Landgericht Aachen, 8 O 267/22

Datum:	26.05.2023
Gericht:	Landgericht Aachen
Spruchkörper:	8. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	8 O 267/22
ECLI:	ECLI:DE:LGAC:2023:0526.8O267.22.00

Tenor:

Die Klage wird abgewiesen.

Die Kosten des Rechtsstreits trägt der Kläger.

Das Urteil ist gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

Tatbestand 1

Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (DSGVO). 2

Die Beklagte ist die Betreiberin der Webseite I. und der Dienste auf dieser Seite für Nutzer in der Europäischen Union (nachfolgend: A.). Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Klägerseite nutzt X., insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern. 3

Im Rahmen einer Registrierung bei A. gibt der angehende Nutzer Vornamen und Nachnamen, Geburtsdatum und Geschlecht an. Zusätzlich wird er aufgefordert, Handynummer oder E-Mail-Adresse anzugeben. Auf der Registrierungsseite findet sich außerdem folgender Passus: „Indem du auf „Registrieren“ klickst, stimmst du unseren Nutzungsbedingungen zu. In unserer Datenrichtlinie erfährst du, wie wir deine Daten erfassen, verwenden und teilen“. Sowohl die Nutzungsbedingungen als auch die Datenrichtlinie waren auf der Registrierungsmaske verlinkt und einsehbar, bevor der Registrierungsvorgang abgeschlossen wurde (vgl. zur Registrierungsmaske Bl. 9 d.A). Im Hilfebereich bzw. in der Datenrichtlinie werden die Nutzer von A. darüber informiert, dass bestimmte Informationen - nämlich Name, Geschlecht, Nutzername und Nutzer-ID – immer 4

öffentlich zugänglich sind, also jedermann, damit auch Personen außerhalb von A., diese Informationen sehen kann.

Unmittelbar nach der Registrierung wird der Nutzer auf die Startseite geführt, wo über verschiedene Links individuelle Einstellungen betreffend die Privatsphäre des jeweiligen Nutzerkontos vorgenommen werden können (vgl. Seite 10 ff. der Klageschrift, Bl. 10 ff. d.A.). 5

Hier sind folgende beiden Privatsphäre-Einstellungen relevant: Zum einen die „Zielgruppenauswahl“ und zum anderen die „Suchbarkeitseinstellungen“. 6

Bei der „Zielgruppenauswahl“ legt der Nutzer fest, wer bestimmte Datenelemente im A.-Profil des Nutzers sehen kann. Dies umfasst Informationen wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse. Nicht von der Zielgruppenauswahl umfasst sind die immer öffentlichen Nutzerinformationen (Name, Geschlecht, Nutzername und Nutzer-ID), da diese immer öffentlich einsehbar sind. Trifft der Nutzer keine Zielgruppenauswahl, richtet sich die Zugänglichkeit seiner über die öffentlichen Informationen hinausgehenden Daten nach der Standardeinstellung, wonach nur „Freunde“ des Nutzers die weiteren Informationen einsehen können. 7

Bei den „Suchbarkeitseinstellungen“ wird u.a. festgelegt, wer das Profil eines Nutzers anhand von dessen Telefonnummer finden kann, zum Beispiel, um ihm dann eine Freundschaftsanfrage zu senden. Passt der Nutzer die Suchbarkeits-Einstellungen nicht an, sieht die Standardeinstellung vor, dass alle Personen, die über die Telefonnummer des Nutzers verfügen, das Profil des Nutzers finden können, sofern dieser seine Telefonnummer hinterlegt hat. 8

Die Suchbarkeit der Klagepartei war seit dem 28. Mai 2015 bis mindestens zum Ende des Relevanten Zeitraums auf „Everyone“, d.h. „Alle“, eingestellt, 9

In der Zeit von Januar 2018 bis September 2019 sammelten Dritte – unter Verstoß gegen die Nutzungsbedingungen von A. - unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Daten (sog. Scraping). Hierzu verwendeten diese Dritten Listen mit (zum Teil möglicherweise fiktiven) Telefonnummern und luden diese in den Kontakt-Importer (Contact-Importer-Tool, kurz CIT) der Plattform hoch, um festzustellen, ob die hochgeladenen Telefonnummern mit dem Konto eines Nutzers verbunden waren. Sofern eine der hochgeladenen Telefonnummern mit dem Konto eines Nutzers, der seine Telefonnummer bereitgestellt und entsprechend der Standardeinstellung die Suchbarkeits-Einstellungen auf „alle“ geschaltet hatte, verknüpft war, meldete der Kontakt-Importer die Verknüpfung von Telefonnummer und Konto an die Dritten. Dies funktionierte auch dann, wenn in dem entsprechenden Profil – in der Zielgruppenauswahl - die hinterlegte Telefonnummer nicht öffentlich freigegeben war. Ausreichend war vielmehr, dass bei den Suchbarkeits-Einstellungen die Standardeinstellung vorlag, wonach „alle“ mittels einer Telefonnummer nach dem entsprechenden A.-Profil suchen können. Die Dritten fügten sodann den öffentlich zugänglichen Informationen aus dem betreffenden Profil des Nutzers die mit dem Konto verknüpfte Telefonnummer hinzu, die sie selbst zuvor in den Kontakt-Importer eingegeben hatten. Dabei waren die öffentlich zugänglichen Informationen zum einen alle Daten, die von vorne herein immer öffentlich sind (Name, Geschlecht, Nutzername und Nutzer-ID) und zum anderen alle weitere Daten, die der jeweilige Nutzer in der „Zielgruppenauswahl“ für „alle“ freigegeben hatte. 10

Im Zuge der Aktualisierung der Nutzungsbedingungen und der Datenrichtlinie im April 2018 wies die Beklagte alle Nutzer in der EU auf die aktualisierte Datenrichtlinie hin. Die Nutzer 11

mussten den aktualisierten Nutzungsbedingungen zustimmen, um die A.-Plattform weiter nutzen zu können. Sowohl die Datenrichtlinie als auch die Nutzungsbedingungen vom 19. April 2018 waren in dem Hinweis unmittelbar verlinkt, so dass die Nutzer – inklusive der Klagepartei – direkten Zugriff auf deren Inhalt hatten.

Anfang April 2021 wurden die wie oben beschrieben gescrapten Daten einer Vielzahl von A.-Nutzern sowie die von den Scrapern mit diesen Datensätzen verknüpften Telefonnummern im Internet frei zum Download bereitgestellt. Hierzu gehörte neben den immer öffentlich zugänglichen Informationen des Profils der Klagepartei jedenfalls auch die mit ihrem Konto verknüpfte Telefonnummer, die die Scraper zum Auffinden des Profils verwendet hatten. 12

Nach dem Vorfall informierte die Beklagte die zuständige Datenschutzbehörde „Irish Q. nicht. 13

Mit Schreiben vom 22.10.21 (Anl. K1, Bl. 53ff. d.A.) begehrte die anwaltlich vertretene Klagepartei u.a. Auskunft darüber, wann und welcher der die Mandantschaft betreffenden , personenbezogenen Daten konkret abhanden gekommen seien. Mit Schreiben vom 17.11.2021, Anlage B 16, Bl. 219ff.GA, erteilte die Beklagte den Prozessbevollmächtigten der Klagepartei die Auskunft, welche Datenkategorien nach den der Beklagten zum Zeitpunkt der Auskunftserteilung verfügbaren Erkenntnissen in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem A.-Profil der Klagepartei verfügbaren Informationen übereinstimmen, durch den Scrapingvorfall seien folgende sog. Datenpunkte betroffen: Nutzer ID, Vorname, Nachname und Geschlecht. Des Weiteren wurde mitgeteilt, dass die Scraper nach dem Verständnis der Beklagten aufgrund der oben beschriebenen Methode der Telefonnummernaufzählung auch über die Telefonnummer der Betroffenen verfügten und von dieser wohl auch auf das Land rückschließen konnten. Beides (Telefonnummer und Land) sei aber gerade nicht von dem jeweiligen A.-Profil abgerufen worden. Darüber hinaus enthielt das Schreiben vom 17.11.2021 allgemein gehaltene Informationen zu den auf A. verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die Daten, die in Bezug auf einen individuellen Nutzer gespeichert sind, eingesehen werden können. 14

Die irische Datenschutzbehörde DPC verhängte gegen die Beklagte am 25.11.2022 eine Geldbuße in Höhe von 265 Mio. Euro. Die Entscheidung ist noch nicht rechtskräftig, da die Beklagte hiergegen Rechtsmittel eingelegt hat. 15

Der Kläger behauptet, dass er von dem Datenschutzvorfall betroffen sei, da infolge der Versäumnisse der Beklagten in der u.a. im Darknet für jedermann abrufbaren Datenbank nachfolgende personenbezogene Daten enthalten seien: 16

H. 17

Dabei handele es sich um die Telefonnummer, die A.-ID, den Namen, Geschlecht, Wohnort, Land und Beschäftigungsverhältnis der Klägerseite. 18

Er behauptet, dass er davon ausgegangen sei, dass die hinterlegte Telefonnummer ausschließlich zum Zwecke der Accountsicherung bzw. Passwortwiederherstellung im Rahmen der sog. Zwei-Faktor-Authentifizierung genutzt werden würde. Bei der Angabe der Handynummer habe es sich um eine Pflichtangabe gehandelt. Sie behauptet weiter, das Scraping sei nur möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen, z.B. Sicherheitscaptcha, vorgehalten habe, um ein automatisiertes Ausnutzen des bereitgestellten Kontakt-Import-Tools zu verhindern. Die für den Kontakt-Importer verwendeten Telefonnummern-Listen seien wahllos generiert worden. Sie ist außerdem der Ansicht, das Scraping sei nur deshalb möglich gewesen, weil die Einstellungen zur Sicherheit der 19

Telefonnummer auf A. so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. A. sei „datenschutzunfreundlich“ eingestellt. Der gesamte Anmeldevorgang sei intransparent und für den Anwender verwirrend. Dies führe letztlich dazu, dass Nutzer im Vertrauen und mit dem Ziel, mehr persönliche Sicherheit zu erreichen, ihre Telefonnummern auf A. preisgäben. Auch die Datenschutzeinstellungen der Beklagten seien undurchsichtig und zu kompliziert gestaltet, denn es bestehe eine Flut an Einstellungsmöglichkeiten allein für die Sicherheit der Mobilnummer. Aufgrund der Vielzahl an Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere. Dies widerspräche - so meint die Klagepartei weiter - allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der „privacy by default“ (=datenschutzfreundliche Voreinstellungen).

Die Klagepartei habe wegen des Scraping-Vorfalls einen erheblichen Kontrollverlust über ihre Daten erlitten und sei in einem Zustand großen Unwohlseins und großer Sorge über möglichen Missbrauch ihrer sie betreffender Daten verblieben. Dies habe sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails und Anrufen von unbekannten Nummern und Adressen manifestiert. Darüber hinaus gebe es bei der Klagepartei seit dem Vorfall unregelmäßig Kontaktversuche von unbekannten Absendern via SMS und E-Mail mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks. Oft würden auch bekannte Plattformen oder Zahlungsdienstleister wie Amazon oder Paypal impersoniert und durch Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Insbesondere erhalte die Klägerseite regelmäßig SMS-Benachrichtigungen mit dubiosen Aufforderungen zum Anklicken von unbekannten Links. Dabei wird durch Absender suggeriert, dass es sich um Warenlieferungen, Rückrufbitten, DHL-Paketzustellungen, aber auch um Nachrichten mit der Bitte um Rückmeldung zwecks angeblichen Erbeintritts, etc. handelt. 20

Die irische Datenschutzbehörde habe in ihrer Entscheidung vom 25.11.2022 ausgeführt, dass die Beklagte es nicht ausreichend verhindert habe, dass etwa 533 Mio. Datensätze mit persönlichen Informationen von A.-Nutzern und -Nutzerinnen abgegriffen und veröffentlicht wurden. Die DPC sehe einen Verstoß der Beklagten insbesondere gegen Art. 25 Abs. 1 und 2 DSGVO. Die DPC habe neben der Geldbuße auch eine Anordnung ausgesprochen, nach der die Beklagte Abhilfemaßnahmen schaffen müsse. 21

Die Klagepartei meint, die Beklagtenseite trage die vollständigen Darlegungs- und Beweislasten, soweit die Einhaltung der DSGVO in Streit stehe. 22

Die Klagepartei beantragt, 23

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 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 Prozentpunkten über dem Basiszinssatz, 24

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, 25

26

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,

a. personenbezogene Daten der Klägerseite, namentlich Telefonnummer, FacebookID, 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, 27

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 A.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, 28

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, 29

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. 30

Die Beklagte beantragt, 31

die Klage abzuweisen. 32

Die Beklagte ist der Ansicht, die Klageanträge zu 1) bis 3) entsprächen nicht den Bestimmtheitsanforderungen, außerdem sei ein Feststellungsinteresse für den Klageantrag zu 2) nicht ersichtlich.. 33

Die Beklagte behauptet, die Angabe von Handynummer und/oder Emailadresse sei freiwillig, jedenfalls habe die Telefonnummer jederzeit entfernt werden können. Sie behauptet weiter, verschiedene Maßnahmen getroffen zu haben, um das Risiko von Scraping zu unterbinden. So habe sie eigene Maßnahmen zur Bekämpfung von Scraping kontinuierlich entwickelt und entwickele sie (auch) als Reaktion auf die sich ständig ändernden Techniken und Strategien immer weiter. Sie habe insbesondere im Einklang mit der Marktpraxis während des relevanten Zeitraums (Januar 2018 bis September 2019) sowohl über Übertragungsbegrenzungen als auch eine Bot-Erkennung verfügt. Diese Schutzmechanismen hätten verhindert, dass die Scraper mittels wahllos generierter Telefonnummern-Listen über den Kontakt-Importer passende A.-Profile hätten auffinden können, weshalb nicht davon auszugehen sei, dass die Telefonnummern-Listen wahllos erstellt worden seien. 34

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen Bezug genommen. 35

Entscheidungsgründe 36

Die Klage ist zulässig, hat aber in der Sache keinen Erfolg. 37

I. 38

Die Klage ist zulässig. 39

a) 40

Das Landgericht ist international, sachlich und örtlich zuständig. 41

aa) 42

Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO (Brüssel Ia- VO). Die Klagepartei hat ihren Wohnort in Jülich in Deutschland. Insoweit ist die deutsche Gerichtsbarkeit zuständig. 43

bb) 44

Das Landgericht Aachen ist gemäß §§ 23 Nr. 1, 71 Abs. 1 GVG für die Klage gegen die Beklagte sachlich zuständig. Der Streitwert liegt bei 6.500,- € (Klageantrag zu 1: 1.000,- €, Antrag zu 2: 500,- €; Antrag zu 3: 4.500,- €, Antrag zu 4: 500,- €) und damit über 5.000,- €. 45

Hinsichtlich des Antrags zu 1) war der dort begehrte Zahlbetrag in Ansatz zu bringen. Hinsichtlich des Feststellungsantrags zu 2) hat die Kammer einen 50%-igen Abschlag von dem mit Ziffer 1) begehrten Zahlbetrag vorgenommen. Hinsichtlich der Höhe des Antrags zu 3) hat die Kammer im Sinne des § 3 ZPO insbesondere auf Tragweite und Umfang des Streitgegenstands abgestellt, den die Beklagte selbst mit 4.500,- € beziffert. Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist letztlich anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen. Bei der Beklagten handelt es sich um einen multinationalen Konzern mit hohen Umsätzen, die Bedeutung der Sache ist auf Grund der Vielzahl der vom Scraping betroffenen Personen für die Beklagte erheblich. Hinsichtlich des Antrags zu 4) erschien ein Streitwert von 500,- € angemessen, da es noch um restliche Auskünfte ging (vgl. auch LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 34 - 48, juris) 46

cc) 47

Die örtliche Zuständigkeit des Landgerichts Aachen folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO. Die Klagepartei hat ihren Wohnsitz in K. und damit im Bezirk des angerufenen Gerichts. 48

b) 49

Der Klageantrag zu 1) ist zulässig. Er ist insbesondere hinreichend bestimmt und entspricht den Anforderungen des § 253 Abs. 2 Nr. 2 ZPO. 50

Grundsätzlich ist ein Klageantrag hinreichend bestimmt, wenn er den erhobenen Anspruch durch Bezifferung oder gegenständliche Beschreibung so konkret bezeichnet, dass der Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) klar abgegrenzt ist sowie Inhalt und Umfang der materiellen Rechtskraft der begehrten Entscheidung (§ 322 ZPO) erkennbar sind. Ferner darf das Risiko des (eventuellen teilweisen) Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit des Antrags auf den Beklagten abgewälzt und eine 51

etwaige Zwangsvollstreckung nicht mit einer Fortsetzung des Streits im Vollstreckungsverfahren belastet werden (vgl. Zöller/Greger, ZPO, 34. Auflage, § 253 Rn. 13 m.w.N.). Der Klageantrag ist der Auslegung zugänglich, wobei dafür auch die Klagebegründung heranzuziehen ist (vgl. Zöller/Greger, ZPO, 34. Auflage, § 253 Rn. 13 m.w.N.).

Zwar stützt die Klagepartei ihr Begehren auf mehrere zeitlich auseinanderfallende angebliche Verstöße gegen die DSGVO – zum einen die dem Scraping-Vorfall vorgelagerten angeblichen Verstöße der Beklagten, zum anderen auf die Verletzung von nachgelagerten Benachrichtigungspflichten. Hierin ist jedoch letztendlich ein einheitlicher, wenn auch zeitlich auseinandergezogener, Lebensvorgang, zu sehen, für den die Klagepartei nun immateriellen Schadensersatz begehrt. Zu beurteilen ist, ob die Beklagte im Vorfeld des Scraping-Vorfalls lediglich unzureichende (oder keine) Datenschutzvorkehrungen getroffen hat, und ob sie danach ihre Nutzer nur unzureichend bzw. intransparent informiert hat, wodurch sich der geltend gemachte immaterielle Schaden noch intensiviert haben könnte (LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818, Rn. 38; LG Gießen Urt. v. 3.11.2022 – 5 O 195/22, GRUR-RS 2022, 30480 Rn. 15). Gegenständlich ist mithin das Verhalten der Beklagten im Zusammenhang mit dem konkret beschriebenen Scrapingvorfall, so dass der Klagegegenstand hier hinreichend abgrenzbar und bestimmt ist. 52

c) 53

Auch der Klageantrag zu 2) ist zulässig und insbesondere hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. 54

Eine fehlende Bestimmtheit folgt vorliegend insbesondere nicht aus der Formulierung „alle künftigen Schäden […], die der Klägerseite […] entstanden sind und/oder noch entstehen werden“. Soweit die Beklagte hierin eine Widersprüchlichkeit erblickt, die ihrer Ansicht nach zur Unzulässigkeit des Antrags führen müsse, kann dem im Ergebnis nicht gefolgt werden. Denn die Auslegung dieses Antrags in Zusammenschau mit dem Klageantrag zu 1) und dem zugrunde liegenden Sachverhaltsvortrag lässt hinreichend deutlich erkennen, dass die Klagepartei hier die Feststellung der Ersatzpflicht für zukünftige Schäden begehrt, welche nicht von dem Klageantrag zu 1) erfasst sind. Es ergibt sich dabei aus der Natur der Sache, dass diese Schäden ihrem Grunde nach aufgrund der Verbreitung der Daten im Internet bereits entstanden sein können, sich dies aber bei der Klagepartei entweder noch nicht ausgewirkt hat oder ihr noch nicht zur Kenntnis gelangt ist. Unter Berücksichtigung des Klageantrags zu 1) und dem hierzu vorgetragenen Sachverhalt wird deutlich, dass die Klagepartei mit dem Klageantrag zu 2) insbesondere *weitere* Schäden meint, die über den mit dem Klageantrag zu 1) geltend gemachten Kontrollverlust hinsichtlich ihrer Daten einschließlich der dazugehörigen subjektiven Befindlichkeit hinausgehen. 55

Auch hat die Klagepartei ein Feststellungsinteresse im Sinne des § 256 Abs. 2 ZPO hinsichtlich des Klageantrags zu 2). Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (BGH, Beschluss vom 9. 1. 2007 - VI ZR 133/06, NJW-RR 2007, 601). Bei den behaupteten Verstößen gegen die DSGVO mit der behaupteten Konsequenz des Kontrollverlustes hinsichtlich der gescrapten Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein (weiterer) materieller oder immaterieller Schaden entstehen könnte. Es ist nicht völlig ausgeschlossen, dass die Klagepartei infolge der Veröffentlichung ihrer Daten zusammen mit ihrer 56

Telefonnummer sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleiden könnte (vgl. LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818, Rn. 39).

d) 57

Auch der Klageantrag zu 3) entspricht dem Bestimmtheitsgebot des § 253 Abs. 2 ZPO. 58

Soweit die Beklagte rügt, der Klageantrag zu 3a) sei hinsichtlich der Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ nicht bestimmt genug, da insofern im Vollstreckungsverfahren geklärt werden müsse, welche Sicherheitsmaßnahmen dem „Stand der Technik“ entsprächen, so ist eine auslegungsbedürftige Antragsformulierung dann hinzunehmen, wenn dies – wie hier - zur Gewährleistung eines effektiven Rechtsschutzes erforderlich ist, mithin die Klägerseite ihren Antrag nicht konkreter fassen kann (BGH, Urt. v. 21.5.2015 – I ZR 183/13, GRUR 2015, 1237). Dies ist vorliegend der Fall. Selbst bei einer Benennung derzeitiger technischer Schutzvorkehrungen würde dies in Anbetracht der schnellen technischen Weiterentwicklung alsbald dazu führen, dass die aktuellen Sicherheitsmaßnahmen bald veralten, sodass die Klagepartei erneut klagen müsste. Dies stünde einem effektiven Rechtsschutz entgegen (LG Gießen Urt. v. 3.11.2022 – 5 O 195/22, GRUR-RS 2022, 30480). Zudem verweist die Klagepartei darauf, dass sie nicht einschätzen kann, was die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen beinhalten, was dann dazu führt, dass das Vollstreckungsorgan gegebenenfalls Wertungen vornehmen muss. Es wäre verfehlt im Lichte des effektiven Rechtsschutzes i. S. d. Art. 19 GG, würde von der Klagepartei verlangt, dass sie für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst ermitteln muss (vgl. LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818). 59

Soweit die Beklagte der Ansicht ist, der Klageantrag zu 3b) entspräche nicht den Bestimmtheitsanforderungen, soweit die Beklagte verurteilt werden soll, die Verwendung der Telefonnummer zu unterlassen, die aufgrund „unübersichtlicher oder unvollständiger Informationen“ erlangt wurden, da es sich bei den Begriffen „unübersichtlich“ und „unvollständig“ um solche handele, die der Wertung offen stehen, führt auch dies nicht zur Unzulässigkeit des Antrags. Der Antrag ist zunächst in seiner Gesamtheit zu lesen. So begehrt die Klagepartei, die Beklagte möge es unterlassen, die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich – nach Auffassung der Klagepartei - ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontaktimporttools genutzt werden kann, um das jeweilige A.-Profil aufzufinden, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der A.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird. Die Klagepartei stellt hier also auf eine von ihr abgegebene Einwilligung ab, die ihrer Meinung nach „unübersichtlich“ und „unvollständig“ ist. Bei Auslegung dieses Klageantrags unter Hinzuziehung der Ausführungen in der Klageschrift (Bl. 11 ff. d.GA) wird hinreichend deutlich, dass die Klagepartei hier die ihrer Meinung nach unübersichtlichen und irreführenden Informationen der Beklagten zur Einstellung der Privatsphäre im A.-Profil beanstandet. 60

II. 61

Die Klage ist indes unbegründet. 62

1. 63

Der Klageantrag zu 1) unterliegt der Abweisung. Die Klagepartei hat gegen die Beklagte keinen Anspruch auf immateriellen Schadensersatz, weder aus Art. 82 Abs. 1 DSGVO noch aus einer anderen Anspruchsgrundlage. 64

a) 65

Der geltend gemachte Anspruch auf immateriellen Schadensersatz ergibt sich nicht aus Art. 82 Abs. 1 DSGVO. 66

Zwar ist hier der räumliche und sachliche Anwendungsbereich der DSGVO bzw. des Art. 82 Abs. 1 DSGVO eröffnet, jedoch ergibt sich aus dem klägerischen Vorbringen weder ein Verstoß der Beklagten gegen die Vorschriften der DSGVO noch ein konkreter Schadenseintritt auf klägerischer Seite. 67

aa) 68

Der räumliche Anwendungsbereich der DSGVO ist gemäß Art. 3 Abs. 1 DSGVO eröffnet, da die Beklagte ihre Niederlassung in der EU hat. 69

Nach Auffassung der Kammer ist – entgegen der Ansicht des LG Essen - auch der sachliche Anwendungsbereich des Art. 82 Abs. 1 DSGVO eröffnet, auch soweit hier die Verletzung von Informationspflichten geltend gemacht und der Schmerzensgeldanspruch zumindest auch darauf gestützt wird. Aus dem Wortlaut der Vorschrift ergibt sich gerade nicht dass Art. 82 Abs. 1 DSGVO durch Art. 82 Abs. 2 DSGVO konkretisiert und eingeschränkt werden soll, so dass nur Pflichtverletzungen im Zusammenhang mit einer *Verarbeitung von Daten* den Schadensersatzanspruch auslösen könnten. Das OLG Köln hat hierzu in seinem Urteil vom 14. Juli 2022 (I-15 U 137/21) zutreffend wie folgt ausgeführt: 70

„In Art. 82 Abs. 1 DSGVO ist von einem "Verstoß gegen diese Verordnung" die Rede und gerade nicht von einer verordnungswidrigen Datenverarbeitung. Die Auffassung des Landgerichts, dass diese in Art. 82 Abs. 1 DSGVO enthaltene Regelung dann durch Art. 82 Abs. 2 DSGVO konkretisiert – sprich: eingeschränkt – werden sollte, ist weder dem Gesamtkontext noch dem Sinn und Zweck oder aber der Entstehungsgeschichte der Norm mit hinreichender Sicherheit zu entnehmen. Zwar spricht auch Erwägungsgrund 146 davon, dass Schäden ersetzt werden sollen, die "einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht". Allerdings ist der Begriff der Verarbeitung in Art. 4 Nr. 2 DSGVO weit gefasst und umfasst beispielsweise auch die "Offenlegung durch Übermittlung", worunter letztlich auch die hier streitgegenständliche Auskunft zu fassen ist. Daneben ergibt sich aus Erwägungsgrund 60, dass die Grundsätze einer fairen und transparenten Verarbeitung es erforderlich machen, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird. Dafür wird ihr (vgl. insoweit Erwägungsgrund 63 und 75) ein entsprechendes Auskunftsrecht ("problemlos und in angemessenen Abständen") zugebilligt, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Wenn aber in dieser Hinsicht der Schutz des Betroffenen gerade durch Auskunfts- und Informationsrechte gestärkt und damit für Fairness und Transparenz beim Verarbeitungsvorgang gesorgt werden soll, spricht dies entscheidend dafür, die Ersatzpflicht nach Art. 82 Abs. 1 DSGVO auf jeden Verstoß gegen Regelungen der Verordnung anzuwenden.“ (OLG Köln, Urteil vom 14. Juli 2022 – I-15 U 137/21 –, Rn. 24, juris) 71

Diesen Erwägungen schließt sich die Kammer vollumfänglich an. 72

73

bb)

Auf der Grundlage des klägerischen Vorbringens ist jedoch ein Verstoß der Beklagten gegen die DSGVO nicht festzustellen. 74

(1) 75

Ein Verstoß gegen Art. 5 Abs. 1 a) DSGVO liegt nicht vor. 76

Nach Art. 5 Abs. 1 a) DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Dieser Grundsatz der Transparenz überträgt sich dann in die Informations- und Aufklärungspflicht nach Art. 13 DSGVO. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. 77

Diesen Anforderungen hat die Beklagte nach Auffassung der Kammer hier genügt. Die Klagepartei selbst hat Screenshots zu den Abläufen und jeweiligen Unterseiten des Internetsauftritts der Beklagten zur Akte gereicht. Diese Inhalte der Website der Beklagten enthalten alle relevanten Informationen zu Art und Umfang der Verarbeitung der Nutzerdaten und alle erforderlichen Hinweise zu Möglichkeiten der individuellen Begrenzung. Zuzugestehen ist der Klagepartei, dass es sich um mehrschichtige Informationen handelt. Die Mehrschichtigkeit schließt aber die Übersichtlichkeit und Transparenz nicht aus. Maßgeblich ist einzig, dass sie verständlich sind, was vorliegend der Fall ist. Insoweit hat die Kammer die zur Akte gereichten Screenshots in Augenschein genommen und ist zu dem Ergebnis gelangt, dass die erteilten Informationen hinreichend verständlich und transparent gestaltet sind. Insoweit dringt die Klagepartei dann auch nicht mit dem Argument durch, dass die Vielzahl der Einstellungsmöglichkeiten dazu führe, dass ein Nutzer es im Zweifel bei den Voreinstellungen belasse. Die internetspezifischen Gepflogenheiten und gerade die DSGVO verlangen vielfältige Einstellungsmöglichkeiten, damit der jeweilige Nutzer die Einstellungen entsprechend seiner spezifischen Bedürfnisse individuell vornehmen kann (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 76, zitiert nach juris). Dann ist es im Lichte der internetspezifischen Gepflogenheiten aber umso wichtiger, dass der Nutzer sich sorgfältig mit den Hinweisen auseinandersetzt, um für sich eine Entscheidung zu treffen, ob und welche Informationen er in welchem Umfang freigibt und wie weitgehend er die Kommunikationsplattform der Beklagten nutzen will (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 78, zitiert nach juris). 78

Zu berücksichtigen ist in diesem Zusammenhang auch, dass die Nutzung der Plattform als solche freiwillig ist. Die Preisgabe der Mobilfunknummer ist selbst für die Nutzung der Plattform, so man sich zu einer solchen entschließt, nicht erforderlich. Selbst wenn man im Rahmen der Registrierung eventuell noch gehalten war, eine Handynummer anzugeben, hat die Beklagte unwidersprochen vorgetragen, dass diese jedenfalls nachträglich jederzeit wieder hätte entfernt werden können. Im Ergebnis war die Klagepartei also nicht zur Angabe bzw. zum Belassen ihrer Handynummer auf der Seite von A. gezwungen. 79

Im Übrigen ist auf den von der Klagepartei vorgelegten Screenshots klar und übersichtlich zu erkennen, dass man als Nutzer festlegen kann, wer einen anhand der Telefonnummer auf A. finden kann. Auf dem Screenshot in der Klageschrift findet sich unter der Rubrik „So kann man dich finden und kontaktieren“ das Thema „Wer kann dich anhand der angegebenen Telefonnummer finden?“. Rechts daneben ist deutlich die Einstellung „Alle“ zu erkennen und wiederum rechts daneben in blau die Schaltfläche „Bearbeiten“, so dass ohne weiteres 80

deutlich zu erkennen ist, wie die Einstellung ist und dass man sie ändern kann.

Nach dem eigenen Vortrag der Klagepartei wird man auf diese Seiten unmittelbar nach der Registrierung weitergeleitet. Abgestellt auf den objektiven Empfängerhorizont gemäß §§ 133, 157 BGB ist es sicherlich mit einem gewissen Aufwand, einer gewissen Geduld und gewissem zeitlichem Aufwand verbunden, sich durch die Seiten und Hinweise zu klicken und sie sorgfältig zu lesen. Dies verkennt die Kammer nicht. Die Hinweise sind, soweit sie die Klagepartei selbst zur Akte reicht, bei genauem Lesen aber verständlich. Im Rahmen der internetspezifischen Gepflogenheiten und vielfältigen Möglichkeiten und den damit einhergehenden datenschutzrechtlichen Fragestellungen sind umfangreiche Hilfethemen und Einstellungshinweise nicht immer zu vermeiden. 81

Die Reichweite des Schutzes der DSGVO ist außerdem im Lichte der jeweiligen konkreten Nutzung (beispielsweise des Internets) zu sehen. Mithin ist vorliegend zu berücksichtigen, dass es sich bei A. um ein soziales Netzwerk handelt, das u.a. auf Kommunikation, Finden von Personen und Teilen von Informationen angelegt ist. In diesem Lichte sind die von der Beklagten gewählten Voreinstellungen nicht zu beanstanden, da der jeweilige Nutzer umfassend und verständlich über individuelle Änderungsmöglichkeiten informiert wird. Insoweit kann dahinstehen, wie es die Klagepartei mit der Replik ausführt, dass A. etwaig auch andere Zwecke verfolgt, wie die Finanzierung über Werbung, denn jedenfalls ist ein (wesentlicher) Zweck der der Kommunikation auf einer sozialen Plattform (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 77, zitiert nach juris). 82

(2) 83

Es liegt ferner kein Verstoß gegen Art. 32 DSGVO bzw. Art. 5 Abs. 1 lit. f) vor. 84

Denn die Beklagte hat nicht gegen ihre Pflicht, die personenbezogenen Daten der Nutzer, inklusive der der Klagepartei, ausreichend gemäß Art. 32 DSGVO zu schützen, verstoßen. Nach Art. 32 DSGVO haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen 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 zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gemäß 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 und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung, und zwar durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“). Art. 32 DSGVO 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 u.a. davor schützen, dass Dritte diese unbefugt oder unrechtmäßig verarbeiten (AG Straußberg, Urteil vom 13.10.2022, 25 C 95/21, Rn. 28, zitiert nach juris; LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 80, zitiert nach juris). 85

Dies zu Grunde gelegt, hat die Beklagte gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, nicht verstoßen. Insbesondere war die Beklagte nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils der Klagepartei aufgrund ihrer selbst gewählten 86

Einstellung zu verhindern.

Es ist angesichts des Vortrags der Beklagten, dem die Klagepartei nicht entgegengetreten ist, davon auszugehen, dass die Suchbarkeitseinstellungen der Klagepartei so eingestellt waren, dass „alle“ sie anhand ihrer Telefonnummer finden konnten. Diese Einstellung beinhaltet dann aber auch das Finden des A.-Profils der Klagepartei durch Dritte über ihre Mobilfunknummer, wenn diese Dritten (unter Zuhilfenahme elektronischer Möglichkeiten) die Telefonnummer der Klagepartei nur zufällig erraten oder anderweitig erlangt haben und diese auf gut Glück, ohne zu wissen, ob es sich bei der Nummer überhaupt um eine Telefonnummer handelt, in den Kontaktimporter von A. hochladen. Denn auch Dritte fallen unter den Begriff "alle". Falls einige Daten der Klagepartei tatsächlich von Dritten gescrapt, mithin verarbeitet worden sein sollten i.S.d. Art. 4 Nr. 2 DSGVO, war die Beklagte nicht verpflichtet, sämtliche vom Kläger aufgeführten Daten vor der Verarbeitung durch die Scraper zu schützen, da die Daten nicht unbefugt bzw. unrechtmäßig verarbeitet worden sind. Es handelt sich bei den nach dem Klägervortrag gescrapten personenbezogenen Daten der Klagepartei teilweise, nämlich in Bezug auf die A.-ID, den Namen und das Geschlecht, um Daten, die ohnehin für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen wie Logins oder ähnliches abrufbar waren, was der Klagepartei bereits durch die Anmeldung bekannt war oder hätte bekannt sein müssen. Die Erhebung dieser öffentlichen Daten als solche erfolgte daher nicht unbefugt bzw. unrechtmäßig. Diese Verarbeitung in Form des Scrapens erfolgt auch durch Dritte und nicht durch die Beklagte (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 81, zitiert nach juris). 87

Selbst dann, wenn der Klagepartei die Standardeinstellungen auf der Plattform A. nicht positiv bekannt gewesen sein sollten, rechtfertigt dies 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 ihre ID, ihr Name und ihr Geschlecht für jedermann öffentlich abrufbar sind. Hierauf wurde sie bereits vor der Registrierung auf A. durch entsprechende Verweise auf die in der Registrierungsmaske verlinkten Datenrichtlinie hingewiesen. Dort heißt es u.a.: „Öffentliche Informationen stehen jedem auf unseren Diensten und außerhalb dieser zur Verfügung und können mithilfe von Online-Suchmaschinen, APIs und Offline-Medien (z.B. im Fernsehen) gesehen werden bzw. es kann so auf sie zugegriffen werden.“ (vgl. S. 5 der Datenrichtlinie) Zudem wurde die Klagepartei unstreitig im Hilfebereich von A. darüber informiert, dass bestimmte Informationen - nämlich Name, Geschlecht, Nutzername und Nutzer-ID – immer öffentlich zugänglich sind, also jeder, damit auch Personen außerhalb von A., diese Informationen sehen kann. Hierzu heißt es unter dem Punkt „Zielgruppenauswahl“: „Deine öffentlichen Informationen, zu denen dein Name, Profilbild, Titelbild, Geschlecht, Nutzername, deine Nutzer-ID (Kontonummer) und Netzwerke gehören, sind für alle sichtbar (erfahre warum).“ Die Beklagte hatte daher keine Veranlassung, diese Daten vor der Erhebung durch Dritte zu schützen, da sie ohnehin öffentlich waren (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 82, zitiert nach juris). 88

Dass nicht öffentlich zugängliche Informationen von Dritten von der Plattform der Beklagten erhoben und erlangt worden sind, kann indes nicht festgestellt werden. Die Telefonnummer der Klagepartei haben die Scraper gerade nicht von der Plattform der Beklagten erhalten. Vielmehr haben sie allenfalls den Kontaktimporter von A. schon mit dieser Telefonnummer „gefüttert“, haben also schon vorher über diese Nummer verfügt, wobei zwischen den Parteien unklar ist, wie die Scraper diese Telefonnummer erlangt bzw. generiert haben könnten. Jedenfalls handelt es sich aber nicht um Daten, die von A. an die Dritten gelangt 89

sind.

Der von den Scrapern unter Nutzung des Kontakt-Importers der Plattform A. hergestellte Abgleich zwischen der von ihnen hochgeladenen Telefonnummer der Klagepartei mit ihrem Konto stellt zwar – soweit unterstellt wird, dieser hat tatsächlich stattgefunden – eine Verarbeitung i.S.d. DSGVO dar. Jedoch war die Beklagte nicht verpflichtet, das Konto der Klagepartei vor dessen Auffinden über die Telefonnummer zu schützen, da ein solcher von den Scrapern hergestellte Abgleich als solcher nicht unbefugt bzw. unrechtmäßig war. Vielmehr entsprach dieses Auffinden den von der Klagepartei gewählten bzw. belassenen Einstellungen in den Suchbarkeitseinstellungen. „Abgegriffen“ wurden von den Dritten sodann nur Daten, die ohnehin öffentlich waren, was der Klagepartei aufgrund der umfangreichen und hinreichend transparenten Information durch A. hätte bekannt sein müssen. Die Klagepartei hat der Beklagten ihre Telefonnummer freiwillig angegeben bzw. die Nummer nach Registrierung dort belassen. Die Klagepartei selbst hat durch entsprechende Einstellung bzw. deren Belassen der Suchbarkeits-Einstellungen dafür gesorgt, dass ihr Profil von jedermann anhand ihrer Telefonnummer gefunden werden konnte. Der von den Scrapern veranlasste Abgleich war folglich jeder Person, die – wie die Scraper – über die Telefonnummer der Klagepartei verfügte oder sie technisch erzeugte, möglich und ist nicht unbefugt bzw. unrechtmäßig im Sinne der DSGVO (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 85, zitiert nach juris). 90

Selbst dann, wenn der Klagepartei nicht positiv bekannt gewesen sein sollte, dass alle Personen über ihre Telefonnummer ihr A.-Konto finden können, hat dies nicht zur Folge, dass die Beklagte verpflichtet war, hiergegen Schutzmaßnahmen zu ergreifen. Denn die Beklagte musste angesichts ihrer Hinweise in den Datenverwendungsrichtlinien, die die Klagepartei als gelesen bei der Registrierung angab, annehmen, dass der Klagepartei bekannt ist, dass ihr Konto über ihre Telefonnummer für jedermann aufzufinden ist. Wenn die Klagepartei dann – trotz hinreichend deutlicher Hinweise - an diesen Einstellungen nichts ändert, musste die Beklagte sogar davon ausgehen, dass die entsprechende Auffindbarkeit von dem betreffenden Nutzer gerade so gewünscht ist; zumal es sich bei A. ja um ein Netzwerk u.a. zur Herstellung von Kontakten handelt (s.o.). Wie bereits oben dargelegt und auch anhand der von der Klagepartei selbst vorgelegten Screenshots ersichtlich, ist die Klagepartei hinreichend deutlich und transparent auf die Einstellung hinsichtlich ihrer eigenen Auffindbarkeit und die entsprechende Abänderungsmöglichkeit hingewiesen worden. Die Klagepartei hatte es daher selbst in der Hand ihr Konto dahingehend anzupassen, dass nicht alle Personen, die ihre Telefonnummer hochladen, ihr Konto auffinden können. Dabei verkennt die Kammer nicht, dass beim Scrapen der jeweilige Scraper sich unter Umständen auch computerunterstützter Hilfe bedient und künstlich Handynummern erzeugt, die dann – wie hier – mit der echten Handynummer eines A.-Nutzers übereinstimmten und so die – öffentlich zugänglichen Daten – abgreift. Diese Vorgehensweise ist aber nur möglich, weil die Klagepartei selbst die Einstellung belassen hat, dass sie jedermann über ihre Mobilfunknummer finden kann. Über die Datenschutzrichtlinie hat die Beklagte die Klagepartei hinreichend auf begrenzende Einstellungsmöglichkeiten hingewiesen. 91

Es widerspricht dem Zweck von A., 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. 92

Dieses Risiko ist aber nicht von der Beklagten, sondern von dem jeweiligen Nutzer 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 nutzt (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 88, zitiert nach juris).

(3) 93

Die Beklagte hat auch nicht gegen das in Art. 24, 25 Abs. 2 DSGVO verankerte Prinzip „Privacy by default“ verstoßen. Demnach muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Dies soll vor allem den technisch nicht versierten Nutzer schützen. Die Voreinstellungen sollen möglichst datenschutzfreundlich eingestellt werden, um die Privatsphäre der Nutzer zu gewährleisten. Der Nutzer kann dann noch individuell Anpassungen nach seinen Wünschen vornehmen. Unstreitig sind durch die Registrierung nur der Name, das Geschlecht und die A.-ID stets öffentlich sichtbar, wozu jeder Nutzer aber durch Akzeptieren der Datenschutzbestimmungen seine Zustimmung erteilt. Soweit jemand sich dann noch entschließt seine Telefonnummer zu hinterlegen, was für die Registrierung bei A. nicht erforderlich ist, sondern es lediglich einfacher machen soll, gefunden zu werden, ist die entsprechende Suchbarkeitseinstellung zwar zunächst so eingestellt, dass „alle“ den jeweiligen A.-Nutzer anhand seiner Telefonnummer finden können. Der technisch unkundige Nutzer wird gleichwohl – wie bereits ausgeführt - über die entsprechenden Hinweise hinreichend informiert und über Einstellungsmöglichkeiten und deren Begrenzungsmöglichkeiten in Kenntnis gesetzt. 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 sich der jeweilige Nutzer, der einer Plattform eines sozialen Netzwerks beitreten will, mit den geltenden Gepflogenheiten vertraut machen. Bei einer Plattform, die auf Kontaktsuche und das Finden von Kontakten ausgerichtet ist, und auf der das nicht zwingend erforderliche Hinterlegen bzw. Belassen 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, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 93, zitiert nach juris). 94

Auch in diesem Zusammenhang ist zu berücksichtigen, dass hier – wie oben ausgeführt – von A. lediglich ohnehin öffentliche Daten „preisgegeben“ worden sind. Die Telefonnummer der Klagepartei wurde gerade nicht von A. an Dritte herausgegeben, sondern lag, auch auf der Grundlage des klägerischen Vortrages, bei diesen –aus ungeklärten Gründen – allenfalls bereits vor. 95

Eine andere Beurteilung ergibt sich nicht aus dem bloßen Umstand, dass die irische Datenschutzbehörde DPC am 25.11.2022 gegen die Beklagte eine Geldbuße in Höhe von 265 Millionen € verhängt hat und dies – nach dem bislang nicht bestrittenen Vortrag der 96

Klagepartei - auf einen Verstoß gegen Art. 25 Abs. 1 bzw. Abs. 2 DSGVO stützt. Denn diese Entscheidung entfaltet insofern keine Bindungswirkung , da sie noch nicht rechtskräftig ist. Außerdem ersetzt der bloße Umstand, dass eine bestimmte Behörde aufgrund eines seitens der Klagepartei nicht näher dargelegten Sachverhalts von einem Verstoß gegen die DSGVO ausgeht, keinen konkreten Klägervortrag im hiesigen Verfahren. Auf der Grundlage des klägerseits dargelegten Sachverhalts vermag die Kammer aus dem oben dargelegten Gründen einen Verstoß gegen Art. 25 DSGVO nicht zu erkennen.

(4) 97

Die Beklagte hat auch nicht eine etwaige Pflicht gemäß Art. 33 DSGVO verletzt, der zuständigen Aufsichtsbehörde einen Datenschutzverstoß zu melden. Gemäß Art. 33 DSGVO meldet der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Meldung gegenüber der Aufsichtsbehörde ermöglicht es dieser über Maßnahmen zur Eindämmung und Ahndung der Rechtsverletzung zu entscheiden (vgl. LG Essen, Urteil vom 23.9.2021, AZ.: 6 O 190/21, ZD 2022, 50, m.w.N.). Der Beklagten wurde der Datenschutzvorfall spätestens am 03.04.2021 bekannt, denn zu diesem Zeitpunkt schilderte sie Ihr Vorgehen zu dem Scraping-Vorfall auf Ihrer Website. Der zuständigen Aufsichtsbehörde, Irish Data Protection Commission (IDPC, gem. Art 55 DSGVO) wurde unstreitig allerdings kein solcher Vorfall gemeldet. Da aber der Beklagten aus den oben ausgeführten Gründen kein Datenschutzverstoß anzulasten ist, musste sie den hier streitgegenständlichen sog. Scraping-Vorfalll auch nicht melden (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 98, zitiert nach juris). 98

(5) 99

Schließich hat die Beklagte auch nicht gegen Art. 15 DSGVO verstoßen, indem sie der Klagepartei keine bzw. unvollständige Auskünfte erteilt hätte. Ein Anspruch auf Auskunftserteilung ergibt sich aus Art 15 Abs. 1 a), c) DSGVO. Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und über die a.) Verarbeitungszwecke und über c.) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 102, zitiert nach juris). 100

Da das Schreiben der Beklagten vom 17.11.2021 die Information enthält, dass von dem Scrapingvorfall generell Nutzer ID, Vorname, Nachname, Land und Geschlecht betroffen waren, ist ein etwaiger Anspruch insoweit jedenfalls erfüllt und erloschen (§ 362 Abs. 1 BGB) (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 102, zitiert nach juris). 101

Nicht beantwortet wird durch die Beklagte in dem besagten außergerichtlichen Schreiben, welchen Empfängern die Daten der Klagepartei durch Ausnutzung des Kontakt-Importer-Tools im Sinne des Art. 15 Abs. 1 c) DSGVO zugänglich gemacht wurden. Das Scraping ist allerdings – wie vorstehend ausgeführt – von außen erfolgt und es ist nicht erkennbar, wer diese Daten gescrapt hat. Die begehrte Auskunftserteilung ist aufgrund des Vorganges des Scrapings unter Ausnutzung von Daten, die auf „öffentlich“ gestellt sind, unmöglich. Ebenso ist im Rechtssinne unmöglich (und es wird auch nicht näher dargelegt, wie die Beklagte 102

mitteilen können soll), zu informieren, *wann* die Daten gescrapt wurden. Die Klagepartei geht selbst von 2019 aus bzw. von der Veröffentlichung dann im April 2021. Dieser Zeitrahmen ist der Klagepartei bekannt; eine genaue Eingrenzung in Bezug auf ihre Daten ist nicht möglich (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 103, zitiert nach juris).

Die Beklagte hat der Klagepartei im Ergebnis also alle Informationen mitgeteilt, die ihr im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Sie ist folglich hierzu auch nicht verpflichtet (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 103, zitiert nach juris). 103

cc) 104

Unabhängig davon, ob hier – von der Kammer verneint – überhaupt ein Verstoß gegen Vorschriften der DSGVO vorliegt, scheitert ein Anspruch aus Art. 82 Abs.1 DSGVO aber jedenfalls daran, dass hier kein restitutionsfähiger (immaterieller) Schaden vorliegt. 105

Für den – hier geltend gemachten – immateriellen Schadensersatz gelten dabei die im Rahmen von § 253 BGB entwickelten Grundsätze; die Ermittlung obliegt dem Gericht nach § 287 ZPO (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31). Es können für die Bemessung die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden, beispielsweise die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die betroffenen Kategorien personenbezogener Daten. Zu berücksichtigen ist auch, dass die beabsichtigte abschreckende Wirkung nur durch für den Anspruchsverpflichtenden empfindliche Schmerzensgelder erreicht wird, insbesondere wenn eine Kommerzialisierung fehlt. Ein genereller Ausschluss von Bagatellfällen ist damit nicht zu vereinbaren (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31; vgl. LG Köln, Urteil vom 07.10.2020 – 28 O 71/20). Die Pflicht zur Erstattung immaterieller Schäden ist daher nicht auf schwere Schäden beschränkt (vgl. LG Landshut, Urteil vom 06.11.2020 – 51 O 513/20) (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 105 - 116, juris). 106

Nach den Erwägungsgründen der europäischen Grundrechtscharta ist der Schadensbegriff weit auszulegen (s. Erwägungsgrund Nr. 146, auch wenn er in der DSGVO nicht näher definiert wird). Schadenersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen (Bergt in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., Art. 82 Rdn. 17 m. w. N.; Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz Rn. 10 b). Darüber hinaus sollen die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden haben. Dabei wird vor allem die abschreckende Wirkung des Schadensersatzes betont, welche insbesondere durch seine Höhe erzielt werden soll. Nach den Erwägungsgründen Nr. 75 kann ein Nichtvermögensschaden insbesondere durch Diskriminierung, Identitätsdiebstahl oder –betrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden persönlichen Daten oder gesellschaftliche Nachteile eintreten. 107

Ein genereller Ausschluss von Bagatellschäden ist im Lichte dieser Erwägungsgründe nicht vertretbar (vgl. LG Essen, Urteil vom 23.9.2021, Az.: 6 O 190/21, ZD 2022, 50; LG Köln, Urteil vom 18.05.2022, Az.: 28 O 328/21, BeckRS 2022, 11236). Dies wird auch aus Art. 4 Abs. 3 AEUV abgeleitet, der die Mitgliedsstaaten dazu anhält, Verstöße wirksam mit Sanktionen zu belegen, denn nur so könne man eine effektive Durchsetzbarkeit des EU-Rechts und damit auch der DSGVO erzielen (LG München I, Urteil vom 09.12.2021, Az.: 31 O 16606/20, BKR 2022, 131) (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 108

105 - 116, juris).

Allein eine Verletzung des Datenschutzrechts als solche – die die Kammer nicht festzustellen vermochte – begründet allerdings nicht bereits für sich gesehen einen Schadensersatzanspruch für betroffene Personen. Die Verletzungshandlung muss in jedem Fall auch zu einer konkreten Verletzung von Persönlichkeitsrechten der betroffenen Personen geführt haben (vgl. LG Hamburg, Urteil vom 04.09.2020 – 324 S 9/19). Die Verletzung der Vorschriften der DSGVO ist nicht mit einem Schadenseintritt gleichzusetzen. Es ist zwar keine schwere Verletzung des Persönlichkeitsrechts erforderlich. Andererseits ist aber auch weiterhin nicht für jede im Grunde nicht spürbare Beeinträchtigung bzw. für jede bloß individuelle empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren. Vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und es muss um eine objektiv nachvollziehbare, tatsächlich erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen (vgl. LG Landshut, Urteil vom 06.11.2020 – 51 O 513/20; LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 109, zitiert nach juris)). 109

In den Erwägungsgründen Nr. 75 und 85 werden einige mögliche Schäden aufgezählt, darunter Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, aber auch der Verlust der Kontrolle über die eigenen Daten sowie die Erstellung unzulässiger Persönlichkeitsprofile. Zudem nennt Erwägungsgrund 75 auch die bloße Verarbeitung einer großen Menge personenbezogener Daten einer großen Anzahl von Personen. Der Schaden ist zwar weit zu verstehen, er muss jedoch auch wirklich „erlitten“ (Erwägungsgrund Nr. 146), das heißt „spürbar“, objektiv nachvollziehbar und tatsächlich eingetreten sein (AG Diez v. 7. 11. 2018, Az. 8 C 130/18), um bloß abstrakte, nicht wirklich eingetretene Beeinträchtigungen auszuschließen (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 105 - 116, juris). 110

Gemessen an diesen Grundsätzen hat die Klagepartei zwar eine spürbare Beeinträchtigung – hervorgerufen durch Datenverlust – von persönlichen Belangen im Rahmen ihrer Anhörung dargelegt. 111

Allerdings sind bei dem Gericht Zweifel verblieben, ob die Beeinträchtigungen tatsächlich auf den sog. Scraping-Vorfall zurückzuführen sind. Zum einen hat der Kläger in der Klageschrift auch auf einen Anstieg beim Eingang verdächtiger E-mails hingewiesen, wobei die Email Anschrift des Klägers gerade nicht zu den betroffenen Daten gehört. Darüber hinaus hat er aber auch ausgeführt, dass er seine Telefonnummer nicht geändert habe, da er unter dieser nicht nur als Privatperson, sondern auch im Rahmen seiner selbständigen Tätigkeit zu erreichen sei. Dies lässt jedoch den Rückschluss auf eine nicht unerhebliche Verbreitung seiner Telefonnummer zu, so dass keine hinreichenden Anhaltspunkte bestehen, dass die ihm zugehenden Anrufe oder sms- Nachrichten tatsächlich auf den streitgegenständlichen Vorfall zurückzuführen sind. 112

Die Klagepartei trägt vor, einen erheblichen Kontrollverlust über ihre Daten erlitten und 113

dd) 114

Es bedurfte auch keiner Aussetzung des Verfahrens und Vorlage an den EuGH nach § 148 ZPO mit Blick auf die anstehende Entscheidung des Gerichtshofs der Europäischen Union zur Rechtssache C 300/21 (Österreichische Post) zu der Frage, ob es im Rahmen des Art. 82 Abs. 1 DSGVO eines konkreten, messbaren Schadens bedarf. 115

116

Nach Auffassung der Kammer hat Art. 82 Abs. 1 DSGVO zwei eigene, separate Voraussetzungen, nämlich: (1.) einen Verstoß gegen die DSGVO und (2.) einen tatsächlich eingetretenen materiellen oder immateriellen Schaden. Läge bei jedem DSGVO-Verstoß automatisch ein immaterieller Schaden vor, wäre der Schaden als Anspruchsvoraussetzung überflüssig. Auf die Frage des konkreten Schadens kommt es hier aber deshalb nicht entscheidungserheblich an, weil die Klage – wie ausgeführt – auch aus anderen Gründen ohne Erfolg bleibt, da schon kein Verstoß gegen die DSGVO festgestellt werden kann und im Übrigen die Klagepartei die Betroffenheit ihres Kontos auch nicht ausreichend dargelegt hat.

Da die Kammer außerdem im vorliegenden Falle nicht letztinstanzlich entscheidet, trifft sie keine Vorlagepflicht gem. Art. 267 Abs. 3 AEUV. Allenfalls wäre ihr eine Vorlagemöglichkeit gem. Art. 267 Abs. 2 AEUV eröffnet, zu der sie aus den nachfolgenden Gründen keinen Anlass sieht. Die Vorlage einer Auslegungsfrage an den EuGH ist dann nicht angezeigt, wenn die gerichtliche Anwendung des Gemeinschaftsrechts derart offenkundig ist, dass für einen vernünftigen Zweifel keinerlei Raum bleibt (EuGH, Urt. v. 06.10.1982 – 283/81 „CILFIT“) oder wenn es – wie hier und bereits ausgeführt - auf diese Frage nicht alleinentscheidend ankommt, da vorliegend ein Anspruch auch an anderen Voraussetzungen scheitert. Daher war die Kammer auch nach Ausübung pflichtgemäßen Ermessens nicht zur Vorlage verpflichtet (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 116, zitiert nach juris). 117

b) 118

Es kann im Ergebnis dahinstehen, ob neben Art. 82 Abs. 1 DSGVO auch nationales Recht anwendbar ist, oder das nationale Recht von den europarechtlichen Vorschriften der DSGVO verdrängt wird. Denn auch bei der Annahme eines Nebeneinanders hat die Klagepartei mangels restitutionsfähigem Schaden keinen Schadensersatzanspruch gegen die Beklagte, weder aus § 280 Abs. 1, 253 Abs. 2 BGB noch aus einer anderen nationalen Schadensersatz gewährenden Anspruchsgrundlage. Auf die obigen Ausführungen wird Bezug genommen. 119

2. 120

Der mit dem Klageantrag zu 2) gestellte Feststellungsantrag ist unbegründet, da Pflichtverstöße der Beklagten und Verstöße gegen die Vorschriften der DSGVO - wie oben ausgeführt - gerade nicht festgestellt werden konnten. Auf die obigen Ausführungen wird Bezug genommen. 121

3. 122

a) 123

Auch der Klageantrag zu 3a) unterliegt der Abweisung. 124

Mit dem Klageantrag 3a) begehrt die Klagepartei die Unterlassung des Zugänglichmachens von personenbezogenen Daten für unbefugte Dritte über eine Software zum Importieren von Kontakten, ohne dass es nach dem Stand der Technik mögliche Sicherheitsmaßnahmen gibt, die Missbrauch verhindern. Missbrauch wird dann angenommen, wenn andere Zwecke als die Kontaktaufnahme verfolgt werden. Im Prinzip möchte die Klagepartei damit erreichen, dass der Kontakt-Importer durch geeignete technische Vorkehrungen vor Scraping geschützt wird. 125

126

Ein solcher Anspruch ergibt sich weder aus § 1004 analog BGB i.V.m. mit dem Recht auf informationelle Selbstbestimmung noch aus § 823 Abs. 2 BGB i.V.m. Art. 6 Abs. 1 sowie Art. 17 DSGVO noch aus einer anderen Anspruchsgrundlage, selbst wenn unterstellt wird, dass ein Konto der Klagepartei vom „Scraping“ betroffen war. Eine Zuwiderhandlung der Beklagten in der Vergangenheit ist nach den obigen Ausführungen weder zu erkennen, noch für die Zukunft zu befürchten.

Hier sind lediglich Daten von der A.-Seite abgegriffen und an anderer Stelle wieder veröffentlicht worden, die ohnehin immer öffentlich waren. Im Rahmen ihrer Registrierung hat die Klagepartei ihre Zustimmung erteilt, dass die Daten veröffentlicht werden dürfen. Dass es keinen Anspruch auf Schutz vor Veröffentlichung von bereits öffentlichen Daten gibt, versteht sich von selbst. Dass die Beklagte die Telefonnummer der Klagepartei Dritten zugänglich gemacht hat, behauptet die Klagepartei schon selber nicht. Vielmehr verfügten die Scraper bereits über diese Telefonnummer und haben den Kontakt-Importer erst damit „gefüttert“. Was die Unterlassung einer Verwendung der Telefonnummer anbelangt, lag es jederzeit in der Hand der Klagepartei, dies in den Einstellungen entsprechend zu verändern und die Suchbarkeitseinstellungen so vorzunehmen, dass ihr Profil nicht anhand der Telefonnummer gefunden werden kann. Dass die Beklagte entgegen der von einem Nutzer getroffenen Einstellungen Telefonnummern freigibt oder anderweitig nutzt, hat die Klagepartei schon nicht behauptet (vgl. auch LG Gießen, Urteil vom 3. November 2022 – 5 O 195/22 –, Rn. 31, zitiert nach juris). Da es hiernach und nach den obigen ausführlichen Ausführungen also keinen Fall der Erstbegehung gibt, ist auch keine rechtswidrige Beeinträchtigung zu befürchten und der Unterlassungsanspruch damit nicht gegeben. 127

b) 128

Mit dem Klageantrag 3b) begehrt die Klagepartei die Unterlassung, ihre Telefonnummer auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde. 129

Auch hier fehlt es bereits an einem Verstoß der Beklagten, der überhaupt zu einem Unterlassungsanspruch führen könnte, selbst wenn man unterstellt, dass ein Konto der Klagepartei vom „Scraping“ betroffen war und Art. 6 DSGVO als Schutzgesetz im Sinne des § 823 Abs. 2 BGB ansieht. 130

Die Beklagte hat die Klagepartei ausreichend aufgeklärt gemäß Art 13 Abs. 1 DSGVO, insbesondere über die Zwecke der Verarbeitung sowie deren Rechtsgrundlage und die etwaigen Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (s.o.). Die Klagepartei hat zudem mit der Zustimmung zu den Nutzungsbedingungen und der Datenrichtlinie die Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben gemäß Art. 6 Abs. 1 S. 1 a.) DSGVO. Insbesondere wurden die Datenlinie sowie die Nutzungsbedingungen in einfach verständlicher Sprache abgefasst und sind und waren nach dem eigenen Vortrag der Klagepartei zugänglich, wenn auch mehrschichtig. Die Website der Beklagten weist den jeweiligen Nutzer sogar mehrfach darauf hin, dass man einen Privatsphärecheck machen kann. Insoweit entspricht das Ersuchen der Einwilligung auch den Voraussetzungen des Art. 7 Abs. 2 DSGVO. Wie ausgeführt, sind bei Auslegung nach dem objektiven Empfängerhorizont gemäß §§ 133, 157 BGB bei entsprechender Sorgfalt und Inanspruchnahme von Zeit die mehrschichtigen Hinweise durchaus nachvollziehbar (s. Screenshots in der Klageschrift) (vgl. LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 145, zitiert nach juris). 131

132

4.

Auch der mit dem Klageantrag zu 4) geltend gemachte Auskunftsanspruch unterliegt der Abweisung. 133

Mit dem Klageantrag zu 4) begehrt die Klagepartei die Auskunft, welcher der klägerischen personenbezogenen Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontakt-Importtools erlangt werden konnten. 134

Die Klagepartei hat hinsichtlich der begehrten Auskunft keinen Auskunftsanspruch gegen die Beklagte aus Art. 15 DSGVO (mehr). 135

Wie bereits ausgeführt, ist der Auskunftsanspruch durch das außergerichtliche Schreiben der Beklagten teilweise i. S. d. § 362 Abs. 1 BGB erloschen, soweit er die eigene Verarbeitung von Daten der Klagepartei betrifft. Die Beklagte ist auch lediglich gehalten, diese von ihr selbst – und nicht etwaig von Dritten – verarbeiteten Daten mitzuteilen. Soweit durch das Scrapen öffentlich einsehbare Daten von Dritten verarbeitet wurden, ist jedenfalls nicht die Beklagte auskunftspflichtig (LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 –, Rn. 147, zitiert nach juris). 136

5. 137

Mangels Hauptanspruch entfällt der Anspruch auf Erstattung der vorgerichtlichen Rechtsanwaltskosten. Das Gleiche gilt hinsichtlich der geltend gemachten Zinsansprüche. 138

6. 139

Die Nebenentscheidungen beruhen auf §§ 91, 708 Nr. 11, 709, 711 ZPO. 140

Streitwert: 6.500,- € 141

G.		

142