können die Nutzer ein persönliches Profil erstellen und dieses mit Freunden teilen. Dabei können verschiedene persönliche Angaben gemacht werden, die von anderen Nutzern – je nach Einstellung – eingesehen werden können. Bei der 3

Anmeldung werden allgemeine Geschäfts- und Nutzungsbedingungen Bestandteil des Nutzungsverhältnisses. Die Beklagte hat außerdem eine eigene Datenrichtlinie (Bl. 227 ff. d. e-Akte), in welcher sie unter anderem über die Verarbeitung und Verwendung von Informationen der Nutzer informiert. Unter der Überschrift „Wie werden diese Informationen geteilt“, wird erläutert, dass die Nutzer ihre hinterlegten Informationen entweder mit einer vom Nutzer selbst gewählten Zielgruppe oder öffentlich teilen können (Bl. 232 f. d. e-Akte). Öffentliche Informationen können von jedem auf oder außerhalb der Produkte der Beklagten gesehen werden, auch wenn kein Konto bei der Beklagten besteht.

Die Beklagte informiert beispielsweise auch darüber, dass Dienste Dritter auf ein öffentliches Profil zugreifen können. Dies umfasst den Benutzernamen oder die Nutzer-ID, das Alter, Land bzw. Sprach, die Freundesliste, sowie jede andere Information, die vom Nutzer mit ihnen geteilt werden. 4

Die Klägerin registrierte sich unter Angabe von Name, Geschlecht und Nutzer-ID – dabei handelt es sich um stets öffentliche Nutzerinformationen – unter Verwendung der E-Mail-Adresse „E-Mail-Adresse01“ auf der Plattform der Beklagten. *Die Sichtbarkeit und Suchbarkeit der sonstigen Daten wie Telefonnummer, E-Mail-Adresse, Geburtsdatum, Land, Stadt und Beziehungsstatus war von der Zielgruppenauswahl des Nutzers abhängig. Die Suchbarkeit der Telefonnummer war von den Suchbarkeits-Einstellungen abhängig. Der Kläger konnte über die Suchbarkeits-Einstellungen bestimmen, ob sein A-Profil auf der Plattform mit Hilfe einer Telefonnummer gefunden werden kann. Der Kläger gab sodann seine Mobilnummer an und stellte ihre Suchbarkeit in dem Zeitraum vor September 2019 auf „öffentlich“. Sein Konto konnte daher auch von „Scrapern“ (siehe dazu unten) mit Hilfe der Methode der Telefonnummernaufzählung gefunden werden. Die Beklagte gibt den Nutzern auch Informationen darüber, wofür sie die Mobilnummer der Nutzer verwendet, beispielsweise um Personen, die der Nutzer kennen könnte, diesem vorzuschlagen (Bl. 223 d. e-Akte). Mit der Registrierung geht ebenfalls die Einstellung der Privatsphäre einher, zu der der Nutzer aufgefordert wird. Trifft der Nutzer keine Auswahl, bleibt es bei den Standardeinstellungen der Beklagten. *Der Nutzer kann separat festlegen, wer seine Telefonnummer und E-Mail-Adresse in seinem Profil sehen kann. *Wird eine dieser Informationen geteilt, kann der ausgewählte Personenkreis den Nutzer anhand dieser Informationen finden (Bl. 222 d. e-Akte). Die Beklagte stellt in dem Zusammenhang eine Funktion bereit, anhand derer Kontakte importiert werden, dh. die Nutzer laden ihre Kontakte auf A hoch und können auf der Plattform die passenden Personen anhand ihrer Telefonnummern finden (sog. Kontakt-Importer-Funktion bzw. Contact Importer Tool, kurz CIT). 5

Im Zeitraum von Januar 2018 bis September 2019 kam es in dem sozialen Netzwerk der Beklagten zu sogenannten Scraping-Vorfällen. Dabei sammelten Dritte (sog. Scraper) unter Nutzung automatisierter Softwareprogramme einige auf der Plattform verfügbare öffentliche Informationen der Nutzer. Sie generierten dabei automatisiert Telefonnummern, die sie in das CIT hochluden, um ggf. ein mit der Telefonnummer verknüpftes Profil und die dort auffindbaren Daten mit der Telefonnummer zu verknüpfen und abzugreifen. Wenn die Plattform anhand der möglichen Telefonnummer ein vorhandenes A-Profil fand, luden die Scraper die öffentlich zugänglichen Informationen des entsprechenden Profils herunter. *So entstanden große Datensätze über Millionen von Nutzern, die von den „Scrapern“ im April 2021 im Internet veröffentlicht wurden. 6

Bekannt wurden die Vorfälle Anfang des Jahres 2021. Die Beklagte informierte ihre Nutzer in dem Zusammenhang und gab dabei auch Informationen, wie sich die Nutzer schützen 7

können, zb. indem sie ihre Telefonnummern nicht öffentlich zugänglich machen. Nach dem Scraping-Vorfall veröffentlichte die Beklagte gezielte Hinweise darüber, wie sie sich dafür schützen können. Insbesondere wird darauf hingewiesen, dass sich das Scraping oft auf öffentliche Daten bezieht (Bl. 261 ff d. e-Akte).

Mit vorgerichtlichem Schreiben vom 16.07.2022 per E-Mail (Bl. 53 ff. d. e-Akte) ließ der Kläger die Beklagte unter Fristsetzung binnen 4 Wochen zur Zahlung von 1.000,00 EUR Schadensersatz nach Art. 82 Abs. 1 DSGVO und zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte sowie zur darüber auf, welche Daten des Klägers von dem Vorfall im April 2021 betroffen waren. 8

Die Beklagte antwortete mit Schreiben vom 17.08.2022 (Bl. 264 ff. d. e-Akte). 9

Der Kläger behauptet, die Telefonnummern der Benutzer konnten aufgrund einer Sicherheitslücke mit den restlichen Personendaten korreliert werden und seien somit Bestandteil des jeweiligen unbefugt verbreiteten Datensatzes. Es sei den Scrapern durch Nutzung des CIT gelungen, auch Telefonnummern zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben waren. Die Beklagte habe für diesen Fall keinerlei Sicherheitsmaßnahmen vorgehalten und daneben die Einstellungen zur Sicherheit so undurchsichtig und kompliziert gestaltet, dass ein Nutzer keine sichere Einstellung erreichen könne. Personenbezogene Daten seien sodann im Internet auf Seiten veröffentlicht worden, die illegale Aktivitäten begünstigten, z. B. auf der Seite „B“.com. Auch seine Daten wie Telefonnummer, Name, Wohnort und Mailadresse seien abgegriffen worden. Die Daten wie Name und Rufnummer würden insbesondere für gezielte Phishing Attacken genutzt. Der Kläger habe sein Telefonnummer zu dem Zweck auf der Plattform hinterlegt, sein Profil sicherer zu gestalten. Der Kläger behauptet außerdem, er habe einen erheblichen Kontrollverlust über seine Daten erlitten und verbleibe in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten. Dies manifestiere sich in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen unbekannter Nummern und Adressen. Er erhalte seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail sowie diverse Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks und sei verstärkt misstrauisch gegenüber bzgl. E-Mails und Anrufen Unbekannter. Möglich sei in dem Zusammenhang auch ein Identitätsdiebstahl oÄ. Ein Schmerzensgeld von mindestens 1.000,00 € entspreche der abschreckenden Präventionsfunktion des Art. 82 DSGVO. 10

Der Kläger ist der Ansicht, er habe gegen die Beklagte aufgrund von Datenschutzverstößen und nicht ausreichenden Auskünften unter anderem einen Anspruch auf Zahlung eines Schmerzensgeldes. Insgesamt habe die Beklagte die Daten des Klägers nicht hinreichend geschützt und keine Sicherheitsvorkehrungen getroffen, um ein Daten-Scraping zu verhindern. Sie sei auch ihren aus der DSGVO folgenden Informations- und Aufklärungspflichten nicht hinreichend nachgekommen. Weiterhin habe die Beklagte im Jahr 2019 die personenbezogenen Daten ihrer Nutzer, so auch die des Klägers, nicht im ausreichenden Maße und nicht den Anforderungen der DSGVO entsprechend, geschützt. Daneben habe die Beklagte gegen die Pflicht aus Artt. 24, 32 DSGVO verstoßen, angemessene technische und organisatorische Maßnahmen zu ergreifen. Darüber hinaus liege ein Verstoß gegen Art. 25 DSGVO vor. Danach besteht die Pflicht, Daten durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu schützen. Sie habe den Auskunftsanspruch, der dem Kläger zustehe, außergerichtlich nicht erfüllt, sodass ein solcher weiterhin bestehe. Daneben sei die Beklagte für die Einhaltung der Vorschriften der DSGVO darlegungs- und beweisbelastet. 11

Am 28.11.2022 habe die irische Datenschutzbehörde DPC gegen die Beklagte eine Geldbuße in Höhe von 265.000.000,00 € verhängt, da das Abgreifen und Veröffentlichen der Daten von A-Nutzern nicht ausreichend verhindert worden sei. Die DPC bejahe insbesondere einen Verstoß gegen Art. 25 Abs. 1 und 2 DSGVO. Neben der Geldbuße sei auch angeordnet worden, dass die Beklagte Abhilfemaßnahmen schaffen müsse. 12

Der Kläger beantragt, 13

1. die Beklagte zu verurteilen, an ihn immateriellen Schadensersatz in angemessener Höhe, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz zu zahlen, 14

2. festzustellen, dass die Beklagte verpflichtet ist, ihm alle künftigen Schäden zu ersetzen, die ihm 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, 15

3. die Beklagte zu verurteilen, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, 16

a. personenbezogenen Daten des Klägers, namentlich Telefonnummer, „A“ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern, 17

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 und, im Falle der Nutzung der „A“-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, 18

4. die Beklagte zu verurteilen, ihm Auskunft über die ihne betreffenden personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten; 19

5. die Beklagte zu verurteilen, an ihn vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz. 20

Die Beklagte beantragt, 21

die Klage abzuweisen. 22

Sie ist der Ansicht, der Kläger habe keinerlei Ansprüche gegen sie. Die Klage sei bereits weitgehend unzulässig. Die Klageanträge zu 1.), 2.) und 3.) seien nicht hinreichend bestimmt. 23

Zudem sei ein Feststellungsinteresse für den Klageantrag zu 2.) nicht gegeben.

Sie ist weiter der Ansicht, die geltend gemachten Verstöße fielen nicht in den Schutzbereich des Art. 82 DSGVO. Mangels Verstoßes gegen die DSGVO sei Art. 82 DSGVO außerdem bereits nicht einschlägig. Scraping sei überdies auch vom sog. Hacking von Daten zu unterscheiden. Dem Kläger sei insofern auch kein Schaden entstanden. Selbst wenn sie einen Schaden erlitten hätte, sei dies der Beklagten weder zuzurechnen noch sei ein kausaler Zusammenhang zu einem Pflichtverstoß erkennbar. Die Beklagte habe ihre Pflichten aus der DSGVO nicht verletzt. Sie bestreitet insbesondere einen Verlust der Kontrolle über die personenbezogenen Daten und ein Unwohlsein des Klägers diesbezüglich mit Nichtwissen. Sie bestreitet außerdem mit Nichtwissen, dass der Kläger infolge des Scraping-Vorfalls unerwünscht kontaktiert wird. Der Kläger habe außerdem nicht hinreichend dargelegt, welche seiner Daten von etwaigen Datenschutzverstößen betroffen seien. Etwaige gescrapte Daten des Klägers seien entweder tatsächlich nicht abgerufen worden oder seien ohnehin bereits öffentlich einsehbar gewesen, sodass kein Datenschutzverstoß vorliege. Bei dem Scraping seien keine Sicherheitssysteme der Beklagten überwunden worden. Die Beklagte habe Dritten nicht den Zugang zu Daten des Klägers ermöglicht, vielmehr habe er durch seine selbst vorgenommenen Einstellungen die Möglichkeit geschaffen, dass seine Telefonnummer in andere Kontakte importiert werden könnte. Obwohl ihrer Ansicht nach weder eine Melde-noch eine Benachrichtigungspflicht bestand, habe die Beklagte bezüglich des Scraping-Sachverhalts eine Vielzahl von Maßnahmen ergriffen und den Nutzern zB. Informationen zur Verfügung gestellt. Der geltend gemachte Auskunftsanspruch sei durch außergerichtliches Schreiben vom 17.08.2022 bereits erfüllt worden; für Datenverarbeitungen von Dritten sei die Beklagte nicht verantwortlich. Außerdem habe sie während des relevanten Zeitraums bereits Anti-Scraping Maßnahmen eingesetzt, die den in der Branche zur Anwendung kommenden Standards entsprechen. 24

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die wechselseitigen Schriftsätze nebst Anlagen Bezug genommen. 25

Entscheidungsgründe: 26

Die zulässige Klage ist unbegründet. Dem Kläger stehen die geltend gemachten Ansprüche gegen die Beklagte nicht zu. 27

A. 28

Die Klage ist zulässig. Insbesondere ist das Landgericht Detmold international, sachlich und örtlich zuständig. Die internationale Zuständigkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO (Brüssel IaVO). Es handelt sich vorliegend um eine Zivilsache. Die Klägerin ist Verbraucherin mit Wohnsitz in Deutschland. Die örtliche Zuständigkeit des Landgerichts Detmold ergibt sich unter anderem aus Art. 18 Abs. 1 Alt. 2 EUGVVO sowie aus Art. 79 Abs. 2 S. 2 DSGVO iVm. Art. 82 Abs. 6 DSGVO. 29

B. 30

Die Klage ist jedoch nicht begründet. 31

I. 32

Der mit dem Klageantrag zu 1.) verfolgte Schmerzensgeldanspruch besteht unter keinem rechtlichen Gesichtspunkt. 33

Ein Anspruch aus Art. 82 Abs. 1 DSGVO kommt nicht in Betracht. Danach hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Gemäß Art. 82 Abs. 2 S. 1 DSGVO haftet jeder an einer Verarbeitung beteiligte Verantwortliche für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Aus Sicht der Kammer mangelt es bereits an einem Verstoß gegen die DSGVO wie auch an einem bei dem Kläger eingetretenen Schaden. Auch der Anwendungsbereich der DSGVO ist aus Sicht der Kammer nicht für jeden der geltend gemachten Verstöße eröffnet. Dazu Folgendes: 34

1. 35

Es liegt kein Verstoß gegen Art. 5 Abs. 1 lit. f) DSGVO vor, da die Beklagte nicht gegen die sie treffende Obliegenheit, personenbezogene Daten vor unbefugter oder unrechtmäßiger Verarbeitung zu schützen, verstoßen hat. 36

a. 37

Zwar sind die öffentlich zugänglichen Informationen des A-Profils des Klägers von Dritten gescrapt und damit auch im Sinne von Art. 4 Nr. 2 DSGVO verarbeitet worden. Die Verarbeitung erfolgte jedoch nicht „unbefugt“ oder „unrechtmäßig“ im Sinne von Art. 5 Abs. 1 lit. f) DSGVO. Damit trifft die Beklagte auch keine Obliegenheitsverletzung in Form der angemessenen Sicherheit und eines entsprechenden Schutzes vor einer solchen Verarbeitung. Bei den gescrapten Daten des Klägers (Name, Geschlecht, Nutzer-ID) handelt es sich um Daten, die für jedermann öffentlich ohne Zugangskontrolle und ohne Überwindung technischer Zugangsbeschränkungen abrufbar waren. Da der Kläger selbst entschieden hatte, diese Daten öffentlich zugänglich zu machen, war die Erhebung dieser auch nicht unbefugt oder unrechtmäßig. Sie ging mit der durch sie vorgenommenen Einstellung seiner Daten einher. Er hat für die übrigen Informationen durch die Vornahme entsprechender Privatsphäre-Einstellungen selbst entschieden, die betreffenden Daten öffentlich zugänglich zu machen. Dass er vorträgt, keine Kenntnis von den Möglichkeiten der verschiedenen Einstellungen bezüglich Suchbarkeit und Sichtbarkeit gehabt zu haben, verfängt aus Sicht der Kammer nicht, denn die Beklagte weist an verschiedenen Stellen und insbesondere bereits bei der Registrierung darauf hin. 38

b. 39

Auch der Abgleich zwischen den von den „Scrapern“ über das Contact-Import-Tool hochgeladenen Telefonnummern mit der des Klägers und der anschließenden Verknüpfung der öffentlichen Daten mit der Telefonnummer, stellt keine unbefugte bzw. unrechtmäßige Verarbeitung dar, vor der die Beklagte den Kläger hätte schützen müssen. Auch wenn diese Vorgehensweise (Scraping) nicht im Sinne der Nutzung der A-Plattform sein dürfte, so wurde die zur Verfügung gestellte Funktion in der von den Beteiligten vorgesehenen Weise genutzt. Der Kläger hat ihre Telefonnummer freiwillig angegeben. Die Beklagte verwendete sie bestimmungsgemäß im Rahmen der Suchbarkeits-Einstellungen, um festzulegen, welche Personen das A-Konto des Klägers anhand seiner Telefonnummer finden konnten. Dies sollten nach den nicht abgeänderten Standardeinstellungen alle Personen sein, die in ihrem Adressbuch die Nummer des Klägers abgespeichert haben. Somit war letztlich jeder Person – damit auch den „Scrapern“ – der Abgleich über die Telefonnummer des Klägers möglich und deshalb nicht unbefugt oder unrechtmäßig. Anzunehmen ist daher, dass die „Scraper“ nichts anderes getan haben, als das, was der Kläger aufgrund der Einstellungen der Suchbarkeits-Funktion erwarten konnte, wenn er seine Telefonnummer angibt und die Suche 40

„allen“ ermöglicht.

Das Vorbingen des Klägers, die Standardeinstellungen würden gegen den datenschutzrechtlichen Grundsatz „privacy by default“ (= datenschutzfreundliche Voreinstellungen) verstoßen, vermögen an dieser Bewertung nichts zu ändern. Eine Verpflichtung der Beklagten, Schutzmaßnahmen zu ergreifen, folgt daraus nicht. Die Beklagte durfte vielmehr annehmen, dass dem Kläger bekannt ist, dass sein Konto über seine Telefonnummer für jedermann aufzufinden ist. Da er vor seiner Registrierung zwangsläufig auch die Datenschutzrichtlinie bestätigt hat, die ihn über die Funktion aufgeklärt hat, durfte die Beklagte annehmen, der Kläger habe entsprechende Kenntnis. Die Datenschutzrichtlinie informiert die Nutzer darüber, dass es den Nutzern, die über die Telefonnummer des Klägers verfügen, ermöglicht wird, ihn zu finden. Zudem heißt es, dass der Nutzer über seine Privatsphäre-Einstellungen auswählen kann, wer mithilfe seiner Telefonnummer nach diesem suchen kann. Der Kläger hätte also die Suchbarkeits-Einstellungen abändern können. Dass aufgrund der Fülle an Informationen und Einstellungen eine Abänderung der Standardeinstellungen nicht zu erwarten sei, vermag die Kammer nicht nachzuvollziehen. Die Einstellung der Privatsphäre ist vergleichsweise einfach und kann schrittweise erfolgen. Eine gewisse Verantwortung im Umgang mit persönlichen Daten in sozialen Netzwerken oder im Internet im Allgemeinen kann den Nutzern durchaus abverlangt werden, sodass die Befassung mit den Privatsphäre-Einstellungen vor dem Hintergrund des Schutzes eigener persönlicher Daten erwartet werden kann. Die Angabe der Handynummer auf der Plattform der Beklagten stellte eine besondere Vorgehensweise dar, die nicht in der Natur der Sache lag und besonders überdacht werden musste. 41

2. 42

Ein Verstoß gegen Art. 24, 32 DSGVO ist ebenso nicht gegeben. Art. 32 Abs. 1, 2 DSGVO formt den allgemeinen Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO) näher aus. Er verlangt Verarbeitungsprozessen ab, ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten zu gewährleisten, um damit angemessenen Systemdatenschutz sicherzustellen. Das Gebot soll personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen unter anderem davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten. Dass die Beklagte gegen ihre Verpflichtung, Datenverarbeitungssicherheit zu gewährleisten, verstoßen hat, ist aus den oben genannten Gründen nicht ersichtlich. Da die abgegriffenen Daten ohnehin immer öffentlich zugänglich waren und der Abgleich von im CIT hochgeladenen Telefonnummern mit der verknüpften Telefonnummer des Klägers nicht unrechtmäßig war, bestand keine Verpflichtung zu weitergehenden Schutzmaßnahmen. 43

3. 44

Nach Auffassung der Kammer liegt auch kein Verstoß gegen Art. 25 DSGVO vor. Hiernach wird vom Verantwortlichen die Sicherstellung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (privacy by design und privacy by default) verlangt. Auch wenn die Voreinstellung der Beklagten, wonach die Suchbarkeit der Telefonnummer für „Alle“ möglich sein soll, nicht das höchste Schutzniveau darstellt, so vermag in einer Gesamtschau dennoch kein Verstoß festgestellt zu werden. Die Beklagte informiert den Nutzer hinreichend über ihre Vorgehensweise und setzt ihn über die verschiedenen Einstellungsmöglichkeiten, die durch Abänderung der Voreinstellung erzielt werden können, in Kenntnis. Daneben dürfte von einem Internetnutzer auch zu erwarten sein, dass er sich mit den entsprechenden Gepflogenheiten vertraut macht, die mit der Nutzung eines sozialen Netzwerkes einhergehen. Im Hinblick auf den Zweck der Funktionsweise, die 45

Nutzer unkompliziert miteinander zu vernetzen, muss der jeweilige Nutzer selbst entscheiden, ob er seine Telefonnummer angibt oder nicht. Zwar ist es Sinn und Zweck der DSGVO, ein hohes Schutzniveau der Daten zu erreichen. Einen umfassenden Schutz dürfte man von der Vorschrift des Art. 25 DSGVO nicht erwarten können, da der zu schützende Personenkreis dennoch eigenverantwortlich handelt. Hinzu kommt, dass auch der Zweck der Contact-Import-Funktion nicht außer Acht gelassen werden darf. Die Beklagte arbeitet mit Werbung und verdient letztlich auch Geld mit den Daten der Nutzer. Dies wiederum muss jedem Nutzer auch bewusst sein, wenn er sich dafür entscheidet, sich auf dem sozialen Netzwerk der Beklagten zu registrieren. Ihm bleibt die Möglichkeit von einer Registrierung abzusehen oder sein Profil wieder zu entfernen. Auch wenn die DSGVO ein möglichst hohes Schutzniveau erreichen soll, muss der Zweck der jeweiligen Datenverarbeitung beachtet werden. So besteht der Unternehmenszweck unter anderem darin, Menschen miteinander zu verknüpfen. Dementsprechend müssen vor allem neue A-Nutzer in der Lage sein, ihre Kontakte und andere Nutzer, die sie gegebenenfalls kennen, zu finden. Die Standard-Einstellung zur Suchbarkeit der Telefonnummer dient genau diesem Zweck. Insoweit war auch die Zugänglichmachung der Telefonnummer für einen größeren Personenkreis, entgegen Art. 25 Abs. 2 S. 3 DSGVO, sach- und zweckdienlich. Dies gilt vor allem deswegen, da der Nutzer durch entsprechende Änderung der Einstellungen intervenieren kann.

Auch der weitere Vorwurf des Klägers, die Beklagte habe nicht in ausreichendem Umfang Anti-Scraping-Maßnahmen getroffen und den Zugang zu Nutzerdaten nicht hinreichend beschränkt und geschützt, verfängt nicht. Entscheidend ist insoweit nicht die von dem Kläger vorgenommene ex-post-, sondern vielmehr eine ex-ante-Betrachtung. Hiernach hat die Beklagte ausreichend substantiiert dargetan, dass sie verschiedene Anti-Scraping-Maßnahmen ergriffen hat (Bl. 138 ff. d. e-Akte): Einsetzen eines EDM-Teams (= External Data Misue-Team), das Aktivitätsmuster und Verhaltensweisen, die typischerweise mit automatisierten Computeraktivitäten in Zusammenhang stehen, identifizieren; Anpassung des Systems an sich entwickelnde Scraping-Taktiken; Implementieren von Übertragungsbeschränkungen, die die Anzahl von Anfragen von bestimmten Daten reduzieren, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden können; Geltendmachung von Unterlassungsaufforderungen, Kontosperrungen und Gerichtsverfahren gegen „Scraper“. Mit der Anpassung des Systems an die entwickelten Scraping-Taktiken sollte sichergestellt werden, dass das Verknüpfen von Telefonnummern mit bestimmten A-Nutzern durch die Contact-Import-Funktion nicht mehr möglich war. Die Beklagte nahm außerdem Captcha-Abfragen (vollständig automatisierter öffentlicher Turing-Test, um Computer von Menschen zu unterscheiden), also die Möglichkeit, herauszufinden, ob hinter der Anfrage ein menschlicher Nutzer steht oder nicht, vor. 46

Warum die Implementierung dieser Maßnahmen im maßgeblichen Zeitraum nicht zutreffend sein sollte und diese dem damals maßgeblichen Stand der Technik nicht entsprochen haben sollten, ist nicht ersichtlich und auch von dem Kläger nicht weiter ausgeführt worden. Letztlich muss in diesem Zusammenhang durchaus beachtet werden, dass Scraping ein bekanntes und stets vorkommendes Problem darstellt, welches vom „Hacking“ unterschieden werden muss. Die Möglichkeiten der Risikominimierung sind begrenzt, da die Preisgabe persönlicher Daten im Internet stets ein gewisses Risiko birgt. Insofern hält die Kammer die Maßnahmen der Beklagten für ausreichend, da in diesen Fällen zudem vor allem die Anpassung solcher an die sich entwickelnden Scraping-Methoden immer erst nachgelagert zum Scraping-Vorfall erfolgen kann. Die Überprüfung vermeintlich „auffälliger“ Telefonnummern kann zudem durch Unterbrechung der Sequenzen leicht umgangen und auf verschiedene Geräte bzw. Nutzer verteilt werden. 47

48

Hinzu kommt, dass auch nicht allein auf einzelne Sicherheitsmechanismen abgestellt werden kann. Insoweit hat die Beklagte einen Ermessensspielraum, welche einzelnen technischen und organisatorischen Maßnahmen sie umsetzt, um im Rahmen einer ganzheitlichen Bewertung aller Maßnahmen ein angemessenes Schutzniveau zu gewährleisten (Jandt, in: Kühlung/Buchner, DSGVO, Art. 32, Rn. 5, 8). Letztlich ist im Wege einer Gesamtbetrachtung davon auszugehen, dass aufgrund der Anzahl der implementierten Sicherheitssysteme ein ausreichender Schutz gewährleistet wurde. Zwar konnte die nicht im eigentlichen Sinne vorgenommene Verwendung des Contact-Import-Tool nicht verhindert werden, jedoch kann aus dem Umstand, dass ein Scraping-Vorfall geschehen ist, nicht gefolgert werden, dass das Sicherheitssystem gegen die DSGVO verstoßen hat.

Letztlich verbleibt es im Übrigen auch hier bei den unter Ziff. 1 und 2 dargestellten Erwägungen. Sinn und Zweck der Vorschriften ist der Schutz personenbezogener Daten vor unrechtmäßigem und rechtswidrigem Zugriff. Da ein solcher nicht vorliegt, bestand keine Verpflichtung zu weitergehenden Schutzmaßnahmen. 49

4. 50

Soweit der Kläger der Beklagten weitere Verstöße gegen die DSGVO vorwirft, nämlich ungenügende Information und Aufklärung über die Verarbeitung der sie betreffenden Daten durch ungenügende Aufklärung zur Verwendung und Geheimhaltung der Telefonnummer (Art. 5 Abs. 1 lit. a), einen unmittelbaren Verstoß gegen Art. 13, 14 DSGVO, die konkrete Informationspflichten enthalten, die seitens der Beklagten nicht eingehalten worden seien, unvollständige Auskunftserteilung nach Art. 15 DSGVO, da nicht mitgeteilt worden sei, welchen Empfängern ihre Daten zugänglich gemacht worden seien (Art. 33, 34 DSGVO), sind solche Verstöße bereits weder vom Schutzzweck des Art. 82 DSGVO noch von dessen sachlichen Anwendungsbereich umfasst (LG Essen, Urt. v. 10.11.2022 - 06 O 111/22). Art. 82 Abs. 1 DSGVO erfasst nur solche Pflichtverstöße, die im Rahmen einer „Verarbeitung“ geschehen, was sich aus dem Wortlaut des Art. 82 Abs. 2 DSGVO ergibt („durch eine nicht dieser Verordnung entsprechende Verarbeitung“). Datenverarbeitung bezeichnet jedoch nur jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgehensweise 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. Art. 5 Abs. 1 lit. a), 13, 14, 15 DSGVO begründen Informationspflichten gegenüber betroffenen Personen. Auch Art. 33, 34 DSGVO begründen eine Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) bzw. die Pflicht zur Benachrichtigung der betroffenen Person (Art. 34 DSGVO). 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 keine Verarbeitungen im Sinne von Art. 4 Nr. 2 DSGVO dar, sodass sich aus ihrer etwaigen Verletzung kein Anspruch aus Art. 82 Abs. 1 DSGVO ableiten lässt. 51

5. 52

Im Übrigen fehlt es auch an einem Schaden im Sinne von Art. 82 Abs. 1 DSGVO. Anders als der Kläger meint, genügt nicht allein der Verstoß gegen die DSGVO, um einen Ausgleich / eine Kompensation verlangen zu können. Dies widerspricht dem Schadensrecht, unabhängig vom Wortlaut des Art. 82 Abs. 1 DSGVO. Ein Schadens- und auch Schmerzensgeldanspruch setzt stets einen immateriellen oder materiellen Schaden voraus. Dies lässt sich nach 53

Auffassung der Kammer auch dem Wortlaut des Art. 82 Abs. 1 DSGVO entnehmen, wonach sowohl ein Verstoß gegen diese (DSGVO) Verordnung nötig ist, als auch ein daraus resultierender materieller oder immaterieller Schaden. Die – hier nicht feststellbare – Verletzungshandlung muss in jedem Fall zu einer konkreten, nicht nur völlig unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten der betroffenen Person geführt haben (LG Hamburg, Urt. v. 04.09.2020 – 324 S 9/19). Verletzung und Schaden sind nicht gleichzusetzen. Es ist nicht für jede bloß individuell empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren; vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und es muss um eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen (LG Essen, Urt. v. 10.11.2022 - 06 O 111/22). Allein der Kontrollverlust des Klägers über seine Daten stellt keinen Schaden dar. Seine Sorge oder Angst um die verwendeten Daten und die Befürchtung, Opfer von Betrugsfällen oder Identitätsdiebstahl zu werden, kann zwar nicht gemessen werden, ist hierfür jedoch noch nicht ausreichend. Immerhin darf nicht außer Acht gelassen werden, dass jedenfalls Name, „A“-ID und Geschlecht von ihm öffentlich bekanntgegeben wurden und damit bereits nicht mehr unter seiner ausschließlichen Kontrolle standen (LG Bielefeld, Urt. v. 19.12.2022 – 8 O 182/22). Letztlich ist also insoweit überhaupt nicht mehr bekannt geworden als das, was von ihm selbst bereits im Internet veröffentlicht wurde. In Bezug auf die bekannt gewordene Telefonnummer mag ein gewisser Kontrollverlust vorliegen. Ob und inwieweit jedoch der Kontrolle über die Telefonnummer überhaupt ein Wert zukommt, mag bezweifelt werden. Im Übrigen reicht für einen Schadensersatzanspruch ein bloßes Unmutsgefühl nach Auffassung der Kammer nicht aus.

Dass der Erhalt dubioser Anrufe unbekannter Nummern und der Erhalt von Spamanrufen tatsächlich auf das Bekanntwerden seiner Telefonnummer zurückzuführen sind, ist nicht zwingend. Es ist bekannt, dass unerwünschte E-Mails, SMS und Anrufe auch Personen erhalten, die keinen A-Account haben oder Nutzer, die dort ihre Telefonnummer nicht hinterlegt haben. Dass der Kläger – nach seinem Vortrag - seit der Veröffentlichung seiner Daten unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail erhalte, die Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks enthalten, ist allein nicht ausreichend, um einen sicheren Zusammenhang zu dem streitgegenständlichen Datenverlust herzustellen. Es ändert auch nichts an dem Erfordernis eines Datenschutzverstoßes seitens der Beklagten als vorgelagerter Voraussetzungen für einen Anspruch auf Schadensersatz. 54

II. 55

Auch der Klageantrag zu 2.) bleibt ohne Erfolg. Ein Feststellungsanspruch hinsichtlich der Einstandspflicht der Beklagten bezüglich künftiger Schäden kommt aus den unter I. dargestellten Gründen mangels einer Haftung dem Grunde nach nicht in Betracht. 56

III. 57

Aus den dargestellten Gründen vermag der Kläger ebenso wenig mit Erfolg einen Unterlassungsanspruch gegen die Beklagte geltend zu machen. Dabei kann letztlich dahinstehen, ob neben der DSGVO, die in Art. 79 DSGVO Ansprüche der Berechtigten abschließend regelt, überhaupt ein Unterlassungsanspruch nach Art. 1004 Abs. 1 S. 1 BGB analog iVm. § 823 Abs. 1 BGB in Betracht kommt, oder ob ein solcher aufgrund der Regelungen der DSGVO gesperrt ist. Da bereits keine Verletzung der DSGVO vorliegt und damit auch das Recht des Klägers auf informationelle Selbstbestimmung als Ausfluss des Absoluten Persönlichkeitsrechts des § 823 Abs. 1 BGB nicht verletzt ist, kommt ein Unterlassungsanspruch nicht in Betracht. Es wurden lediglich Daten abgeschöpft und weiter 58

veröffentlicht, die ohnehin öffentlich sind. Was die Verwendung der Telefonnummer angeht, so liegt es jederzeit in der Hand des Klägers, dies in den Einstellungen zu verändern (vgl. LG Gießen, Urt. v. 03.11.2022 – 5 O 195/22). Die Beklagte weist an verschiedenen Stellen auf ihre Datenschutz- und -verwendungsrichtlinien, die der Kläger bei seiner Registrierung als gelesen angab, hin, sodass sie davon ausgehen konnte, dass dem Kläger bekannt war, dass sein Konto über seine Telefonnummer auffindbar war. Bei einer sorgfältigen Lektüre der Richtlinien hätte der Kläger die Möglichkeit gehabt, seine Privatsphäreeinstellungen zu ändern, sein Konto entsprechend anzupassen und den Kreis der Personen zu reduzieren, für die seine Telefonnummer sichtbar war.

IV. 59

Ein weiterer Auskunftsanspruch nach Art. 15 DSGVO besteht nicht. Zwar wurden Daten des Klägers sowohl von der Beklagten als auch von Dritten verarbeitet. Der Auskunftsanspruch ist jedoch durch das außergerichtliche Antwortschreiben der Beklagten vom 17.08.2022 (Bl. 264 ff. d. e-Akte) gemäß § 362 Abs. 1 BGB durch Erfüllung erloschen. Ein weitergehender Anspruch besteht nicht. 60

1. 61

Mit dem Schreiben hat die Beklagte dem Kläger mitgeteilt, welche Datenkategorien gescrapt wurden und mit den auf dem „A“-Profil des Klägers verfügbaren Informationen übereinstimmen (Nutzer-ID, Vor- und Nachname, Land, Geschlecht, Telefonnummer). Zudem erfolgte ein Hinweis auf die maßgeblichen Abschnitte der Datenrichtlinie sowie die verfügbaren Selbstbedienungstools, die es Nutzern ermöglichen, ihre A-Daten aufzurufen und einzusehen. Dabei handelt es sich um eine dem Art. 15 DSGVO entsprechende ausreichende Information. 62

2. 63

Zu der Erteilung weitergehender Auskünfte war und ist die Beklagte nicht verpflichtet. Art. 15 DSGVO bezieht sich nur auf die eigene Verarbeitung der Beklagten, nicht jedoch auf die von Dritten vorgenommene Verarbeitung. Es handelt sich bei der von dem Kläger begehrten Auskunft inhaltlich vielmehr um die Meldepflicht nach Art. 33, 34 DSGVO. 64

V. 65

Mangels Hauptanspruch kann der Kläger auch nicht den Ersatz vorgerichtlicher Rechtsanwaltskosten geltend machen. 66

C. 67

Die Kostenentscheidung beruht auf § 91 Abs. 1 S. 1 ZPO. 68

Die Entscheidung über die vorläufige Vollstreckbarkeit folgt aus §§ 708 Nr. 11, 711 ZPO. 69

D. 70

Der nach Schluss der mündlichen Verhandlung eingegangene, nachgelassene Schriftsatz der Beklagten-Vertreter vom 19.05.2023 bot für das Gericht keine Veranlassung, erneut in die mündliche Verhandlung einzutreten. 71

E. 72

Der Streitwert wird auf insgesamt 6.500,00 € festgesetzt. 73

Der Streitwert setzt sich wie folgt zusammen: 74

- Klageantrag zu Ziffer 1): 1.000,00 € 75
- Klageantrag zu Ziffer 2): 500,00 € 76
- Klageantrag zu Ziffer 3): Gemäß § 3 ZPO wird der Wert des Unterlassungsanspruchs mit 4.000,00 € bemessen. 77
- Klageantrag zu Ziffer 4): Gemäß § 3 ZPO wird der Wert des Auskunftsanspruchs mit 1.000,00 € bemessen. 78

* 79

Am 29.06.2023 erging folgender **Berichtigungs**beschluss: 80

In dem Rechtsstreit pp. 81

Gemäß § 320 ZPO wird der Tatbestand des Urteils vom 02.06.2023 wie folgt berichtigt: 82

1) 83

Der 2. Satz des 2. Absatz auf Seite 3 des Urteils lautet nunmehr: 84

„Die Sichtbarkeit der sonstigen Daten wie Telefonnummer, E-Mail-Adresse, Geburtsdatum, Land, Stadt und Beziehungsstatus war von der Zielgruppenauswahl des Nutzers abhängig.“ 85

2) 86

Die Sätze 10 und 11 des 2. Absatz auf Seite 3 des Urteils lauten nunmehr: 87

"Der Nutzer kann separat festlegen, wer seine Telefonnummer und E-Mail-Adresse in seinem Profil finden kann. Wird eine dieser Informationen anhand der Suchbarkeitseinstellungen als auffindbar eingestellt, kann der ausgewählte Personenkreis den Nutzer anhand dieser Informationen finden (Bl. 222 d. e-Akte).“ 88

3) 89

Der letzte Satz des 1. Absatzes auf Seite 4 des Urteils lautet nunmehr: 90

„Im April 2021 wurde durch die Medien öffentlich über den Scraping-Sachverhalt berichtet, wonach die gescrapten Datensätze von ca. 533 Millionen A-Nutzern von Dritten in einer ungesicherten Datenbank veröffentlicht wurden.“ 91

Gründe: 92

Soweit der Kläger der beantragten Berichtigung des Tatbestandes allein im Hinblick auf die Ziffer 3) dieses Beschlusses entgegengetreten ist, war der Tatbestand des Urteils auf den Antrag der Beklagten entsprechend zu berichtigen. 93

Die Beklagte hatte in der Klageerwiderung vom 28.01.2023 vorgetragen, dass im April 2021 von den Medien über den Scraping-Sachverhalt berichtet wurde, wonach die Nutzerdaten 94

von Dritten in einer ungesicherten Datenbank veröffentlicht wurden (vgl. Bl. 135 d.e.-Akte). Dieser Vortrag ist von dem Kläger nicht bestritten worden.
