LG Memmingen, Endurteil v. 16.02.2023 – 24 O 913/22

Titel:

Erfolglose Schadensersatzklage wegen öffentlich zugänglicher Nutzerdaten

Normenketten:

DSGVO Art. 4, Art. 5, Art. 13, Art. 14, Art. 15, Art. 34, Art. 82

ZPO § 253, § 256, § 287, § 291

Leitsätze:

1. In Anbetracht der Vorgaben der DSGVO und der damit verbundenen vielseitigen Informationspflichten bestehen naturgemäß vielfältige Einstellungsmöglichkeiten betreffend die Verwendung personenbezogener Daten des Nutzers einer Social-Media-Plattform, sodass jeder Nutzer die Einstellungen individuell entsprechend seiner spezifischen Bedürfnisse vornehmen kann. (Rn. 53) (redaktioneller Leitsatz)

2. Der Betreiber einer Social-Media-Plattform ist nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils eines seiner Nutzer aufgrund seiner selbst gewählten Einstellung zu verhindern. (Rn. 61) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatz, Schadensersatzanspruch, Verletzung, Schmerzensgeld, Beschwerde, Unterlassungsanspruch, Ersatzpflicht, Internet, Streitwert, Unterlassung, Ermessen, Einstellung, Anspruch, Auskunft, Kosten des Rechtsstreits, Ermessen des Gerichts, Vorbringen der Parteien

Fundstelle:

GRUR-RS 2023, 4562

Tenor

1. Die Klage wird abgewiesen.

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

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

Beschluss

Der Streitwert wird auf 11.000,00 € festgesetzt.

Tatbestand

1
Die Parteien streiten um Ansprüche auf Schadensersatz, Unterlassung und Auskunft wegen behaupteter Verletzung von Persönlichkeitsrechten, Grundrechten und Grundfreiheiten, insbesondere um Verletzung der Rechte auf Schutz personenbezogener Daten.

2
Die Beklagte betreibt die Social Media Plattform „www.f..com“, welche es den Nutzern der Plattform ermöglicht, ein persönliches Profil zu erstellen, wobei der Nutzer hier Angaben zu seiner Person machen kann, Bilder hochladen kann, seine Interessen eingeben kann, etc. In dem von der Beklagten vorgegebenen Rahmen kann der Nutzer entscheiden, inwiefern andere Nutzer auf seine angegebenen Daten Zugriff nehmen können.

3
Der Kläger nutzt die von der Beklagten betriebene Social Media Plattform, um mit Freunden zu kommunizieren und mit anderen Nutzern im Netz in Kontakt zu treten.

4
Vermutlich ab 2018, jedenfalls ab 2019 sammelten Dritte unter Nutzung automatisierter Verfahren eine Vielzahl der auf der Plattform der Beklagten verfügbaren öffentlichen Informationen (sog. Scraping). Beim

Scraping werden typischerweise öffentlich verfügbare, also öffentlich zugängliche Daten gesammelt, wobei Funktionen einer Website verwendet werden, die für ordnungsgemäße Nutzer entworfen wurden und bei diesen beliebt sind. Scraping unterscheidet sich insofern von der zulässigen Nutzung einer Website oder App, dass die Scraper Verfahren einsetzen, um in großem Umfang Daten zu sammeln.

5
Das Sammeln von Daten über diese automatisierten Methoden ist durch die Nutzungsbedingungen der Beklagten verboten.

6
Das Scraping lief dergestalt ab, dass die Scraper Listen mit möglichen Telefonnummern in den Kontakt-Importer der Plattform hochluden, um festzustellen, ob die hochgeladenen Telefonnummern mit einem Konto eines Nutzers verbunden sind. Der Kontakt-Importer gab, sofern eine der hochgeladenen Telefonnummern mit dem Konto eines Nutzers, der seine Telefonnummer bereitgestellt und die standardmäßig voreingestellten Suchbarkeits-Einstellungen nicht geändert hatte, verknüpft war, diese Information, also den Umstand der Verknüpfung von Telefonnummer und Konto, an die Scraper. Die Scraper fügten sodann den öffentlich zugänglichen Informationen aus dem betreffenden Profil des Nutzers die mit dem Konto verknüpfte Telefonnummer hinzu.

7
Jedenfalls seit Anfang April 2021 ist öffentlich bekannt, dass es zu dem Scraping Vorfall gekommen war und dass die abgegriffenen Daten von ca. 533 Millionen F.-Nutzern aus 106 Ländern im Internet öffentlich verbreitet werden. Hierzu gehörten auch die vom Kläger auf seinem Profil öffentlich zugänglich gemachten Informationen und die mit seinem Konto verknüpfte Telefonnummer. Die Daten der Klägerseite wurden im Internet auf Seiten, die illegale Aktivitäten begünstigen, veröffentlicht, beispielsweise auf der Seite raidforums.com.

8
Strittig ist, ob die Veröffentlichung der Daten selbst bereits vorher erfolgt ist oder auch erst ab April 2021 stattfand.

9
Bei dem Anlegen eines F.-Profils muss der künftige Nutzer Datenschutz- und Cookie Richtlinien zustimmen. Diese sind durch eine Verlinkung getrennt abrufbar. Nach der Anmeldung sind zunächst die Vor- bzw. Standardeinstellungen aktiv. Demnach können „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse „finden“. Ebenso ist für alle Informationen, die ein Nutzer in sein Profil einträgt, standardmäßig „öffentlich“ als Voreinstellung ausgewählt.

10
Der Nutzer kann diese Einstellungen individuell verändern und sich im Hilfebereich einlesen, wie F. insbesondere die Mobilfunknummer verwendet. Die Angabe der Mobilfunknummer ist nicht zwingend. Entscheidet sich ein Nutzer aber diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Die Grundeinstellung lautet auch insoweit zunächst „alle“.

11
Neben den gewöhnlichen Funktionen auf der F.-Website wird von der Beklagten noch eine Messenger-App betrieben, die als Schnittstelle für die F.-Applikation auf Mobilgeräten arbeitet und eine Messenger-Funktion für Nutzer darstellt. Nutzer melden sich dafür mit ihren bestehenden F.-Profilen an. Die Messenger-App und die gewöhnlichen Funktionen von F. sind über denselben Zugang zum Account verknüpft. Auch in dieser App können separate Sicherheitseinstellungen vorgenommen werden. Diese Einstellungen werden unabhängig von den Einstellungen des Accounts im sonstigen F.-Dienst vorgenommen. Es kann separat eingestellt werden, ob Telefonkontakte mit dem F.-Dienst synchronisiert werden sollen.

12
Mit E-Mail vom 12.02.2022 forderte die Klageseite die Beklagte zur Zahlung von 500 € Schadensersatz nach Art. 82 Abs. 1 DSGVO auf sowie zur Unterlassung zukünftiger Zugänglichmachung der Klägerdaten an unbefugte Dritte. Zudem forderte die Klageseite die Beklagte auf, Auskunft darüber zu geben, welche konkreten Daten im April 2021 veröffentlicht wurden.

13
Die Beklagte wies die geltend gemachten Ansprüche zurück.

14
Die Klageseite behauptet, seine Daten auf „Privat“ gestellt zu haben. Bei der Sichtbarkeit seiner Telefonnummer habe er die Einstellung „nur ich“ gewählt. Das „scrapen“ sei nur möglich gewesen, weil die Beklagte keinerlei Sicherheitsmaßnahmen vorgehalten habe, um ein Ausnutzen des bereitgestellten Tools zu verhindern und weil die Einstellungen zur Sicherheit der Telefonnummer auf F. so undurchsichtig und kompliziert gestaltet seien, dass ein Nutzer tatsächlich keine sicheren Einstellungen erreichen könne. 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 F. preisgäben. Die neben der von der Beklagten betriebene Website noch betriebene Messenger-App als Schnittstelle für die F.-Applikation auf Mobilgeräten und die besagte Website seien miteinander verknüpft. Bei erster Anmeldung fragte der Messenger-Dienst die Synchronisierung bereits an, ohne über die Risiken der Verwendung aufzuklären. Es könne separat auf der App eingestellt werden, ob eine Synchronisierung erfolgen solle, ohne über Risiken aufzuklären. Insgesamt gebe es drei verschiedene Einstellungsmöglichkeiten zur Verwendung der Telefonnummer, über die ein Nutzer keine transparenten Informationen für eine Gewährleistung einer effektiven digitalen Sicherheit erhalte. Diese Sicherheitslücke werde seit 2019 ausgenutzt, ohne dass die Beklagte etwas dagegen unternehme. Der Kläger behauptet weiter, er habe so ungewollt die Kontrolle über seine Daten verloren und werde bis heute wiederholt ungewollt von Unbekannten via E-Mail und SMS kontaktiert.

15
Nur aufgrund der fehlenden Sicherheitsvorkehrungen der Beklagten hätten auch seine Daten auf sog. Hackerforen wie „raidforums.com“ geraten können. Dass eine automatisierte Massenabfrage möglich war, stelle eine Sicherheitslücke dar, für die die Beklagte einzustehen habe.

16
Die Klageseite ist der Ansicht, die Beklagte verstoße gegen die DSGVO, indem sie ohne ausreichende Grundlage im Sinne der Art. 6 und 7 DSGVO Informationen im Sinne von Art. 13, 14 DSGVO verarbeite, Daten unbefugten Dritten zugänglich mache sowie seine Rechte aus Art. 15, 17 und 18 DSGVO verletze und Seine Betroffenenrechte gemäß Art. 15, 17 und 18 DSGVO verletzte.

17
Der Kläger beantragte daher,

1. die Beklagte zu verurteilen, an ihn 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, sowie

2. festzustellen, dass die Beklagte verpflichtet ist, ihm alle künftigen Schäden zu ersetzen, die dem Kläger 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, sowie

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

a. personenbezogenen Daten der Klägerseite, namentlich Telefonnummer, F.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 F.-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird, und

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.

18
Die Beklagte beantragte,

die Klage abzuweisen.

19
Die Beklagte führt aus, der Sachverhalt und Vorgang zum sog. Scraping sei falsch wiedergeben. Insbesondere sei zu berücksichtigen, dass die Telefonnummern nicht von den F.-Profilen stammen, sondern die Telefonnummern von den Scrapern generiert wurden, um diese dann im Rahmen der Telefonnummernaufzählung zu nutzen. Der klägerische Vortrag beruhe insgesamt auf einem Missverständnis zum Scraping als solchen. Es sei zudem unschlüssig und unsubstantiiert, welche Daten des Klägers genau gescrapt worden sein sollen. Es seien weder Geschlecht, E-Mail-Adresse, Wohnort, Geburtsdatum und Beziehungsstatus in den durch Scraping abgerufenen Daten enthalten.

20
Ein Datenschutzverstoß liege auf Beklagtenseite, ebenso wie ein Unterlassen des Schließens einer technischen Schwachstelle, nicht vor. Es seien lediglich öffentlich einsehbare Daten durch Dritte in Form des Scraping abgerufen worden, was nach den Nutzungsbedingungen von F. untersagt gewesen sei und auch weiterhin untersagt sei. Die Suchbarkeit der Klagepartei sei seit dem 01.07.2016 bis mindestens zum Ende des relevanten Zeitraums auf „Alle“ eingestellt gewesen.

21
Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der F.-Plattform gestanden. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeits-Einstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem F.-Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe der Kläger jederzeit anpassen können.

22
Im Übrigen sei keinerlei Zusammenhang zwischen etwaigen Phishing-Nachrichten und dem Scraping-Sachverhalt erkennbar. Die vorgetragenen Umstände zu den Folgen seien pauschal und daher nicht nachprüfbar.

23
Die Beklagte ist daher der Auffassung, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. Die Beklagte meint, das Scraping stelle bereits keinen Datenschutzverstoß dar. Es fehle an einer Verletzung der Sicherheit, da „lediglich“ öffentlich zugängliche Profilinformationen des Klägers abgerufen und auch keine spezifischen Sicherheitsmaßnahmen oder Zugriffsberechtigungen umgangen oder überwunden wurden. Eine unbefugte Offenlegung von oder Zugang zu den klägerischen Daten sei nicht gegeben. Der Beklagten könne zudem keine Sicherheitslücke zur Last gelegt werden, da die hergestellte Verknüpfung zwischen der Telefonnummer des Klägers und seinem Nutzerkonto lediglich auf die seinerzeitige Suchbarkeitseinstellung des Klägers zurückzuführen ist.

24
Darüber hinaus fehle es an einem immateriellen Schaden. Mangels Verstoßes gegen die DSGVO sei der (ohnehin unzulässige) Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr.

25
Die Klageschrift vom 01.07.2022 ging beim Landgericht Memmingen am 05.07.2022 ein.

26

Für das weitere Vorbringen der Parteien wird auf die in der Akte befindlichen Schriftsätze samt Anlagen sowie auf das Protokoll der mündlichen Verhandlung vom 26.01.2023 Bezug genommen.

Entscheidungsgründe

27
Die zulässige Klage ist unbegründet.

I.

28
1. Das Landgericht Memmingen ist international, sachlich und örtlich zuständig.

29
a) Die internationale Zuständigkeit ergibt sich aus Art. 6 Abs. 1, Art. 18 Abs. 1 Alt. 2 EuGVVO. Gemäß Art. 18 Abs. 1 Alt. 2 EuGVVO kann ein Verbraucher gegen seinen Vertragspartner vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat, klagen. Gemäß Art. 17 Abs. 1 EuGVVO ist der Kläger als Verbraucher anzusehen. Zwischen den Parteien ist unstrittig, dass der Kläger mit der Beklagten einen Nutzungsvertrag über die Nutzung der Social Media Plattform F. zu privaten Zwecken geschlossen hat.

30
Eine entgegenstehende ausschließliche Zuständigkeit nach Art. 24 EuGVVO ist nicht gegeben.

31
b) Das Landgericht Memmingen ist nach §§ 23, 71 Abs. 1 GVG sachlich und nach Art. 18 Abs. 1 2. Alt EuGVVO örtlich zuständig.

32
2. Die Klage ist zulässig.

33
a) Der unbestimmte Klageantrag in Ziffer 1) der Klage führt nicht zu einer Unzulässigkeit. Vorliegend ist das Stellen eines unbezifferten Klageantrags ausnahmsweise zulässig, da die Bemessung der Höhe des Schmerzensgeldes in das Ermessen des Gerichts gestellt ist. Ein Verstoß gegen den in § 253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach § 287 ZPO oder vom billigen Ermessen des Gerichts abhängig ist. Die nötige Bestimmtheit soll hier dadurch erreicht werden, dass der Kläger in der Klagebegründung die Berechnungs- bzw. Schätzgrundlagen umfassend darzulegen und die Größenordnung seiner Vorstellungen anzugeben hat (vgl. Greger in Zöller, 34. Auflage 2022, ZPO, § 253 Rn. 14). Diese Voraussetzungen liegen hier vor. Der Kläger hat sowohl in der Klagebegründung als auch bereits in dem Klageantrag zu 1) einen Mindestbetrag von 1.000,- € angegeben.

34
Entgegen der Ansicht der Beklagtenseite ist vorliegend lediglich ein Lebenssachverhalt zu betrachten, sodass sich hieraus keine Unbestimmtheit des Klageantrags Ziffer 1) ergibt. Zu beurteilen ist einzig und allein, ob die Beklagte hinreichende Sicherheitsvorkehrungen getroffen hat beziehungsweise ihre Nutzer unzureichend informiert hat.

35
b) Hinsichtlich des Klageantrags Ziffer 2) hat die Klageseite das Feststellungsinteresse hinreichend dargelegt.

36
Das rechtliche Interesse des Klägers an einer alsbaldigen Feststellung der Ersatzpflicht der Beklagten im Sinne des § 256 Abs. 1 ZPO ergibt sich daraus, dass sich der anspruchsbegründende Sachverhalt zur Zeit der Klageerhebung noch in der Entwicklung befand. Bei Klageerhebung war erst ein Teil des Schadens entstanden. Die Entstehung weiteren Schadens war nach dem Vorbringen des Klägers noch zu erwarten. In einer derartigen Fallgestaltung ist die Feststellungsklage nach der ständigen Rechtsprechung des Bundesgerichtshofs insgesamt zulässig (vgl. BGH, Beschluss vom 06.03.2012 – VI ZR 167/11 m.w.N.). Ein Feststellungsinteresse ist nur dann zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger

Würdigung kein Grund besteht, mit dem Eintritt eines Schadens wenigstens zu rechnen (vgl. BGH, Beschluss vom 09. 01.2007 VI ZR 133/06).

37
Bei den von Klageseite behaupteten Verstößen mit der behaupteten unkontrollierten Nutzung der Daten ist bei verständiger Würdigung der Umstände nach Ansicht der Kammer jedenfalls nicht gänzlich ausgeschlossen, dass irgendein materieller oder immaterieller Schaden infolge der Veröffentlichung seiner Daten entstehen könnte. Insgesamt war das erforderliche Feststellungsinteresse daher vorhanden.

38
c) Auch der Klageantrag Ziffer 3) weist nach Ansicht der Kammer die erforderliche Bestimmtheit auf. Eine auslegungsbedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (vgl. BGH, Urt. v. 26.1.2017 – I ZR 207/14 m.w.N.). Eine auslegungsbedürftige Formulierung ist insbesondere dann hinzunehmen, wenn der Antrag nicht hinreichend konkreter gefasst werden konnte (vgl. BGH aaO).

39
Dies ist nach Auffassung des Gerichts der Fall. Selbst bei einer Benennung derzeitiger technischer Schutzvorkehrungen besteht die Gefahr in Anbetracht der technischen Weiterentwicklung, dass die aktuellen Vorkehrungen veralten, sodass der Kläger erneut klagen müsste. Dies stünde letztlich einem effektiven Rechtsschutz entgegen.

II.

40
Die zulässige Klage ist jedoch unbegründet.

41
Der Klageseite stehen die von ihr geltend gemachten Ansprüche nicht zu.

42
1. Ein Anspruch auf Ersatz des immateriellen Schadens in der geltend gemachten Höhe von 1.000 € steht der Klagepartei nicht zu.

43
a) Der Anspruch auf Ersatz des immateriellen Schadens ergibt sich nicht aus Art. 82 DSGVO.

44
aa) Der Anspruch ergibt sich bereits nicht aus Art. 82 DSGVO, da der Schutzbereich nicht eröffnet ist.

45
Art. 82 DSGVO erfasst Verstöße, welche durch eine nicht der Verordnung der DSGVO entsprechende Verarbeitung (von Daten) entstanden sind, vgl. Art. 82 Abs. 2 DSGVO. Erforderlich ist daher von vornherein eine Verarbeitung von Daten im Sinne von Art. 4 Nr. 2 DSGVO. Gemäß Art. 4 Nr. 2 DSGVO handelt es sich bei um jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

46
Soweit die Klageseite der Beklagten Verstöße gegen Informationspflichten vorwirft, kann sich hieraus somit bereits kein Anspruch aus Art. 82 DSGVO ergeben, da es sich um keinen Verstoß im Hinblick auf die Verarbeitung von Daten handelt.

47
Die von Klageseite vorgebrachten Verstöße gegen Art. 13, 14 DSGVO, Art. 34 DSGVO und Art. 15 DSGVO betreffen einzig und allein Informationspflichten gegenüber den betroffenen Personen. Die Information über die Verarbeitung von personenbezogenen Daten stellt aber keine Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO dar, sodass der Klageseite ein entsprechender

Schadensersatzanspruch aus etwaigen (nicht vorliegenden, siehe unten) Verstößen nicht zustehen kann (vgl hierzu u.a in Gola/Heckmann 3. Aufl. 2022, DS-GVO Art. 82 Rn. 20; LG Essen, Urteil vom 10.11.2022 – 6 O 111/22).

48
bb) Unabhängig von der Frage, ob der Schutzbereich eröffnet ist, scheitert der geltend gemachte Anspruch jedoch vorliegend an den entsprechenden Pflichtverletzungen der Beklagten.

49
(1) Ein Verstoß gegen die Transparenzpflichten aus Art. 5 Abs. 1 lit. a), Art. 13, 14 DSGVO fällt der Beklagten nicht zur Last.

50
Gemäß Art. 5 Abs. 1 lit. a DSGVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Diese Grundsätze sind sodann auf die Informations- und Aufklärungspflicht nach Art. 13 DSGVO zu übertragen. Die Aufklärung über die Zwecke der Verarbeitung muss insbesondere für den Nutzer klar verständlich und nachvollziehbar sein. Ähnliche Anforderungen sieht dabei auch Art. 14 DSGVO für den Fall vor, dass der Verantwortliche die Daten nicht direkt bei der betroffenen Person erhebt. Art. 12 DSGVO sieht ebenso eine Information in präziser, transparenter und leicht zugänglicher Form vor.

51
Diese Vorgaben hält die Beklagte vorliegend ein. Die Klageseite selbst legt mit ihrer Klageschrift ab Bl. 8 d.A. diverse Screenshots der Social Media Plattform F. vor, welche die auf der Plattform enthaltenen Inhalte abbilden. Diese Inhalte sind jedem Nutzer als offenkundige Tatsache gemäß § 291 ZPO öffentlich zugänglich und enthalten sämtliche relevanten Informationen zu Art und Umfang der Verarbeitung sowie Hinweise zur Begrenzung der Verarbeitung der Daten.

52
Ausweislich der vorliegenden Screenshots handelt es sich dabei um Informationen auf mehreren Ebenen. Jedoch schließt gerade dies die Übersichtlichkeit und Transparenz nicht aus. Die Beklagte versuchte über mehrere Ebenen, die vielschichtigen Themen abzuschichten und einzelne Themenbereiche zu bilden. Dies dient nach Ansicht der Kammer letztlich der Vermeidung der Überforderung des Nutzers mit einer Flut an Informationen im Hinblick auf die verarbeiteten Daten. Die Kammer verkennt dabei nicht, dass das Lesen sämtlicher Informationen und Unterbereiche letztlich mit einem gewissen Zeitaufwand verbunden ist, jedoch ist ein solcher Zeitaufwand beim Lesen auch bei Allgemeinen Geschäftsbedingungen der Fall. Hierauf kann es jedoch nicht ankommen. Einzig und allein ist letztlich zu beachten, ob der Nutzer hinreichend klar und verständlich informiert wird. Dies ist vorliegend der Fall. Dabei fand die Aufklärung über die Verwendung der Daten auch in verständlicher Sprache statt, wie es nach Inaugenscheinnahme der streitgegenständlichen Bestimmungen der Datenrichtlinie und des Hilfebereiches zur Überzeugung des Gerichts feststeht.

53
Das Argument der Klageseite, dass die Vielzahl der Einstellungsmöglichkeiten letztlich dazu führe, dass der Nutzer es im Zweifel bei den Voreinstellungen belasse, verfängt dabei nicht. Es ist gerade zu berücksichtigen, dass in Anbetracht der Vorgaben der DSGVO und der damit verbundenen vielseitigen Informationspflichten vielfältige Einstellungsmöglichkeiten nahezu zwingend sind, sodass jeder Nutzer die Einstellungen individuell entsprechend seiner spezifischen Bedürfnisse vornehmen kann.

54
Für eine sachgerechte Betrachtung der Frage ist auch zu berücksichtigen, dass es sich um eine freiwillig von Klageseite genutzte Plattform handelt. Soweit die Klageseite vorliegend neben den für die Anmeldung erforderlichen Daten wie Name, Geschlecht, Geburtsdatum und E-Mail Adresse zusätzlich seine Mobilfunknummer angab, ist zu bedenken, dass es sich bei der Mobilfunknummer um eine nicht erforderliche Angabe handelte. Denn soweit man sich zur Nutzung der Plattform entschließt, ist jedenfalls die Angabe der Mobilfunknummer dafür nicht erforderlich. Hierbei handelt es sich um ein zusätzliches Angebot der Beklagten, mit welcher der jeweilige Nutzer wie hier die Klagepartei – weitere Funktionen und Informationen nutzen kann. Hierbei wird der Nutzer darüber aufgeklärt, dass die Verwendung der Mobilfunknummer gegebenenfalls erfolgt, „um dir interessante Menschen und Themen auf unseren Plattformen vorzustellen“ (vgl. Bl. 15 d.A.). Ebenso wird darauf hingewiesen „Beachte: Du kannst festlegen,

wer deine Telefonnummer sehen kann und wer auf F. nach dir suchen kann“ (vgl. ebenso Bl. 15 d.A.). Selbst wenn das Auffinden dieser Hinweise unter Umständen mit zeitlichem Aufwand verbunden ist, sind die Hinweise selbst klar und verständlich formuliert. Insbesondere ist auch deutlich, dass zwischen dem Sehen der Telefonnummer und dem auf F. nach dir suchen zu unterscheiden ist. Insbesondere ist auch die Einstellung „Wer kann dich anhand der angegebenen Telefonnummer finden?“ mit der Antwort „Alle“ (vgl. Bl. 13 d.A.) eindeutig.

55
Insgesamt ist damit festzuhalten, dass es der Eingabe der Mobilfunknummer zur Nutzung der Plattform eigentlich nach nicht bedarf, dass jedoch, wenn der Nutzer sich für die Verwendung der Plattform mit seiner Mobilfunknummer entscheidet, er hinreichend verständlich und übersichtlich aufgeklärt wird, wie die Mobilfunknummer verwendet wird und wie eine solche Verwendung eingeschränkt werden kann. Letztlich ist dabei auch zu bedenken, dass die Plattform „F.“ gerade dem Finden und dem Austausch von Informationen in der Form eines sozialen Netzwerks dient. In diesem Fall ist es dem Nutzer auch zuzumuten, sich mit den ihm gegebenen Informationen zum Schutz seiner Daten zu befassen.

56
Hierbei ist auch beachtlich, dass der Kläger die Einstellungen zur Suchbarkeit über seine Mobilfunknummer trotz dem diesem Rechtsstreit zu Grunde liegenden Scraping Vorfall und den von Klageseite seitdem in den Raum gestellten Unannehmlichkeiten bis zum Zeitpunkt der mündlichen Verhandlung am 26.01.2023 nach eigenen Angaben nicht geändert hat. Dies führte der Kläger im Rahmen der persönlichen Anhörung entsprechend aus, wobei er angab, von den unterschiedlichen Einstellungen bis heute, also dem Tag der mündlichen Verhandlung, nichts zu wissen. Dies stößt insofern bei der Kammer auf Verwunderung, da die Klageseite bereits mit der Klageschrift auf die unterschiedlichen Einstellungen deutlich hinwies und hierzu die Screenshots vorlegte. Insofern war der Kläger ohne weiteres jedenfalls spätestens ab dem Zeitpunkt der Einreichung der Klage in der Lage, sich hierüber – aus der „eigenen“ Klageschrift – zu informieren.

57
Soweit der Kläger ausführte, die Klageschrift zwar gelesen, jedoch aufgrund der Fülle diese „nicht so intensiv“ gelesen zu haben, zeigt dies nach Ansicht des Gerichts deutlich die Bedeutung der Sache für die Klagepartei. Das Gericht ist in Anbetracht der Vorlage der Unterlagen von Beklagtenseite auch überzeugt (§ 286 BGB), dass der Kläger die Suchbarkeitseinstellung jedenfalls seit dem 01.07.2016 auf „Alle“ eingestellt hatte (Vgl. hierzu Screenshots Bl. 97 d.A.).

58
Unter Berücksichtigung all dieser Umstände ist ein Verstoß auf Beklagtenseite gegen Art. 5 Abs. 1 lit. A) DSGVO nicht zu erkennen.

59
(2) Es liegt auch kein Verstoß der Beklagten gegen Art. 24 Abs. 1, 32 Abs. 1 DSGVO vor.

60
Nach diesen Vorschriften hat der Verantwortliche bei der Verarbeitung personenbezogener Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Anknüpfend an den Gedanken der Schaffung eines Schutzniveaus kann sich eine derartige Verpflichtung in Anbetracht des Wortlautes des Art. 32 Abs. 1 lit. b) DSGVO allerdings nur auf solche Datensätze beziehen, die nicht gerade einem Schutz der Vertraulichkeit entzogen werden sollen.

61
Bei Zugrundelegung dieses Maßstabs hat die Beklagte gegen ihre Verpflichtung, die Sicherheit der Datenverarbeitung zu gewährleisten nicht verstoßen. Die Beklagte war nicht verpflichtet, Schutzmaßnahmen zu treffen, um die Erhebung der immer öffentlich zugänglichen Informationen des Profils des Klägers aufgrund seiner selbst gewählten Einstellung zu verhindern (vgl. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22).

62
Soweit auf die Daten des Klägers wie Name, Geschlecht und Benutzername im Rahmen des Scraping Vorfalls zugegriffen wurde, handelt es sich gerade um Daten die für jedermann öffentlich zugänglich waren.

Diesbezüglich können diese Daten für sich bereits kein erhöhtes Schutzniveau in Anspruch nehmen. Denn die Beklagte durfte aufgrund der von ihr zur Verfügung gestellten Nutzungshinweisen sowie der vor Registrierung vom Nutzer zwingend zu bestätigenden Datenverwendungsrichtlinien davon ausgehen, dass der Klageseite klar ist, dass sein Name, Geschlecht und Benutzername jederzeit für jedermann abrufbar ist (vgl. Landgericht Essen aaO, so auch LG Halle Urteil vom 28.12.2022 – 6 O 195/22).

63
Soweit man unterstellt im Rahmen des Scraping Vorfalls sei auch die Mobilfunknummer der Klageseite abgegriffen worden, ist auch hier kein Verstoß der Beklagten festzustellen.

64
Wie oben bereits ausgeführt hatte der Kläger die Suchbarkeitseinstellung für seine Mobilfunknummer auf „Alle“ eingestellt. Diese Einstellung beinhaltet, dass Dritte den Kläger über seine Mobilfunknummer finden konnten. Hierunter fällt letztlich auch die Möglichkeit, dass Dritte über eine zufällig mittels elektronischer Möglichkeiten erzeugte Mobilfunknummer letztlich eine Verknüpfung zum Kläger über dessen zum Finden freigegebene Mobilfunknummer herstellen.

65
Zwar ist die Beklagte durchaus verpflichtet, zu gewährleisten, dass nicht jedermann ohne weiteres an die sensibleren Daten, wie beispielsweise die Mobilfunknummer gelangt. Dieser Anforderung kam die Beklagte jedoch nach, indem es sich hier zum einen um eine freiwillige, nicht zwingend erforderliche Preisgabe von Daten des Nutzers gegenüber der Beklagten handelt und zum anderen, indem der Nutzer unter Verweis auf die möglichen Nutzungen der Mobilfunknummer die Möglichkeit hat, jederzeit die Einstellungen zur Suchbarkeit zu ändern. Diese Einstellungen waren – wie bereits dargestellt – hinreichend klar und verständlich. Insofern ist die Beklagte ihrer Verpflichtung nachgekommen, sodass ein Verstoß ebenfalls nicht festzustellen war. Soweit die Klageseite die hierzu erforderliche Zeit zur Information über die Einstellungen nicht aufbringen wollte, kann dies nicht zu Lasten der Beklagten gehen.

66
Dass nicht öffentlich zugängliche Informationen von Dritten erlangt worden sind, kann die Kammer hingegen nicht feststellen. Die Klageseite, welche bereits nicht angeben kann, um welche personenbezogenen Daten es sich hierbei handeln soll, tritt hierbei zudem keinen tauglichen Beweis an.

67
(3) Auch ein Verstoß gegen Art. 25 Abs. 2 DSGVO ist nicht gegeben.

68
Nach Art. 25 Abs. 2 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden.

69
Der Anwendungsbereich von Abs. 2 bezieht sich vor allem auf internetbasierte Dienste wie die der streitgegenständlichen Plattform, bei denen durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen sicherzustellen ist, dass Nutzer ihre Daten nur den Personenkreisen und nur in dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben (in Gola/Heckmann, 3. Aufl. 2022, DS-GVO Art. 25 Rn. 28). Insofern hat der Betreiber in seinen Voreinstellung vorzusehen, dass alle nicht für den Zweck der Nutzung erforderlichen personenbezogenen Daten anderen nicht zugänglich gemacht werden, es sei denn der Nutzer nimmt entsprechende Einstellungen vor.

70
Auch hier kann sich der Sinn und Zweck letztlich nicht auf die für die Registrierung erforderlichen Daten Name, Nutzer ID und Geschlecht beziehen, da der Nutzer der öffentlichen Zugänglichmachung bei der Registrierung bereits zustimmt (vgl. oben). Soweit jedoch erneut die Mobilfunknummer des Nutzer betrachtet wird, kann das Gericht auch hier keinen Verstoß erkennen. Der Nutzer, der sich entschließt auch seine Mobilfunknummer preis zu geben – obwohl dies für die Nutzung der Plattform in keiner Weise erforderlich ist – macht dies regelmäßig unter anderem aufgrund der damit einhergehenden Komfortfunktion, einfacher gefunden zu werden.

71

Die initiale Einstellung der Suchbeziehungsweise Auffindbarkeit für alle Nutzer dient gerade dem Sozialaspekt und damit dem Verarbeitungszweck der Plattform. Auch wenn die Beklagte mit ihrer Plattform Marketingzwecke verfolgen mag, so ist für den Nutzer aber in der Regel nicht etwa der kommerzielle Aspekt, wie es der Kläger in seiner Replik ausführt, sondern gerade die soziale Komponente des Netzwerks von Bedeutung. Diese soziale Komponente besteht gerade darin, mit anderen Nutzern in Kontakt zu treten oder in Kontakt zu bleiben, Inhalte aller Art mit der Öffentlichkeit zu teilen, seine Teilnahme an Veranstaltungen zu signalisieren oder sich an öffentlichen Diskussionen zu beteiligen.

72
Soweit der Nutzer nicht an den ausgeführten Möglichkeiten teil haben möchte, bleibt es ihm unbenommen, mit Vornahme der entsprechenden Einstellungen, seine öffentliche Darstellung auf der Plattform einzuschränken. Sowohl der kommunikative Zweck des Netzwerks als auch die Möglichkeit der Anpassung der Privatsphäre-Einstellungen war dem Kläger bekannt, wie er auch grundsätzlich im Rahmen seiner persönlichen Anhörung in der mündlichen Verhandlung vom 26.01.2023 bestätigte, da er sein Profil auf nicht öffentlich eingestellt hat. Überdies war es ihm ohne Weiteres möglich, bei entsprechendem Interesse den Hilfebereich aufzusuchen, wo er über den Reiter „Privatsphäre-Check“ sodann unmittelbar zu den einschlägigen Einstellungen gelangen konnte.

73
Soweit der Kläger hierzu behauptet, dass der kommunikative Zweck ebenso erreicht werden könne, wenn die entsprechenden Voreinstellungen für die Telefonnummern der Nutzer von Anfang an auf „nicht-öffentlich“ beziehungsweise „nicht sichtbar“ gestellt seien, weil die Nutzer der Plattform sich lediglich über ihre Namen und nicht über ihre Telefonnummer suchen, trifft dies nicht zu. Auch wenn es in der Tat unwahrscheinlich erscheint, dass sich Freunde oder Familienmitglieder über ihre Nummern suchen, so ist dies in Bezug auf Externe nicht unbedingt der Fall. Gerade in Anbetracht der Vielzahl an aktiven Nutzern der Plattform können sich die Namen wiederholen, sodass ein einfaches Auffinden des angesteuerten Kontakts nicht immer möglich ist. Vor diesem Hintergrund kann aber gerade die Auffindbarkeit durch die Telefonnummer oder E-Mail-Adresse Abhilfe schaffen, um so eine schnellere und bequemere Kontaktaufnahme zu ermöglichen (so auch LG Kiel Urt. v. 12.1.2023 – 6 O 154/22).

74
Das Gericht verkennt dabei nicht, dass die Voreinstellungen der Zielgruppenauswahl sowie der Suchbarkeit bei der erstmaligen Nutzung der Plattform nach Eingabe der Mobilfunknummer eine Zugänglichkeit in Form der Einsichtnahme in das Profil des Betroffenen durch einen unbestimmt weit gefassten Personenkreis vorsieht. Dennoch ist es – wie oben bereits ausführlich dargestellt dem Nutzer gleich nach der Anmeldung möglich, diese Konfiguration zu ändern, um so sein Interesse an der Vertraulichkeit bezogen auf seine Daten zu wahren. Durch diese Möglichkeit, auf die der Nutzer nach seiner Anmeldung durch die Beklagte hingewiesen wird, wird so letztlich dem Zweck der unkontrollierten Weitergabe der Daten des Betroffenen entsprochen.

75
(4) Ein Verstoß gegen Art. 33 DSGVO liegt ebenfalls nicht vor. Gemäß Art. 33 DSGVO ist der Verantwortliche verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten 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.

76
Einer solche Verpflichtung unterlag die Beklagte jedoch nicht, da eine Verletzung des Schutzes personenbezogener Daten aufgrund der oben dargelegten Umstände gerade nicht vorlag.

77
(5) Auch ein Verstoß gegen Art. 35 DSGVO ist nicht gegeben.

78
Selbst wenn ein Verstoß gegen Art. 35 DSGVO vorlag, indem die Beklagte nach dem Vorfall keine Folgenabschätzung durchführte, ist nicht ersichtlich inwiefern dies für den von Klageseite geltend gemachten Schaden ursächlich bzw. mitursächlich gewesen sein soll. Hiergegen spricht bereits, dass es

sich bei den gescrapten Daten um öffentlich zugängliche Informationen auf dem Profil des Klägers auf F. handelte. Darüber hinaus nahm der Kläger, wie er selbst in der mündlichen Verhandlung ausführte, bis zur Durchführung der mündlichen Verhandlung keinerlei Änderungen seiner Einstellungen vor. Der Kläger führte zwar aus, dass er von der Einstellung der Suchbarkeitsfunktion keine Kenntnis hatte, dies überzeugt die Kammer jedoch im Hinblick auf die Ausführungen in der Klageschrift nicht. Soweit dem Kläger tatsächlich vorrangig der Schutz seiner Daten wichtig wäre, wäre die erste Frage im Rahmen des dem hiesigen Rechtsstreit zugrunde liegenden Mandatsverhältnisses, wie er weitere Zugriffe auf seine Daten verhindern könnte.

79
(6) Auch einen Verstoß gegen die Auskunftspflicht gemäß Art. 15 DSGVO kann die Kammer vorliegend nicht erkennen.

80
Die betroffene Person hat gemäß Art. 15 Abs. 1 a) und Abs. 1 c) DSGVO das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob er betreffend den Nutzer personenbezogene Daten verarbeitet hat. Ist dies der Fall, so hat der Nutzer ein Recht auf Auskunft über diese personenbezogenen Daten und über die Verarbeitungszwecke (a) und die Empfänger oder Kategorien von Empfängern (c), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen.

81
Das Schreiben der Beklagten (Anl. B 16) informiert den Kläger insoweit umfassend. Damit ist der Anspruch insoweit erfüllt und erloschen (§ 362 Abs. 1 BGB).

82
Nicht beantwortet wird durch die Beklagte in dem außergerichtlichen Schreiben einzig, welchen Empfängern die Daten des Klägers durch Ausnutzung des Kontakt-Import 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 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 dies mitteilen können soll) zu informieren, wann die Daten gescrapt wurden. Die Beklagte hat dem Kläger im Ergebnis also alle Informationen mitgeteilt, die ihr selbst bezüglich des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Die Beklagte ist folglich hierzu auch nicht verpflichtet (so auch LG Essen, aaO; LG Ellwangen, Urteil vom 25.01.2023 – 2 O 198/22).

83
cc) Der geltend gemachte Schadensersatzanspruch scheitert darüber hinaus auch daran, dass ein ersatzfähiger Schaden im Sinne von Art. 81 Abs. 1 DSGVO nicht vorliegt.

84
Der Eintritt des Schadens muss dabei im Sinne des § 287 ZPO als überwiegend wahrscheinlich dargetan werden (in Musielak/Voit, ZPO, 19. Aufl. 2022, § 287, Rn. 7). Das Gericht verkennt dabei nicht, dass der Schadensbegriff im Lichte des Erwägungsgrundes Nr. 146 der DSGVO weit zu verstehen ist, sodass ein genereller Ausschluss von Bagatellschäden im Lichte dieser Erwägungsgründe nicht vertretbar ist (vgl. LG Köln, Urteil vom 18.05.2022 – 28 O 328/21). Dennoch muss jedenfalls ein Schaden tatsächlich „erlitten“ worden sein (Erwägungsgrund Nr. 146 S. 6), das heißt jedenfalls ersichtlich, spürbar, objektiv nachvollziehbar und von einem gewissen Gewicht sein (vgl. LG Essen, aaO. m.w.N.).

85
Dem Kläger ist es letztlich nicht gelungen, eine solche spürbare Beeinträchtigung unter Berücksichtigung der vorgenannten Umstände konkret darzulegen.

86
Die Klageseite führt als immaterielle Schadenspositionen Ängste, unter denen der leide, die daraus resultierten, dass er einen erheblichen Kontrollverlust über seine Daten erlitten habe und deshalb großem Unwohlsein und Sorgen in Bezug auf einen potentiellen Missbrauch seiner Daten durch Dritte ausgesetzt sei. Zudem sei es seit dem Scraping-Vorfall zu einem Anstieg an offenkundigen Betrugsversuchen in Form von Phishing-Mails und Anrufen gekommen. Gleichzeitig berichtet der Kläger im Rahmen der persönlichen

Anhörung gemäß § 141 ZPO in der mündlichen Verhandlung jedoch, dass er zum einen die Einstellungen nicht geändert hat, da er nicht gewusst haben will, wie dies funktionieren soll sowie, dass er weder auf eine unerwünschte Nachricht hin, Gelder an die vermeintlichen Betrüger bezahlt hat sowie, noch dass er bei der Polizei Anzeige erstattet hat hinsichtlich der Betrugsversuche zu seinen Lasten. Die Darstellung des Klägers lassen die in der Klageschrift geschilderten Ängste bereits unplausibel erscheinen.

87
Selbst bei Unterstellung der geschilderten Umstände als wahr, genügt dies den obigen Anforderungen jedoch nicht. Selbst Personen, die keinen F. Account nutzen und dort nicht ihre Mobilfunknummer hinterlegt haben, erhalten gerichtsbekannt unerwünschte E-Mails und Nachrichten.

88
Soweit die Klageseite vorbringt, dass nur den Wenigsten eine konkrete Schadendarstellung aufgrund der Reichweite und der Größe des Datenlecks gelingen dürfte und daher schon aufgrund einer bloßen Gefährdung einen Schaden annehmen will, kann sich die Kammer diesen Erwägungen nicht anschließen. Insgesamt erscheint ein Identitätsmissbrauch allein aufgrund einer Telefonnummer eher unwahrscheinlich (so auch LG Karlsruhe, Urteil vom 09.02.2021 – 4 O 67/20). Insbesondere würde der Schadenbegriff so aufgeweicht und ausgedehnt und es würde der konkrete Nachweis einer möglichen Betroffenheit genügen, um eine Haftung zu begründen. Dies käme einer reinen Gefährdungshaftung gleich und widerspricht letztlich auch dem Erwägungsgrund Nr. 75 (vgl. LG Essen, Urteil vom 10.11.2022 – 6 O 111/22, so auch LG Ellwangen, Urteil vom 25.01.2023 – 2 O 198/22).

89
Eine Vorlagepflicht gemäß § 267 Abs. 3 AEUV trifft die Kammer hierbei nicht, da sie nicht letztinstanzlich über die Sache entscheidet. Von der Möglichkeit zur Vorlage nach § 267 Abs. 2 AEUV macht die Kammer schon deshalb keinen Gebrauch, weil die Sache darüber hinaus bereits aus anderen Gründen keinen Erfolg hat (vgl. oben die Ausführungen unter bb)).

90
dd) Zudem fehlt es an der Kausalität zwischen dem Vorwurf und dem in den Raum gestellten Schaden. Soweit der Kläger behauptet, er erhalte unerwünschte SMS und E-Mails, so handelt es sich um ein „Phänomen“, das bereits mit der Nutzung des Internets als solcher zusammenhängt. Der Kammer ist bekannt, dass selbst Personen, welche keinen F. Account besitzen unerwünschte Anrufe und Nachrichten erhalten. Insbesondere sind Spam-E-Mails mit Werbung oder Hinweis auf eine ausstehende Paketlieferung weit verbreitet. Auch Nachrichten, in welchen sich die Unbekannten Täter als Kind in Not mit neuer Handynummer ausgeben, sind üblich und gehen beinahe überall ein. Selbst wenn beim Kläger tatsächlich derartige Anrufe und Nachrichten seit April 2021 zugenommen haben mögen, so kann dies vielerlei Ursachen haben. Es ist völlig unklar und unbekannt, ob und welche Daten der Kläger an anderer Stelle freigegeben hat (beispielsweise im Rahmen weiter verbreiteter Phishing E-Mails) und ob ein unberechtigter Datenzugriff an anderer Stelle zu dem vom Kläger behaupteten vermehrten unerwünschten Nachrichtenaufkommen geführt hat.

91
ee) Ausführungen zur Höhe des geltend gemachten Schmerzensgeld können daher aufgrund der vorgenannten Umstände unterbleiben.

92
b) Ein etwaiger Anspruch auf Schmerzensgeld steht der Klageseite auch nicht aus sonstigen, nationalen Vorschriften zu.

93
Das Verhältnis der Vorschriften der DSGVO zu denen des materiellen Rechts kann dabei letztlich dahinstehen, da sich auch aus dem nationalen Recht kein Anspruch ergibt.

94
aa) Auf die Vorschriften §§ 280 Abs. 1, Abs. 3, 281, 327, 327e, 327i BGB kann die Klageseite ein Anspruch bereits deshalb nicht stützen, da die Normen der §§ 327 ff. BGB erst zum 01. Januar 2022 in Kraft getreten sind und damit auf den Zeitpunkt des Abschlusses des Nutzungsvertrags, wie auch auf den Zeitpunkt des Verstoßes nicht anzuwenden sind.

95
bb) Den Anspruch auf Schadensersatz kann der Kläger auch nicht auf § 280 Abs. 1 BGB i.V.m. Nutzungsvertrag als Vertrag sui generis stützen (vgl. Hierzu, OLG München, Urteil vom 18.12.2020 – 18 U 5493/19).

96
Unabhängig von der Frage, ob die Beklagte eine Pflicht aus dem Nutzungsvertrag verletzt haben soll, fehlt es jedenfalls an einem Schaden gemäß §§ 249 ff. BGB. Das nationale Schadensrecht verlangt für einen Schadensersatzanspruch jedenfalls eine spürbare Beeinträchtigung (s. Herberger/Martinek/Rüßmann/Weth/Würdinger, jurisPK-BGB, 9. Aufl. 2020, § 249 BGB, Stand: 8. September 2021, Rn. 26 ff.). An einer solchen fehlt es gerade.

97
cc) An der Darlegung des konkreten materiellen Schadens scheitert letztlich auch der Anspruch aufgrund einer möglichen Verletzung des allgemeinen Persönlichkeitsrechts gemäß §§ 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG ebenso wie ein möglicher Anspruch aus § 823 Abs. 2 BGB i.V.m. dem Recht auf informationelle Selbstbestimmung.

98
dd) Aufgrund der obigen Ausführungen kommt auch ein Anspruch aus §§ 1004 BGB analog, 823 Abs. 2 BGB i.V.m. Art. 13, 14 DSGVO nicht in Betracht. Es kann dahin stehen, ob die DSGVO als Schutzgesetz im Sinne von § 823 Abs. 2 BGB anzusehen ist.

99
2. Aufgrund der dargelegten Umstände ist auch der Antrag auf Feststellung einer Ersatzpflicht künftiger materieller und immaterieller Schäden unbegründet.

100
3. Dem Kläger steht zudem kein Anspruch auf Unterlassung gemäß §§ 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 6 Abs, 1, 17 DSGVO gegen die Beklagte zu. Eine Zuwiderhandlung der Beklagten ist nicht ersichtlich, im Übrigen aber auch für die Zukunft nicht zu befürchten.

101
Soweit vorliegend überhaupt gesichert Daten durch den Scraping Vorgang durch die unbekannten Täter erlangt wurden, handelte es sich dabei um öffentliche Daten bzw. Daten, auf welche der Kläger den Zugriff erlaubte.

102
Der Kläger hat der Veröffentlichung seiner Daten bei der Registrierung unter Zustimmung zu den Nutzungsbedingungen zugestimmt. Insofern hat die Beklagte den Kläger hinreichend über die Verarbeitung der Daten aufgeklärt (vgl. hierzu die Ausführungen unter (1)). Soweit der Scraping-Vorfall sich auf die Mobilfunknummer des Klägers bezieht, ist auch hier zu berücksichtigen, dass der Kläger jederzeit die Einstellungen zur Suchbarkeitsfunktion hätte ändern können. Auch dies war für einen verständigen und interessierten Nutzer ohne weiteres bei Anlegung der entsprechenden Sorgfalt und Inanspruchnahme von Zeit möglich.

103
Dass die Beklagte entgegen der von einem Nutzer getroffenen Einstellungen Telefonnummern eigenständig oder aktiv freigibt oder anderweitig nutzt, hat der Kläger schon nicht behauptet.

104
4. Der Klageseite steht auch kein Anspruch auf weitergehende Auskunft nach Art. 15 DSGVO zu.

105
Der Kläger hat auch keinen Anspruch auf eine weitergehende Auskunft gemäß Art. 15 DSGVO. Mit Schreiben vom 09.03.2022 (vorgelegt als Anlage B16) hat die Beklagte dem Kläger Auskunft über die von ihr verarbeiteten Daten in angemessener Weise zur Verfügung gestellt, sodass der Anspruch bereits teilweise gemäß § 362 Abs. 1 BGB erloschen ist. Die Beklagte ist lediglich angehalten, die von ihr selbst verarbeiteten Daten mitzuteilen soweit Dritte durch das Scrapen vorliegend (öffentlich einsehbare) Daten des Klägers verarbeitet haben, ist die Beklagte hierzu nicht zur Auskunft verpflichtet. Die Beklagte legt darüber hinaus nachvollziehbar dar, dass sie hierzu keine weiteren Angaben machen kann.

106
5. Mangels Anspruch in der Hauptsache besteht auch kein Anspruch auf Zahlung außergerichtlicher Rechtsanwaltskosten gemäß § 280 Abs. 1 BGB oder aus Art. 82 Abs. 1 DSGVO.

III.

107
Die Kostenentscheidung ergibt sich aus § 91 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit folgt § 709 ZPO.

108
Die Streitwertfestsetzung beruht auf § 3 ZPO.