Landgericht Duisburg, 10 O 126/22

Datum:	14.06.2023
Gericht:	Landgericht Duisburg
Spruchkörper:	10. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	10 O 126/22
ECLI:	ECLI:DE:LGDU:2023:0614.10O126.22.00

Rechtskraft: nicht rechtskräftig

Tenor:

Die Klage wird abgewiesen.

Die Klägerseite hat die Kosten des Rechtsstreits zu tragen.

Das Urteil ist vorläufig vollstreckbar. Die Klagepartei darf die Vollstreckung durch Sicherheitsleistung in Höhe von 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110% des jeweils zu vollstreckenden Betrags leistet.

1

Tatbestand: 2

Die Klagepartei macht gegen die Beklagte Schadensersatz-, Unterlassungs- und Auskunftsansprüche im Zusammenhang mit einem sog. „*Scraping-Vorfall*“ geltend. 3

Die Beklagte mit Sitz in Z., R., betreibt die Social-Media-Plattform *H.* die unter anderem über die Website-URL *I01* abrufbar ist. 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 ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können. 4

Im Rahmen der Registrierung – nach Eingabe einer E-Mail-Adresse oder einer Telefonnummer – müssen die Nutzer für ihr Profil zwingend einen Namen, einen 5

Nutzernamen, ein Geschlecht und eine Nutzer-ID angeben. Darüber hinausgehende Informationen sind optional.

Bei den verpflichtend bei der Registrierung anzugebenden Nutzerdaten für das Nutzerprofil – Name, Nutzername, Geschlecht und Nutzer-ID – handelt es sich um immer öffentliche Nutzerinformationen, die für jedermann, auch für Nicht-Nutzer der Plattform, auf dem Profil des jeweiligen Nutzers einsehbar sind. Die Öffentlichkeit der darüber hinausgehenden Daten – wie z. B. der Telefonnummer, des Wohnorts, des Beziehungsstatus, des Geburtstags und der E-Mail-Adresse – ist durch den jeweiligen Nutzer steuerbar. Durch die *Zielgruppenauswahl* kann der Nutzer auswählen, wer einzelne Informationen im H.-Profil eines Nutzers sehen kann, z. B. „Nur ich“, „*Freunde“*, „*Freunde von Freunden*“ und „*Alle*“. Unter „*Freunden*“ sind dabei andere Nutzer zu verstehen, mit denen sich der Betroffene bereits auf der Plattform vernetzt hat. In den *Sichtbarkeits-Einstellungen* kann der Nutzer auswählen, für wen sein Nutzerprofil auffindbar ist. 6

Jedenfalls im Jahr 2019 bestand für die Nutzer zudem die Möglichkeit, eine Telefonnummer zu ihrem Profil hinzuzufügen. Über das sog. *Contact-Import-Tool* (nachfolgend: CIT) der Beklagten war es dann möglich, die im Smartphone eines Nutzers gespeicherten Kontakte mit den Nutzern der Plattform der Beklagten – soweit diese ihre Telefonnummern ebenfalls hinterlegt und die Auffindbarkeit innerhalb der Suchbarkeits-Einstellungen aktiviert hatten – abzugleichen und sich darüber mit den gefundenen Nutzern zu vernetzen. 7

Zudem bot die Beklagte unter Verwendung der Telefonnummer eine sog. *Zwei-Faktor-Authentifizierung* an, die der Sicherung des Nutzerkontos dienen sollte. 8

Soweit keine individuellen Einstellungen getroffen wurden, richteten sich die Einsehbarkeit und Suchfunktion nach den Standardeinstellungen der Beklagten. Für den Fall der Angabe einer Telefonnummer war die Suchbarkeits-Einstellung auf „*Alle*“ voreingestellt. 9

Die Plattform der Beklagten verfügt über einen allgemein zugänglichen Hilfebereich, in dem über die vorgenannten Einstellungsmöglichkeiten informiert wird. Darin befinden sich unter anderem Anleitungen, wie man eine Anpassung der Zielgruppenauswahl und der Suchbarkeits-Einstellungen vornehmen kann, Anlagen B 2 – 8, Bl. 231 ff. d. A. Sie verfügt zudem über einen sog. *Privatsphäre-Check*, der es den Nutzern ermöglicht, die eigenen Privatsphäre-Einstellungen zu kontrollieren. Auch können Nutzer über das Tool „*Wer kann nach mir suchen?*“ überprüfen, wer ihr Profil finden kann. 10

Von der Beklagten wird zudem noch eine Messenger-App betrieben, die eine Versendung von kurzen Nachrichten der Nutzer der Plattform ermöglicht. Nutzer melden sich dafür mit ihren bei der Beklagten bereits bestehenden Nutzerkonten an. Auch in dieser App können einzelne Sicherheitseinstellungen vorgenommen werden. Es kann unter anderem separat eingestellt werden, ob Telefonkontakte mit der Plattform via CIT synchronisiert werden sollen. 11

Die Klagepartei ist registrierte Nutzerin der von der Beklagten betriebenen Plattform. Das klägerische Profil konnte aufgrund der hinterlegten Telefonnummer und der auf „*Alle*“ standardmäßig eingestellten Sichtbarkeit von jedem Nutzer gefunden werden, der die Nummer der Klagepartei in das CIT hochlud, Anlage B 17, Bl. 286 d. A. 12

Im Jahr 2019 griffen Dritte auf die bei der Plattform der Beklagten hinterlegten Daten zu und schöpften diese ab (sog. „*Scraping-Vorfall“*). In welchem Umfang die Daten abgeschöpft – „*gescraped“* – wurden ist zwischen den Parteien streitig. In Hinblick auf den Abschöpfungsvorgang gehen die Parteien übereinstimmend davon aus, dass Dritte das auf 13

der Plattform der Beklagten hinterlegte CIT verwendeten, um einzelne Telefonnummern den Profilen einzelner Nutzer zuzuordnen, ohne dass diese auf den Profilen der Nutzer öffentlich einsehbar waren. Hierzu wurden Nummern in ein virtuelles Telefonbuch hochgeladen und dann über das CIT mit den auf der Plattform der Beklagten hinterlegten Telefonnummern synchronisiert. Das jeweils ausgeworfene Profil wurde daraufhin durch die Dritten besucht, die darauf befindlichen öffentlichen Daten abgeschöpft und dann mit der verwendeten Telefonnummer korreliert. Einer Sichtbarkeit der Telefonnummer auf dem Profil des jeweiligen Nutzers bedurfte es dafür nicht.

Eine Unterrichtung der Klagepartei über den Vorfall erfolgte seitens der Beklagten zunächst nicht. 14

Anfang April 2021 wurden die in diesem Vorgang abgeschöpften Daten von ca. 533 Millionen H.-Nutzern im Internet veröffentlicht. Darunter befanden sich auch Daten der Klagepartei. Die Daten wurden unter anderem auf der Webseite *I02* veröffentlicht, bei der es sich um ein Hacker-Forum handelt. In welchem Umfang die Daten der Nutzer veröffentlicht wurden, ist zwischen den Parteien streitig. Jedenfalls wurden der Vorname, die Nutzer-ID und die Telefonnummer der Klagepartei veröffentlicht. 15

Mit E-Mail vom 16.06.2021 forderte die Klagepartei die Beklagte zur Zahlung von 500,00 € Schadensersatz, zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zu einer Auskunft darüber auf, welche konkreten Daten abgegriffen und veröffentlicht worden seien. Wegen der Einzelheiten wird auf die Anlage K 1, Bl. 53 ff. d. A., verwiesen. 16

Die Beklagte wies das Schadensersatz- und Unterlassungsbegehren der Klagepartei mit Schreiben vom 09.09.2021, Anlage B 16, Bl. 273 ff. d. A., zurück. Mit demselben Schreiben teilte die Beklagte der Klagepartei zudem mit, dass unter den abgegriffenen Daten auch Daten der Klägerseite gewesen seien. Danach seien die Nutzer-ID, der Vorname, das Land und Geschlecht sowie die Telefonnummer der Klagepartei betroffen. Für die Details wird auf das Schreiben der Beklagtenseite vom 09.09.2021, Anlage B 16, Bl. 273 ff. d. A., verwiesen. 17

Am 28.01.2022 verhängte die irische Datenschutzbehörde Y. gegen die Beklagte eine Geldbuße in Höhe von 265 Mio. € mit der Begründung, die Beklagte habe es nicht hinreichend verhindert, dass etwa 533 Mio. Datensätze mit persönlichen Informationen von H.-Nutzern abgegriffen und veröffentlicht worden seien. Wegen der Details wird auf die Entscheidung der Y. vom 25.11.2022, Anlage K 3, Bl. 374 ff. d. A., Bezug genommen. 18

Die Klagepartei behauptet, dass neben ihrer Telefonnummer und Nutzer-ID – was zwischen den Parteien unstreitig ist – auch der Nachname, der Wohnort, das Geburtsdatum, die Stadt, der Beziehungsstatus und „*weitere korrelierende Daten*“ abgeschöpft worden seien. 19

Ihre Telefonnummer habe sie nur aufgrund der Zwei-Faktor-Authentifizierung angegeben. Diese habe dann aufgrund einer Sicherheitslücke bei der Beklagten mit den restlichen Personendaten korreliert werden können, obwohl die bei den entsprechenden Profilen hinterlegten Telefonnummern öffentlich nicht freigegeben gewesen seien. Die Beklagte habe im Zeitpunkt des Vorfalls keinerlei Sicherheitsmaßnahmen vorgehalten, um ein Ausnutzen des CIT zu verhindern. Dabei sei die Klagepartei ohne konkrete Ausführungen der Beklagten zu angeblich ergriffenen technischen und organisatorischen Maßnahmen nicht in der Lage, hierzu weiter vorzutragen. 20

21

Zudem seien die Sicherheitseinstellungen auf der Webseite der Beklagten so undurchsichtig und kompliziert gestaltet, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. Die Nutzer würden mit einer Vielzahl an Informationen hinsichtlich der Nutzungsbedingungen, der Verwendung von Cookies und Datenschutzrichtlinien konfrontiert. Hierzu verweist die Klagepartei auf einzelne Screenshots von der Plattform der Beklagten, Bl. 9 ff. d. A. Aufgrund der großen Menge an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen, wonach standardmäßig alle Angaben öffentlich seien, beibehalte und nicht selbstständig ändere. Die Klagepartei ist daher der Ansicht, dass die von der Beklagten vorausgewählten Standardeinstellungen dem in der DSGVO niedergelegten Prinzip der Datenminimierung und der datenschutzfreundlichen Einstellungen widersprechen würden.

Die Klagepartei ist der Ansicht, die Vertraulichkeit der Telefonnummer des jeweiligen Nutzers sei besonders schützenswert. Sie behauptet hierzu, nicht darauf hingewiesen worden zu sein, dass durch die angegebene Nummer in irgendeiner Weise das Profil des Nutzers identifiziert werden könne. Hätte die Beklagte die Klagepartei in ausreichendem und angemessenem Umfang über die Folgen der Preisgabe der Telefonnummer informiert, so hätte die Klagepartei ihre Einwilligung zur Datenverarbeitung nicht erteilt, insbesondere wenn sie darauf hingewiesen worden wäre, dass kein Schutz vor dem Abgreifen durch automatische Verfahren bestehe. 22

Die Veröffentlichung der Daten habe weitreichende Folgen für die Klagepartei. Die Zuordnung von Telefonnummern zu weiteren Daten wie E-Mail-Adresse oder Anschrift eröffne Kriminellen die Möglichkeit des „*Identitätsdiebstahls*“, der Übernahme von Accounts und gezielter „*Phishing*“-Nachrichten. Die Klagepartei habe daher einen erheblichen Kontrollverlust erlitten, sie fühle sich unwohl und sorge sich über möglichen Missbrauch der abgeschöpften Daten. Dies manifestiere sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Adressen und Nummern. Die Klägerseite erhalte seit dem Vorfall Kontaktversuche via SMS und E-Mail. Diese enthielten offensichtliche Betrugsversuche und potentielle Virenlinks. Die Klagepartei könne daher nur noch mit äußerster Vorsicht auf jegliche E-Mails und Nachrichten reagieren, da sie jedes Mal einen Betrug fürchten müsse und Unsicherheit verspüre. Die unterlassene Information durch die Beklagte habe zudem zu einer Intensivierung des Schadens geführt. 23

Die Klagepartei ist der Ansicht, dass die Datenverarbeitung durch die Beklagte ohne Rechtsgrundlage erfolgt sei und die Beklagte sie nicht im ausreichenden Maße über die Verarbeitung sie betreffender Daten informiert bzw. aufgeklärt habe; dies gelte insbesondere im Hinblick auf die fehlende Aufklärung über die Verwendung und Geheimhaltung ihrer Telefonnummer. Darüber hinaus seien die Daten der Klagepartei durch die Beklagte nicht im ausreichenden Maße geschützt worden. Zudem sei die Beklagte ihrer Informationspflicht nicht nachgekommen, da sie die Klagepartei nicht über den Datenschutzverstoß informiert habe. Des Weiteren habe die Beklagte keine nach der DSGVO erforderliche Folgeabschätzung getroffen. Das Antwortschreiben der Beklagten auf das Auskunftsersuchen der Klagepartei sei außerdem insgesamt unzureichend. 24

Sie ist weiter der Ansicht, dass die Beklagte die Darlegungs- und Beweislast im Hinblick darauf trage, dass sie keine Pflichten aus der DSGVO verletzt habe. Zudem führe bereits die Verletzung der DSGVO zu einem auszugleichenden immateriellen Schaden, ein darüber hinaus entstandener Schaden sei durch die Klagepartei nicht darzulegen; es bedürfe insoweit der Vorlage an den EuGH. 25

Die Klagepartei beantragt, 26

1. die Beklagte zu verurteilen, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 € nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz, 27

2. festzustellen, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden, 28

3. die Beklagte zu verurteilen, 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, 29

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, H.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, 30

b. die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der H.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, 31

4. die Beklagte zu verurteilen, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten, 32

5. die Beklagte zu verurteilen, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen zuzüglich Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz. 33

Die Beklagte beantragt, 34

die Klage abzuweisen. 35

Die Beklagte ist der Ansicht, der klägerische Vortrag zum „*Scraping-Vorfall*“ beruhe auf einem Missverständnis. Es sei nicht substantiiert vorgetragen, welche Daten der Klagepartei genau abgeschöpft worden seien. Der Vorfall sei nicht Folge eines Datenschutzverstoßes durch die Beklagte oder einer technischen Schwachstelle, vielmehr seien – so behauptet die Beklagte – lediglich automatisch gesammelte öffentlich einsehbare Daten „gescraped“ worden. 36

Die Beklagte stelle darüber hinaus ihren Nutzern alle erforderlichen Informationen zur Datenverarbeitung zur Verfügung. Sie ist daher der Ansicht, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Es habe zudem eine umfassende und 37

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 Nutzerkonto hinterlegt habe, einsehen könne. Diese Einstellungen habe - so behauptet die Beklagte – die Klagepartei jederzeit anpassen können.

Im Einklang mit der Marktpraxis habe die Beklagte während des relevanten Zeitraums sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt. Die Beklagte entwickle ihre Maßnahmen zur Verringerung von „*Scraping*“ und als Reaktion auf sich ständig ändernde Bedrohungen fortlaufend weiter. Sie beschäftige hierzu ein Team von Datenwissenschaftlern, -analysten und Softwareingenieuren (External Data Misuse-Team, EDM-Team). Die Beklagte habe auch auf die Verwendung des CIT durch „*Scraper*“ reagiert und eine Verknüpfung mit den Telefonnummern der Nutzer sei auf diesem Wege nun nicht mehr möglich. Auch nutze die Beklagte Captcha-Abfragen, die dazu genutzt würden, herauszufinden, ob hinter einer Anfrage ein menschlicher Nutzer stehe oder nicht. 38

Eine weitergehende Auskunft als in dem an die Klagepartei gerichteten Antwortschreiben sei der Beklagten nicht möglich, da sie über keine Kopie der Rohdaten, welche die durch „ *Scraping*“ abgerufenen Daten enthalte, verfüge. 39

Entscheidungsgründe: 40

Die zulässige Klage ist unbegründet. 41

A. 42

Die Klage ist zulässig. 43

I. 44

Das Landgericht Duisburg ist in internationaler, örtlicher und sachlicher Hinsicht zuständig. 45

1. 46

Die internationale und örtliche Zuständigkeit des Landgerichts Duisburg folgt aus Artt. 79 Abs. 2 Satz 2, 28 Abs. 4 DSGVO und § 44 Abs. 1 Satz 2 BDSG sowie aus Art. 17 Abs. 1 lit. c) EuGVVO i. V. m. Art. 18 Abs. 1 EuGVVO, jeweils i. V. m. §§ 12, 13 ZPO. Da die Vorschriften dieselbe internationale und örtliche Zuständigkeit begründen, kann vorliegend dahinstehen, in welchem Verhältnis diese zueinanderstehen, wobei von einem Vorrang des besonderen Gerichtsstands des Art. 79 Abs. 2 Satz 2 DSGVO als *lex specialis* gegenüber den besonderen Gerichtsständen der EuGVVO auszugehen sein dürfte, vgl. Art. 67 EuGVVO und Erwägungsgrund 147 DSGVO. 47

Nach Art. 79 Abs. 2 DSGVO und § 44 Abs. 1 Satz 2 BDSG sind für Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter die Gerichte des Mitgliedsstaats zuständig, in dem der Verantwortliche oder Auftragsverarbeiter seine Niederlassung hat; wahlweise können solche Klagen auch bei den Gerichten des Mitgliedsstaates erhoben werden, in dem die betroffene Person ihren Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist. Dabei spricht eine Vermutung dafür, dass es sich bei einem bestehenden Wohnsitz um den Aufenthaltsort der Klagepartei im Sinne der Norm handelt (*Mundil* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.11.2021, DS-GVO Art. 79, Rn. 18). Die Klagepartei mit Wohnsitz im Landgerichtsbezirk 48

Duisburg richtet ihre Klage gegen die Beklagte als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO. Die diesbezügliche Behauptung reicht in Anbetracht des Vorliegens einer doppeltrelevanten Tatsache zur Begründung der Zuständigkeit aus.

Nach Art. 18 Abs. 1 EuGVVO kann darüber hinaus die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat. Nach Art. 17 Abs. 1 EuGVVO gilt Art. 18 EuGVVO, wenn Gegenstand des Verfahrens ein Vertrag oder Ansprüche aus einem Vertrag sind, den eine Person, der Verbraucher, zu einem Zweck geschlossen hat, der nicht der beruflichen oder gewerblichen Tätigkeit dieser Person zugerechnet werden kann und wenn – lit. c) – der andere Vertragspartner im Mitgliedsstaat, in dessen Hoheitsgebiet der Verbraucher seinen Wohnsitz hat, eine berufliche oder gewerbliche Tätigkeit ausübt oder eine solche auf irgendeinem Wege auf diesen Mietgliedstaat oder auf mehrere Staaten, einschließlich dieses Mitgliedstaates, ausrichtet und der Vertrag in den Bereich dieser Tätigkeit fällt. Die Beschränkung des EuGVVO auf die Erbringung von Dienstleistungen und die Lieferung beweglicher Sachen ist damit entfallen (*Stadler* in: Musielak/Voit, ZPO, 19. Aufl. 2022, EuGVVO Art. 17 Rn. 6). 49

Vorliegend ist nach den klägerischen Behauptungen zwischen den Parteien jedenfalls ein Nutzungsvertrag über die durch die Beklagte betriebene Plattform zustande gekommen, §§ 133, 157 BGB. Wer dem Verbraucher die Bereitstellung digitaler Inhalte gegen die Preisgabe von Daten anbietet, sei es die Nutzung einer Social-Media-Plattform oder einer Suchmaschine, unterbreitet typischerweise ein Angebot auf Abschluss eines Vertrags, welches innerhalb der AGB in der Regel konkretisiert wird (*Metzger* in: MüKo, BGB, 9. Aufl. 2022, BGB § 327 Rn. 17). 50

Die Klagepartei ist hier als Verbraucherin aufgetreten. Der geschlossene Nutzungsvertrag diente weder ihrer gewerblichen noch beruflichen Tätigkeit. Die Klagepartei hat ihren Wohnsitz zudem im Gerichtsbezirk des Landgerichts Duisburg, § 13 ZPO. 51

Darüber hinaus findet Art. 18 Abs. 1 EuGVVO auch Anwendung auf deliktische Ansprüche nach §§ 823 ff. BGB. Nach der Rechtsprechung des EuGH ist für die Einbeziehung deliktischer Ansprüche in das Verbraucherschutzregime der Art. 17 ff. erforderlich, dass die deliktische Klage „*untrennbar mit einem zwischen dem Verbraucher und dem Gewerbetreibenden tatsächlich geschlossenen Vertrag verbunden ist*“ (*Stadler* in: Musielak/Voit, 19. Aufl. 2022, EuGVVO Art. 17 Rn. 1e). Die durch die Klagepartei geltend gemachten Verletzungen beziehen sich allesamt auf solche, die im Zusammenhang mit dem vorliegend geschlossenen Nutzungsvertrag stehen. 52

2. 53

Die sachliche Zuständigkeit des Landgerichts Duisburg folgt aus § 39 Satz 1 ZPO. Das Landgericht Duisburg ist vorliegend mangels Erreichung des erforderlichen Zuständigkeitsstreitwerts im Sinne des § 1 ZPO i. V. m. §§ 23 Nr. 1, 71 Abs. 1 ZPO zwar grundsätzlich sachlich unzuständig, allerdings hat sich die Beklagte rügelos zur Sache eingelassen, § 39 Satz 1 ZPO. 54

II. 55

Die Klageanträge zu 1) und zu 3) sind auch hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO. 56

1. 57

Der Zulässigkeit des Klageantrags zu 1) steht weder entgegen, dass der Schadensersatzanspruch nicht hinreichend beziffert worden sei, noch die von der Beklagten eingewandte Alternativität der zugrunde gelegten Lebenssachverhalte. 58

Die Bezifferung eines Geldzahlungsantrages kann dann unterbleiben, wenn statt der Bezifferung jedenfalls die Größenordnung des Betrags angegeben wird oder sich aus dem übrigen Klagevortrag ergibt. Das Gericht muss in die Lage versetzt werden, auf der Grundlage des klägerischen Vortrags eine Entscheidung über die Anspruchshöhe im Sinne des § 287 ZPO treffen zu können. Die Klagepartei hat in ihrem Antrag einen Mindestbetrag in Höhe von 1.000,00 € aufgenommen und der Entscheidung des Gerichts zulässigerweise 59

Entgegen des Beklagtenvortrags liegt der Streitsache auch ein einheitlich zu bewertender Lebenssachverhalt zugrunde; eine unzulässige Alternativität ist nicht festzustellen. Die Klagepartei stützt ihr Klagevorbringen zwar auf – von ihr behauptete – unterschiedliche Datenschutzverletzungen, diese sind aber innerhalb eines Lebenssachverhaltes danach zu bewerten, ob die von der Klagepartei angegebenen Daten vor dem „*Scraping-Vorfall*“ hinreichend geschützt und die Nutzer zuvor hinreichend informiert wurden. Eine Aufspaltung des Antrags nach einzelnen Datenschutzverstößen würde den Streitgegenstand hingegen unnatürlich aufspalten. 60

2. 61

Der Bestimmtheit des Klageantrags zu 3) steht nicht entgegen, dass die Klagepartei hierin Bezug auf die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen nimmt. Auch wenn es sich hierbei um einen auslegungsbedürftigen Begriff handelt und daraus resultierende Vollstreckungsprobleme denkbar sind, so ist dies zur Gewährleistung eines effektiven Rechtsschutzes hinzunehmen (LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 mit Verweis auf BGH, Urteil vom 04.03.2004 – I ZR 221/01, NJW 2004, 2080). 62

Dies muss nicht zuletzt deshalb gelten, weil sich aus der DSGVO schon kein Anspruch auf bestimmte konkrete Sicherungsmaßnahmen ableiten lässt und dem Störer insoweit ein Wahlrecht zukommt, Art. 32 DSGVO. 63

III. 64

Die Klagepartei hat im Hinblick auf den Klageantrag zu 2) auch ein hinreichendes Feststellungsinteresse, § 256 Abs. 1 ZPO. 65

Das Feststellungsinteresse wäre nur dann zu verneinen, wenn aus der Sicht der Klagepartei bei verständiger Würdigung kein Grund bestehen würde, mit dem Eintritt eines Schadens wenigstens zu rechnen (LG Essen, *aaO* mit Verweis auf BGH, Beschluss vom 09.01.2007 – VI ZR 133/06, juris). Nach dem vorliegenden Klagevortrag im Hinblick auf eine mögliche Verwendung der unstreitig abgeschöpften Daten durch Dritte, die der Öffentlichkeit zur Verfügung stehen, ist bei lebensnaher Betrachtung nicht völlig ausgeschlossen, dass solche durch Dritte schädigend verwendet werden und der Klagepartei hieraus ein künftiger Schaden entstehen könnte (vgl. LG München I, Urteil vom 09.12.2021 – 31 O 16606/20, GRUR-RS 2021, 41707). 66

B. 67

Die Klage ist unbegründet. 68

I. 69

Die klägerische Partei hat unter keinem rechtlichen Gesichtspunkt einen Anspruch auf Ersatz eines immateriellen Schadens gegen die Beklagte. Der Anspruch ergibt sich weder aus Art. 82 Abs. 1 DSGVO noch aus einer vertraglichen oder deliktischen Haftung der Beklagten nach Normen des BGB. 70

1. 71

Die Voraussetzungen des Art. 82 Abs. 1 DSGVO sind nicht erfüllt. 72

Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. 73

a. 74

Ein nach Art. 82 Abs. 1 DSGVO erforderlicher Verstoß gegen die DSGVO ist nicht festzustellen. Teilweise dürfte der Anwendungsbereich des Art. 82 DSGVO für die durch die Klagepartei geltend gemachten Verstöße bereits nicht eröffnet sein (aa.), jedenfalls aber ist der Beklagten kein Verstoß gegen die DSGVO zur Last zu legen (bb.). 75

Insoweit ist umstritten, wer die Darlegungs- und Beweislast für das Vorliegen der Pflichtverletzung trägt. Aus Sicht der Kammer sprechen gute Gründe dafür, die Darlegungs- und Beweislast nach allgemeinen schadensrechtlichen Grundsätzen dem Anspruchsteller aufzuerlegen (so auch LG Essen, *aaO*; OLG Stuttgart, Urteil vom 31.03.2021 – 9 U 34/21, BeckRS 2021, 6282; LG München I, Urteil vom 09.12.2021 – 31 O 16606/20, GRUR-RS 2021, 41707; OLG Brandenburg, Beschluss vom 11.08.2021 – 1 U 69/20, ZD 2021, 693). 76

Die in Art. 82 Abs. 3 DSGVO geregelte Beweislastverteilung – Beweislast des Verantwortlichen – bezieht sich seinem Wortlaut nach einzig auf das Verschulden des Verantwortlichen gegenüber den Behörden und nicht auf den zugrundeliegenden DSGVO-Verstoß. Auch aus der in Art. 5 Abs. 2 DSGVO statuierten Rechenschaftspflicht des Verantwortlichen kann nicht auf eine diesbezügliche Beweislastumkehr geschlossen werden. Andernfalls würde hierdurch auf einem Umweg der Verantwortliche gegenüber jedem Betroffenen rechenschaftspflichtig, wobei die DSGVO dem Betroffenen aber gerade nur eingeschränkte Rechte zugesteht, wie z. B. das Auskunftsrecht aus Art. 15 DSGVO. Das Prozessrecht bietet darüber hinaus hinreichend Möglichkeiten, einer unter Umständen bestehenden Darlegungs- und Beweisnot des Anspruchstellers – gerade im Hinblick auf Vorgänge, in welche der Betroffene keinen Einblick hat – zu begegnen, wie z. B. die aus der DSGVO folgenden Informationsrechte oder aber die Begründung einer sekundären Darlegungslast der Verantwortlichen (OLG Stuttgart, *aaO*). 77

Im vorliegenden Fall kommt es hierauf aber nicht an, da die Klagepartei dem Vorbringen der Beklagten jedenfalls nicht hinreichend entgegengetreten ist. 78

Im Einzelnen gilt Folgendes: 79

aa. 80

81

Soweit die Klagepartei sich im Rahmen ihres Schadensersatzbegehrens auf Informationspflichtverletzungen (Artt. 13, 14 DSGVO), Meldepflichtverletzungen (Art. 33 DSGVO) und unterlassene Auskünfte (Artt. 15, 34 DSGVO) der Beklagten beruft, sind diese bereits nicht vom Anwendungsbereich der Art. 82 DSGVO umfasst, da es sich hierbei nicht um eine Verarbeitung personenbezogener Daten i. S. d. Art. 4 Nr. 2 DSGVO handelt.

Nach Art. 4 Nr. 2 DSGVO ist unter Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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 zu verstehen. 82

Personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. 83

Der Anwendungsbereich des Art. 82 Abs. 1 DSGVO umfasst allein solche Verstöße gegen die DSGVO, die auf einer Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO beruhen, Art. 82 Abs. 2 Satz 1 DSGVO (so auch LG Essen, *aaO*; LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, juris; AG Straußberg, Urteil vom 13.10.2022 – 25 C 95/21, BeckRS 2022, 27811; LG Düsseldorf, Urteil vom 28.10.2021 – 16 O 128/20, ZD 2022, 48; andere Ansicht OLG Köln, Urteil vom 14.07.2022 – 15 U 137/21, ZD 2022, 617; *Quaas* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.08.2022, DS-VO Art. 82 Rn. 14 *mwN*). 84

Auch wenn der Wortlaut des Art. 82 Abs. 1 DSGVO allein auf einen Verstoß „*gegen diese Verordnung*“ Bezug nimmt, ergibt sich aus Art. 82 Abs. 2 DSGVO eindeutig, dass eine Haftung nur für solche Schäden entstehen soll, die durch eine nicht der DSGVO entsprechenden *Verarbeitung* verursacht wurden. Diese Auslegung steht auch im Einklang mit den Erwägungsgründen 146 und 75 der DSGVO. Der Erwägungsgrund 146 stellt auf eine *Verarbeitung* der personenbezogenen Daten ab. Der Erwägungsgrund 75 beschreibt beispielhaft Risiken, die aus der *Verarbeitung* personenbezogener Daten resultieren und aus denen materielle und immaterielle Schäden entstehen können, welche gerade über Art. 82 Abs. 1 DSGVO Ersatz finden sollen. Die dort benannten Risiken wie z. B. Diskriminierung, „Identitätsdiebstahl“ oder -betrug, finanzieller Verlust, Rufschädigung und der Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten gehen alle mit der *Verarbeitung* personenbezogener Daten einher und können nicht aus einer nicht Art. 4 Nr. 2 DSGVO unterfallenden Informationspflichtverletzung, Meldepflichtverletzung oder einer unterlassenen Auskunft resultieren. 85

Selbst wenn man dies aber anders sehen wollte, bestünden keine Ansprüche der klagenden Partei, da die durch sie geltend gemachten Informations- und Aufklärungspflichtverletzungen jedenfalls auch in der Sache nicht gegeben sind. 86

bb. 87

88

Der Beklagten ist kein Verstoß gegen die DSGVO zur Last zu legen.

(1) 89

Die bei der Beklagten stattfindende Verarbeitung der personenbezogenen Daten der Klagepartei erfolgte aufgrund einer wirksamen Einwilligung der Klagepartei gemäß Artt. 6 Abs. 1 UAbs. 1 lit. a), 7, 5 Abs. 1 lit. a) Var. 1 DSGVO. 90

Die Beklagte hat die durch die Klagepartei angegebenen Daten, die sich auf die Klagepartei als identifizierbare Person beziehen lassen und damit personenbezogene Daten darstellen, im Rahmen ihrer Dienste auf der Plattform verarbeitet, indem sie diese erfasste, organisierte und speicherte, Artt. 4 Nrn. 1 und 2 DSGVO. 91

Hierzu hat die Klagepartei auch eine wirksame Einwilligung erteilt. 92

Die Einwilligung ist eine privatautonome Entscheidung des Betroffenen, mittels derer dieser sein Einverständnis zu einer bestimmten Verarbeitung von auf ihn verweisenden Informationen und Daten durch den Datenverarbeiter erklärt (*Albers/Veit* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.08.2022, DS-VO Art. 6 Rn. 29). Die Willensbekundung muss dabei freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich sowie durch Erklärung oder sonstige bestätigende Handlung erfolgen, Art. 4 Nr. 11 DSGVO. Dabei ist das Erfordernis der hinreichenden Information die Ausprägung des in Art. 5 Abs. 1 lit. a) Var. 3 DSGVO niedergelegten Transparenzgrundsatzes, der seine Ausgestaltung in Artt. 12 ff. DSGVO findet (*Albers/Veit* in: Wolff/Brink, BeckOK Datenschutzrecht, 42. Ed. Stand: 01.08.2022, DS-VO Art. 6 Rn. 36). 93

Aus Art. 5 Abs. 1 lit. a) Var. 3 DSGVO folgt das Erfordernis einer umfassenden Information der betroffenen Person über die Verarbeitung der auf sie bezogenen Daten; die betroffene Person muss hinreichend informiert sein, um als autonomes Individuum auf die Verarbeitung reagieren zu können und ihre Betroffenenrechte wahrnehmen zu können (*Herbst* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 18). Die Aufklärung muss dabei insbesondere auch im Hinblick auf die Zwecke der Verarbeitung erfolgen; für den Nutzer muss klar verständlich und nachvollziehbar sein, zu welchen Zwecken seine personenbezogenen Daten verwendet werden, vgl. Art. 13 Abs. 1 lit. c) DSGVO. 94

Die Klagepartei hat vorliegend auf der Grundlage hinreichender Informationen in die Verarbeitung ihrer personenbezogenen Daten durch die Beklagte eingewilligt. 95

Die Klagepartei trägt vorliegend selbst unter Beibringung von Screenshots, die unter anderem die Registrierungsmaske der Beklagten zeigen, zu dem auch durch sie durchlaufenden Registrierungsprozess auf der Plattform der Beklagten vor. Danach werden die Neunutzer bei ihrer Registrierung auf die Nutzungsbedingungen, die Verwendung von Cookies und die Datenschutzrichtlinien verwiesen, welche jeweils durch eine weitere Verlinkung für den Nutzer zugänglich sind. Die Zustimmung zu diesen Bedingungen und Richtlinien ist zwingende Registrierungsvoraussetzung. Auch die Klagepartei selbst hat in diese Bestimmungen durch ihre Registrierung eingewilligt. Die durch die Beklagte bereitgestellten Informationen betreffen dabei insbesondere auch die durch die Beklagte vorgehaltenen Einschränkungsfunktionen betreffend die Zielgruppenauswahl und Suchbarkeits-Einstellungen. 96

Der Wirksamkeit der Einwilligung steht insbesondere nicht entgegen, dass es sich um eine Vielzahl von Informationen handeln mag, die nur über unterschiedliche Verlinkungen 97

erreichbar sind. Hieraus kann nicht auf eine unzureichende Information der Klagepartei geschlossen werden.

Der Umfang der Informationen muss in Relation zu der stattfindenden Verarbeitung stehen. Je umfangreicher die Verarbeitung der Daten ist, desto umfangreicher und komplexer müssen auch die die Verarbeitung betreffenden Informationen sein, da mit diesen dann auch umfangreichere Eingriffe bzw. Risiken verbunden sind, über welche die Nutzer nach der DSGVO gerade zu informieren sind. Äußere Grenze ist dabei die hierüber hinausgehende Überladung der bereitgestellten Informationen, aus der dann eine Intransparenz folgen kann, vgl. Art. 5 Abs. 1 lit. c) DSGVO. 98

Eine solche Überladung mit Informationen ist nach dem unstreitigen Parteivorbringen und den beigebrachten Screenshots von der Plattform der Beklagten nicht festzustellen. 99

Im vorliegenden Fall ist Grundlage der von der Beklagten betriebenen und durch die Klagepartei freiwillig genutzten Social-Media-Plattform der Austausch personenbezogener Daten im Internet. Dies hat zwangsläufig umfangreiche und komplexe Verarbeitungsvorgänge zur Folge. 100

Die Beklagte darf und muss in diesem Kontext von einem durchschnittlichen Internet- und Plattformnutzer erwarten können, dass sich dieser bei seiner Registrierung auf der Plattform der Beklagten im hinreichenden Maße über die für ihn maßgeblichen und in seinem Interesse liegenden datenschutzrechtlichen Aspekte informiert und hierzu auch durchaus umfangreichere Informationen durchdringt. Die bestehende Mehrschichtigkeit der Informationen spricht dabei nicht für das Fehlen der erforderlichen Transparenz (vgl. LG Essen, *aaO*). 101

Die durch die Beklagte – auch nach dem Vortrag der Klägerseite – bereitgestellten Informationen enthalten alle relevanten Informationen zu Art und Umfang der Verarbeitung sowie Hinweise und Hilfestellungen, um eine Begrenzung der Öffentlichkeit der Daten zu ermöglichen. Dass hierin erforderliche Informationen fehlten oder falsche Informationen enthalten waren, hat die Klagepartei nicht vorgetragen. 102

Auch der klägerischen Auffassung, die Vielzahl der Einstellungsmöglichkeiten führe dazu, dass ein Nutzer es im Zweifel bei den Voreinstellungen belasse, kann nicht gefolgt werden. Die internetspezifischen Gepflogenheiten und gerade die DSGVO verlangen vielfältige Einstellungsmöglichkeiten, damit der jeweilige Nutzer die Einstellungen entsprechend seiner spezifischen Bedürfnisse individuell vornehmen kann (LG Essen, *aaO*). Im Umkehrschluss kann hieraus keine Verletzung des Transparenzgrundsatzes folgen. 103

Die Kammer schließt sich zudem der Auffassung des LG Essen an, wonach in die Beurteilung einfließen muss, dass es sich um eine freiwillige Nutzung einer Social-Media-Plattform handelt, in deren Rahmen die Preisgabe der personenbezogenen Daten – unter anderem der nach der Klägerseite besonders schutzbedürftigen Telefonnummer – allein in der Entscheidungsgewalt des Nutzers liegt (LG Essen, *aaO*). Der Nutzer entscheidet selbst, welche Sichtbarkeitseinstellungen er wählt und inwiefern er seine eigene Privatsphäre dadurch gegenüber der Öffentlichkeit schützt. 104

Als autonomem Individuum muss einem Nutzer nach hinreichender Information abverlangt werden können, sich gezielt unter Zuhilfenahme der dargebotenen Informationen über die mit der Verwendung seiner personenbezogenen Daten einhergehende Verarbeitung zu informieren, sich hierfür auch in umfangreiche Informationen einzulesen und auf dieser 105

Grundlage eine eigenverantwortliche Entscheidung zu treffen.

Auch hat die Klagepartei insbesondere in die Verarbeitung ihrer Telefonnummer durch die Beklagte eingewilligt. Der anfänglichen Behauptung der Klagepartei, dass diese ihre Telefonnummer nur zur Verwendung der *Zwei-Faktor-Authentifizierung* angegeben habe, ist die Beklagte unter Vorlage der Einstellungs-Dokumentation des klägerischen Nutzerskontos entgegengetreten, Anlage B 17, Bl. 286 d. A. Daraus ergibt sich, dass die Suchbarkeits-Einstellungen im Hinblick auf die Telefonnummer der Klagepartei auf „*Alle*“ eingestellt waren und die Auffindbarkeit über das CIT aktiviert war. Unabhängig davon, ob nach der hier vertretenen Auffassung die Darlegungs- und Beweislast für eine Pflichtverletzung durch die Beklagte bei der Klägerseite liegt (s. zuvor), oder diese im Wege der Beweislastumkehr auf die Beklagte übergegangen ist, ist die Klagepartei diesem Vortrag der Beklagten jedenfalls nicht hinreichend substantiiert entgegengetreten, was eine Beweisaufnahme insoweit jedenfalls entbehrlich macht, § 138 Abs. 2 ZPO. 106

(2) 107

Die Verarbeitung der personenbezogenen Daten erfolgte entsprechend Art. 5 Abs. 1 lit. a) Var. 3 DSGVO auch in einer für die Klagepartei nachvollziehbaren Weise (Transparenzgrundsatz). Unabhängig davon, dass mögliche mit Art. 5 Abs. 1 lit. a) DSGVO einhergehende Informationspflichtverletzungen über Art. 82 DSGVO nicht ersatzfähig sind (s. zuvor), ist der Beklagten ein solcher Verstoß aber auch nicht anzulasten. Es wird insoweit auf die Ausführungen unter (1) verwiesen. 108

(3) 109

Es bestehen zudem keine Anhaltspunkte dafür, dass die Beklagte vorliegend gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c) DSGVO verstoßen hat. Auch insoweit wird auf die vorigen Ausführungen unter (1) verwiesen. 110

(4) 111

Des Weiteren liegt auch kein Verstoß der Beklagten gegen Artt. 5 Abs. 1 lit. f), 32 DSGVO vor. 112

Nach Art. 5 Abs. 1 lit. f) DSGVO müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung. Eine unbefugte Verarbeitung ist insbesondere in der Verarbeitung von Daten durch unbefugte Dritte zu sehen (*Herbst* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 5 Rn. 74). 113

Die vorgeschriebenen Schutzmaßnahmen finden ihre Konkretisierung in Art. 32 DSGVO. Danach sind durch den Verantwortlichen oder den Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, Art. 32 Abs. 1 DSGVO. Bei der Beurteilung des angemessenen Schutzniveaus sind die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von 114

beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden, Art. 32 Abs. 2 DSGVO.

(a) 115

Die Beklagte war entgegen der klägerischen Auffassung nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Nutzerkontos der Klagepartei aufgrund der selbst gewählten Einstellung zu verhindern. 116

Auch wenn die immer öffentlich zugänglichen Daten der Klagepartei durch Dritte unstreitig abgeschöpft und damit verarbeitet wurden, war die Beklagte insoweit nicht verpflichtet, diese Daten vor der Verarbeitung durch die „*Scraper*“ zu schützen, da die Daten nicht unbefugt bzw. unrechtmäßig verarbeitet worden sind. 117

Es handelt sich bei den unstreitig „*gescrapeden*“ Daten um solche, die für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen wie Logins oder Ähnliches abrufbar sind, worüber die Klagepartei bereits bei der Registrierung informiert wurde. Die Klagepartei hat über ihre Daten – nach hinreichender Information – frei verfügt. Die Erhebung dieser Daten – zumal durch Dritte und nicht durch die Beklagte – erfolgte daher nicht unbefugt bzw. unrechtmäßig. Die Zugänglichkeit gegenüber „*Allen*“ betrifft insoweit auch die Zugänglichkeit gegenüber potentiellen „*Scrapern*“ (vgl. LG Essen, *aaO*; AG Strausberg, *aaO*). 118

Auch das Vorbringen der Klagepartei, ihr sei zum Zeitpunkt der Registrierung die auf „*Alle*“ gerichtete Standardeinstellungen nicht bekannt gewesen, rechtfertigt nicht die Annahme, die Beklagte habe gegen ihr obliegende Schutzpflichten verstoßen. Denn die Beklagte durfte und musste aufgrund der internetspezifischen Gepflogenheiten und der von ihr erteilten Hinweise und Hilfestellungen davon ausgehen, dass der Klagepartei bekannt ist, dass diese Daten für jedermann abrufbar sind. Die Beklagte hatte daher keine Veranlassung, diese Daten vor der Erhebung durch Dritte zu schützen (LG Essen, *aaO*). 119

(b) 120

Dazu, dass nicht öffentlich zugängliche Informationen von Dritten abgeschöpft worden seien, trägt die Klagepartei bereits nicht schlüssig vor. So ist schon nicht ersichtlich, welche Daten unter den Begriff „*sonstige korrelierende Daten*“ zu fassen sein sollen. 121

(c) 122

Der unter Verwendung des CIT durch die Dritten erfolgte Abgleich der von ihnen hochgeladenen Telefonnummern mit den auf den Nutzerkonten hinterlegten Telefonnummern stellt zwar eine Verarbeitung personenbezogener Daten dar. Jedoch war die Beklagte auch insoweit nicht verpflichtet, das Nutzerkonto der Klagepartei vor dessen Auffinden über die Telefonnummer über die bereits implementierten Schutzmaßnahmen hinaus zu schützen, da der von den „*Scrapern*“ hergestellte Abgleich als solcher nicht unbefugt bzw. unrechtmäßig war. 123

Die Klagepartei hat auf der Grundlage hinreichender Informationen selbst die Entscheidung getroffen, ihre Telefonnummer auf der Plattform der Beklagten anzugeben und die Suchbarkeits-Einstellungen auf „*Alle*“ belassen. Der von den Dritten veranlasste Abgleich war folglich jeder Person, die über die Telefonnummer der Klagepartei verfügte oder sie technisch 124

erzeugte, möglich und war damit nicht unbefugt bzw. unrechtmäßig im Sinne der DSGVO (vgl. LG Essen, *aaO*).

Soweit die Klagepartei vorträgt, dass ihr nicht bekannt gewesen sei, dass alle Personen über ihre Telefonnummer ihr Nutzerkonto finden konnten, hat dies nicht zur Folge, dass die Beklagte verpflichtet war, weitere Schutzmaßnahmen zu ergreifen. Denn die Beklagte musste angesichts der Zustimmung der Klagepartei zu den Datenverwendungsrichtlinien annehmen, dass der Klagepartei die Auffindbarkeit und Suchbarkeits-Einstellungen bekannt waren. Der Klagepartei war es möglich, selbst über ihre Auffindbarkeit zu verfügen und ihre Privatsphäre hierüber zu schützen. Davon hat die Klagepartei aber unstreitig keinen Gebrauch gemacht. Auch wenn der Vorstellung der Klagepartei dabei nicht zugrunde gelegen habe mag, dass Dritte, die die Telefonnummer der Klagepartei unter Zuhilfenahme von digitalen Programmen künstlich erzeugen, auch unter „*Alle*“ im Sinne der Suchbarkeits-Einstellungen zu fassen sind, so folgt die Auffindbarkeit dennoch aus der Entscheidung der Klagepartei, die Suchbarkeits-Einstellungen bei der Standardeinstellung zu belassen (vgl. LG Essen, *aaO*). 125

Die 6. Zivilkammer des LG Essen führt insoweit zutreffend aus: 126

„*Es widerspricht dem Zweck von F., einerseits eine Social Media Plattform zur leichten Kontaktaufnahme und Kommunikation einzurichten, die der jeweilige User durch Hinweis und Zustimmung auf die Datenrichtlinien freiwillig nutzen kann und selbst nach Aufklärung bestimmen kann, ob und in welchem Umfang er Daten dort hinterlegt, um andererseits der Beklagten solche technischen Hürden abzuverlangen, die dem o.g. Nutzungszweck diametral entgegenstehen. Ein gewisses Risiko, dass über technische Programme selbst gewählte Freigaben ausgenutzt und missbraucht werden, verbleibt bei der Internetnutzung stets, ist aber nicht von der Beklagten, sondern vom Kläger zu tragen, der sich eigenverantwortlich zur Nutzung entschlossen hat und nach Zustimmung zur Datenschutzrichtlinie und nach Bereitstellung von Hilfestellungsmöglichkeiten selbst entscheiden konnte, wie weit er die Angebote nutz*t“ (LG Essen, *aaO*). 127

Die Kammer schließt sich diesen Ausführungen im vollen Umfang an. 128

Darüber hinaus folgt aus Art. 32 DSGVO einzig die Pflicht, unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu erreichen, woraus eindeutig kein Anspruch auf die Vornahme spezieller Sicherungsmaßnahmen resultiert, zu welchen die Klagepartei ohnehin nicht hinreichend vorgetragen hat. 129

Das Gericht vermag sich allein aufgrund der klägerseits geäußerten Vermutungen nicht die Überzeugung zu bilden, dass die Beklagte nicht alle im konkreten Fall erforderlichen Sicherheitsvorkehrungen – die nie jede Art von Hackerangriff sicher ausschließen können und nach der gesetzlichen Regelung auch nicht müssen – einhielt. Auch lässt allein der Umstand eines erfolgreichen Hackerangriffs keinen begründeten Schluss darauf zu, dass es an Sicherheitsvorkehrungen gemangelt hat (OLG Stuttgart, *aaO*). 130

Die Beklagte hat Maßnahmen vorgehalten, die ein ausreichendes Schutzniveau erreicht haben. Jedenfalls hat die Klagepartei nicht hinreichend schlüssig dargelegt, dass die Beklagte ihren Verpflichtungen insoweit nicht hinreichend nachgekommen sei. Selbst wenn der Beklagten hierfür die Darlegungs- und Beweislast aufzuerlegen wäre (dagegen s. zuvor), 131

so hat die Beklagte zu den durch sie implementierten Sicherungsmaßnahmen, wie der Aufstellung eines EDM-Team, der Verwendung von Datenübertragungsbeschränkungen, Bot-Erkennungen und der Verwendung von Captcha-Anfragen umfassend und substantiiert in ihrer Klageerwiderung vorgetragen, woraufhin eine einfaches Bestreiten der Klagepartei jedenfalls nicht mehr hinreichend war, § 138 Abs. 2 ZPO. Einer Beweisaufnahme bedurfte es insofern nicht. Hinzukommend ist zwischen den Parteien unstreitig geblieben, dass sich Scraping-Vorfälle im Internet nicht vollständig vermeiden lassen.

(d) 132

Soweit die Klagepartei auf die Entscheidung der irischen Datenschutzbehörde Y. verweist, ist das Gericht an eine solche Entscheidung bereits nicht gebunden und teilt darüber hinaus auch die von der irischen Datenschutzbehörde vertretene Auffassung im Hinblick auf eine Verpflichtung der Beklagten zum Ergreifen weiterer Maßnahmen nicht. Es wird insoweit auf die obigen Ausführungen verwiesen. 133

(5) 134

Das Gericht vermag auch keinen Verstoß der Beklagten gegen die aus Artt. 25 Abs. 2, 24 DSGVO folgende Pflicht zur Einrichtung von datenschutzfreundlichen Voreinstellungen festzustellen. Die von der Beklagten getroffenen Voreinstellungen sind vor dem Hintergrund der Zweckbestimmung der durch die Beklagte betriebenen Social-Media-Plattform nicht zu beanstanden. 135

Nach Art. 25 Abs. 2 DSGVO soll im Grundsatz ein Produkt oder Dienst für den Nutzer bereits ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen; der Verantwortliche ist verpflichtet, geeignete technisch-organisatorische Maßnahmen zu treffen (*Hartung* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 24 f.). Nach Art. 25 Abs. 2 Satz 3 DSGVO sollen personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen einer Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden, was gerade für soziale Netzwerke gilt. Dies muss allerdings dort seine Grenze haben, wo ein Dienst die öffentlich zugängliche Verbreitung – z. B. Blogs, Kommentarfunktionen – gerade beabsichtigt und dies auch hinreichend transparent ist (*Hartung* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 25 Rn. 26; *Baumgartner* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2 Aufl. 2018, DS-GVO Art. 25 Rn. 20). 136

Auf der Plattform der Beklagten sind allein die zur Registrierung zwingend erforderlichen immer öffentlichen Daten – Name, Nutzername, Geschlecht und Nutzer-ID – von Beginn an für jedermann einsehbar, wobei dem Nutzer auch insoweit die Entscheidung obliegt, ob er seinen tatsächlichen Namen oder einen davon unterschiedlichen Nicknamen oder Ähnliches verwendet. Alle darüber hinausgehenden Informationen sind optional durch den jeweiligen Nutzer anzugeben und zu veröffentlichen. Die nicht abdingbare Öffentlichkeit der immer öffentlichen Daten ist Grundvoraussetzung für die von der Beklagten betriebene Plattform, die gerade der Vernetzung der einzelnen Nutzer dient. Die Vernetzung mit einem Nutzer, dessen Profil ohne jede öffentliche Angabe geführt wird und somit “heimlich“ auf der Plattform der Beklagten registriert wäre, wäre unter diesen Voraussetzungen nicht möglich und würde dem grundliegenden Zweck einer Social-Media-Plattform zuwiderlaufen. Zudem handelt es sich bei den immer öffentlichen Daten – auch unter dem Gesichtspunkt der freien Wählbarkeit des eigenen Namens – auch nicht um besonders sensible Daten, für die ein darüber hinausgehender Schutz erforderlich wäre. 137

138

Soweit der Nutzer sich unter Zustimmung zu den Datenschutzrichtlinien dazu entscheidet, seine Telefonnummer anzugeben, um so über das CIT durch andere Nutzer gefunden werden zu können, sieht die Standardeinstellung zwar die Voreinstellung „*Alle*“ vor, was gegen die Datenschutzfreundlichkeit sprechen könnte, allerdings ist hier zu beachten, dass die Telefonnummer unter den hierzu erfolgten Informationen gerade dazu verwendet wird, dass der jeweilige Nutzer von noch nicht in seiner Kontaktliste befindlichen Kontakten gefunden werden soll. Jedenfalls eine Einstellung auf „*Nur ich*“ oder „*Freunde*“ (als Personen, die sich bereits in der Kontaktliste des Nutzers befinden), würden den Sinn und Zweck der Auffindbarkeitsfunktion damit konterkarieren. Die Funktion des CIT setzt die Zugänglichkeit für die Öffentlichkeit daher gerade voraus, um so neue Vernetzungen zu generieren.

Die 6. Zivilkammer des Landgerichts Essen führt auch insoweit zutreffend aus: 139

„*Zudem muss sich jeder Internetnutzer, der insbesondere eine Plattform eines sozialen Netzwerkes wie das der Beklagten nutzt, bewusst sein, dass es Internetgepflogenheiten gibt, mit denen man sich vertraut zu machen hat, will man solche Kommunikationsplattformen gebrauchen. Der Schutz des Art. 25 DSGVO reicht nicht so weit, dass er den jeweiligen Nutzer vor den internetspezifischen Gepflogenheiten vollends schützt; vielmehr muss der jeweilige Nutzer, der einer Plattform eines sozialen Netzwerks beitreten will, mit den geltenden Gepflogenheiten vertraut sein. Bei einer Plattform, die auf Kontaktsuche und das Finden von Kontakten ausgerichtet ist und auf der die Beklagte angibt, dass das nicht zwingend erforderliche Hinterlegen der Telefonnummer es ermöglicht, leichter gefunden zu werden und die Zwecke der Plattform besser zu nutzen, muss der jeweilige Nutzer eigenverantwortlich entscheiden, in welchem Umfang er diese Möglichkeiten nutzt und entsprechende Daten freigibt*“ (LG Essen, *aaO*). 140

Auch diesen Ausführungen schließt sich die Kammer vollumfänglich an. 141

Die von der Beklagten getroffenen technisches-organisatorischen Maßnahmen sind insoweit nicht zu beanstanden. Wie bereits dargelegt, ist die Klägerseite dem Vortrag der Beklagten zu den durch diese vorgehaltenen Schutzmaßnahmen jedenfalls nicht hinreichend substantiiert entgegengetreten. 142

Auch insoweit führen die Ausführungen der irischen Datenschutzbehörde im Hinblick auf eine Verletzung des Art. 25 Abs. 2 DSGVO nicht zu einer anderen Bewertung der Rechtslage. 143

(6) 144

Es liegt auch kein Verstoß gegen Art. 35 DSGVO vor. Nach Art. 35 DSGVO ist für den Fall, dass eine Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine Folgenabschätzung durchzuführen. Es ist insoweit bereits nicht ersichtlich, dass eine solche durch die Beklagte nicht erfolgt sein soll. Die Beklagte hat auch hierzu im Rahmen der ergriffenen Maßnahmen umfassend vorgetragen, ohne dass die Klägerseite dem hinreichend substantiiert entgegengetreten ist, § 138 Abs. 2 ZPO. 145

(7) 146

Unabhängig davon, dass ein Verstoß gegen Art. 15 DSGVO nach hiesiger Auffassung bereits nicht dem Anwendungsbereich des Art. 82 DSGVO unterfällt (s. zuvor), hat die Beklagte auch nicht gegen ihre Auskunftspflicht aus Art. 15 DSGVO verstoßen. 147

148

Nach Art. 15 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat die Person unter anderem ein Recht auf Auskunft über diese Daten, die Verarbeitungszwecke, die Kategorien der verarbeiteten Daten und den Empfänger, gegenüber welchem die Daten offengelegt worden sind oder noch offengelegt werden.

Das Informationsbegehren der Klägerseite wurde durch das Antwortschreiben der Beklagten erfüllt, § 362 Abs. 1 BGB. Die Beklagte hat die Klägerseite über die ihr zur Verfügung stehenden Informationen aufgeklärt, wobei der Beklagten gerade nicht angelastet werden kann, dass sie keine Auskunft über die Personen der „*Scraper*“ geben kann. Die Klägerseite verkennt insoweit, dass das über das Antwortschreiben der Beklagten hinausgehenden Informationsbegehren im Hinblick auf die Empfänger der verarbeiteten Daten nicht dem Anwendungsbereich der Norm unterfällt. Es ist zwischen den Parteien unstreitig, dass keine *Offenlegung* der Daten durch die Beklagte gegenüber den Dritten im Rahmen des *Scraping-Vorfalls* erfolgt ist, sondern diese eigenmächtig handelten. 149

(8) 150

Unabhängig davon, dass ein Verstoß gegen die Meldepflicht nach Art. 33 DSGVO und die Auskunftspflicht nach Art. 34 DSGVO bereits nicht dem Anwendungsbereich des Art. 82 DSGVO unterfällt (s. zuvor), war die Beklagte auch nicht verpflichtet, sich an die zuständigen Behörden oder die Klagepartei zu wenden. 151

Nach Art. 33 Abs. 1 DSGVO hat der Verantwortliche einen Datenschutzverstoß unverzüglich und möglichst binnen 72 Stunden nachdem ihm die Verletzung bekannt wurde, an die zuständige Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der natürlichen Person führt. Nach Art. 34 Abs. 1 DSGVO ist der Betroffene durch die Verantwortliche zudem über Verletzung personenbezogener Daten zu benachrichtigen, wenn die Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Diese Voraussetzungen sind nicht erfüllt. Wie bereits dargelegt ist der Beklagten kein Datenschutzverstoß zur Last zur legen. 152

b. 153

Darüber hinaus fehlt es an einem ersatzfähigen immateriellen Schaden der Klagepartei. 154

Nach Auffassung der Kammer setzt ein Anspruch auf Schadensersatz nach Art. 82 DSGVO neben der Verletzung einer Vorschrift der DSGVO auch einen hierauf beruhenden Schaden voraus, der durch den Anspruchsteller darzulegen und notfalls zu beweisen ist (so auch OLG Frankfurt a. M., Urteil vom 02.03.2022 – 13 U 206/20, GRUR-RS 2022, 4491; LG Essen, *aaO* ; AG Strausberg, *aaO*; LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, juris; LG München, Urteil vom 09.12.2021 – 31 O 16606/20, GRUR-RS 2021, 41707; LG Düsseldorf, Urteil vom 28.10.2021 – 16 O 128/20, ZD 2022, 48; LG Karlsruhe, Urteil vom 09.02.2021 – 4 O 67/20, ZD 2022, 55; LG Hamburg, Urteil vom 05.09.2020 – 324 S 9/19, ZD 2021, 9; andere Ansicht BAG, Beschluss vom 26.08.2021 – 8 AZR 253/20, NZA 2021, 1713). 155

Aus dem Wortlaut des Art. 82 Abs. 1 DSGVO geht hervor, dass der betroffenen Person ein materieller oder immaterieller Schaden *entstanden* sein muss. Auch der Erwägungsgrund 146 der DSGVO sieht insoweit vor, dass solche Schäden ersetzt werden sollen, die einer Person aufgrund einer Verarbeitung *entstehen*. Des Weiteren ergibt sich aus den im 156

Erwägungsgrund 75 der DSGVO aufgezählten möglichen immateriellen Schäden, dass der Verordnungsgeber den Datenschutzverstößen unterschiedliche Schadensfolgen zuschreibt, was denknotwendig ebenfalls gegen die Gleichsetzung eines Datenschutzverstoßes mit einem Schadenseintritt spricht.

Der Begriff des Schadens ist nach dem Erwägungsgrund 146 der DSGVO unter Berücksichtigung der Ziele der DSGVO weit auszulegen. Danach soll der Anspruch einen vollständigen und wirksamen Ersatz des erlittenen Schadens sicherstellen. Schadensersatzforderungen sollen abschrecken und weitere Verstöße der Verantwortlichen unattraktiv machen (*Bergt* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17). Der Schadensbegriff ist autonom auszulegen; es kommt nicht darauf an, ob bestimme Schadenspositionen im nationalen Recht als Schaden anerkannt sind (*Bergt* in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17). Insofern ist auch die bisherige deutsche Rechtsprechung zu immateriellen Schäden nicht anwendbar, wonach nur schwerwiegende Persönlichkeitsverletzungen zu einem ersatzfähigen Schadensersatz führen (LG Karlsruhe, Urteil vom 02.08.2019 – 8 O 26/19, ZD 2019, 511). Der Erwägungsgrund 75 der DSGVO nennt als mögliche immaterielle Schäden eine Diskriminierung, den „*Identitätsdiebstahl*“ oder -betrug, eine Rufschädigung, einen Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten. Als Bewertungskriterien können zudem die in Art. 83 DSGVO genannten Kriterien der Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die betroffenen Kategorien personenbezogener Daten herangezogen werden. 157

Ein genereller Ausschluss von Bagatellschäden ist im Lichte dieser Erwägungsgründe nicht vertretbar. Dies wird auch aus Art. 4 Abs. 3 AEUV abgeleitet, der die Mitgliedsstaaten dazu anhält, Verstöße wirksam mit Sanktionen zu belegen, da nur so eine effektive Durchsetzbarkeit des EU-Rechts und damit auch der DSGVO erzielt werden könne (LG Essen, *aaO*; LG München I, Urteil vom 09.12.2021 – Az.: 31 O 16606/20, GRUR-RS 2021, 41707). 158

Der Schaden ist demnach zwar weit zu verstehen, er muss jedoch auch wirklich *erlitten*, das heißt *spürbar*, objektiv nachvollziehbar und von gewissem Gewicht sein (LG Essen, *aaO*). 159

Diese Auslegung wird bestätigt durch die aktuelle Entscheidung des EuGH vom 04.05.2023, C-30021, wonach Art. 82 Abs. 1 DSGVO dahin auszulegen ist, dass der bloße Verstoß gegen die Bestimmungen dieser Verordnung gerade nicht ausreicht, um einen Schadenersatzanspruch zu begründen. 160

Die Klagepartei hat einen solchen *erlittenen* und *spürbaren* immateriellen Schaden nicht hinreichend dargelegt. 161

Die Klagepartei trägt vor, dass die unstreitig erfolgte Veröffentlichung weitreichende Folgen gehabt habe, so würde die Zuordnung von Telefonnummern zu weiteren Daten wie E-Mail-Adresse oder Anschrift Kriminellen eine weite Bandbreite an Möglichkeiten eröffnen, wie z.B. den „*Identitätsdiebstahl*“, die Übernahme von Accounts und gezielte Phishing-Nachrichten. Die Klagepartei habe daher einen erheblichen Kontrollverlust erlitten und es verbleibe ein Zustand des Unwohlseins und der Sorge über möglichen Missbrauch der abgeschöpften Daten. Diese Darlegungen sind nicht ausreichend. 162

Soweit die Klagepartei auf die mögliche Zuordnung ihrer Telefonnummer zu weiteren Daten wie ihrer E-Mail-Adresse oder der Wohnanschrift verweist, hat die Klagepartei bereits nicht 163

schlüssig dargelegt, dass solche Daten überhaupt abgeschöpft bzw. veröffentlicht wurden. Eine diesbezügliche Gefahr ist demnach nicht festzustellen und kann jedenfalls nicht auf die geltend gemachten Verstöße zurückgeführt werden.

Der darüber hinaus geltend gemachte Kontrollverlust und der vermehrte Anfall von unbekannten Anrufen und Nachrichten stellen ebenfalls keine Umstände dar, aus denen auf einen spürbaren Schaden der Klagepartei geschlossen werden kann. Dabei ist in die Bewertung – entsprechend des Art. 85 DSGVO – einzubeziehen, dass die hier betroffenen Daten nach Art und Umfang solche Daten darstellen, die nicht als besonders sensible Daten zu kategorisieren sind und deren Veröffentlichung kein besonderes Gefahrenpotential für einen möglichen Identitätsmissbrauch oder Ähnliches bärgen (zur Gefährdung eines Identitätsmissbrauch bei der Veröffentlichung von Ausweis- und Kontodaten, LG München I, Urteil vom 09.12.2021 – Az.: 31 O 16606/20, GRUR-RS 2021, 41707). 164

Dass aus dem Bekanntwerden einer Telefonnummer ein Identitätsmissbrauch entstehen kann, ist eher unwahrscheinlich (so auch LG Essen, *aaO*; LG Karlsruhe, Urteil vom 09.02.2021 – Az.: 4 O 67/20, ZD 2022, 55). 165

Der Sinn der DSGVO wird aber nicht gewahrt, wenn man jeglichem „Unwohlsein“ eine Schadensposition einräumt. Vielmehr muss zumindest ein ernsthaftes Risiko bestehen, dass die Daten missbraucht werden (LG Essen, *aaO*). Ein derartiges Risiko ist weder vorgetragen noch sonst ersichtlich. 166

Zudem ist zu beachten, dass gewissenhafte Nutzer digitaler Inhalte und Medien ohnehin gehalten sind, Nachrichten und Anrufe von unbekannten Absendern kritisch zu hinterfragen. Ein daraufhin gerichtetes „*Unwohlsein*“ besteht damit ohnehin nicht. 167

Im Hinblick auf den klägerischen Vortrag zu einer Intensivierung des Schadens infolge einer fehlenden Auskunft bzw. Meldung der Datenschutzverstöße ist nicht ersichtlich, worin hier der immaterielle Schaden begründet sein soll. Die abgeschöpften Daten waren zu diesem Zeitpunkt bereits abgeschöpft; davon, dass durch die Auskunft eine Veröffentlichung hätte verhindert werden können, ist nach allgemeinen Lebensbetrachtung nicht auszugehen. 168

Schließlich kann von einer konkreten Betroffenheit, die einen immateriellen Schadensersatzanspruch begründen würde, auch deshalb nicht ausgegangen werden, weil die Klagepartei gerade keine individuellen Folgen vorträgt. Die angeblichen Beeinträchtigungen finden sich vielmehr als identische Textbausteine in einer Vielzahl der von den Klägervertretern angestrengten – im Wesentlichen wortgleichen – Klagen. 169

c. 170

Schließlich fehlt es vorliegend jedenfalls auch an der erforderlichen Kausalität zwischen den geltend gemachten Datenschutzverstößen und dem angeblichen Schaden. 171

Sowohl der geltend gemachte Kontrollverlust als auch die seit der Abschöpfung – nach den klägerischen Behauptungen – vermehrt erfolgenden unbekannten Anrufe und Nachrichten können auf unterschiedliche Ursachen zurückzuführen sein. Es handelt sich dabei um Phänomene der digitalen Welt, die auf unterschiedlichen Gründen beruhen können und im digitalen Zeitalter vermehrt auftreten, § 291 ZPO. 172

2. 173

174

Der klägerische Anspruch auf immateriellen Schadensersatz ergibt sich auch nicht aus einer vertraglichen oder deliktischen Haftung nach dem BGB.

aa. 175

Ob die nationalen Regelungen über eine vertragliche oder deliktische Schadensersatzverpflichtung neben der DSGVO Anwendung finden, kann vorliegend dahinstehen, da die Voraussetzungen für einen vertraglichen oder deliktischen Schadensersatzanspruch im Sinne des BGB jedenfalls nicht vorliegen. 176

bb. 177

Der Klagepartei steht kein Schadensersatzanspruch nach §§ 280 Abs. 1, 241 Abs. 2 BGB zu. 178

Zwar ist zwischen den Parteien jedenfalls ein Nutzungsvertrag über die durch die Beklagte angebotenen Dienstleistungen geschlossen worden, auf dessen rechtliche Qualifizierung es darüber hinaus aufgrund der Maßgeblichkeit einer Nebenpflichtverletzung nicht ankommt, §§ 133, 157 BGB. 179

Allerdings fehlt es bereits an der nach §§ 280 Abs. 1, 241 Abs. 2 BGB erforderlichen Pflichtverletzung und jedenfalls aber der Darlegung eines spürbaren immateriellen Schadens, § 253 BGB. Weder ist ein Datenschutzverstoß festzustellen, noch hat die Klagepartei eine darüber hinausgehende Pflichtverletzung der Beklagten dargelegt. Auch ein immaterieller Schaden kann nicht festgestellt werden. Es wird insoweit zur Vermeidung von Wiederholungen auf die vorstehenden Ausführungen verwiesen. 180

cc. 181

Auch eine mögliche deliktische Haftung aus §§ 823 Abs. 1, 253 Abs. 2 BGB i. V. m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG (allgemeines Persönlichkeitsrecht) oder aus § 823 Abs. 2 BGB i. V. m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung) oder i. V. m. Artt. 5 Abs. 1 lit. a), 13 DSGVO scheitert jedenfalls daran, dass das Entstehen eines (spürbaren) immateriellen Schadens nicht dargelegt worden ist. Auch insoweit wird auf die vorstehenden Ausführungen verwiesen. 182

II. 183

Der mit dem Klageantrag zu 2) verfolgte Anspruch auf Feststellung der Ersatzpflicht aller künftiger Schäden, die der Klägerseite durch den Zugriff Dritter auf das Datenarchiv der Beklagten „*entstanden sind*“, scheitert daran, dass der klägerische Anspruch schon dem Grunde nach nicht besteht. Es wird auf die diesbezüglichen Ausführungen unter I. verwiesen. 184

III. 185

Auch steht der Klagepartei der gegenüber der Beklagten geltend gemachte Unterlassungsanspruch nicht zu. Ein solcher Anspruch folgt weder aus Art. 17 DSGVO noch aus §§ 1004 analog, 823 Abs. 1 oder Abs. 2 i. V. m. Art. 6 DSGVO. 186

Es fehlt bereits an einer hierfür erforderlichen Beeinträchtigung der Klagepartei durch die durch die Beklagte erfolgte Verarbeitung der klägerischen personenbezogenen Daten (s. hierzu ausführlich zuvor). Im Hinblick auf die Telefonnummer wendet die Klagepartei zudem selbst nicht ein, dass die Beklagte die Nummer freigebe oder anderweitig nutze (vgl. LG Gießen, Urteil vom 03.11.2022 – 5 O 195/22, juris). 187

IV. 188

Der Auskunftsanspruch aus Art. 15 DSGVO ist – wie bereits unter I. dargelegt – durch das Antwortschreiben der Beklagten teilweise im Wege der Erfüllung nach § 362 Abs. 1 BGB erloschen. Das darüber hinaus geltend gemachte Auskunftsbegehren der Klagepartei unterfällt dabei nicht dem Anwendungsbereich des Art. 15 DSGVO. 189

V. 190

Ein Anspruch auf Ersatz der geltend gemachten vorgerichtlichen Rechtsanwaltskosten sowie auf Zahlung von Rechtshängigkeitszinsen besteht mangels Hauptanspruch nicht. 191

VI. 192

Die Kammer ist nicht gehalten, die Sache dem EuGH zur Entscheidung vorzulegen, weil das vorliegende Urteil nicht als Entscheidung eines Gerichts ergeht, dessen Entscheidungen selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden können. 193

Die prozessualen Nebenentscheidungen folgen aus §§ 91 Abs. 1 Satz 1, 708 Nr. 11, 711 Satz 1 ZPO. 194

Der Streitwert wird auf 3.000,00 € festgesetzt (Klageantrag zu 1 = 1.000,00 €; Klageantrag zu 2 = 500,00 €; Klageantrag zu 3 = 1.000,00 €; Klageantrag zu 4 = 500,00 €). 195

196