LG Landshut, Endurteil v. 16.05.2024 – 82 O 2544/23

Titel:

Ausschluss nationaler Unterlassungsansprüche aufgrund unionsrechtlicher Abschlusswirkung der DSGVO

Normenketten:

DSGVO Art. 15, Art. 82 Abs. 1
ZPO § 256 Abs. 1

Leitsätze:

1. Bei reinen Vermögensschäden reicht bereits die Möglichkeit materieller oder weiterer immaterieller Schäden für die Annahme eines Feststellungsinteresses i.S.v. § 256 Abs. 1 ZPO grundsätzlich aus. Ein Feststellungsinteresse ist nur zu verneinen, wenn aus Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen. Ein rein theoretischer Schaden ist jedoch nicht geeignet, ein Feststellungsinteresse zu begründen. (Rn. 30 – 31 und 34) (redaktioneller Leitsatz)
2. Der Schadensbegriff des Art. 82 Abs. 1 DSGVO ist weit auszulegen. Schadensersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen. Darüber hinaus sollen die Betroffenen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden haben. Dennoch begründet allein eine etwaige Verletzung des Datenschutzrechts als solches für sich genommen keinen Schadensersatzanspruch für die Betroffenen. (Rn. 43 – 44) (redaktioneller Leitsatz)
3. Art. 82 Abs. 1 DSGVO setzt zwar keine schwere Verletzung des Persönlichkeitsrechts voraus, jedoch ist nicht in jedem Fall für jede im Grunde nicht spürbare Beeinträchtigung bzw. für jede bloß individuell empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren. Vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und es muss sich um eine objektiv nachvollziehbare, tatsächlich erfolgte Beeinträchtigung von Persönlichkeitsbezogenen Belangen gehen. (Rn. 44) (redaktioneller Leitsatz)
4. Ein Unterlassungsanspruch aus Art. 82 DSGVO ist nur dann gegeben, wenn der Betroffene einen Schaden erlitten hat und entweder die erfolgte Verletzungshandlung noch andauert oder der pflichtwidrig geschaffene Zustand fortdauert. Nationalrechtliche Unterlassungsansprüche sind aufgrund der unionsrechtlichen Abschlusswirkung der DSGVO ausgeschlossen. (Rn. 53 – 55) (redaktioneller Leitsatz)

Schlagworte:

Zulässigkeit, Internationale Zuständigkeit, Feststellungsinteresse, Schadensersatz, Unterlassungsanspruch, Auskunftsanspruch, Kostenentscheidung

Fundstelle:

GRUR-RS 2024, 31086

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger trägt die Kosten des Verfahrens.

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

4. Der Streitwert wird auf 17.000,00 € festgesetzt.

Tatbestand

1
Die Parteien streiten um die klägerischen Schadensersatz-, Feststellungs-, Unterlassungs- und Auskunftsbegehren wegen behaupteter Verstöße gegen die Datenschutzgrundverordnung (DSGVO) im Rahmen eines angeblichen „Datenlecks“ bei der Beklagten.

2

Die Beklagte ist die Betreiberin eines Online-Musikstreaming-Dienstes (www.deezer.com), der unter anderem einen Katalog von etwa 90 Millionen Titeln streamt. Seit dem 15.12.2011 ist das Angebot der Beklagten auch in Deutschland verfügbar.

3
Mit anwaltlichem Schreiben der Klägerseite vom 23.05.2023 (Anlage 2) wurde die Beklagte zu einer Zahlung von 3.000,00 € Schadensersatz nach Art. 82 Abs. 1 DSGVO aufgefordert. Außerdem wurde ein entsprechendes Unterlassungs- und Auskunftsbegehren geltend gemacht.

4
Mit Schriftsatz vom 17.07.2023 (Anlage 1) wurden die geltend gemachten Schadensersatzforderungen durch die Beklagtenvertreter zurückgewiesen. Außerdem erfolgten Darlegungen der Beklagten unter anderem zum Auskunftsverlangen der Klagepartei.

5
Die Klagepartei behauptet, bereits im Jahr 2019 seien 229 Millionen Datensätze von Deezer-Nutzern gestohlen worden. Aus Deutschland würden 14,1 Millionen Nutzer zu den Betroffenen zählen. Die Beklagte habe hierüber nicht informiert. Daher hätten die Betroffenen erst ab Ende 2022 bzw. Anfang 2023 aus den Medien vom Datenleck erfahren. Durch diesen Datenschutzvorfall habe eine Vielzahl personenbezogener Daten von Deezer-Nutzern abgegriffen werden können.

6
Am 23.12.2022 hätten Unbekannte im sogenannten Darknet diese Datensätze veröffentlicht, wobei ein solcher Datensatz mindestens eine der nachfolgenden Informationen beinhaltet:

7
Vollständiger Name, Geburtsdatum, E-Mail-Adresse, Geschlecht, das Beitrittsdatum, die Nutzer ID, den Nutzernamen, geographische Standorte (Stadt und Land), verwendete Sprache, Dienstnutzungsdaten wie den Hörverlauf, allgemeine Informationen zum Abonnement.

8
Dies alles sei möglich gewesen, weil die Beklagte und ihre Auftragsverarbeiter keine angemessenen Sicherheitsmaßnahmen vorgehalten hätten.

9
Aus dem Datenleck resultierend seien unter anderem auch die Klägerseite betreffende personenbezogenen Daten im Internet veröffentlicht worden, insbesondere im Darknet und in sogenannten Hecker-Foren.

10
Auch die Klagepartei habe sich unter den betroffenen Personen befunden.

11
Auch von ihr seien Daten wie Name, Geburtsdatum und Mailadresse abgegriffen worden.

12
Die Klagepartei habe durch den Datenschutzvorfall einen erheblichen Kontrollverlust über die sie betreffenden Daten erlittenen und verbleibe in einem Zustand großen Unwohlseins und großer Sorge über einen möglichen Missbrauch der sie betreffenden Daten. Dies manifestierte sich unter anderem in einem verstärkten Misstrauen bezüglich E-Mails von bekannten und unbekannten Adressen. Darüber hinaus erhalte die Klägerseite seit dem Vorfall unregelmäßig unbekannte Kontaktversuche via E-Mail. Diese würden Nachrichten mit offensichtlichen Betrugsversuchen und potentiellen Virenlinks enthalten. Oft würden auch bekannte Plattformen oder Zahlungsdienstleister wie oder impersoniert und durch die Angabe der entwendeten Daten versucht, ein gesteigertes Vertrauen zu erwecken. Wegen des gesamten Agierens und Verhaltens der Beklagten sei die Klagepartei verunsichert und verärgert. Zudem habe sich der Vorfall bereits im Jahr 2019 ereignet. Die Beklagte habe die Klägerseite jedoch zu keinem Zeitpunkt darüber informiert, dass ihre Informationen durch Dritte entwendet und veröffentlicht worden seien. Weder eine persönliche Benachrichtigung, noch eine allgemeine öffentliche Bekanntmachung über den Datenklau hätten stattgefunden. Stattdessen verharmlose die Beklagte den Datenschutzfall auf einer Unterseite ohne Öffentlichkeitswirksamkeit mit nebulösen Ausführungen. Die Beklagte habe es aber unterlassen, die zuständige Datenschutzbehörde über den Vorfall zu informieren.

13
Die Klagepartei meint, die Verstöße der Beklagten gegen die DSGVO bestünden darin, dass die Beklagte als verantwortliche (Art. 4 Nummer 7 DSGVO) die Klägerseite betreffende personenbezogene Daten, Art. 4 Nummer 1 DSGVO, unbefugten Dritten zugänglich gemacht habe und hierbei insbesondere die Pflichten aus Art. 32 (Sicherheit der Verarbeitung), 34 Abs. 1, Absatz 2 (Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen) DSGVO sowie betroffenen Rechte der Klägerseite gemäß Art. 15 verletzt habe.

14
Die Klagepartei beantragt,

1. Die Beklagte wird verurteilt, an die Klagepartei einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 3.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle materiellen künftigen Schäden zu ersetzen, die der Klagepartei durch die unbefugte Veröffentlichung ihrer personenbezogenen Daten im Internet durch die Beklagte im Zeitraum vom 28.04.2020 bis zum 05.08.2020 entstanden sind und/oder entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen, personenbezogenen Daten der Klagepartei, namentlich Famliennamen, Vornamen, Geburtsdatum, Geschlecht, Wohnort, Land, E-Mail-Adresse, IP-Adresse, Anmeldedatum, Akquise-Herkunft, bevorzugte Sprache, User ID, Dritten zugänglich zu machen, ohne dass eine Einwilligung der Klagepartei vorliegt oder ein berechtigtes Interesse der Beklagten vorliegt.

4. Die Beklagte wird verurteilt, der Klagepartei Auskunft über deren personenbezogene Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch die unbefugte Veröffentlichung im Internet im Zeitraum vom 28.04.2020 bis zum 05.08.2020 erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerin für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft i.S.d. Art. 15 DSGVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

6. Die Beklagte wird verurteilt, die Klägerseite von den außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von 1.390,87 € nebst Zinsen in Höhe von 5 Prozentpunkten über dem jeweiligen Basiszinssatz der EZB ab Rechtshängigkeit freizuhalten.

15
Die Beklagte beantragt,

die Klage abzuweisen.

16
Die Beklagte behauptet, sie hätte am 08.11.2022 gegen 15:33 Uhr Kenntnis darüber erlangt, dass Heckerdaten von Nutzern der Beklagten seit dem 06.11.2022 im Darkweb – einem speziellen Forum, dass nur über bestimmte Webbrowser zu erreichen ist und typischerweise für kriminelle Aktivitäten genutzt werde – zum Verkauf angeboten hätten. Die Daten der Beklagten seien Teil eines großen erbeuteten Datensatzes gewesen, welche auch Daten anderer Unternehmen enthalten habe. Die Hecker hätten behauptet, dass sie die Daten durch den Heck eines nicht näher bekannten „Drittdienstleisters“ erbeutet hätten und der Datensatz aus dem Jahr 2019 stamme. Außerdem hätten die Hecker den erfolgreichen Cyberangriff erst am

06.11.2022 öffentlich bekannt gemacht. Die Beklagte habe sofort nach Kenntniserlangung reagiert und seit dem unter Hochdruck daran gearbeitet, einen Missbrauch von Daten und das Risiko für ihre Nutzer zu verhindern, den Cyberangriff aufzuarbeiten und ähnliche Vorfälle in Zukunft zu vermeiden. Ermittlungen hätten ergeben, dass die Beklagte einen Cyberangriff auf die eigene IT-Infrastruktur mit Sicherheit ausschließen könne, die eigene IT-Infrastruktur der Beklagten sei in keiner Weise von dem Cyberangriff betroffen gewesen.

17
Der Cyberangriff habe nicht bereits im Jahr 2019 stattgefunden, lediglich der Betroffene Datensatz stamme aus dem Jahr 2019. Dies ergebe sich auch eindeutig aus dem von der Klagepartei selbst vorgelegten Screenshots der Website www.restoreprivacy.com. Auf die von der Klagepartei vorgebrachte Mitteilung der Beklagten auf ihrer eigenen Website sei in diesem Punkt falsch. Diese öffentliche Mitteilung habe zu einem Zeitpunkt stattgefunden, als der genaue Hergang des Angriffs noch nicht bekannt gewesen sei. Die Ermittlungsergebnisse würden den Schluss nahelegen, dass der Cyberangriff kurz vor der Veröffentlichung der Daten am 06.11.2022 gewesen sei. Die von dem Cyberangriff betroffenen personenbezogenen Daten würden eine hohe Ähnlichkeit zu Daten aufweisen, die ein ehemaliger Dienstleister der Beklagten für Kundenverwaltungsdienste nutze. Die Vertragsbeziehung mit diesem Dienstleister sei zum 30.11.2020 beendet worden und der Dienstleister habe der Beklagten versichert, dass er sämtliche Daten am 01.12.2020 löschen werde und habe dies auch am 22.02.2023 erneut bestätigt.

18
Die Beklagte trägt weiter vor, sie habe in Bezug auf die Klagepartei keine positive Kenntnis darüber, ob und falls ja, welche ihrer Informationen tatsächlich Gegenstand eines unberechtigten Zugriffs geworden seien. Die Beklagte verfüge nur über sehr wenige Informationen über die Klagepartei. Hinsichtlich der einzelnen Daten wird auf Seite 6 der Klageerwiderung Bezug genommen. Daher sei es nahezu ausgeschlossen, dass ein unbeteiligter Dritter die Klagepartei mittels ihrer User-ID, ihres Nutzernamens, Ihre E-Mail-Adresse, der Information, dass sie in Deutschland wohnhaft ist, sowie den rudimentären Informationen über die Nutzung eines Musistream-Dienstes eindeutig identifizieren könne, ohne dass einem solchen Dritten weitere Informationen über die Klagepartei zur Verfügung stehen.

19
Ferner habe die Beklagte den Cyberangriff unverzüglich am 10.11.2022 gegen 18:00 Uhr der zuständigen französischen Datenschutzbehörde gemeldet. Die Beklagte habe die von dem Vorfall betroffenen Personen unverzüglich nach Bekanntwerden am 11.11.2022 auf der unternehmenseigenen Webseite informiert. Anfang 2023 habe es zusätzlich eine individuelle Betroffenheitsbenachrichtigung per E-Mail gegeben. In der Kommunikation habe die Beklagte den Nutzern insbesondere geraten, ihre Passwörter als vorbeugende Sicherheitsmaßnahme zu ändern und die aktuellen Sicherheitsempfehlungen der Behörden zu beachten.

20
Zudem sei die Sicherheit der Datencenter der Netzwerke gewahrt gewesen. Alle Rechenzentren seien durch physische, organisatorische und elektronische Sicherheitsmaßnahmen gesichert, sowie durch hinreichende Zugangskontrollen.

21
Die Beklagte meint, der Klageantrag zu 2) entspreche nicht den Bestimmtheitsanforderungen, außerdem sei ein Feststellungsinteresse der Klagepartei für den Klageantrag zu 2 nicht ersichtlich.

22
Hinsichtlich der weiteren Einzelheiten wird auf die wechselseitigen Schriftsätze der Parteivertreter nebst Anlagen verwiesen.

Entscheidungsgründe

23
Die Klage ist teilweise zulässig, jedoch unbegründet

I.

24
Die Klage ist hinsichtlich der Anträge Ziffer 1,3 und 4 zulässig, hinsichtlich Ziffer 2 unzulässig.

25
Das Landgericht Landshut ist international, örtlich und sachlich zuständig.

26
Die internationale Zuständigkeit deutscher Gerichte folgt aus Art. 6 Abs. 1, Art. 18 Abs. 1 EuGV- VO. Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist nicht ersichtlich. Gemäß Art. 18 Abs. 1 Alternative 2 EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher, hier der Kläger, seinen Wohnsitz, hier Bundesrepublik Deutschland, hat.

27
Die internationale Zuständigkeit deutscher Gerichte ergibt sich ferner aus Art. 79 Abs. 2 DSGVO, deren zeitlicher, sachlicher und räumlicher Anwendungsbereich eröffnet ist.

28
Das Landgericht Landshut ist örtlich zuständig. Dies folgt aus Art. 18 Abs. 1 Alternative 2 EuGVVO und aus Art. 79 Abs. 2 Satz 2 DSGVO.

II.

29
Die mit dem Antrag zu 2) verfolgte Feststellungsklage ist bereits unzulässig, denn es fehlt am notwendigen Feststellungsinteresse im Sinne des § 256 Abs. 1 ZPO.

30
Wenn es wie hier nur um reine Vermögensschäden geht, reicht bereits die Möglichkeit materieller oder weiterer immaterieller Schäden für die Annahme eines Feststellungsinteresses grundsätzlich aus. Hierbei ist die Rechtsprechung zum allgemeinen Persönlichkeitsrecht auf den vorliegenden Fall zur Verletzung des nach Art. 82 DSGVO absolut geschützten Rechtsgut Datenschutz als abschließende europarechtliche Ausformung des deutschen allgemeinen Persönlichkeitsrechts zu übertragen (Vergleiche OLG Hamm Urteil vom 15.08.2023 7 U 19/23).

31
Ein Feststellungsinteresse ist also nur zu verneinen, wenn aus Sicht des geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen (Vergleiche BGH Urteil vom 16.01.2001 VI ZR 381/99).

32
Gemessen an diesen Grundsätzen ist hier die Möglichkeit eines Schadenseintritts durch die Klagepartei nicht hinreichend dargelegt. Die Klagepartei meint, die Möglichkeit eines Schadenseintritts ergebe sich aus drohenden Spam-Anrufen, Spam-SMS oder Spam-E-Mails. Sie könne sich (versehentlich) auch mit ihrem Namen melden und hänge dann in irgendwelchen dubiosen Verträgen. Selbiges gelte wegen links in SMS oder E-Mails, diese zeigten auch allgemein die durch WhatsApp-Betrug, Enkeltrick und das Vortäuschen einer Bank- oder Behördenmitarbeiterstellung entstandene Schäden. Diese seien die direkte Folge des Datenlecks.

33
Dieser Vortrag genügt nicht.

34
Mangels konkreter Anhaltspunkte dafür, dass der Klagepartei bis heute aufgrund des unbefugten Zugriffs Dritter auf das Datenarchiv der Beklagten ein kausaler materieller Schaden entstanden ist, ist davon auszugehen, dass mit dem Eintritt eines materiellen Schadens nicht zu rechnen ist. Ein solcher Schaden in der von der Klagepartei beschriebenen Art und Weise ist rein theoretischer Natur und begründet kein Feststellungsinteresse (Vergleiche OLG Hamm Urteil vom 15.08.2023 7 U 19/23 GRUR-RS 2023, 22505).

35

Entsprechendes gilt für den immateriellen Schaden. Ein solcher ist bislang nicht hinreichend dargetan und es ist mit Blick auf die vergangene Zeit auch nicht damit zu rechnen, dass ein solcher noch eintritt (Vergleiche OLG Hamm siehe oben).

36
Begründet werden kann der Feststellungsanspruch auch nicht mit entstandenen Anwaltskosten. Zum einen sind diese Gegenstand eines gesonderten Leistungsantrages und zum anderen sind diese bereits vor Klageerhebung entstanden und damit nicht vom Feststellungsantrag umfasst.

III.

37
Im Übrigen ist die Klage hinsichtlich der Anträge Ziifer 1,3,4 und 5 vollumfänglich unbegründet.

38
Der Klageanträge zu Ziffer 1) und 5) waren abzuweisen.

39
Die Klagepartei hat insbesondere keinen Anspruch auf Ersatz immaterieller Schäden gemäß Art. 82 Abs. 1 DSGVO und auf Ersatz immaterieller Schäden wegen Nichterfüllung einer außergerichtlichen Datenauskunft im Sinne des Art. 15 DSGVO.

40
Zwar ist der räumliche und sachliche Anwendungsbereich der DSGVO eröffnet, ein Verstoß gegen die DSGVO ist jedoch fernliegend, kann vorliegend aber offenbleiben.

41
Denn ungeachtet eines etwaigen Verstoßes gegen die DSGVO fällt es jedenfalls an einem ersatzfähigen Schaden im Sinne des Art. 82 Abs. 1 DSGVO.

42
Für den hier geltend gemachten immateriellen Schadensersatz gelten dabei die im Rahmen von § 253 BGB entwickelten Grundsätze, wobei die Ermittlung dem Gericht nach § 287 ZPO obliegt (Vergleiche Beckok-Datenschutzr/QasQUAAS, 43. Edition 01.02.2023, DS-GVO Art. 82 Rz. 31). Es können für die Bemessung der 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 betreffenden Kategorien personenbezogener Daten. Zu berücksichtigen ist auch, dass die beabsichtigte abschreckende Wirkung nur durch für den anspruchsverpflichtenden empfindliche Schmerzensgeld erreicht wird, insbesondere wenn eine Kommerzialisierung fehlt. Ein genereller Ausschluss von Bagatellefällen ist damit nicht zu vereinbaren. Die Pflicht zur Erstattung immaterieller Schäden ist daher nicht auf schwere Schäden beschränkt. Nach dem Urteil des EuGH (Vergleiche EuGH Urteil vom 04.05.2023 C-300/21 Rz. 43 ff., juris). Ist der Ersatz eines immateriellen Schadens im Sinne des Art. 82 Abs. 1 DSGVO nicht davon abhängig, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat.

43
Nach den Erwägungen der europäischen Grundrechtscharta ist der Schadensbegriff weit auszulegen. Schadensersatzforderungen sollen abschrecken und weitere Verstöße unattraktiv machen. Darüber hinaus sollen die betroffenen Personen einen vollständigen und wirksamen Schadensersatz für den erlittenen Schaden haben. Somit ist ein genereller Ausschluss von Bagatellschäden im Lichte dieser Erwägungsgründe nicht vertretbar.

44
Allein eine etwaige Verletzung des Datenschutzrechts als solches, die hier ohnehin fernliegend ist, begründet allerdings nicht bereits für sich gesehen einen Schadensersatzanspruch für betreffende Personen. Die Verletzungshandlung muss in jedem Fall auch zu einer konkreten Verletzung von Persönlichkeitsrechten der betroffenen Personen geführt haben. Die Verletzung der Vorschriften der DSGVO ist nicht mit einem Schadenseintritt gleichzusetzen. Es ist zwar keine schwere Verletzung des Persönlichkeitsrechts erforderlich. Andererseits ist aber auch weiterhin nicht für jede im Grunde nicht spürbare Beeinträchtigung bzw. für jede bloß individuell empfundene Unannehmlichkeit ein Schmerzensgeld zu gewähren. Vielmehr muss dem Betroffenen ein spürbarer Nachteil entstanden sein und

es muss um eine objektiv nachvollziehbare, tatsächlich erfolgte Beeinträchtigung von Persönlichkeitsbezogenen Belangen gehen (Vergleiche LG Aachen Urteil 10.02.2023 8 O 177/22, GRUR-RS 2023, 2621 Rz. 77 mit weiteren Nachweisen).

45
Art. 82 Abs. 2 DSGVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt nämlich die 3 Voraussetzungen für die Entstehung des Schadensersatzanspruchs, nämlich die Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO, ein der betreffenden Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden.

46
Gemessen an diesen Grundsätzen hat die Klagepartei schon keine spürbare Beeinträchtigung von persönlichen Belangen dargelegt, für die überhaupt Anhaltspunkte bestehen, dass sie kausal auf den hier streitgegenständlichen Scraping-Vorfall zurückzuführen sein könnte.

47
Die Klagepartei trägt im Rahmen einer standardisierten Klageschrift vor, einen erheblichen Kontrollverlust über ihre Daten erlitten und Sorge vor Missbrauch ihrer Daten zu haben. Seit dem angeblichen Datenleck sei es ferner zu einem Anstieg von unerwünschten E-Mails und sonstigen Spam Nachrichten gekommen.

48
Als Schaden im Sinne der DSGVO kann nicht das von der Klagepartei behauptet erhöhte Spamaufkommen gewertet werden. Es ist schon zweifelhaft, ob diese Behauptung überhaupt ausreichend konkret dargelegt ist, denn die Behauptung eines immensen Spamaufkommens ist äußerst pauschal. Es handelt sich um keinen hinreichend substantiierten Vertrag.

49
Letztlich kann dies dahinstehen, denn es ist bereits der Kausalzusammenhang zwischen diesem erhöhten Spamaufkommen und dem Scraping-Vorfall klägerseits nicht nachgewiesen worden. Ebenso wenig reicht der von der Klagepartei mit formelhaften Wendungen vorgetragene Kontrollverlust über die persönlichen Daten und die damit verbundene Unsicherheit aus, um einen Schaden im Sinne des Art. 82 Abs. 1 DSGVO zu begründen.

50
Ferner kann dem Ergebnis dahinstehen, ob neben Art. 82 Abs. 1 DSGVO auch nationales Recht anwendbar ist oder das nationale Recht von den europarechtlichen Vorschriften der DSGVO verdrängt wird. Denn auch bei der Annahme eines Nebeneinanders hat die Klagepartei mangels restitutionsfähigen Schadens keinen Schadensersatzanspruch gegen die Beklagte, weder aus §§ 82 Abs. 1, 253 Abs. 2 BGB noch als einer anderen nationalen Schadensnummer.

IV.

51
Der Klageantrag zu Ziffer 3) ist unbegründet.

52
Vorliegend kann dahinstehen, ob der geltend gemachte Unterlassungsantrag eigentlich eine verdeckte Leistungsklage darstellt und damit den Anforderungen des § 259 ZPO genügen müsste.

53
Ein etwaiger Unterlassungsanspruch folgt hier jedenfalls nicht aus Art. 82 DSGVO. Denn ein Unterlassungsanspruch aus Art. 82 DSGVO ist nur dann gegeben, wenn der Betroffene einen Schaden erlitten hat und entweder die erfolgte Verletzungshandlung noch andauert oder der pflichtwidrig geschaffene Zustand fortdauert. Hier ist jedoch ein irgendwie gearteter Schaden, wie bereits ausgeführt, nicht ansatzweise ersichtlich.

54
Ein solcher Anspruch ergibt sich auch weder aus § 1004 analog BGB in Verbindung mit dem Recht auf informationelle Selbstbestimmung noch aus § 823 Abs. 2 BGB in Verbindung mit der DSGVO.

55
Denn Unterlassungsansprüche nach nationalem Recht, insbesondere ein Anspruch aus §§ 1004 Absatz 1 Satz 2, 823 Abs. 2 BGB in Verbindung mit der verletzten Norm der DSGVO sind wegen der durch die DSGVO unionsweit abschließend vereinheitlichten Regelung des Datenschutzrechts ausgeschlossen.

V.

56
Der Klageantrag zu Ziffer 4) ist unbegründet. Die Klagepartei hat hinsichtlich der begehrten Auskunft keinen Auskunftsanspruch gegen die Beklagte aus Art. 15 DSGVO.

57
Dieser Auskunftsanspruch ist durch das außergerichtliche Schreiben der Beklagten teilweise erloschen im Sinne von § 362 Abs. 1 BGB.

58
Die Beklagte ist auch lediglich gehalten, diese von ihr selbst verarbeiteten Daten mitzuteilen. Soweit öffentlich einsehbare Daten von Dritten verarbeitet wurden, ist jedenfalls die Beklagte nicht auskunftspflichtig.

VI.

59
Da der Hauptsacheanspruch unbegründet ist, ist auch der Anspruch auf vorgerichtliche Rechtsanwaltskosten sowie auf Zinsen unbegründet.

VII.

60
Die Kostenentscheidung folgt aus § 91 Abs. 1 Satz 1 ZPO.

61
Die vorläufige Vollstreckbarkeit folgt aus § 709 ZPO.