LG Regensburg, Endurteil v. 11.05.2023 – 72 O 731/22 KOIN

Titel:

Erfolglose Schadensersatzklage wegen öffentlich zugänglicher Nutzerdaten

Normenketten:

DSGVO Art. 5, Art. 13, Art. 25, Art. 32, Art. 33, Art. 82

ZPO § 253, § 256, § 287

Leitsätze:

1. Der Betreiber einer Social-Media-Plattform ist im Zuge seiner Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten, nicht gehalten, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils eines Nutzers aufgrund der von diesem selbst gewählten Einstellung zu verhindern. (Rn. 45) (redaktioneller Leitsatz)

2. Ein Verstoß gegen die Vorgaben des Art. 25 DSGVO, welcher bereits vor dem eigentlichen Beginn der Datenverarbeitung seinen Regelungscharakter entfaltet, führt wegen seines organisatorischen Charakters nicht zu einem Schadensersatzanspruch nach Art. 82 DS-GVO. (Rn. 47 – 49) (redaktioneller Leitsatz)

Schlagwort:

Datenschutz

Fundstellen:

ZD-Beil 2024, 766

GRUR-RS 2023, 17446

LSK 2023, 17446

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten 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 zu vollstreckenden Betrags leistet.

Beschluss

Der Streitwert wird auf 7.000,00 € festgesetzt.

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 www.f2..com und der Dienste auf dieser Seite für Nutzer in der Europäischen Union (nachfolgend: F2.). Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Klagepartei nutzt F2. insbesondere um mit Freunden zu kommunizieren, zum Teilen privater Fotos und für Diskussionen mit anderen Nutzern.

3

Im Rahmen einer Registrierung bei F2. 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 S. 9 der Klageschrift = Bl. 10 d.A.). Im Hilfebereich bzw. in der Datenrichtlinie werden die Nutzer von F2. darüber informiert, dass bestimmte Informationen – nämlich Name, Geschlecht, Nutzername und Nutzer-ID – immer öffentlich zugänglich sind, also jedermann, damit auch Personen außerhalb von F2., diese Informationen sehen kann.

4
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. S. 9 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 F2.-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. So war auch die Einstellung im klägerischen Profil hinsichtlich der Telefonnummer.

7
Bei den „Suchbarkeitseinstellungen“ wird u.a. festgelegt, wer das Profil eines Nutzers anhand von dessen Telefonnummer finden kann – beispielsweise, 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. Die Suchbarkeitseinstellungen in dem F2.-Profil der Klagepartei waren bis zum 19.04.2023 auf „Everyone“, d.h. „alle“, eingestellt, danach änderte der Kläger die Einstellungen auf „Only Me“, d.h. „nur ich“.

8
In der Zeit von Januar 2018 bis September 2019 sammelten Dritte – unter Verstoß gegen die Nutzungsbedingungen von F2. – 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 Standarteinstellung 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 Standarteinstellung vorlag, wonach „alle“ mittels einer Telefonnummer nach dem entsprechenden F2.-Profil suchen können. Diese 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 vornherein 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.

9
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 mussten den aktualisierten Nutzungsbedingungen zustimmen, um die F2.-Plattform weiter nutzen zu können. Sowohl die

Datenrichtline 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.

10
Anfang April 2021 wurden die wie oben beschrieben gescrapten Daten einer Vielzahl von F2.-Nutzern sowie die von den Scrapern mit diesen Datensätzen verknüpften Telefonnummern im Internet frei zum Download bereitgestellt.

11
Nach dem Vorfall informierte die Beklagte die zuständige Datenschutzbehörde „Irish Data Protection Commission“ (DPC) nicht.

12
Mit anwaltlichem, vorgerichtlichem Email-Schreiben der Klägerseite vom 22.7.2021 (Anlage K1) wurde die Beklagte zur Zahlung von 500,- € Schadensersatz nach Art. 82 Abs. 1 DSGVO sowie zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte und zur Auskunft darüber aufgefordert, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht worden waren. Mit Schreiben vom 23.8.2021 (Anlage K2) erteilte die Beklagte den Prozessbevollmächtigten der Klagepartei die allgemein für alle vom Scraping-Vorfall betroffenen Nutzer geltende Auskunft, dass von dem Scrapingvorfall generell folgende Datenpunkte betroffen waren: 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 auf das Land rückschließen konnten. Beides (Telefonnummer und Land) sei aber gerade nicht von dem jeweiligen F2.-Profil abgerufen worden. Darüber hinaus enthielt das Schreiben vom 23.8.2021 allgemein gehaltene Informationen zu den auf F2. 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.

13
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.

14
Die Klagepartei behauptet, sie sei davon ausgegangen, 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. Aufgrund des oben beschriebenen Vorfalls seien aufgrund der Versäumnisse der Beklagten folgende Daten der Klagepartei gescrapt worden: Telefonnummer, F2.-ID, Namen, Geschlecht, Beziehungsstatus und Arbeitgeber der Klägerseite.

15
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. Dass die beannten Daten in Kombination sogar im sog. Darknet gehandelt werden, vergrößere die Ängste und den stress der Klägerseite. Darüber hinaus gebe es bei der Klagepartei seit dem Vorfall unregelmäßig Kontaktversuche von unbekannten Absendern via SMS und EMail mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks.

16
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 F2.-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.

17
Die Klagepartei meint, die Verstöße der Beklagten gegen die DSGVO bestünden darin, dass die Beklagte als Verantwortlicher (Art. 4 Nr. 7 DSGVO) im Jahr 2019 die Klägerseite betreffende personenbezogene Daten, Art. 4 Nr. 1 DSGVO,

- zum einen ohne Rechtsgrundlage, Artt. 6, 7 DSGVO, und ausreichender Informationen im Sinne von Artt. 13, 14 DSGVO verarbeitet, Art. 4 Nr. 2 DSGVO,

- sowie diese Daten unbefugten Dritten zugänglich gemacht habe und hierbei die Pflichten aus Artt. 5 Abs. lit. a, lit. b, lit. c, lit. f (Grundsätze für die Verarbeitung personenbezogener Date), 25 Abs. 1, Abs. 2 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), 32 (Sicherheit der Verarbeitung), 34 Abs. 1, Abs. 2 (Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person) DSGVO

- sowie Betroffenenrechte der Klägerseite gemäß Artt. 15, 17, 18 DSGVO verletzt habe.

18
Denn das sog. Scraping sei nur deshalb möglich gewesen, weil die Einstellungen zur Sicherheit der Telefonnummer auf F2. so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. F2. 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 F2. 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).

19
Die Klagepartei beantragt zuletzt,

1. Die Beklagte wird verurteilt, 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.

2. Es wird festgestellt, 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.

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

a. personenbezogene Daten der Klägerseite, namentlich Telefonnummer, F2.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,

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 F2.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird;

4. Die Beklagte wird verurteilt, 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.

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

20
Die Beklagte beantragt zuletzt,

die Klage abzuweisen.

21
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 BotErkennung und Captchas verfügt. Diese Schutzmechanismen hätten verhindert, dass die Scraper mittels wahllos generierter Telefonnummern-Listen über den Kontakt-Importer passende F2.-Profile hätten auffinden können, weshalb nicht davon auszugehen sei, dass die Telefonnummern-Listen wahllos erstellt worden seien.

22
Ferner beziehe sich das Schreiben vom 23.8.2021 (Anlage K2) nicht auf das klägerische Nutzerkonto.

23
Die Beklagte ist der Ansicht, die Klageanträge zu 1) bis 3) entsprächen nicht den Bestimmtheitsanforderungen, außerdem sei ein Feststellungsinteresse der Klagepartei für den Klageantrag zu 2) nicht ersichtlich.

24
Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen und – hinsichtlich der durchgeführten Anhörung des Klägers – auf das Protokoll vom 20.04.2023 Bezug genommen.

Entscheidungsgründe

25
Der Klage ist kein Erfolg beschieden.

A.

26
Die Klage ist zulässig.

27
I. Insbesondere ist das Landgericht Regensburg international, örtlich und sachlich zuständig (zum Folgenden etwa LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, GRUR-RS 2023, 1098 Rn. 27 ff.).

28
1. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 EuGVVO. Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann 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 – hier der Kläger – seinen Wohnsitz – hier: in der Bundesrepublik Deutschland – hat.

29
Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DS-GVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

30
2. Das Landgericht Regensburg ist örtlich zuständig. Das folgt zum einen aus Art. 18 Abs. 1 Alt. 2 EuGVVO, zum anderen aus Art. 79 Abs. 2 Satz 2 DS-GVO.

31
3. Die sachliche Zuständigkeit ergibt sich aus §§ 23, 71 Abs. 1 GVG (näher zum Streitwert sub C.).

32
II. Hinsichtlich des Klageantrags Ziffer 2 hat die Klagepartei ein Feststellungsinteresse im Sinne des § 256 Abs. 2 ZPO. 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 Telefonnummer sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleiden könnte (vgl. LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 37 unter Bezugnahme auf LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818, Rn. 39).

33
III. Entgegen der Ansicht der beklagten Partei sind die Klageanträge zu Ziffer 1, Ziffer 2 und Ziffer 3 jeweils hinreichend bestimmt i.S.d. § 253 Abs. 2 ZPO (ausführlich hierzu LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 32 ff., Rn. 35 ff. und Rn. 38 ff.; vgl. auch LG Hamburg Urt. v. 1.3.2023 – 316 O 188/22, GRUR-RS 2023, 3283 Rn. 16 f.).

B.

34
Die ist indes vollumfänglich unbegründet.

35
I. Der Klageantrag zu Ziffer 1 unterliegt der Abweisung.

36
1. Die Klagepartei hat insbesondere keinen Anspruch auf Ersatz immaterieller Schäden gem. Art. 82 Abs. 1 DSGVO.

37
a) Der räumliche und sachliche Anwendungsbereich der DSGVO ist eröffnet (ausführlich hierzu LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 45 ff.).

38
b) Allerdings liegt schon kein Verstoß gegen die DSGVO vor.

39
aa) Ein Verstoß gegen Art. 5 Abs. 1 a) DSGVO liegt nicht vor (zum Folgenden LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 49 ff.).

40
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.

41
Diesen Anforderungen hat die Beklagte nach Auffassung des Gerichts hier genügt. Die Klagepartei selbst hat Screenshots zu den Abläufen und jeweiligen Unterseiten des Internetsauftritts der Beklagten zur Akte gereicht (vgl. S. 9 bis 21 der Klageschrift = Bl. 10 bis 22 d.A.) und die dortigen Screenshots). 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; die erteilten Informationen sind hinreichend verständlich und transparent gestaltet. 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 geradezu vielfältige Einstellungsmöglichkeiten, damit der jeweilige Nutzer die Einstellungen entsprechend seiner spezifischen Bedürfnisse individuell vornehmen kann (LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 50). 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 (LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 51).

42
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. Die Mobilfunknummer hätte jedenfalls nachträglich jederzeit wieder entfernt werden können. Im Ergebnis war die Klagepartei also nicht zur Angabe bzw. zum Belassen ihrer Handynummer auf der Seite von F2. gezwungen (LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 51; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 52).

43
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 F2. finden kann. Auf dem Screenshot auf Seite 12 der Klageschrift (Bl. 13 d.A.) 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 deutlich zu erkennen ist, wie die Einstellung ist und dass man sie ändern kann (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 53). Das Gericht verkennt nicht, dass es sicherlich mit einem gewissen Aufwand, einer gewissen Geduld und gewissem zeitlichem Aufwand verbunden ist, sich durch die betreffenden Hinweise zu klicken und sie sorgfältig zu lesen. Allerdings sind diese jedenfalls bei genauem Lesen verständlich. Im Rahmen der internetspezifischen Gepflogenheiten samt vielfältiger Möglichkeiten und den damit einhergehenden datenschutzrechtlichen Fragestellungen sind umfangreiche Hilfethemen und Einstellungshinweise nicht immer zu vermeiden, sondern vielmehr schlicht angezeigt (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 54).

44
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 F2. 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, dass F2. auch andere Zwecke verfolgt, wie die Finanzierung über Werbung, denn jedenfalls besteht ein (wesentlicher) Zweck auch in der Kommunikation über eine soziale Plattform (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 55; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 51).

bb) Zudem liegt auch kein Verstoß gegen Art. 32 DSGVO bzw. Art. 5 Abs. 1 lit. f) DSGVO vor. Insofern sei auf die nachfolgenden Ausführungen des LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 56 ff. verwiesen (vgl. auch LG Fulda Urt. v. 14.3.2023 – 3 O 73/22, GRUR-RS 2023, 4570 Rn. 29 ff.):

„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).

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 Einstellung zu verhindern. Die Suchbarkeitseinstellungen der Klagepartei waren so eingestellt, dass „alle“ sie anhand ihrer Telefonnummer finden konnten. Diese Einstellung beinhaltet dann aber auch das Finden des F2.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 F2. hochladen. Denn auch Dritte fallen unter den Begriff „alle“. Unstreitig sind einige Daten der Klagepartei von Dritten gescrapt, mithin verarbeitet worden i.S.d. Art. 4 Nr. 2 DSGVO. Allerdings war die Beklagte nicht verpflichtet, diese Daten vor der Verarbeitung durch die Scraper zu schützen, da die Daten nicht unbefugt bzw. unrechtmäßig verarbeitet worden sind. Es handelt sich bei den unstreitig gescrapten personenbezogenen Daten der Klagepartei, nämlich dem Namen, dem Geschlecht und dem Benutzernamen, 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).

Selbst dann, wenn der Klagepartei die Standardeinstellungen auf der Plattform F2. 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 ihr Name, ihr Geschlecht und ihr Benutzername für jedermann öffentlich abrufbar ist. Hierauf wurde sie bereits vor der Registrierung auf F2. 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 Anl. B9. Zudem wurde die Klagepartei unstreitig im Hilfebereich von F2. darüber informiert, dass bestimmte Informationen – nämlich Name, Geschlecht, Nutzername und Nutzer-ID – immer öffentlich zugänglich sind, also jeder, damit auch Personen außerhalb von F2., 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).

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 den Kontaktimporter von F2. 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. Jedenfalls handelt es sich aber nicht um Daten, die von F2. an die Dritten gelangt sind.

Der von den Scrapern unter Nutzung des Kontakt-Importers der Plattform F2. hergestellte Abgleich zwischen der von ihnen hochgeladenen Telefonnummer der Klagepartei mit ihrem Konto stellt zwar 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 der 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 F2. 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).

Selbst dann, wenn der Klagepartei nicht positiv bekannt gewesen sein sollte, dass alle Personen über ihre Telefonnummer ihr F2.-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 F2. 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 F2.-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.

Es widerspricht dem Zweck von F2., 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. 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).“

46
Diesen Ausführungen, die – mutatis mutandis – auch für den vorliegenden Fall Geltung beanspruchen, ist nichts hinzuzufügen.

47
cc) Ob die Beklagte gegen die Vorgaben des Art. 25 DSGVO verstoßen hat, kann dahinstehen (gegen einen solchen Verstoß etwa LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 64 ff.). Denn selbst ein unterstellter Verstoß führte nicht zu einem Schadensersatzanspruch nach Art. 82 DSGVO (zum Folgenden LG Berlin Urt. v. 7.3.2023 – 13 O 79/22, GRUR-RS 2023, 3826 Rn. 62-64).

48
Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen bereits bei der Entwicklung von Produkten, Diensten und Anwendungen sicherzustellen, dass die Anforderungen der DSGVO erfüllt werden („Privacy by Design“). Abs. 2 konkretisiert diese allgemeine Verpflichtung und verlangt, vorhandene Einstellungsmöglichkeiten standardmäßig auf die „datenschutzfreundlichsten“ Voreinstellungen („Privacy by default“) zu setzen. „Datenschutz durch Voreinstellungen“ soll insbesondere diejenigen Nutzer schützen, welche die datenschutztechnischen Implikationen der Verarbeitungsvorgänge entweder nicht zu erfassen in der Lage sind oder sich darüber keine Gedanken machen und sich deshalb auch nicht dazu veranlasst sehen, aus eigenem Antrieb datenschutzfreundliche Einstellungen vorzunehmen, obwohl der Verantwortliche ihnen diese Möglichkeit prinzipiell eröffnet. Die Nutzer sollen keine Änderungen an den Einstellungen vornehmen müssen, um eine möglichst „datensparsame“ Verarbeitung zu erreichen. Vielmehr soll umgekehrt jede Abweichung von den datenminimierenden Voreinstellungen erst durch ein aktives „Eingreifen“ der Nutzer möglich werden. Die Regelung soll die Verfügungshoheit der Nutzer über ihre Daten sicherstellen und sie vor einer unbewussten Datenerhebung schützen. Abs. 2 verlangt aber nicht, dass der Verantwortliche stets die jeweils denkbar datenschutzfreundlichste Voreinstellung trifft. Der Verantwortliche entscheidet vielmehr durch die Festlegung eines bestimmten Verarbeitungszweckes auch über den Umfang der dafür erforderlichen Daten. Dem Wortlaut nach ist daher auch eine besonders datenintensive Voreinstellung mit Abs. 2 vereinbar, wenn der Zweck der Verarbeitung dies erfordert. Vor dem Hintergrund der Schutzrichtung des Abs. 2, den Nutzer vor einer Überrumpelung oder dem Ausnutzen seiner Unerfahrenheit zu schützen, muss der Verantwortliche aber stets sicherstellen, dass die geplante Datennutzung auch für einen nicht-technikaffinen Nutzer hinreichend transparent ist (LG Paderborn, Urteil vom 13. Dezember 2022 – 2 O 212/22, juris Rn. 120-122 m.w.N.; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22, juris Rn. 114 m.w.N.).

49
Ob die Beklagte diesen Anforderungen genügt, kann hier offen bleiben (vgl. zum Folgenden LG Paderborn, Urteil vom 13. Dezember 2022 – 2 O 212/22, juris Rn. 128; LG Paderborn, Urteil vom 19. Dezember 2022 – 3 O 99/22, juris Rn. 120). Allein aus einem Verstoß gegen Art. 25 DSGVO kann wegen seines organisatorischen Charakters ein Anspruch nach Art. 82 Abs. 1 DSGVO nicht begründet werden (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DSGVO Art. 25 Rn. 31). Die Vorschrift entfaltet bereits vor dem eigentlichen Beginn der Datenverarbeitung ihren Regelungscharakter. Zu diesem, einer tatsächlichen Datenverarbeitung vorgelagerten Zeitpunkt entfaltet die DSGVO jedoch nach Art. 2 Abs. 1 DSGVO noch keine Wirkung. Die Anwendbarkeit der DSGVO setzt vielmehr eine tatsächliche Verarbeitung personenbezogener Daten voraus (vgl. Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DSGVO kommt daher nur in Betracht, wenn weitere Verstöße gegen die DSGVO vorliegen (vgl. Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3). Das ist hier indes, wie vorstehend ausgeführt, gerade nicht der Fall (zum Vorstehenden LG Berlin Urt. v. 7.3.2023 – 13 O 79/22, GRUR-RS 2023, 3826 Rn. 62-64).

50
dd) Zudem besteht kein Schadenersatzanspruch infolge eines etwaigen Verstoßes gegen Art. 33 DSGVO.

51
Zwar wird nicht verkannt, dass ein derartiger Verstoß grundsätzlich eine Schadensersatzpflicht gem. Art. 82 DSGVO begründen kann (vgl. Kühling/Buchner/Jandt, 3. Aufl. 2020, DS-GVO Art. 33 Rn. 27 f.).

52
Gem. Art. 33 Abs. 1 S. 1 DSGVO hat im Falle einer Verletzung des Schutzes personenbezogener Daten der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Zwar ist unstreitig, dass der zuständigen Datenschutzbehöre „Irish Data Commission“ der Scraping-Vorfall nicht gemeldet worden ist, aber dies führt nicht zu einem Entschädigungsanspruch.

53
Insofern ist zunächst zu bemerken, dass der Beklagten aus den oben ausgeführten Gründen ohnehin kein Datenschutzverstoß anzulasten ist; daher musste sie den hier streitgegenständlichen sog. Scraping-Vorfalll auch nicht melden (übereinstimmend LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 67; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 69).

54
Dessen ungeachtet fehlt es jedenfalls an der erforderlichen Kausalität zwischen Rechtsverstoß und Schaden. Für den vom Kläger vorgetragenen Schaden ist es ohne Relevanz, ob der Scraping-Vorfall pflichtgemäß gemeldet wurde oder nicht. Die Daten waren ohnehin schon durch Dritte gesammelt worden und es sind keine Anhaltspunkte ersichtlich, dass auf Grund der Meldung an die Aufsichtsbehörde die Folgen irgendwie hätten reduziert werden können (LG Itzehoe Urt. v. 9.3.2023 – 10 O 87/22, GRUR-RS 2023, 3825 Rn. 66-68).

55
ee) Auch eine etwaige Verletzung der Auskunftspflicht (vgl. Art. 15 DSGVO) in Bezug auf das Auskunftsersuchen der Klagepartei (Anlage K1) vermag keinen Anspruch der Klagepartei aus Art. 82 DSGVO zu begründen. Denn selbst eine unterstellte Auskunftspflichtverletzung konnte schon in zeitlicher Hinsicht nicht für den Scrapingvorfall und damit auch nicht für die behaupteten, dadurch verursachten Beeinträchtigungen der Klagepartei kausal werden (LG Berlin Urt. v. 7.3.2023 – 13 O 79/22, GRUR-RS 2023, 3826 Rn. 61).

56
c) Ungeachtet eines etwaigen Verstoßes gegen die DSGVO fehlt es jedenfalls (auch) an einem ersatzfähigen Schaden i.S.d. Art. 82 Abs. 1 DSGVO.

57
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, 43. Ed. 1.2.2023, 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, 43. Ed. 1.2.2023, DS-GVO Art. 82 Rn. 31). Die Pflicht zur Erstattung immaterieller Schäden ist daher nicht auf schwere Schäden beschränkt (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 74 m.w.N.). Bestätigt wurde dies jüngst durch eine Entscheidung des EuGH, wonach der Ersatz eines immateriellen Schadens im Sinne des Art. 82 Abs. 1 DSGVO nicht davon abhängig gemacht werden kann, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (EuGH, Urteil vom 04.05.2023, C-300/21, Celex-Nr. 62021CJ0300, Rn. 43 ff. – juris).

58
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 (Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 17). 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 (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 75 m.w.N.).

59
Ein genereller Ausschluss von Bagatellschäden ist im Lichte dieser Erwägungsgründe nicht vertretbar (vgl. LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 72 ff.). 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 Rn. 38; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 74).

60
Allein eine etwaige Verletzung des Datenschutzrechts als solche – die das Gericht ohnehin nicht festzustellen vermochte – begründete 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 (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 77). 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 (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 77 m.w.N.).

61
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, um bloß abstrakte, nicht wirklich eingetretene Beeinträchtigungen auszuschließen (LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 76; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 78).

62
Diese Grundsätze erfuhren jüngst Bestätigung durch eine Entscheidung des EuGH; danach reicht der bloße Verstoß gegen Bestimmungen der DSGVO nicht aus, um einen Schadensersatzanspruch zu begründen (EuGH, Urteil vom 04.05.2023, C-300/21, Celex-Nr. 62021CJ0300, Rn. 28-42 – juris). Denn die gesonderte Erwähnung eines „Schadens“ und eines „Verstoßes“ in Art. 82 Abs. 1 DSGVO wäre überflüssig, wenn der Gesetzgeber davon ausgegangen wäre, dass ein Verstoß gegen die Bestimmungen der DSGVO für sich allein in jedem Fall ausreichend wäre, um einen Schadenersatzanspruch zu begründen (EuGH, Urteil vom 04.05.2023, C-300/21, Celex-Nr. 62021CJ0300, Rn. 34 – juris). Ferner führt der EuGH aus (EuGH, Urteil vom 04.05.2023, C-300/21, Celex-Nr. 62021CJ0300, Rn. 35-37 – juris):

„Die vorstehende Wortauslegung [wird] durch den Zusammenhang bestätigt, in den sich diese Bestimmung einfügt.

Art. 82 Abs. 2 DSGVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt nämlich die drei Voraussetzungen für die Entstehung des Schadenersatzanspruchs, nämlich eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden.

Diese Auslegung wird auch durch die Erläuterungen in den Erwägungsgründen 75, 85 und 146 der DSGVO bestätigt. Zum einen bezieht sich der 146. Erwägungsgrund der DSGVO, der speziell den in Art. 82 Abs. 1 dieser Verordnung vorgesehenen Schadenersatzanspruch betrifft, in seinem ersten Satz auf „Schäden, die

einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht". Zum anderen heißt es in den Erwägungsgründen 75 und 85 der DSGVO, dass „[d]ie Risiken … aus einer Verarbeitung personenbezogener Daten hervorgehen [können], die zu einem … Schaden führen könnte" bzw. dass eine „Verletzung des Schutzes personenbezogener Daten … einen … Schaden … nach sich ziehen [kann]". Daraus ergibt sich erstens, dass der Eintritt eines Schadens im Rahmen einer solchen Verarbeitung nur potenziell ist, zweitens, dass ein Verstoß gegen die DSGVO nicht zwangsläufig zu einem Schaden führt, und drittens, dass ein Kausalzusammenhang zwischen dem fraglichen Verstoß und dem der betroffenen Person entstandenen Schaden bestehen muss, um einen Schadenersatzanspruch zu begründen."

63
Dem wird beigetreten.

64
Gemessen an diesen Grundsätzen hat die Klagepartei schon keine spürbare Beeinträchtigung von persönlichen Belangen dargelegt, für die überhaupt Anhaltspunkte bestehen, dass sie kausal auf den hier streitgegenständlichen Scraping-Vorfall zurückzuführen sein könnte.

65
Die Klagepartei trägt – im Rahmen ihrer standardisierten Klageschrift – vor, einen erheblichen Kontrollverlust über ihre Daten erlitten und Sorge vor Missbrauch ihrer Daten zu haben. Seit dem Scraping-Vorfall 2019 und Veröffentlichung im April 2021 sei es ferner zu einem Anstieg von unerwünschten Anrufen, SMS und E-Mails gekommen.

66
Als Schaden i.S.d. DSGVO kann nicht das vom Kläger behauptete erhöhte Spam-SMS-Aufkommen gewertet werden. Es ist schon zweifelhaft, ob diese Behauptung überhaupt ausreichend konkret dargelegt ist, denn die Behauptung eines immensen Spam-Aufkommens ist äußerst pauschal. Für einen hinreichend substantiierten Vortrag bedarf es der Darstellung bis zu welchem Zeitpunkt wieviele solcher Nachrichten auf dem Handy eingegangen sind und ab wann sich dieses in welcher Form verändert hat (LG Itzehoe Urt. v. 9.3.2023 – 10 O 87/22, GRUR-RS 2023, 3825 Rn. 75).

67
Letztlich kann dies dahinstehen, denn es ist bereits der Kausalzusammenhang zwischen diesem erhöhten Spam-Aufkommen und dem Scraping-Vorfall klägerseits nicht nachgewiesen worden. Denn unerwünschte SMS und Anrufe erhalten gerichtsbekannt auch Personen, die keinen F2.-Account haben und dort ihre Telefonnummer deshalb nicht hinterlegt haben (LG Münster Urt. v. 7.3.2023 – 02 O 54/22, GRUR-RS 2023, 4183 Rn. 57; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 80; LG Itzehoe Urt. v. 9.3.2023 – 10 O 87/22, GRUR-RS 2023, 3825 Rn. 75).

68
Ebenso wenig reichen – eingedenk der oben dargelegten Grundsätze – der vom Kläger mit formelhaften Wendungen vorgetragene Kontrollverlust über seine persönlichen Daten und die damit verbundene Unsicherheit aus, um einen Schaden i.S.d. Art. 82 Abs. 1 DSGVO zu begründen. Diese angeblichen Ängste haben sich in der mündlichen Verhandlung indes nicht bestätigt. Dies belegt zum einen die Tatsache, dass die Klagepartei trotz des laufenden Verfahrens nicht für nötig befunden hat, die entsprechenden Suchbarkeitseinstellungen zu ändern; vielmehr wurden diese ausweislich der Angaben der Klagepartei im Rahmen seiner informatorischen Anhörung erst einen (!) Tag vor der mündlichen Verhandlung angepasst. Die schriftsätzlich vorgetragenen Ängste infolge des angeblichen Kontrollverlustes sind im Lichte dieses Verhaltens nicht plausibel (vgl. auch LG Bielefeld Urt. v. 19.12.2022 – 8 O 182/22, GRUR-RS 2022, 38375 Rn. 32). Zum anderen gab der Kläger ohnehin nur an, dass das ganze „nicht direkt" eine Belastung sei, sondern nur „extrem nervig". Ungeachtet des unbelegten Kausalzusammenhangs vermögen diese bloßen Unannehmlichkeiten keinen Ersatzanspruch nach Art. 82 Abs. 1 DSGVO auszulösen (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 77; i.E. auch LG Bonn Urt. v. 8.3.2023 – 17 O 165/22, GRUR-RS 2023, 3854 Rn. 41 ff.).

69
2. Ferner 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

(vgl. hierzu etwa Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 67). Denn auch bei der Annahme eines Nebeneinanders hat die Klagepartei mangels restitutionsfähigen Schadens keinen Schadensersatzanspruch gegen die Beklagte, weder aus §§ 280 Abs. 1, 253 Abs. 2 BGB noch aus einer anderen nationalen Schadensersatznorm (vgl. LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 87). Auf die obigen Ausführungen wird Bezug genommen.

70
II. Der mit dem Klageantrag zu Ziffer 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.

71
III. Ebenso unbegründet ist der Klageantrag zu Ziffer 3.

72
1. Mit dem Klageantrag zu Ziffer 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.

73
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. Eine Zuwiderhandlung der Beklagten in der Vergangenheit ist nach den obigen Ausführungen weder zu erkennen, noch für die Zukunft zu befürchten.

74
Hier sind lediglich Daten von der F2.-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 (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 90-92).

75
2. Mit dem Klageantrag zu Ziffer 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.

76
Auch hier fehlt es bereits an einem Verstoß der Beklagten, der überhaupt zu einem Unterlassungsanspruch führen könnte, selbst wenn man Art. 6 DSGVO als Schutzgesetz im Sinne des § 823 Abs. 2 BGB ansieht.

77
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. 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 lit.

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 (s. auch die Screenshots in der Klageschrift) durchaus nachvollziehbar (LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 93-95; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 100).

78
IV. Auch der mit dem Klageantrag zu Ziffer 4 geltend gemachte Auskunftsanspruch unterliegt der Abweisung. Mit dem Klageantrag zu Ziffer 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 KontaktImporttools erlangt werden konnten.

79
Die Klagepartei hat hinsichtlich der begehrten Auskunft keinen Auskunftsanspruch gegen die Beklagte aus Art. 15 DSGVO (mehr).

80
Dieser Auskunftsanspruch ist 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 Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 96-98; LG Essen Urt. v. 10.11.2022 – 6 O 111/22, GRUR-RS 2022, 34818 Rn. 101).

81
V. Mangels Hauptanspruch besteht kein Anspruch auf Ersatz der vorgerichtlichen Rechtsanwaltskosten; selbiges gilt hinsichtlich der geltend gemachten Zinsansprüche.

C.

82
1. Die Kostenentscheidung fußt auf § 91 Abs. 1 ZPO.

83
2. Der Ausspruch zur vorläufigen Vollstreckbarkeit ergibt sich aus § 708 Nr. 11 (vgl. allgemein Dölling, NJW 2014, 2468, 2469, wonach – faustformelartig – davon ausgegangen werden könne, dass erst bei einem Streitwert von über 8000 Euro die für den Beklagten vollstreckbaren Kosten die Wertgrenze von 1500 Euro übersteigen) und § 711 ZPO.

84
3. Der Streitwert war auf 7.000,00 EUR festzusetzen (ebenso LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, GRUR-RS 2023, 1098 Rn. 116 unter Berufung auf OLG Stuttgart, Beschluss vom 03.01.2023 – 4 AR 4/22; LG Ellwangen Urt. v. 25.1.2023 – 2 O 198/22, GRUR-RS 2023, 1146 Rn. 125 ff.; LG Heilbronn Urt. v. 3.3.2023 – 1 O 78/22, GRUR-RS 2023, 3278 Rn. 77).

85
a) Der Streitwert für den Klagantrag Ziffer 1 ergibt sich aus dem vom Kläger vorgestellten (Mindest-)Schadenersatzbetrag in Höhe von 1.000,00 € (OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, Rn. 22, juris).

86
b) Soweit der Kläger mit dem Klagantrag Ziffer 2 festgestellt haben möchte, dass die Beklagte verpflichtet ist, ihm (auch) alle künftigen Schäden zu ersetzen, die ihm durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten entstanden sind und/oder noch entstehen werden, so ist diesem Antrag ein eigener wirtschaftlicher Wert beizumessen. Dieser orientiert sich grundsätzlich an den Vorstellungen des Klägers zum Klagantrag Ziffer 1, ist aber nur mit einem Bruchteil zu bemessen, wobei 50% und damit ein

Betrag in Höhe von 500,00 € angemessen erscheint (OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, Rn. 23, juris; LG Stuttgart und LG Ellwangen jeweils a.a.O.).

87

c) Der Streitwert der Unterlassungsanträge (Ziffer 3) ist als nichtvermögensrechtlicher Streitgegenstand anhand des betroffenen Interesses des Klägers zu bestimmen, wobei gemäß § 48 Abs. 2 Satz 1 GKG die Umstände des Einzelfalls zu beachten sind. Dabei ist davon auszugehen, dass in Anlehnung an § 23 Abs. 3 S. 2 RVG bei mangelnden genügenden Anhaltspunkten für ein höheres oder geringeres Interesse von einem Streitwert von 5.000 € auszugehen ist. Auch wenn bei der Bemessung des Streitwerts das Gesamtgefüge der Bewertung nichtvermögensrechtlicher Streitgegenstände nicht aus den Augen verloren werden darf (vgl. BGH, Beschluss vom 26.11.2020; III ZR 124/20 Rn. 11), erscheint es unter Berücksichtigung aller Umstände des vorliegenden Einzelfalls (vgl. § 48 Abs. 2 Satz 1 GKG) angemessen, auf die Gedanken der allgemeinen Wertvorschrift des § 23 Abs. 3 S. 2 RVG zurückzugreifen. Das Gericht begreift die beiden Unterlassungsanträge im Übrigen wertmäßig als Einheit, weil sie letztlich auf dasselbe Ziel gerichtet sind, die Beklagte zu einem besseren Schutz der überlassenen Daten zu verpflichten. Insgesamt sind die Unterlassungsanträge sub Ziffer 3 damit mit 5.000,00 EUR zu bewerten (zum Vorstehenden OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, Rn. 26-28, juris).

88

d) Der mit Klagantrag Ziffer 4 geltend gemachte Auskunftsanspruch ist mit 500,00 EUR zu bewerten (insofern übereinstimmend LG Stuttgart Urt. v. 26.1.2023 – 53 O 95/22, GRUR-RS 2023, 1098 Rn. 116; LG Ellwangen Urt. v. 25.1.2023 – 2 O 198/22, GRUR-RS 2023, 1146 Rn. 125; LG Aachen Urt. v. 10.2.2023 – 8 O 177/22, GRUR-RS 2023, 2621 Rn. 28; LG Görlitz Endurteil v. 27.1.2023 – 1 O 101/22, BeckRS 2023, 1148 Rn. 50; LG Krefeld Urt. v. 22.2.2023 – 7 O 113/22, GRUR-RS 2023, 2539; LG Heilbronn Urt. v. 3.3.2023 – 1 O 78/22, GRUR-RS 2023, 3278 Rn. 77; letztlich offen lassend OLG Stuttgart, Beschluss vom 3. Januar 2023 – 4 AR 4/22 –, Rn. 30, juris, wonach dieser Auskunftsanspruch wertmäßig weitgehend in den Klaganträgen Ziffer 1 und 2 aufgehe und – wenn überhaupt – nur mit einem Wert in überschaubaren Umfang berücksichtigt werden könne).