LG Bamberg, Endurteil v. 06.06.2023 – 42 O 782/22

Titel:

Erfolglose Schadensersatzklage wegen Zugriff auf personenbezogene Nutzerdaten

Normenketten:

DSGVO Art. 13, Art. 14, Art. 18, Art. 24, Art. 25, Art. 79, Art. 82
ZPO § 253, § 256, § 287

Leitsatz:

Eine Verletzung des Datenschutzrechts als solche begründet noch keinen Schadensersatzanspruch, vielmehr muss die Verletzungshandlung zu einer konkreten, nicht nur völlig unbedeutenden Verletzung von Persönlichkeitsrechten geführt haben; für einen Bagatellverstoß ohne ernsthafte Beeinträchtigung bzw. für jede bloß individuell empfundene Unannehmlichkeit ist kein Schmerzensgeld zu gewähren, wenn kein spürbarer Nachteil entstanden ist und es um keine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen geht. (Rn. 61) (redaktioneller Leitsatz)

Schlagwort:

Datenschutzverstoß

Fundstellen:

GRUR-RS 2023, 13792
ZD 2023, 637
LSK 2023, 13792

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 6.500,00 € festgesetzt.

Tatbestand

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

2
Der Kläger nutzt die von der Beklagten betriebene Social Media Plattform www.f..com, um mit Freunden zu kommunizieren, private Fotos zu teilen und mit anderen Nutzern im Netz zu diskutieren. Die Beklagte betreibt die Website www.f..com und die darauf enthaltenen Dienste (im Folgenden: „F."). Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Nutzer können auf den persönliChen Profilen Angaben zu verschiedenen Daten zu ihrer Person machen und im von der Beklagten vorgegebenen Rahmen darüber entscheiden, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

3
Zwischen Januar 2018 und September 2019 lasen und persistierten („Scraping") Dritte Telefonnummer, F.-ID, Name, Vorname, Geschlecht und weitere korrelierende Daten – wobei streitig ist, ob hierzu auch Bundesland, Land, Stadt, Beziehungsstatus gehörten – über das F.-Tool ContactImport aus zum Teil öffentlich zugänglichen Daten bei F. Die Beklagte geht davon aus, dass das Contact-Import-Tool zur

Bestimmung der Telefonnummern der einzelnen Benutzer genutzt wurde. Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, gelang es Unbekannten, die Telefonnummern konkreten F.-Profilen zuzuordnen. Um die Telefonnummer jeweils zu korrelieren, wurden mit Hilfe des Contact-Import-Tools fiktive Nummern erzeugt und geprüft und die zugehörigen F.-Nutzer wurden angezeigt. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft“).

4
Anfang April 2021 wurden diese Daten von ca. 533 Millionen F.-Nutzern aus 106 Ländern im Internet öffentlich verbreitet.

5
Daraus resultierend wurden den Kläger betreffende Daten abgegriffen und im Internet auf Seiten veröffentlicht, die illegale Aktivitäten begünstigen sollen.

6
Bei dem Anlegen eines F.-Profils wird der künftige Nutzer auf Datenschutz- und Cookie-Richtlinien hingewiesen. 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 hat oder mit wem er befreundet ist. Der Nutzer kann diese Einstellungen individuell verändern und im Hilfebereich lesen, 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“.

7
Der Kläger hat bei Anlegung seines Profils seine Mobilfunknummer angegeben und ist von diesen Grundeinstellungen nicht abgewichen. Erst eine Woche vor dem Termin zur mündlichen Verhandlung am 10.03.2023 hat er die Einstellung bzgl. seiner Mobilfunknummer insoweit abgeändert, als diese nun für Dritte nicht mehr einsehbar ist – mithin auf „nur ich“ eingestellt ist.

8
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.

9
Inhalt und Bedeutung des Scraping werden von den Parteien unterschiedlich interpretiert.

10
Mit außergerichtlicher E-Mail vom 20.10.2021 wurde die Beklagte vergeblich zur Zahlung von 500,- € und Unterlassung künftiger Zugänglichmachung der Daten des Klägers sowie Erteilung einer Auskunft, welche konkreten Daten im April 2021 abgegriffen und veröffentlicht wurden, aufgefordert (K 1). Die Beklagte erteilte daraufhin mit Schreiben ihrer Prozessbevollmächtigten vom I I . I .2021 einige Auskünfte (Anlage BI 5), die dem Kläger aber nicht genügen.

11
Der Kläger ist der Ansicht, die Beklagte verstoße gegen ihre Pflichten aus der DSGVO, insbesondere

- die Pflicht nach Art. 13, 14 DSGVO zur ausreichenden Information über die Verarbeitung personenbezogener Daten,

- die Pflichten nach Art. 32, 24, 25 DSGVO zum ausreichenden Schutz von Daten,

- die Pflicht nach Art. 25 Abs. 2 DSGVO zur datenschutzfreundlichsten Voreinstellung,

- die Pflicht nach Art. 33, 34 DSGVO zur Information der zuständigen Aufsichtsbehörde und

- die Pflicht nach Art. 15 DSGVO zur ausreichenden Auskunftserteilung.

12

Der Kläger behauptet, 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. Nur so hätten auch seine Daten auf sog. Hackerforen geraten können. Die Daten seien dann für sog. Phishing Attacken genutzt worden. F. sei „datenschutz-unfreundlich“ eingestellt, es werde unnötig zwischen Datenschutzrichtlinien und Cookie-Verwendung differenziert, obwohl die Verwendung von Cookies – so meint der Kläger – ein inhärent datenschutzrechtliches Thema sei. Der gesamte Anmeldevorgang sei intransparent und für den Anwender verwirrend. Dies führe letztlich – so behauptet der Kläger – 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 frage 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 – so auch er als Kläger – keine transparenten Informationen für eine Gewährleistung einer effektiven digitalen Sicherheit erhalte. Diese Sicherheitslücke werde seit 2019 ausgenutzt, ohne dass die Beklagte etwas dagegen unternehme. Er – der Kläger – habe so ungewollt die Kontrolle über seine Daten verloren und werde bis heute wiederholt ungewollt von Unbekannten via E-Mail und SMS kontaktiert. Auch nach dem Vorfall 2019 habe die Beklagte – so meint der Klägernicht adäquat reagiert. Sie habe versäumt, die zuständige Datenschutzbehörde „Irish Data Protection Commission“ unverzüglich zu informieren. Soweit vorgerichtlich Auskünfte über abgegriffene Daten mitgeteilt worden seien, sei diese Auskunft ungenügend.

13
Die Datenschutzeinstellungen der Beklagten seinen undurchsichtig und 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 der Kläger weiter – allerdings den Grundsätzen eines nutzerfreundlichen Datenschutzes und dem in der DSGVO niedergelegten Prinzips der „privacy by default“ datenschutzfreundliche Voreinstellungen).

14
Die Auskunft, die die Beklagte ihm habe zukommen lassen, sei unzureichend. Das Antwortschreiben der Beklagten enthalte lediglich allgemein gehaltene Informationen zu den auf F. verarbeiteten Daten sowie einen Link zur Seite der Beklagten, auf der die Daten über einen individuellen Nutzer gespeicherten Daten eingesehen werden können. Dieses Vorgehen allein sei schon nicht geeignet, dem nach Art. 15 DSGVO umfassenden Auskunftsanspruch gerecht zu werden. Unabhängig davon enthalte das „Auskunftsschreiben“ der Beklagten aber auch keinerlei konkrete Aussagen dazu, welche Daten der Klägerseite im Wege des Scrapings von unbekannten Dritten abgegriffen wurden. So bleibe offen, wann genau die Daten entwendet worden seien oder wie viele verschiedene Beteiligte diese Funktion hinsichtlich seiner – des Klägers – Daten ausgenutzt hätten.

15
Der Kläger beantragt,

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

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

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. personenbezogene 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 Contact-import-tools 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,

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

16
Die Beklagte beantragt,

die Klage abzuweisen.

17
Die Beklagte meint, der Sachverhalt und Vorgang zum sog. Scraping sei falsch wiedergeben. Der klägerische Vortrag beruhe auf einem Missverständnis zum Scraping als solchen. Es sei unschlüssig und unsubstantiiert, welche Daten des Klägers genau gescrapt worden sein sollen.

18
Die Beklagte bestreitet die Begehung eines Datenschutzverstoßes und eines Unterlassens des Schließens einer technischen Schwachstelle. Vielmehr seien lediglich automatisch gesammelte öffentlich einsehbare Daten entweder von der App oder der Website F. gescraped worden, was nach den Nutzungsbedingungen von F. untersagt gewesen sei und noch untersagt sei. Das Abrufen habe im Einklang mit den jeweiligen Privatsphäre-Einstellungen „öffentlich“ auf der F.-Plattform gestanden. Es seien allenfalls öffentlich einsehbare Daten abgerufen und an anderer Stelle erneut zugänglich gemacht worden. Sie – die Beklagte – stelle allen Nutzern, inklusive dem Kläger, alle in Art. 13 und 14 DSGVO festgelegten Informationen zur Datenverarbeitung zur Verfügung, die sie zum Zeitpunkt der Datenerhebung im Anwendungsbereich der Datenrichtlinie durchführe. Sie ist daher der Ansicht, nicht gegen die Transparenzpflichten der DSGVO verstoßen zu haben. 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.

19
Die Beklagte ist der Ansicht, nicht gegen Art. 24, 32 DSGVO verstoßen zu haben, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen zu haben, das Risiko von Scraping zu unterbinden und Maßnahmen zur Bekämpfung von Scraping zu ergreifen. Es fehle konkreter Vortrag, welche Maßnahmen in welchem Umfang nicht genügen würden. Außerdem müsse eine solche Beurteilung ex ante und nicht ex post erfolgen. Den Anforderungen des Art. 25 DSGVO sei genügt. Es dürfe dabei der zentrale Zweck von F., sich mit Freunden, Familien und Gemeinschaften zu verbinden nicht außer Betracht bleiben. Es bestehe keine Melde- oder Benachrichtigungspflicht, da es an einer Verletzung der Sicherheit i. S. d. Art. 4 Nr. 12 DSGVO und an einer unbefugten Offenlegung von Daten fehle. Unabhängig davon habe sie – die Beklagte – wegen der Medienberichterstattung freiwillig eine Vielzahl von Maßnahmen ergriffen, über Scraping und Begrenzungsmöglichkeiten einschließlich einer Änderung von Privatsphäre-Einstellungen zu informieren.

20

Schließlich – so meint die Beklagte darüber hinaus – fehle es an einem immateriellen Schaden. Art. 82 DSGVO umfasse keine Verstöße gegen Art. 13 – 15, 24, 25 DSGVO. Zudem fehle es an einem Verstoß gegen Art, 82 DSGVO. Ein kompensationsgeeigneter messbarer Schaden sei auch nicht dargelegt. Selbst bei einem angenommenen vorübergehenden Kontrollverlust über personenbezogene Daten des Klägers wäre dies nicht ihr – der Beklagten – zuzurechnen, weil die öffentliche Einsehbarkeit den Privatsphäre-Einstellungen des Klägers entsprochen habe.

21
Schließlich fehle es an einer schlüssigen Darlegung der Kausalität.

22
Mangels Verstoßes gegen die DSGVO sei der (ohnehin unzulässige) Feststellungsantrag unbegründet. Der Unterlassungsanspruch scheitere an einer Erstbegehungs- und einer Wiederholungsgefahr. Anwaltskosten seien mangels Verzuges unbegründet.

23
Das Gericht hat den Kläger in der mündlichen Verhandlung vom 23.05.2023 persönlich angehört. Wegen des Ergebnisses der persönlichen Anhörung wird auf das Protokoll vom 23.05.2023 Bezug genommen.

24
Wegen der weiteren Einzelheiten des Sachvortrags der Parteien wird auf die gewechselten Schriftsätze nebst Anlagen, das Protokoll der mündlichen Verhandlung vom 23.05.2023 und den sonstigen Akteninhalt Bezug genommen.

Entscheidungsgründe

A. Zulässigkeit der Klage

25
Die Klage ist zulässig.

I. Zuständigkeit des Landgerichts Bamberg

26
Das Landgericht Bamberg ist international, sachlich und örtlich zuständig.

27
1. Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO (Brüssel Ia-VO).

28
a. Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen.

29
Vorliegend handelt es sich um eine Zivilsache.

30
b. Die deutsche Gerichtsbarkeit folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 2. Alt EuGVVO. Ein ausschließlicher Gerichtstand gemäß Art. 24 EuGVVO ist hier nicht ersichtlich. Gemäß Art. 18 Abs. 1 2. Alt EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Sitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat.

31
Der Kläger ist gemäß Art. 17 Abs. 1 EuGVVO Verbraucher. Er gibt an, einen Nutzungsvertrag mit der Beklagten geschlossen zu haben über die Nutzung der Social-Media-Plattform F. mittels eines Benutzerkontos zu privaten Zwecken. Als doppelrelevante Tatsache reicht in der Zulässigkeit das Behaupten von Tatsachen, aus denen sich ein solcher vertraglicher Anspruchs ergeben kann.

32
c. Der Kläger hat seinen Wohnort in der Stadt … in Deutschland. Insoweit ist die deutsche Gerichtsbarkeit zuständig,

33
2. Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO. Danach können Klagen gegen einen Verantwortlichen oder gegen einen Auftragsverarbeiter bei den Gerichten des Mitgliedstaats erhoben werden, in dem die betroffene Person ihren gewöhnliChen Aufenthaltsort hat, es sei denn, es handelt sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

34
Gemäß Art. 4 Nr. 7, 8 DSGVO sind Verantwortliche natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Auftragverarbeitende sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

35
Die Beklagte selbst erklärt, dass sie in den meisten Fällen die Rolle als Verantwortliche bekleide. Lediglich, wenn sie Werbekunden bediene, könne sie ausnahmsweise als Auftragsverarbeitende fungieren (https://www…com/business/gdpr). Die Beklagte ist zudem keine Behörde eines Mitgliedstaats, die in Ausübung ihrer hoheitlichen Befugnisse tätig geworden ist.

36
Der Kläger als betroffene Person hat seinen Wohnsitz in der Stadtin Deutschland. Die deutsche Gerichtsbarkeit ist international zuständig.

37
3. Das Landgericht Bamberg ist gemäß SS 23 Nr. 1, 71 Abs. 1 GVG für die Klagen gegen die Beklagte sachlich zuständig. Der Streitwert liegt bei 6.500,- € (Klageantrag zu I: 1000,- €, Antrag zu 2: 500,- €; Antrag zu 3: 4.500,- €, Antrag zu 4: 500,- €) und damit über 5.000,- €.

38
Hinsichtlich des Antrags zu 1) war der dort begehrte Zahlbetrag in Ansatz zu bringen. Hinsichtlich des Feststellungsantrags zu 2) hat die Kammer einen 50% igen Abschlag von dem mit Ziffer 1) begehrten Zahlbetrag zur Bezifferung vorgenommen.

39
Hinsichtlich der Höhe des Antrags zu 3) hat die Kammer im Sinne des S. 3 ZPO insbesondere auf Tragweite und Umfang des Streitgegenstands abgestellt, den die Beklagte selbst mit 4.500,- € beziffert. Der Streitwert bei nicht vermögensrechtlichen Streitigkeiten ist letztlich anhand aller Umstände des Einzelfalls, insbesondere auch anhand der Einkommensverhältnisse und der Bedeutung der Sache, zu bemessen. Bei der Beklagten handelt es sich um einen multinationalen Konzern mit hohen Umsätzen, die Bedeutung der Sache ist auf Grund der Vielzahl der vom Scraping betroffenen Personen für die Beklagte erheblich.

40
Hinsichtlich des Antrags zu 4) erschien ein Streitwert von 500,- € angemessen, da es noch um restliche Auskünfte ging.

41
4. Die örtliche Zuständigkeit folgt aus Art. 18 Abs. 1 2. Alt. EuGVVO. Danach 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 seinen Wohnsitz hat. Das Landgericht ist unabhängig davon nach Art. 79 Abs. 2 S. 2 DSGVO, S. 44 Abs. 1 S. 2 BDSG örtlich zuständig (besonderer Gerichtsstand). Der Kläger hat seinen Wohnsitz in der Stadt und damit im Bezirk des angerufenen Gerichts.

II. Hinreichend bestimmter Klageantrag zu l)

42
Der Zulässigkeit der Klage steht nicht die Unbestimmtheit des Klageantrags zu 1) (S. 253 Abs. 2 ZPO) entgegen. Da die Bemessung der Höhe des Schmerzensgeldes in das Ermessen des Gerichts gestellt ist, ist die Stellung eines unbezifferten Zahlungsantrags ausnahmsweise zulässig. Ein Verstoß gegen den in S.

253 Abs. 2 Nr. 2 ZPO normierten Bestimmtheitsgrundsatz liegt dann nicht vor, wenn die Bestimmung des Betrages von einer gerichtlichen Schätzung nach S. 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, 33. Aufl. 2020, S. 253 ZPO 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 I .OOO,- € angegeben.

43
Soweit die Beklagte meint, der Antrag zu 1) sei deshalb unbestimmt, weil er auf zwei Lebenssachverhalten fuße und damit zwei Streitgegenstände betreffe, deren Verhältnis zueinander nicht hinreichend bestimmt sei, so dürfte dem entgegenzuhalten, dass tatsächlich nur ein Lebenssachverhalt zu beurteilen ist, nämlich derjenige, ob die Beklagte vor dem Scraping durch Dritte im April 2021 hinreichende Datenschutzvorkehrungen getroffen hatte und danach etwaige Lücken geschlossen hat bzw. ihre Nutzer unzureichend bzw. intransparent informiert hat.

III. Feststellungsinteresse bezüglich des Antrags zu 2)

44
Der Kläger hat sein Feststellungsinteresse gemäß S. 256 Abs. 2 ZPO hinreichend dargelegt. Ein Feststellungsantrag ist schon zulässig, wenn die Schadensentwicklung noch nicht abgeschlossen ist und der Kläger seinen Anspruch deshalb ganz oder teilweise nicht beziffern kann (OLG Hamm, Urteil vom 21 . Mai 2019 – 9 U 56/18 –, Rn. 22, juris). 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 09. Januar 2007 – VI ZR 133/06 e, juris; BGH, Urteil vom 16. Januar 2001 – VI ZR 381/99 e, juris; Saarländisches Oberlandesgericht Saarbrücken, Urteil vom 20. Februar 2014 – 4 U 41 1/12, Rn. 46, juris, m.w.N.). Bei den behaupteten Verstößen gegen die DSGVO mit der behauptet dargelegten unkontrollierten Nutzung gescrapter Daten ist bei verständiger Würdigung zumindest nicht ausgeschlossen, dass irgendein materieller oder immaterieller Schaden entstehen könnte. Denn der Kläger gibt an, ein solches Feststellungsinteresse wegen der behauptet einmal gescrapten Daten und damit behauptet einhergehenden unbefugten und unkontrollierten Datenverwendung zu haben, die auch zu künftigen Schäden führen könne, deren Art und Umfang noch unbekannt sind. Es ist nicht völlig ausgeschlossen, dass der Kläger infolge der Veröffentlichung seiner Telefonnummer in Verbindung mit seinem Namen sowie weiteren persönlichen Daten einen irgendwie gearteten Schaden erleidet.

IV. Hinreichende Bestimmtheit des Antrags zu 4 (Unterlassungsantrag)

45
Der Antrag zu 4) – Unterlassungsanspruch – ist hinreichend bestimmt. Zuzugestehen ist der Beklagten zwar, dass die Formulierung „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ auslegungsbedürftig ist und Vollstreckungsprobleme denkbar sind. Allerdings ist nach höchstrichterlicher Rechtsprechung eine gewisse Auslegungsbedürftigkeit zur Gewährleistung effektiven Rechtsschutzes hinzunehmen (BGH, GRUR 2015, 1237, Rn. 15, BGH NJW 2004, 2080). Zutreffend verweist der Kläger darauf, dass er nicht einschätzen kann, was die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen beinhalten, was dann dazu führt, dass das Vollstreckungsorgan gegebenenfalls Wertungen vornehmen muss. Es wäre verfehlt im Lichte des effektiven Rechtsschutzes i. S. d. Art. 19 GG, würde vom Kläger verlangt, dass er für eine hinreichend konkrete Antragstellung den aktuellen Stand der Technik selbst ermitteln muss.

B. Begründetheit der Klage

1. Klageantrag zu 1) – Anspruch auf immateriellen Schadensersatz in Höhe von 1 .000.- €

46
Der Kläger hat unter keinem rechtlichen Gesichtspunkt einen Anspruch auf immateriellen Schadenersatz in geltend gemachter Höhe von 1.000,- €. Ein Anspruch gegen die Beklagte ergibt sich weder aus nationalen Vorschriften noch aus Art. 82 DSGVO.

Im Einzelnen:

I. Kein Anspruch aus Art. 82 DSGVO

47
Es fehlt sowohl an einer schadenersatzauslösenden Pflichtverletzung der Beklagten im Sinne von Art. 82 DSGVO als auch an einem ersatzfähigen Schaden.

a) Schutzzweck / Anwendungsbereich des Art. 82 DSGVO

48
Soweit der Kläger der Beklagten mehrere Verstöße vorwirft, nämlich

- ungenügende Information und Aufklärung über die Verarbeitung der ihn betreffenden Daten durch ungenügende Aufklärung zur Verwendung und Geheimhaltung der Telefonnummer (Art. 5 Abs. 1 a DSGVO),

- unmittelbaren Verstoß gegen Art. 13, 14 DSGVO, die konkrete Informationspflichten enthielten, die seitens der Beklagten nicht eingehalten worden seien,

- ungenügender Schutz der personenbezogenen Daten der Nutzer von F. (Art. 24, 25, 32 DSGVO),

- fehlerhafte, weil nicht datenschutzfreundlichste Voreinstellung (Art. 25 Abs. 2 DSGVO),

- nicht erfolgte Information der zuständigen Aufsichtsbehörde (Art. 33, 34 DSGVO) und

- unvollständige Auskunftserteilung nach Art. 15 DSGVO, da nicht mitgeteilt worden sei, welchen Empfängern die Daten des Klägers durch Ausnutzung des Kontakt-Import Tools zugänglich gemacht worden seien (Art. 33, 34 DSGVO), sind solche Verstöße schon nicht vom Schutzzweck des Art. 82 DSGVO umfasst.

49
Der räumliche Anwendungsbereich der DSGVO ist eröffnet. Er umfasst gemäß Art. 3 Abs. I DSGVO die Niederlassung eines Verantwortlichen oder eines Auftragverarbeiters in der Union, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Die Beklagte als Verantwortliche hat ihren Sitz in Irland. Irland ist Mitglied der europäischen Union.

50
Der sachliche Anwendungsbereich von Art. 82 DSGVO ist hingegen nicht eröffnet. Nach Art. 82 Abs. 1 DSGVO steht jeder Person, der „wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“ Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter zu. Ausreichend ist aber nicht ein Verstoß gegen jegliche Vorgabe der DSGVO, sondern aus Art. 82 Abs. 2 DSGVO ergibt sich, dass Schutzgegenstand der Vorschrift, die verletzt wurde, die Datenverarbeitung selbst sein muss. Art. 82 Abs. 1 DSGVO ist demgegenüber lediglich als generelle Umschreibung bzw. Klarstellung der Haftungsverpflichtung von allen Anspruchsverpflichteten zu verstehen. Anknüpfungspunkt für eine Haftung ist also eine der Verordnung nicht entsprechende Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO. Dies steht im Einklang mit Erwägungsgrund 146, wonach der Verantwortliche oder der Auftragverarbeiter Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit der DSGVO nicht im Einklang stehen, ersetzen sollte (vgl. etwa Cola/Heckmann/Gola/Piltz, 3. Aufl. 2022, DS-GVO Art. 82 Rn. 5; Sydow/Marsch DS-GVO/BDSG/Kreße, 3. Aufl. 2022, DS GVO Art. 82 Rn. 7; Kühling/Buchner/Bergt, 3. Aufl. 2020, DS-GVO Art. 82 Rn. 23; Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DS-GVO Art. 82 Rn. 8; vgl. Erwägungsgrund 146 S. 1 DS-GVO; LG Bonn, Urteil vom 1.7.2021 – 15 O 372/20 ZD 2021, 586; LG Essen, Urteil vom 10.11.2022 – nach juris; a. A.: u.a. OLG Stuttgart, Urteil vom 31.03.2021 – 9 U 34/21 BeckRS 2021, 6282).

51
Verstöße gegen Pflichten bei der Datenverarbeitung sind indes nicht ersichtlich.

52
Gemäß Art. 4 Nr. 2 DSGVO ist Verarbeitung jeder 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, durch den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

53
Gemäß Art. 4 Nr. I DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

54
Die in jedem Fall veröffentlichten Informationen des Klägers umfassen den Namen, die Nutzer-ID sowie das Geschlecht, ohne die die Nutzung der Plattform F. nicht möglich ist, worauf direkt bei der Anmeldung hingewiesen wird. Damit ist es möglich, den Kläger zu identifizieren. Es handelt sich mithin um personenbezogene Daten. Die übrigen Daten wie Telefonnummer und E-Mail-Adresse sind ebenfalls personenbezogen, aber nicht in jedem Fall öffentlich, worauf später noch näher einzugehen ist.

55
Die von Klägerseite geltend gemachten Pflichtverletzungen unterliegen diesem Verarbeitungsbegriff bzw. dem Verarbeitungsvorgang in Bezug auf die Daten des Klägers nicht:

56
Benachrichtigungs-, Aufklärungs- und Informationspflichten nach Art. 5 Abs. 1 a DSGVO, nach Art. 13, 14, 15 DSGVO und nach Art. 33, 34 DSGVO stellen keine Datenverarbeitung dar, so dass Verstöße gegen diese Normen von Art. 82 Abs. 1, 2 DSGVO nicht umfasst sind (so auch LG Essen a.a.O., AG Strausberg, Urteil vom 13.10.2022 – 25 C 95/21 – BeckRS 2022, 27811, Rn. 17; bzgl. Art. 34 DSGVO weiter auch s. a.: OLG Stuttgart, Urteil vom 31.3.2021, 9 IJ 34/21, juris Rn. 61; LG Düsseldorf, Urteil vom 28.10.2021, 16 O 128/20, GRUR-RS 2021, 33076, Rn. 27; LG Bonn, Urteil vom 1.7.2021, 15 O 372/20, juris, Rn. 41).

57
Schließlich lässt sich auch von vornherein aus Artikel 24 DSGVO kein subjektives Recht herleiten (Taeger/Gabel, DSGVO, 4. Auflage 2022, Artikel 24, Rn. 89). Selbiges gilt für Art. 25 DSGVO (Tager/Gabel, DSGVO, a. a. O., Art. 25, Rn. 100).

b) Schaden im Sinne von Art, 82 Abs. I, 2 DSGVO

58
Unabhängig davon fehlt es an einem ersatzfähigen Schaden des Klägers im Sinne des Art. 82 Abs. 1 DSGVO. Für den – hier geltend gemachten – immateriellen Schadensersatz gelten dabei die im Rahmen von S. 253 BGB entwickelten Grundsätze; die Ermittlung obliegt dem Gericht nach S. 287 ZPO (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31). Es können für die Bemessung die Kriterien des Art. 83 Abs. 2 DSGVO herangezogen werden, beispielsweise die Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie die betroffenen Kategorien personenbezogener Daten. Zu berücksichtigen ist auch, dass die beabsichtigte abschreckende Wirkung nur durch für den Anspruchsverpflichtenden empfindliche Schmerzensgelder erreicht wird, insbesondere wenn eine Kommerzialisierung fehlt. Ein genereller Ausschluss von Bagatellfällen ist damit nicht zu vereinbaren (BeckOK DatenschutzR/Quaas, 32. Ed. 1.2.2020, DS-GVO Art. 82 Rn. 31; vgl. LG Köln, Urteil vom 07.10.2020 – 28 O 71/20). Die Pflicht zur Erstattung immaterieller Schäden ist daher nicht nur auf schwere Schäden beschränkt (vgl. LG Landshut, Urteil vom 06.11.2020- 51 O 513/20).

59
Nach den Erwägungsgründen der europäischen Grundrechtscharta ist der Schadensbegriff weit auszulegen (s. Erwägungsgrund Nr. 146, auch wenn er in der DSGVO nicht näher definiert wird). Schadenersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen (Bergt in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl., Art. 82 Rdn. 17 m. w. N.; Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Artikel 82 Haftung und Recht auf Schadenersatz Rn. 10 b). Darüber hinaus sollen die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden haben. Dabei wird vor allem die abschreckende Wirkung des Schadensersatzes betont, welche insbesondere durch seine Höhe erzielt werden soll. Nach den Erwägungsgründen Nr. 75 kann ein Nichtvermögensschaden durch

Diskriminierung, Identitätsdiebstahl oder -betrug, Rufschädigung, Verluste der Vertraulichkeit von dem Berufsgeheimnis unterliegenden persönlichen Daten oder gesellschaftliche Nachteile eintreten.

60
Ein genereller Ausschluss von Bagatellschäden ist im Lichte dieser Erwägungsgründe nicht vertretbar (vgl. LG Essen, Urteil vom 23.9.2021, Az.: 6 O 190/21, ZD 2022, 50; LG Köln, Urteil vom 18.05.2022, Az.: 28 O 328/21, BeckRS 2022, 11236). Dies wird auch aus Art. 4 Abs. 3 AEUV abgeleitet, der die Mitgliedsstaaten dazu anhält, Verstöße wirksam mit Sanktionen zu belegen, denn nur so könne man eine effektive Durchsetzbarkeit des EU-Rechts und damit auch der DSGVO erzielen (LG München I, Urteil vom 09.12.2021, Az.: 31 0 16606/20, BKR 2022, 131).

61
Allein eine Verletzung des Datenschutzrechts als solche begründet allerdings nicht bereits für sich gesehen einen Schadensersatzanspruch für betroffene Personen. Die Verletzungshandlung muss in jedem Fall auch zu einer konkreten, nicht nur völlig unbedeutenden oder empfundenen Verletzung von Persönlichkeitsrechten der betroffenen Personen geführt haben (vgl. LG Hamburg, Urteil vom 04.09.2020 – 324 S 9/19). Verletzung und Schaden sind nicht gleichzusetzen. Es ist zwar eine schwere Verletzung des Persönlichkeitsrechts nicht (mehr) erforderlich. Andererseits ist auch weiterhin nicht für einen Bagatellverstoß ohne ernsthafte 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, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen gehen (vgl. LG Landshut, Urteil vom 06. I I .2020 – 51 O 513/20).

62
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 S. 6), das heißt „spürbar“, objektiv nachvollziehbar, von gewissem Gewicht sein (AG Diez v. 7. 11. 2018, Az. 8 C 130/18), um bloße Unannehmlichkeiten oder Bagatellschäden auszuschließen, s. Urteil der Kammer 6 O 190/21, nicht rechtskräftig).

63
Gemessen an diesen Grundsätzen hat der Kläger schon keine spürbare Beeinträchtigung – hervorgerufen durch Datenverlust – von persönlichen Belangen dargelegt.

64
Der Kläger hat zunächst pauschal und offenbar durch seine Prozessbevollmächtigen standardisiert in einer Vielzahl von Prozessen gleichartig vorgetragen, einen erheblichen Kontrollverlust über seine Daten erlitten und Sorge vor Missbrauch seiner Daten zu haben. Seit dem Scraping-Vorfall 2019 und Veröffentlichung im April 2021 auf der eingangs benannten Seite sei es zu einem Anstieg von SMS und Mails gekommen.

65
Im Rahmen seiner persönlichen Anhörung gemäß S. 141 ZPO hat er bekundet, seit dem Jahre 2018 oder 2019 vermehrt SMS auf seinem Handy angekommen seien, die nach der äußeren Aufmachung von Paketdienstleistern oder Banken herrührten. Diese Nachrichten seien relativ leicht als nicht von demjenigen, von dem sie herrührten sollten, erkennbar gewesen. Er selbst sei Programmierer und habe insoweit Grundkenntnisse. Auch sei es zu relativ vielen Anrufen gekommen, in denen es um Investments in Form von Trades gegangen sei. Er habe aus bloßem Interesse auf seinem mit einem ausreichenden Virenschutz versehenen Rechner auf den Link, der ihm mit einer solchen SMS mitgeteilt wurde, geklickt, habe jedoch anhand des Designs ohne weiteres erkennen können, dass es sich nicht um eine berechtigte Nachricht gehandelt habe. Er selbst wüsste nicht, wie ein potentieller Missbrauch seiner Daten erfolgen solle, er empfinde es lediglich als nervig, kontaktiert zu werden. Sein altes F.-Profil nutze er nicht mehr, in seinem neu erstellten Profil habe er die Einstellungen so gewählt, dass alles nur für ihn selbst sichtbar sei.

66

Die Angaben des Klägers sind dabei nicht ausreichend, einen spürbaren Nachteil und eine objektiv nachvollziehbare, mit gewissem Gewicht erfolgte Beeinträchtigung von persönlichkeitsbezogenen Belangen zu begründen:

67
Zunächst ist zu sehen, dass der Kläger – unterstellt man, dass die Kontaktaufnahmen per SMS und Telefon tatsächlich auf das Geschehen bei der Beklagten zurückzuführen sind – immer wieder auf die gleiche, offenbar plumpe und auf den ersten Blick als „verdächtig“ erkennbare Art und Weise kontaktiert wurde. Die Gefahr hierdurch tatsächlichen Schaden zu erleiden, war damit äußerst gering, zumal der Kläger selbst darauf hinweist, als Programmierer tätig zu sein, so dass er damit etwaige Betrugsversuche leichter erkennen dürfte als ein durchschnittlicher Verbraucher.

68
Der geschilderte Kontrollverlust nebst Angst vor betrügerischen Nachrichten und Anrufen ist hingegen unplausibel. Der Kläger hat im Rahmen der informatorischen Anhörung hierzu selbst angegeben, keine Möglichkeit erkennen zu können, wie seine Daten tatsächlich missbraucht werden könnten – wenngleich nachvollziehbar ist, dass er die unberechtigten Kontaktaufnahmen als „nervig“ empfindet.

69
Der Hinweis des Klägers darauf, dass nur den Wenigsten eine konkrete (und wohl auch erhebliche) Schadendarstellung gelingen dürfte und er wegen der Reichweite und der Größe des behaupteten Datenlecks schon aufgrund einer bloßen Gefährdung einen Schaden unter Bezugnahme auf LG München (Urteil vom 9.12.2021 – 31 0 16606/20, BeckRS 21/41707 und Urteil vom 20.1.2022 – 3 0 17493/20 – BeckRS 6105) bejahen will, ist diese Rechtsprechung nicht ohne Weiteres auf die vorliegende Konstellation übertragbar. Das LG München hat Schadensersatz aufgrund einer Gefahr eines Identitätsmissbrauchs zugesprochen. In dem zu Grunde liegenden Fall wurden Daten veröffentlicht, nämlich „Personalien und Kontaktdaten, Daten zur gesetzlich erforderlichen Identifizierung des Kunden (etwa Ausweisdaten), die im Rahmen der Geeignetheitsprüfung erfassten Informationen, Daten bezogen auf Konto und/oder Wertpapierdepot (etwa Referenzkontoverbindung, Berichte, Wertpapierabrechnungen, Rechnungen) sowie steuerliche Daten (etwa Steueridentifikationsnummer)“. Vorliegend geht es um ein öffentliches Profil nebst Telefonnummer und damit deutlich weniger sensible Daten. Eine Telefonnummer kann man wechseln. Dass aus dem Bekanntwerden einer Telefonnummer ein Identitätsmissbrauch entstehen kann, ist eher unwahrscheinlich (so auch: LG Karlsruhe, Urteil vom 09.02.2021, Az.: 4 O 67/20, ZD 2022, 55). 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. Der Erwägungsgrund Nr. 75 stützt die bisher vertretene Auffassung der Kammer (s. Urteil des Landgerichts Essen vom 23.9.2021, Az.: 6 O 190/21, ZD 2022, 50), da aus Risiken für die Rechte und Freiheiten natürlicher Personen physische, materielle oder immaterielle Schaden entstehen können. Insoweit sind Schäden aber kein zwangsweise Produkt aus einem Risiko für die Rechte und Freiheiten natürlicher Personen aus einer Verarbeitung personenbezogenen Daten, vielmehr sind diese nur fakultativ. Der Sinn der Verordnung wird aber nicht gewahrt, indem man jeglichem „Unwohlsein“ eine Schadensposition einräumt. Vielmehr muss zumindest ein ernsthaftes Risiko bestehen, dass die Daten missbraucht werden. Dies konnte die Kammer im Lichte der Angaben des persönlich gehörten Klägers nicht feststellen, der seine Suchbarkeitseinstellungen trotz der behaupteten – seit knapp zwei Jahren bestehenden – Angst erst eine Woche vor dem Termin auf Anraten seines Prozessbevollmächtigten verändert hat.

2. Kein Anspruch aus nationalem Recht

70
Ansprüche aus nationalem Recht gemäß SS 280 Abs. 1, Abs. 3, 281, 327, 327 e, 327 i BGB, gemäß S. 280 Abs. 1 BGB i.V.m. Nutzungsvertrag sui generis, gemäß S. 823 Abs. 1, 253 Abs. 2 BGB i.V. m. Art. 2 Abs. 1 und Art. 1 Abs. 1 GG, gemäß S. 823 Abs. 2 BGB i.V. m. dem Recht auf informationelle Selbstbestimmung und gemäß SS 1004 analog, 823 Abs. 2 i. V, m. Art, 13, 14 DSGVO bestehen ebenfalls nicht.

71
Insoweit kann auf die diesbezüglichen Ausführungen in dem Urteil des LG Essen, Urteil vom 10. November 2022 – 6 O 111/22 = zitiert nach juris Bezug genommen werden, denen sich das Gericht uneingeschränkt anschließt.

II. Klageantrag zu 2) – Feststellungsanspruch

72
Die Klage auf Feststellung einer Ersatzpflicht künftiger materieller und immaterieller Schäden ist mangels Anspruchsgrundlage – gleich ob nach nationalen Vorschriften oder nach den Bestimmungen der DSGVO – unbegründet.

III. Klageantrag zu 3) – Unterlassungsanspruch

73
Auch der mit dem Klageantrag zu 3) geltend gemachte Unterlassungsanspruch (SS 1004 analog, 823 Abs. 2 BGB i.V.m. Art. 6 Abs. 1, Art. 17 DSGVO) unterliegt der Abweisung.

74
Es ist unstreitig, dass die Beklagte die Kontakt-Import-Funktion (Contact Importer Tool (CI T)) als Reaktion auf den Scraping-VorfaII in der früheren Form nicht mehr bereitstellt und Abhilfemaßnahmen ergriffen hat. Eine – grundsätzlich durch einen einmaligen Verstoß indizierte – Wiederholungsgefahr kann auf dieser Grundlage nicht mehr angenommen werden (vgl. BGH, Urteil vom 14.10.1994 – V ZR 76/93, juris Rn. 22; BeckOK BGB/Fritzsche, 64. Ed. 01.11.2022, BGB S. 1004 Rn. 94), zumal die Klägerseite mit der Klageschrift (BI. 33, 34 d.A.) selbst vorgetragen hat, dass die Beklagte nach dem Bekanntwerden des Vorfalls durch die Sicherstellung von Sicherheitsmaßnahmen nach dem Stand der Technik die Möglichkeit des Datenabgriffs bzw. der Datenzusammenführung verhindert hat.

75
Zudem liegt es jederzeit in der Hand des Klägers, der spätestens mit den im vorliegenden Verfahren gewechselten Schriftsätzen über die Möglichkeit der Suchbarkeitseinstellungen bei F. umfassend informiert ist, die Suchbarkeitseinstellungen zu verändern und hat dies nach eigener Angabe eine Woche vor der mündlichen Verhandlung auch getan. Dass die Beklagte entgegen der von einem Nutzer getroffenen Profileinstellungen oder Suchbarkeitseinstellungen Telefonnummern freigibt oder anderweitig nutzt, hat auch der Kläger nicht behauptet.

IV. Klageantrag zu 4) – Auskunftsansprwch

76
Der mit dem Klageantrag zu 4) verfolgte Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO unterliegt der Abweisung, weil dieser nach Überzeugung des Gerichts durch das außergerichtliche Schreiben der Beklagten vom 23.08.2021 (Anlage K 2) bereits erfüllt wurde (S. 362 Abs. I BGB).

77
Weitergehende Auskunft kann der Kläger nicht verlangen. Ihm ist nämlich einerseits bekannt, welche Daten durch den Scraping-Vorfall erlangt und veröffentlicht wurden. Schließlich hat er in der Replik vom 07.10.2022 (BI. 168 d.A.) den behauptet geleakten Datensatz selbst vorgetragen. Andererseits hat die Beklagte glaubhaft vorgetragen, sie selbst halte keine „Rohdaten“ des Scraping-Vorfalls.

78
Nicht beantwortet wird durch die Beklagte in dem außergerichtlichen Schreiben, welchen Empfängern die Daten des Klägers durch Ausnutzung der Kontakt-Import-Funktion im Sinne des Art. 15 Abs. I lit. c) DSGVO zugänglich gemacht wurden. Das Scraping ist allerdings von außen erfolgt, und es nicht erkennbar, wer diese Daten gescrapt hat. Die begehrte Auskunftserteilung ist aufgrund des Vorgangs des Scrapings unter Ausnutzung von Daten, die öffentlich sichtbar sind, unmöglich. Ebenso ist im Rechtssinne unmöglich (und es wird auch nicht näher dargelegt, wie die Beklagte dazu imstande sein soll), zu informieren, wann genau die Daten gescrapt wurden. Die Beklagte hat dem Kläger im Ergebnis also alle Informationen mitgeteilt, die ihr im Zuge des Scraping-Vorfalls zur Verfügung standen. Weitere Angaben kann sie nicht machen. Sie ist folglich hierzu auch nicht verpflichtet.

V. Klageantrag zu 5) – Nebenforderung Rechtsanwaltskosten

79
Die Nebenforderungen (Klageantrag zu 5) teilen das Schicksal der übrigen Klageanträge und unterliegen der Abweisung.

C.

80
Die Kostenentscheidung beruht auf S. 91 Abs. 1 ZPO.

D.

81
Der Ausspruch über die vorläufige Vollstreckbarkeit richtet sich nach S. 709 S. I, 2 ZPO.

E.

82
Die Höhe des Streitwertes ergibt sich aus den obigen Darlegungen (Begründetheit, Teil A., I, 3.).